# TS226
# -
# Codes correcteur d'erreur

**Romain Tajan**

11 septembre 2019

# 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

1. Introduction générale
   - ▷ Histoire de code correcteur
   - ▷ Rappels sur la couche PHY
   - ▷ Premier code : codage par répétition
   - ▷ Enjeux des codes correcteurs d'erreur

2. Introduction au codage / définitions
   - ▷ Sur la modélisation du canal
   - ▷ Code correcteur d'erreur
   - ▷ Probabilité d'erreur
   - ▷ Retour sur les enjeux

# Exemple de QCM

**Comment allez vous aujourd'hui ?**

- A Très bien
- B Bien
- C Mal
- D Très mal

#QDLE#S#ABCD#30#

# Plan

1. Introduction générale
   - Histoire de code correcteur
   - Rappels sur la couche PHY
   - Premier code : codage par répétition
   - Enjeux des codes correcteurs d'erreur
2. Introduction au codage / définitions

# 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)

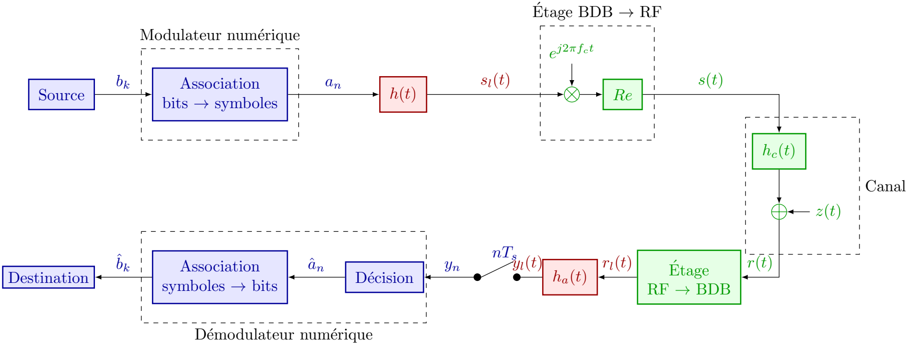
# Exemple de QCM

**Comment situez vous le cours de 1A (TS113) ?**

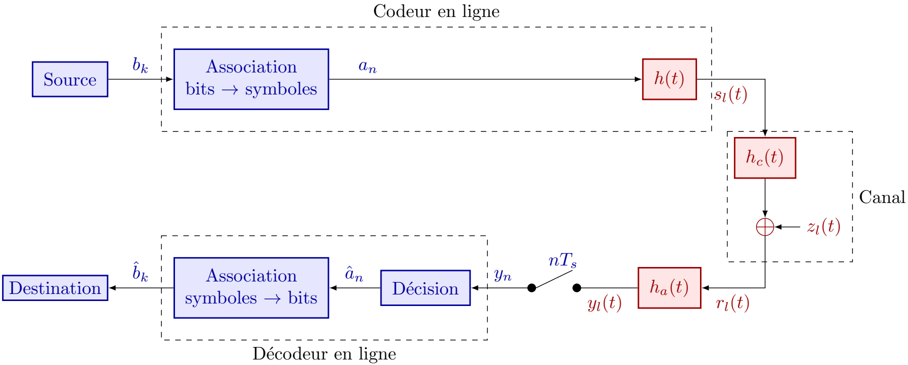
- A Très difficile
- B Difficile
- C Moyen
- D Simple
- E Très simple

#QDLE#S#ABCDE#30#

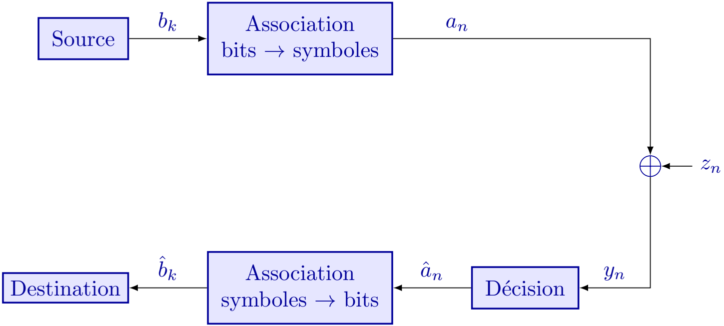
# Rappels sur les communications numériques



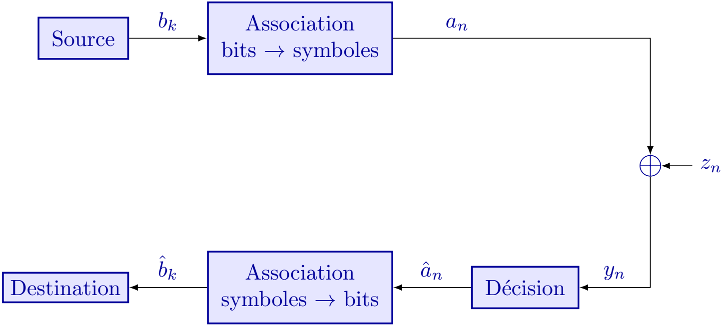
# Rappels sur les communications numériques

