# Une introduction au codage de canal

C. Poulliat

2 novembre 2011

# Plan

# Plan

# Entropie, entropie conjointe

**X** une variable aléatoire discrète à valeurs dans l'alphabet $\mathcal{X}$ de d.d.p. $p(x) = Prob(X = x),\ x \in \mathcal{X}$

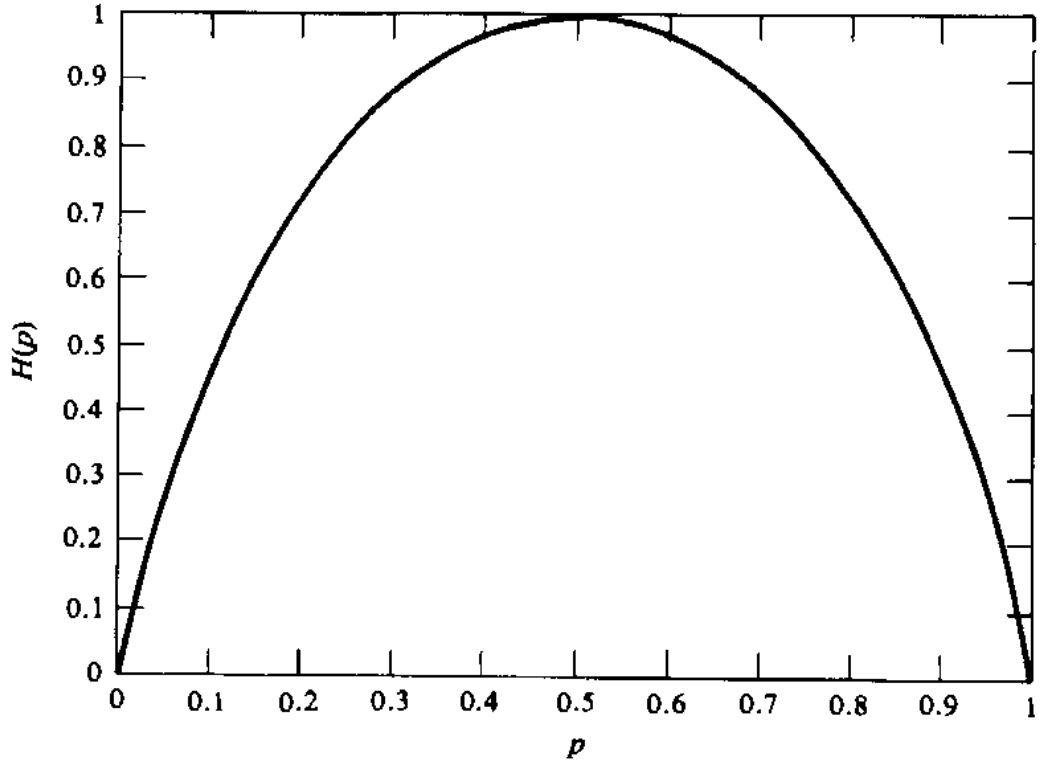
## Entropie

$$\begin{aligned} \mathbf{H}(X) &= -\sum_{x\in\mathcal{X}} p(X=x)\log_2\left(p(X=x)\right) \\ &= -\mathbb{E}(\log_2 p(X)) \end{aligned} \tag{1}$$

## Entropie conjointe

$$\begin{aligned} \mathbf{H}(X,Y) &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(X=x,Y=y)\log_2\left(p(X=x,Y=y)\right) \\ &= -\mathbb{E}(\log_2 p(X,Y)) \end{aligned} \tag{2}$$

# Entropie binaire




$$X \in \{0,1\} \text{ avec } p(X=1) = p$$

$$\mathbf{H}(X) = -p\log_2(p) - (1-p)\log_2(1-p) \triangleq H_2(p)$$

# Entropie conditionnelle et propriétés

## Entropie conditionnelle

$$\begin{aligned}\mathbf{H}(Y|X) &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(X=x, Y=y)\log_2\left(p(Y=y|X=x)\right) \\ &= -\mathbb{E}(\log_2 p(Y|X)) \qquad (3)\end{aligned}$$

## Propriétés

1. $0 \leq \mathbf{H}(X) \leq \log_2 |\mathcal{X}|$
   égalité si $X$ uniformément distribué
2. $\mathbf{H}(X, Y) = \mathbf{H}(X) + \mathbf{H}(Y|X)$
3. $\mathbf{H}(X|Y) \leq \mathbf{H}(X)$
   égalité si $X$ et $Y$ indépendants

