Rappel de codage canal, critères de décodage

C. Poulliat

19 novembre 2020

Plan

Plan

1. Rappel sur le codage de canal
   - Quelques définitions
2. Notion de décodage souple et utilisation de LLR
   - Décodage souple
3. Modulations codées à bits entrelacés

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 $\mathbf{c}$.

$$\begin{aligned} g : \mathbb{F}_2^K &\rightarrow \mathbb{F}_2^N \\ \mathbf{u} &\mapsto \mathbf{c} = g(\mathbf{u}) \end{aligned} \tag{1}$$

- $\#$ 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

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

- Espace du code : $\mathrm{Im}(\mathcal{C}) = \{\mathbf{c} \in \mathbb{F}_2^N | \mathbf{c} = \mathbf{u}\mathbf{G}, \;\; \forall \mathbf{u} \in \mathbb{F}_2^K\}$
- $\mathrm{rang}(G) = K$ (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 $\mathbf{H}$.
- On a alors $\{\mathbf{c} \in \mathcal{C}(N, K) | \mathbf{c}\mathbf{H}^{\top} = \mathbf{0}\}$
- Relation avec $\mathbf{G}$: $\mathbf{G}\mathbf{H}^{\top} = \mathbf{0}$
- 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 $\mathbf{e}$ 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 :

$$\begin{aligned} d_{\min} &= \min\{d_H(c_i, c_j) | c_i, c_j \in \mathcal{C}(N, K); c_i \neq c_j\} \\ &= \min\{\boldsymbol{w}(c) | c \in \mathcal{C}(N, K), c \neq 0\} \end{aligned} \quad (2)$$

- 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.

Quelques codes particuliers

- Un **code de répétition** consiste en la répétition de N fois un bit d'information.

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

- Un **code de vérification de parité** est construit tel que $c_{N-1} = u_0 \oplus u_1 \oplus \dots \oplus u_{N-2}$ définissant un code $\mathcal{C}(N, N-1)$.

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

On peut alors remarquer que les deux codes précédents sont duaux, ie.

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

Critères de décodage

Décodage par Maximum a Posteriori (MAP) séquence

$$\begin{aligned} \hat{\mathbf{c}} &= \arg\max_{\mathbf{c}'} p(\mathbf{c}'|\mathbf{y}) && (3) \\ &= \arg\max_{\mathbf{c}'} \frac{p(\mathbf{y}|\mathbf{c}')p(\mathbf{c}')}{p(\mathbf{y})} && (4) \end{aligned}$$

Décodage par Maximum de Vraisemblance (ML) séquence

$$\hat{\mathbf{c}} = \arg\max_{\mathbf{c}'} p(\mathbf{y}|\mathbf{c}') \quad (5)$$

Exemple de canaux

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

Plan

1. Rappel sur le codage de canal
   - Quelques définitions

2. Notion de décodage souple et utilisation de LLR
   - Décodage souple

3. Modulations codées à bits entrelacés

Décodage "souple"

Utilisation de log-likelihood ratios (LLR)

- LLR associé à

$$l(c_n) \triangleq \log\left(\frac{P(c[n]=0|y[n])}{P(c[n]=1|y[n])}\right)$$

- LLR en fonction des probabiltés de transitions et a priori :

$$l(c_n) = \log\left(\frac{P(y[n]|c[n]=0)}{P(y[n]|c[n]=1)}\right) + \log\left(\frac{P(c[n]=0)}{P(c[n]=1)}\right)$$

- Lien avec critère MAP bit classique en BPSK

$$\begin{aligned} \hat{c}_n &= \arg\max_{c_n} p(c[n]|y[n]) \\ &= \mathrm{signe}(L(c_n)) \end{aligned} \qquad (6)$$

Décodage "souple"

Utilisation de log-likelihood ratios (LLR)