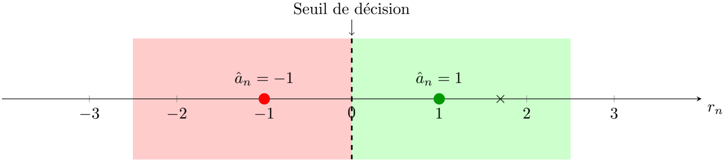


# Rappels sur les communications numériques

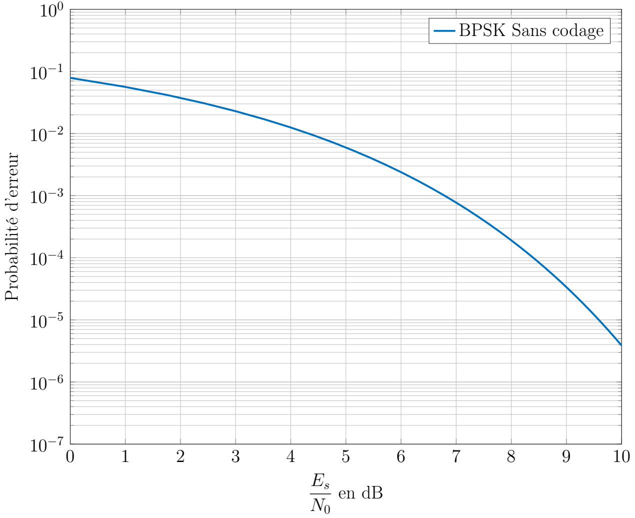


# Rappels sur les communications numériques



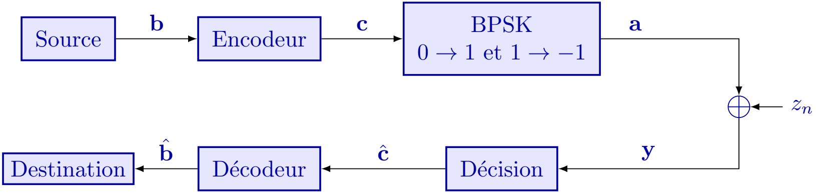



# Rappels sur les communications numériques




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

# Premier exemple de code : codage par répétition




## Encodeur

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

$\mathbf{c} =$

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

## Décodeur

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

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

# QCM

Considérons l'encodage de 1 bit par un code à 3 répétitions.
Quelle taille fait **c** ?

- A 1
- B 2
- C 3
- D 4

#QDLE#S#ABC*D#45#

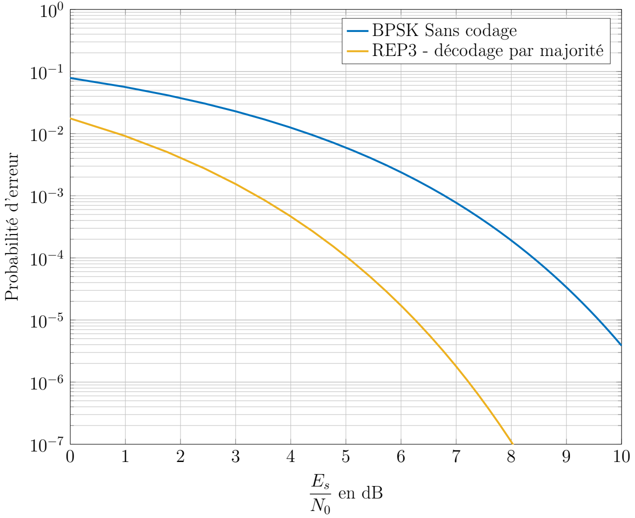
# QCM

Considérons l'encodage de 1 bit par un code à 3 répétitions.
Combien d'erreurs binaires (sur $\hat{\mathbf{c}}$) ce code peut-il corriger ?

- (A) 0
- (B) 1
- (C) 2
- (D) 3

#QDLE#Q#AB*CD#45#

# Codage par répétition : probabilité d'erreur

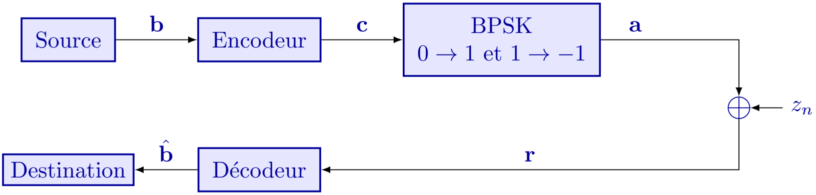



$$p_b = Q\left(\sqrt{2\frac{E_s}{N_0}}\right)$$

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

(Décodage par majorité)