# Information mutuelle

## Information mutuelle

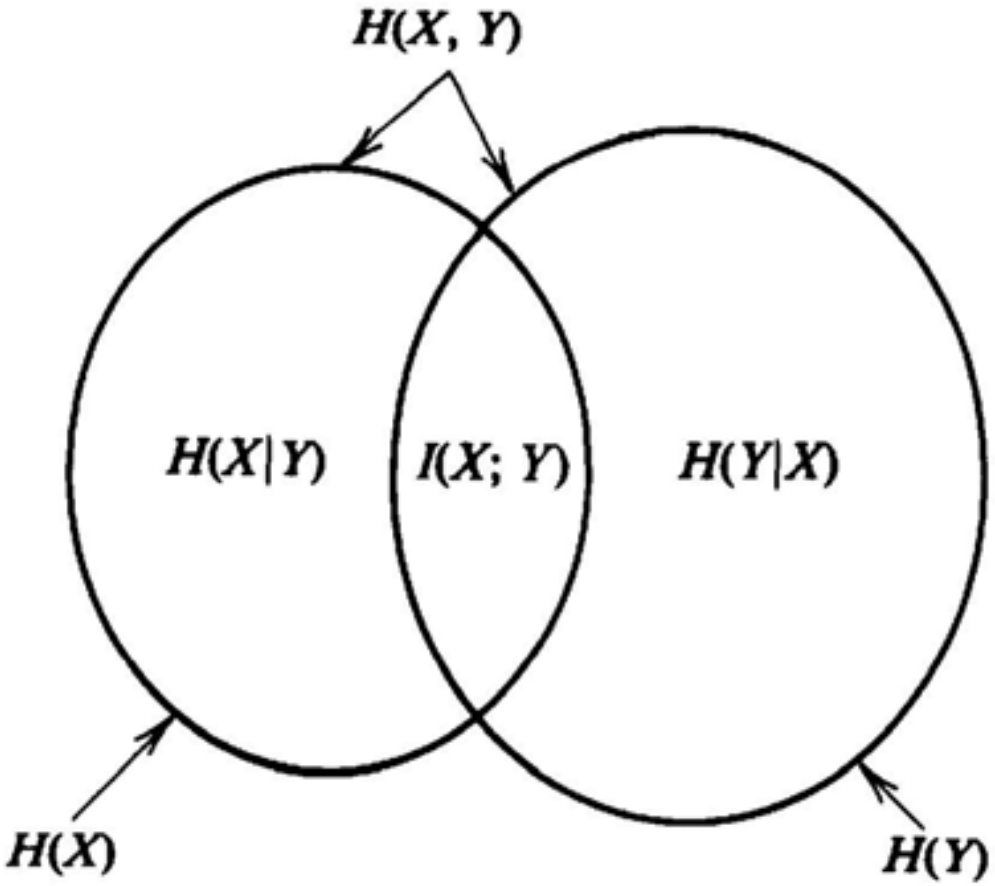
$$\begin{aligned} \mathbf{I}(X;Y) &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(X=x,Y=y)\log_2\left(\frac{p(X=x)p(Y=y)}{p(X=x,Y=y)}\right) \\ &= -\mathbb{E}\left(\log_2\left(\frac{p(X)p(Y)}{p(X,Y)}\right)\right) \geq 0 \end{aligned} \tag{4}$$

## Propriétés

$$\begin{aligned} \mathbf{I}(X;Y) &= \mathbf{H}(X) - \mathbf{H}(X|Y) \\ &= \mathbf{H}(Y) - \mathbf{H}(Y|X) \\ &= \mathbf{H}(X) + \mathbf{H}(Y) - \mathbf{H}(X,Y) \\ &= \mathbf{I}(Y;X) \end{aligned} \tag{5}$$

$$\mathbf{I}(X;X) = \mathbf{H}(X)$$

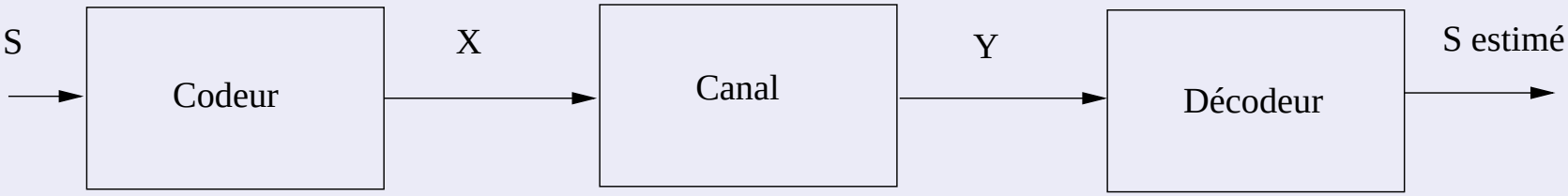
# Interprétations



# Plan

# Capacité d'un canal discret sans mémoire

## Définition




- $X \in \mathcal{X}$, $Y \in \mathcal{Y}$
- Canal sans mémoire caractérisé par $p(Y|X)$