Passage LLR vers probabilités

$$p(u_n = 0|y_n) + p(u_n = 1|y_n) = 1 \tag{7}$$

$$L(u_n) = \log\left(\frac{p(u_n = 0|y_n)}{p(u_n = 1|y_n)}\right) \tag{8}$$

$$\Updownarrow$$

$$p(u_n = 0|y_n) = \frac{e^{L(u_n)}}{1 + e^{L(u_n)}} \tag{9}$$

$$p(u_n = 1|y_n) = \frac{1}{1 + e^{L(u_n)}} \tag{10}$$

Décodage "souple"

Utilisation de log-likelihood ratios (LLR)

Passage LLR vers probabilité : expressions génériques

$$p(u_n|y_n) = \frac{e^{(1-u_n)L(u_n)}}{1 + e^{L(u_n)}}$$

$$p(u_n|y_n) = \frac{e^{x_n \frac{L(u_n)}{2}}}{e^{-\frac{L(u_n)}{2}} + e^{+\frac{L(u_n)}{2}}}$$

Décodage ”souple”

Utilisation de log-likelihood ratios (LLR)

Lien avec l’estimation - *”soft bit”*

$$\hat{x}_n = \mathbb{E}(X_n | Y_n = y_n) = \tanh\left(\frac{L(u_n)}{2}\right)$$

$\hat{x}_n$ est la meilleure estimée non linaire au sens du MMSE, ie.

$$\hat{x}(n) = \arg\min_{x \in \mathbb{R}} \mathbb{E}(|x(n) - \hat{x}(n)|^2)$$

Expression de la capacité BPSK

$$I(X;Y) = \frac{1}{2}\sum_{x=\pm 1}\int_{\mathbb{R}} f(y \mid x)\log_2\left(\frac{2f(y \mid x)}{f(y \mid x=+1)+f(y \mid x=-1)}\right)dy$$

mais plus utile :

$$I(X;Y) = H(X) - H(X \mid Y) = 1 + \mathbb{E}_{X,Y}\left(\log_2(p(X \mid Y))\right)$$

Si $L(y) = \log\left(\frac{p(x=+1|Y=y)}{p(x=-1|Y=y)}\right)$, $p(x \mid y) = \frac{1}{1+e^{-xL(y)}}$
d'où

$$\begin{aligned} \hat{I}(X;Y) &= 1 + \frac{1}{N}\sum_{n=0}^{N-1}\log_2(p(x[n] \mid y[n])) \\ &= 1 - \frac{1}{N}\sum_{n=0}^{N-1}\log_2\left(1 + e^{-x[n]L(y|n])}\right) \qquad (11) \end{aligned}$$

Décodage par Maximum de Vraisemblance révisité

BI-AWGN sans a priori : décodeur par corrélation

$$\begin{aligned} \hat{\mathbf{c}} &= \arg\min_{\mathbf{c}'} \sum_n (y_n - x'_n)^2 \\ &= \arg\max_{\mathbf{c}'} \sum_n l(c'_n) x'_n \end{aligned} \tag{12}$$

où

$$l(c'_n) = \frac{2}{\sigma^2} y[n]$$

Cas général : canal sans mémoire, $P(y_n|c_n)$, $c_n = 0, 1$

$$\hat{\mathbf{c}} = \arg\max_{\mathbf{c}'} \sum_n l(c'_n) \tilde{c}'_n \tag{13}$$

où

$$\tilde{c}'_n = (1 - 2c'_n)$$

Décodage MAP par bit

Décodage par MAP Bit

$$
\begin{aligned}
\hat{c}_n &= \arg\max_{c'_n} p(c'_n|\mathbf{y}) && (14)\\
&= \arg\max_{c'_n} \sum_{\mathbf{c}\in\mathcal{C}|c_n=c'_n} p(\mathbf{y}|\mathbf{c})p(\mathbf{c}) && (15)\\
&= \arg\max_{c'_n} \sum_{\mathbf{c}\in\mathcal{C}|c_n=c'_n} p(\mathbf{y}|\mathbf{c}) && (16)\\
&= \arg\max_{c_n} \sum_{\sim c_n} p(\mathbf{y}|\mathbf{c})\mathbb{1}_{\{\mathbf{c}\in\mathcal{C}\}}. && (17)
\end{aligned}
$$