# Premier exemple de code : codage par répétition (2)




## Encodeur

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

$\mathbf{c} =$

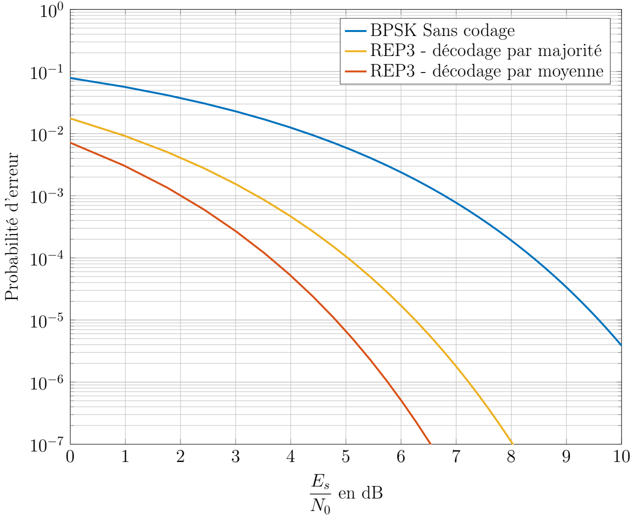
$[\underbrace{b_0, b_0, b_0}_{\mathbf{c}_0}, \underbrace{b_1, b_1, b_1}_{\mathbf{c}_1}, \ldots \underbrace{b_{K-1}, b_{K-1}, b_{K-1}}_{\mathbf{c}_{K-1}}]$

## Décodeur

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

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

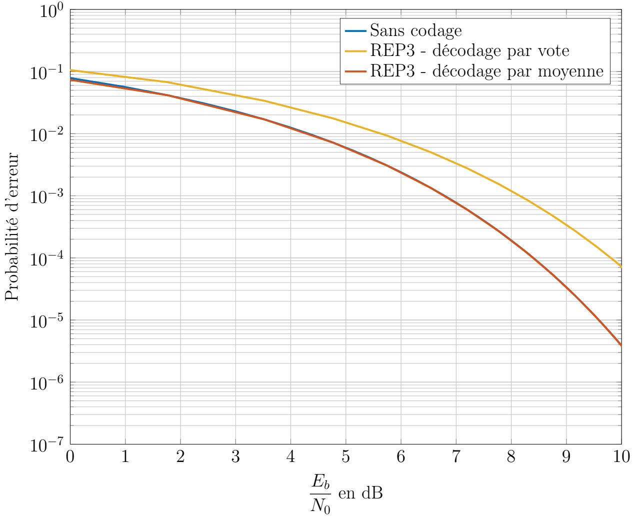
# Codage par répétition : probabilité d'erreur (2)




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

(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

1. Introduction générale

2. Introduction au codage / définitions
   - ▷ Sur la modélisation du canal
   - ▷ Code correcteur d'erreur
   - ▷ Probabilité d'erreur
   - ▷ Retour sur les enjeux

# Redéfinissons le canal...

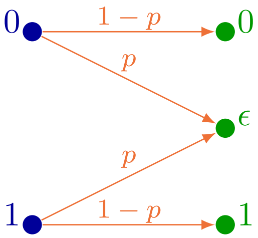
Un **canal** est défini par un triplet : $(\mathcal{X}, \mathcal{Y}, p(y|x))$ où

- $\mathcal{X}$ 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

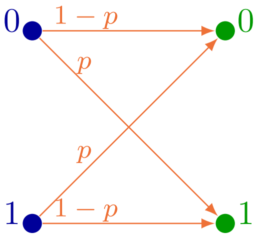
$$p(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} p(y_i|x_i)$$

# Le canal à effacement binaire



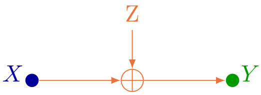

- $\mathcal{X} = \{0, 1\}$ (canal à entrées binaires)
- $\mathcal{Y} = \{0, \epsilon, 1\}$
- $p(\epsilon|0) = p(\epsilon|1) = p$ et $p(0|0) = p(1|1) = 1 - p$
- Canal utile pour les couches hautes, pour le stockage

# Le canal binaire symétrique



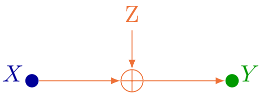

- $\mathcal{X} = \{0, 1\}$ (canal à entrées binaires)
- $\mathcal{Y} = \{0, 1\}$
- $p(1|0) = p(0|1) = p$ et $p(0|0) = p(1|1) = 1 - p$
- Canal utile après décision

# 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




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

# Dernier QCM

**Comment avez-vous trouvé ce cours ?**

- A Très difficile
- B Difficile
- C Moyen
- D Simple
- E Très simple

#QDLE#S#ABCDE#30#