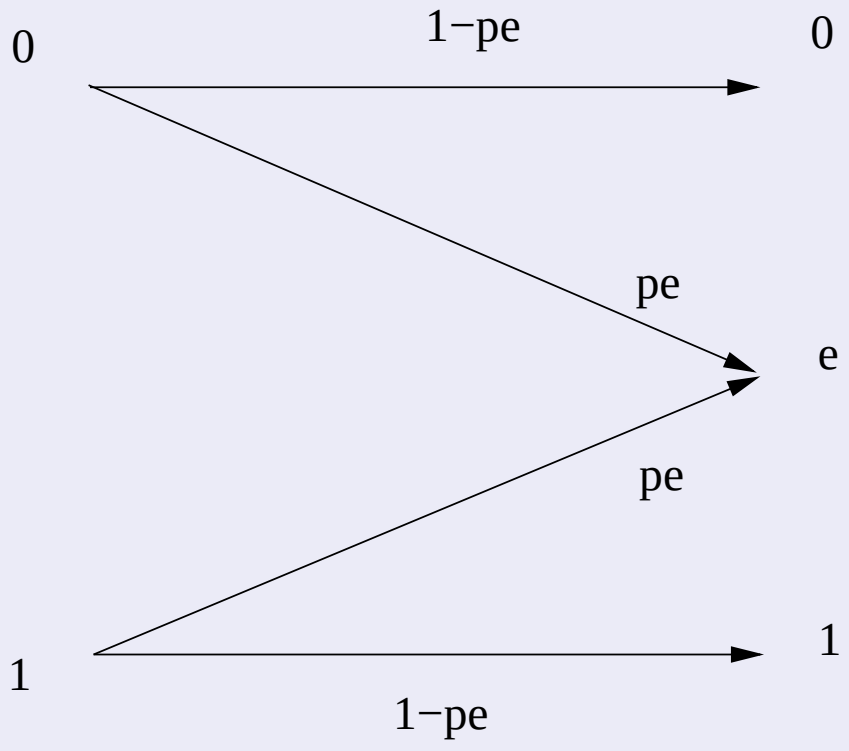
### Définition

$$\begin{aligned} \mathbf{C} &= \max_{p(X)} \mathbf{I}(X;Y) \\ &= \max_{p(X)} \mathbf{H}(X) - \mathbf{H}(X|Y) = \max_{p(X)} \mathbf{H}(Y) - \mathbf{H}(Y|X) \end{aligned} \tag{6}$$

Max. atteint pour distribution uniforme pour les canaux *symétriques*.

# Capacité d'un canal discret sans mémoire

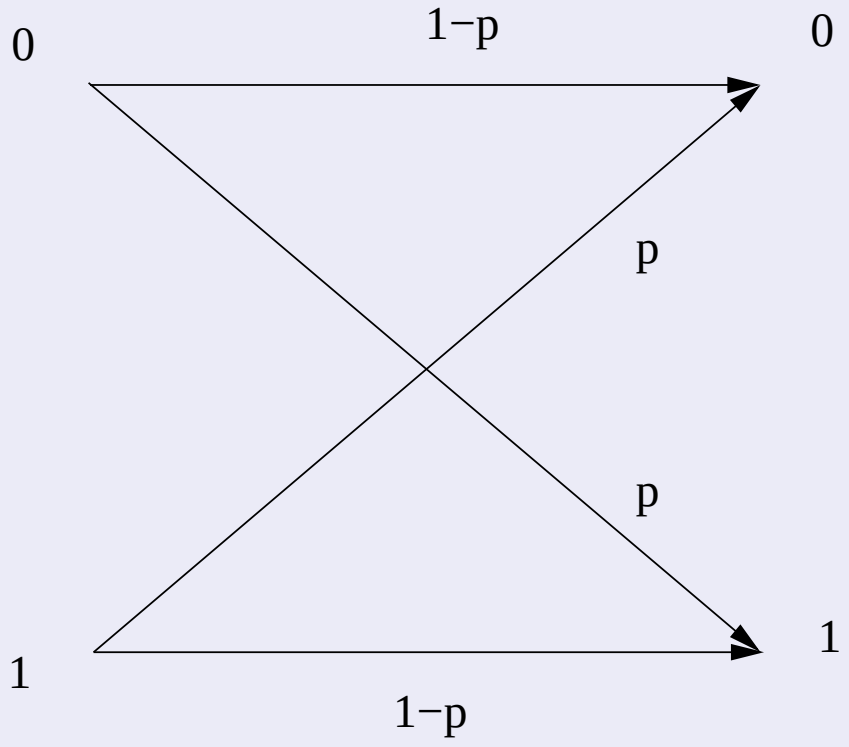
## Canal à effacement (BEC)