Démodulation MAP symbole et bit

Hypothèses

- Les vecteurs binaires $x[n] = [x_1[n] \cdots x_m[n]]$ sont “mappés” sur des symboles $s[n] \in \mathcal{S}$,
- Canal sans mémoire à entrées M-aires équi-distribués.

Vraisemblance Symbole et critère MAP associé

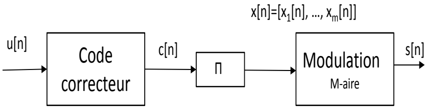
- Symbol Likelihood : $P(y[n]|s[n])$,
- MAP Symbole :

$$\hat{s}_n = \arg\max_{s_n} p(y[n]|s[n])$$

MAP bit

$$L(x_i[n]) \quad = \quad \log \left(\frac{\sum_{s[n]\in\mathcal{S}_0^i} P(y[n]|s[n])P(s[n])}{\sum_{s[n]\in\mathcal{S}_1^i} P(y[n]|s[n])P(s[n])} \right)$$

Modulations codées à bits entrelacés



Bit-Interleaved Coded Modulation

- système de transmission à haute efficacité spectrale : constellation M-aire $\mathcal{S}$ avec $M = 2^m$.
- Peut-être vu comme $\log_2(M)$ canaux parallèles,
- Capacité atteignable dépend du mapping utilisé :

$$C_{\mathrm{bicm}} = m - \frac{1}{2}\sum_{k=0}^{m-1}\sum_{c=0}^{1}\mathbb{E}\left(\log_2\left(\frac{\sum_{s_i\in\mathcal{S}} p(y|s_i)}{\sum_{s_j\in\mathcal{S}_c^k} p(y|s_j)}\right)\right)$$

Modulations codées à bits entrelacés

Bit-Interleaved Coded Modulation

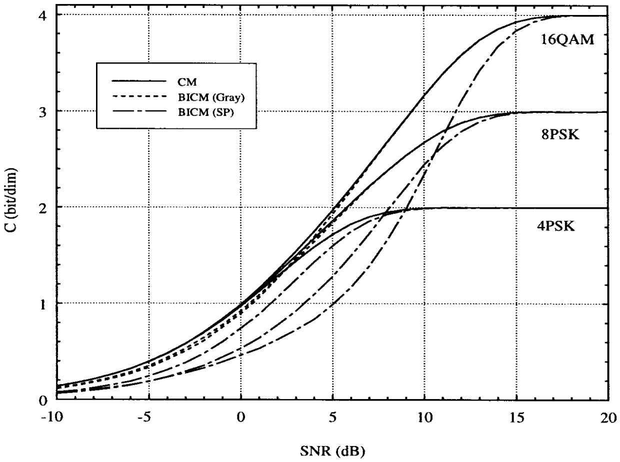
- Peut-être vu comme $\log_2(M)$ canaux parallèles,
- Capacité atteignable dépend du mapping utilisé :

$$C_{\mathrm{bicm}} = \sum_{k=1}^{m} \mathbf{I}(X_k; Y) \leq C_{AWGN},$$

où $\mathbf{I}(X_k; Y) = 1 - \mathbb{E}_{X_k,Y}(\log_2(1 + e^{-(1-2X_k)L(X_k)}))$. $L(X_k)$ est une fonction implicite de Y.

$\Rightarrow$ en général pour les modulations linéaires, le mapping de Gray permet d'être quasi optimal pour les efficacités moyennes à grandes.

Modulations codées à bits entrelacés



Modulations codées à bits entrelacés