$$\mathbf{C} \quad = \quad 1 - p_e \tag{7}$$

atteint pour une distribution d'entrée uniforme

# Canal binaire symétrique (BSC)




$$\mathbf{C} \quad = \quad 1 - H_2(p) \tag{8}$$

atteint pour une distribution d'entrée uniforme

# Théorème du codage de canal

## Canal discret sans mémoire

### Théorème du codage de canal (1/2)

Soit un canal discret sans mémoire de capacité **C**, on peut communiquer à tout débit de transmission inférieur à $C$. En particulier, $\forall R < C$, il existe un code $\mathcal{C}(N, R)$ tel que

$$\mathcal{C}(N, R) : \{0, 1\}^{NR} \longrightarrow \{0, 1\}^{N}$$

telle que la probabilité d'erreur bloc en sortie de décodage optimal soit arbitrairement petite pour $N$ suffisamment grand.

# Plan

# Théorème du codage de canal (2/2)

## Canal à temps discret et entrées/sorties continues

### Théorème du codage de canal

- Extension au cas d'entrées ou de sorties continues.
- Les expressions précédentes mettent en jeu des densités de probabilités.
- Application principale : le cas du canal Gaussien.

# Canal additif gaussien(AWGN)

$$\begin{array}{ccc} & & B(\omega) \\ & & \downarrow \\ X(\omega) & \longrightarrow & \oplus\sum \longrightarrow Y(\omega) \end{array} \tag{9}$$

- $X(\omega)$ tel que $\sigma_x^2 \leq P$
- $B(\omega) \sim \mathcal{N}(0, \sigma_b^2)$
-

$$\mathbf{C} = \frac{1}{2}\log_2\left(1 + \sigma_x^2/\sigma_b^2\right) \text{ bits/symbol} \tag{10}$$

$$= \frac{1}{2}\log_2\left(1 + 2R_bE_b/N_0\right) \tag{11}$$

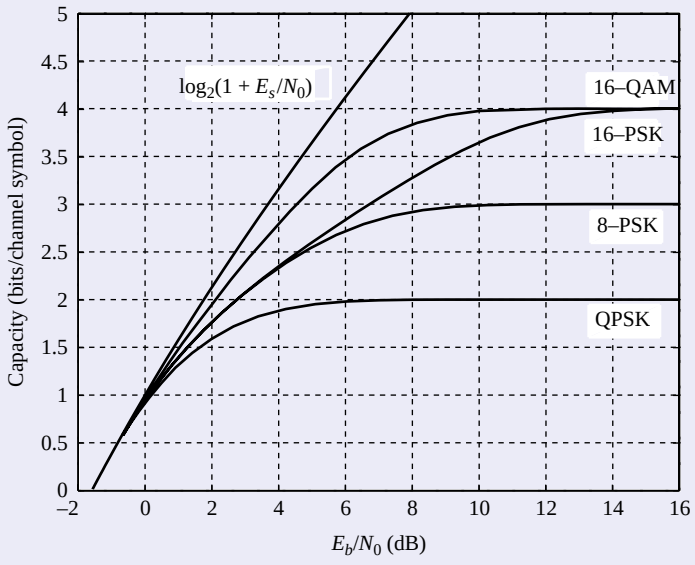
max. atteint pour $X(\omega) \sim \mathcal{N}(0, \sigma_x^2 = P)$

# Canal additif gaussien à entrées binaires (BI-AWGN)

$$\begin{array}{ccccc} & & B(\omega) & & \\ & & \downarrow & & \\ X(\omega) & \longrightarrow & \oplus\!\!\sum & \longrightarrow & Y(\omega) \end{array} \tag{12}$$

- $X(\omega) \in \mathcal{X} = \{0, 1\}$, avec $p(X = 1) = 1/2$
- $B(\omega) \sim \mathcal{N}(0, \sigma_b^2 = N_0/2)$
- canal symétrique : $p(y|x = +1) = p(-y|x = -1)$

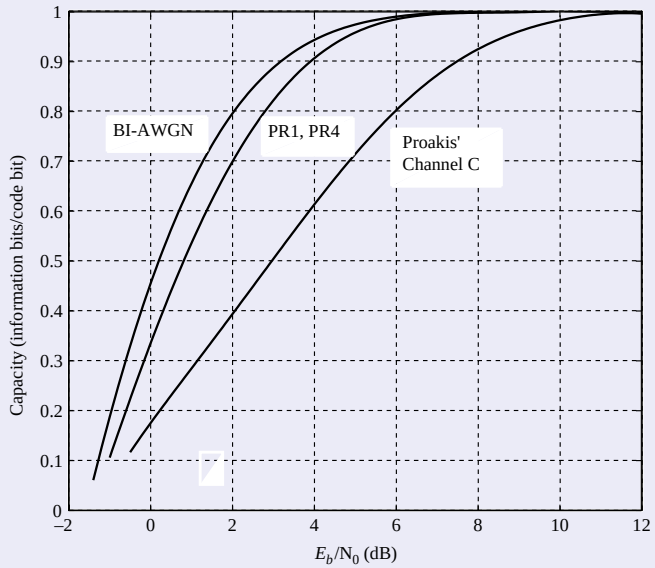
# Canal additif gaussien à entrées M-aire (CI-AWGN)




$$\begin{array}{ccccc} & & B(\omega) & & \\ & & \downarrow & & \\ X(\omega) & \longrightarrow & \bigoplus\!\!\sum & \longrightarrow & Y(\omega) \end{array}$$

- $X(\omega) \in \mathcal{X} = \{0, \ldots, M\}$, avec $p(X = x) = 1/M$
- $B(\omega) \sim \mathcal{CN}(0, \sigma_b^2 = N_0)$

# Canaux sélectif en fréquence à entrées binaires(BI-ISI)




$$y[n] = \sum_{k=0}^{L-1} h[k]x[n-k] + b[n] \quad (13)$$

- $X \in \mathcal{X} = \{-1, +1\}$, avec $p(X = x) = 1/2$
- $B \sim \mathcal{N}(0, \sigma_b^2 = N_0/2)$

# Plan

# Codes en bloc linéaires

## Quelques définitions

On considère des codes définis sur le corps binaire $\mathbb{F}_2 = GF(2)$.

### Codes linéaires en blocs

- Un code en blocs binaire $\mathcal{C}(N, K)$ de longueur $N$ est une application $g(.)$ de l'ensemble $\mathbb{F}_2^K = \{0,1\}^K$ vers l'ensemble $\mathbb{F}_2^N = \{0,1\}^N$ qui associe à tout bloc de données $\mathbf{u}$ un mot de code $\mathbf{c}$.

$$\begin{array}{rcl} g : \mathbb{F}_2^K & \rightarrowtail & \mathbb{F}_2^N \\ \mathbf{u} & \mapsto & \mathbf{c} = g(\mathbf{u}) \end{array} \tag{14}$$

- $\#$ mots de code : $2^K$.
- Rendement : $R = K/N$ ($K$ symb. d'inf., $N$ symb. codés).
- $\mathcal{C}(N, K)$ est dit linéaire si $g(.)$ est une application linéaire (les mots de codes sont un sous-espace vectoriel de $\mathbb{F}_2^N$).

# Codes en bloc linéaires

## Matrice génératrice

### Matrice génératrice

- On note $\mathbf{c} = [c_0, \ldots, c_{N-1}]$ et $\mathbf{u} = [u_0, \ldots, u_{K-1}]$
- la matrice génératrice $\mathbf{G}$ de dimensions $K \times N$ est définie comme étant l'application linaire définie comme

$$\mathbf{c} = \mathbf{uG}$$

- Espace du code : $\mathrm{Im}(\mathcal{C}) = \{\mathbf{c} \in \mathbb{F}_2^N | \mathbf{c} = \mathbf{uG}, \quad \forall \mathbf{u} \in \mathbb{F}_2^K\}$
- $\mathrm{rang}(G) = K$ (les lignes de $\mathbf{G}$ sont $K$ mots de codes indépendants) et $\mathbf{G}$ non unique.
- $\mathbf{G}$ est dite systématique si $\forall k \in [0, K-1], \exists n \in [0, N-1]$ tel que $c[n] = u[k]$. $\mathbf{G}$ peut alors se mettre sous la forme

$$\mathbf{G} = [P | I_K]$$

# Codes en bloc linéaires

## Matrice de parité

### Matrice de parité

- Le code $\mathcal{C}^{\perp}(N-K, K)$, dit code dual, vérifie que tout mot du code dual est orthogonal à tout mot du code $\mathcal{C}(N, K)$. On note sa matrice génératrice **H**.
- On a alors $\{\mathbf{c} \in \mathcal{C}(N,K) | \mathbf{c}\mathbf{H}^{\top} = \mathbf{0}\}$
- Relation avec **G** : $\mathbf{G}\mathbf{H}^{\top} = \mathbf{0}$
- Pour un code systématique, $\mathbf{H} = [I_{N-K} | P^{\top}]$.
- Détection d'erreur à l'aide du *syndrome* : $\mathbf{r} = \mathbf{c} + \mathbf{e}$

$$\mathbf{s} = \mathbf{r}\mathbf{H}^{\top} = \mathbf{e}\mathbf{H}^{\top}$$

- Si **e** est un mot de code, alors on parle d'erreurs *non détectable*.

# Codes en bloc linéaires

## Distance minimum et spectre de distance du code

### Matrice de parité

- Distance de Hamming : $d_H(c_i, c_j) = \boldsymbol{w}(c_i \oplus c_j)$
- Distance minimale :

$$\begin{aligned} d_{\min} &= \min\{d_H(c_i, c_j) | c_i, c_j \in \mathcal{C}(N, K); c_i \neq c_j\} \\ &= \min\{\boldsymbol{w}(c) | c \in \mathcal{C}(N, K), c \neq 0\} \end{aligned} \quad (15)$$

- Spectre de distance d'un code :

$$\forall i = 1 \ldots N, A_i = \#\mathbf{c} \in \mathcal{C}(N, K),\ \boldsymbol{w}(c) = i$$

  $\{A_0, A_1 \ldots A_N\}$ est appelé spectre de distance du code
- $d_{\min}$ est égale au plus petit nombre de colonnes dont la somme est le vecteur nul.
- $d_{\min} - 1$ erreurs détectables, $\lfloor (d_{\min} - 1)/2 \rfloor$ erreurs corrigibles sur BSC.

# Codes en bloc linéaires

## Exemples

### code de répétition

Un code de répétition consiste en la répétition de $N$ fois un bit d'information. On obtient un code $\mathcal{C}(N, 1)$ de matrice génératrice

$$G_1 = [\underbrace{1 \ldots 1 \ldots 1}_{N}]$$

### code de vérification de parité

$c_{N-1} = u_0 \oplus u_1 \oplus \ldots \oplus u_{N-2}$
définissant un code $\mathcal{C}(N, N-1)$

$$G_2 = \begin{pmatrix} \sum & & 1 \\ & & \vdots \\ & I_{N-1} & 1 \\ & & \vdots \\ \sum & & 1 \end{pmatrix} \sum$$

### Relation

les deux codes sont duaux :

$$G_1 G_2^{\top} = \mathbf{0}$$

# Plan

# Critères de décodage

## Décodage par Maximum a Posteriori (MAP)

$$\hat{\mathbf{c}} = \arg\max_{\mathbf{c}'} p(\mathbf{c}'|\mathbf{y}) \quad (16)$$

$$= \arg\max_{\mathbf{c}'} \frac{p(\mathbf{y}|\mathbf{c}')p(\mathbf{c}')}{p(\mathbf{y})} \quad (17)$$

## Décodage par Maximum de Vraisemblance (ML)

$$\hat{\mathbf{c}} = \arg\max_{\mathbf{c}'} p(\mathbf{y}|\mathbf{c}') \quad (18)$$

## Exemple de canaux

- canal BSC : $\hat{\mathbf{c}} = \arg\min_{\mathbf{c}'} d_H(\mathbf{y}, \mathbf{c}')$
- canal BI-AWGN : $\hat{\mathbf{c}} = \arg\min_{\mathbf{c}'} d_E(\mathbf{y}, \mathbf{c}') = \arg\min_{\mathbf{c}'} \sum_n (y_n - c'_n)^2$