Analyse et traitements dans un système de communication numérique avancé

C. Poulliat

4 juin 2012

Plan

Plan

Entropie, entropie conjointe

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

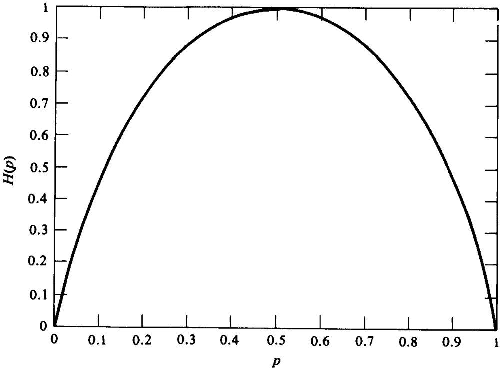
Entropie

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

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

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

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

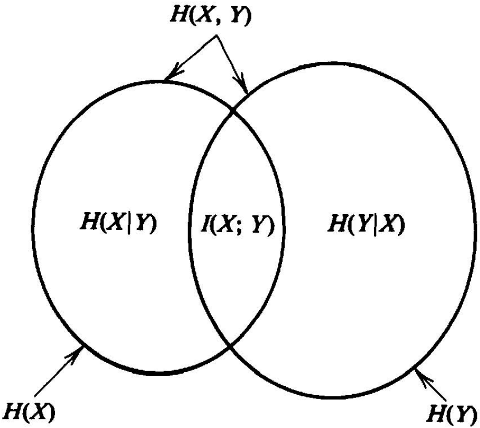
$$\begin{aligned} \mathbf{I}(X;Y) &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(X=x,Y=y)\log_2\left(\frac{p(X=x)p(Y=y)}{p(X=x,Y=y)}\right) \\ &= -\mathbb{E}\left(\log_2\left(\frac{p(X)p(Y)}{p(X,Y)}\right)\right) \geq 0 \end{aligned} \tag{4}$$

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

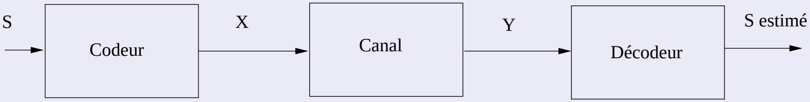


Plan

1. Comment déterminer les performances asymptotiques d'un système ?
   - Rappels de théorie de l'information
   - Capacité d'un canal discret sans mémoire
   - Capacité d'un canal à entrées et/ou sorties continues
2. Rappel sur le codage de canal
   - Quelques définitions
3. Notion de décodage souple et utilisation de LLR
   - Décodage souple
   - Modulations codées à bits entrelacés

Capacité d'un canal discret sans mémoire

Définition



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

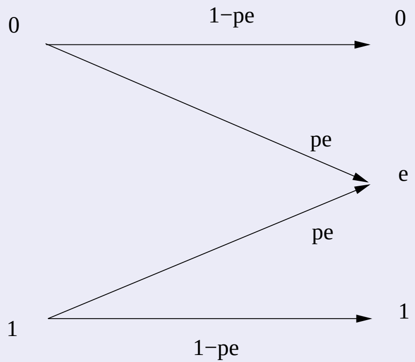
Définition

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

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

Capacité d'un canal discret sans mémoire

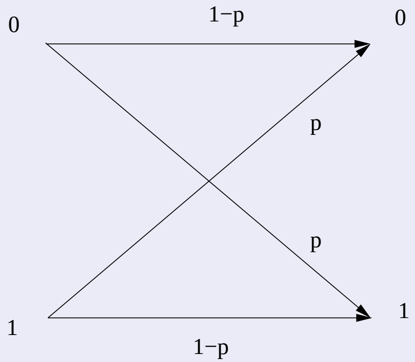
Canal à effacement (BEC)



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

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.

Interprétation

- Communication fiable possible si on considère des communications **codées** (quid du cas non codé ?)
- Il existe un code de rendement $R < C$ qui permet de communiquer de façon fiable,
- fiable = avec une probabilité d'erreur arbitrairement faible.

Plan

1. Comment déterminer les performances asymptotiques d'un système ?
   - Rappels de théorie de l'information
   - Capacité d'un canal discret sans mémoire
   - Capacité d'un canal à entrées et/ou sorties continues
2. Rappel sur le codage de canal
   - Quelques définitions
3. Notion de décodage souple et utilisation de LLR
   - Décodage souple
   - Modulations codées à bits entrelacés

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)

$$
\begin{array}{ccccc}
 & & B(\omega) & & \\
 & & \downarrow & & \\
X(\omega) & \longrightarrow & \bigoplus & \longrightarrow & Y(\omega)
\end{array}
\tag{9}
$$

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

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

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

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

Canal additif gaussien à entrées M-aire (CM-AWGN)

Comment calculer cette capacité pour une modulation donnée ? (1/2)

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

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

- Calculer la capacité revient à évaluer

$$\mathbf{C} = \mathbf{I}(X; Y)$$

- Termes à calculer : $\mathbf{H}(X)$, $\mathbf{H}(X|Y)$.

Canal additif gaussien à entrées M-aire (CM-AWGN)

Comment calculer cette capacité pour une modulation donnée ? (2/2)

- Calcul de $\mathbf{H}(X)$: $\mathbf{H}(X) = 1/M$
- Calcul de $\mathbf{H}(X|Y)$:

$$\mathbf{H}(X|Y) = -\mathbb{E}(\log_2 p(X|Y)) = \mathbb{E}(h(X|Y))$$

  or

$$p(X|Y) = \frac{p(Y|X)}{\sum_{x \in \mathcal{X}} p(Y|X = x)}$$

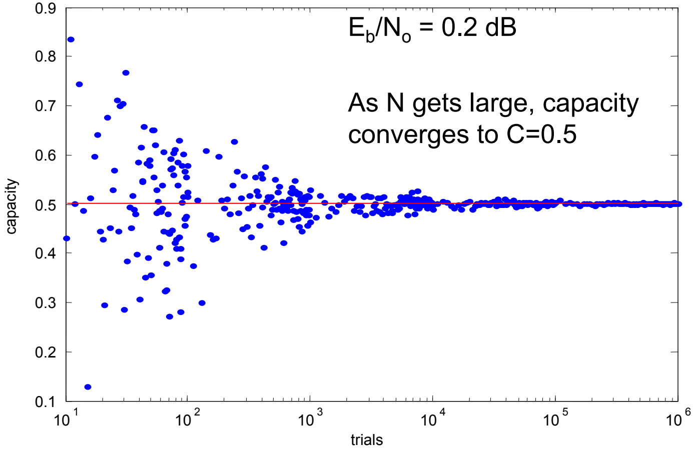
- Estimateur de $\mathbf{H}(X|Y)$: par ergodicité, on a

$$\mathbf{H}(X|Y) = \mathbb{E}(h(X|Y)) = \lim_{N \to +\infty} \frac{1}{N} \sum_{n} h(X(n)|Y(n))$$

- Méthode par Monte-Carlo :
  1. Tirer aléatoirement et uniformément des symboles issue de constellation,
  2. Calculer pour chaque couple $(X(n), Y(n))$, $h(X(n)|Y(n))$ et moyenner.

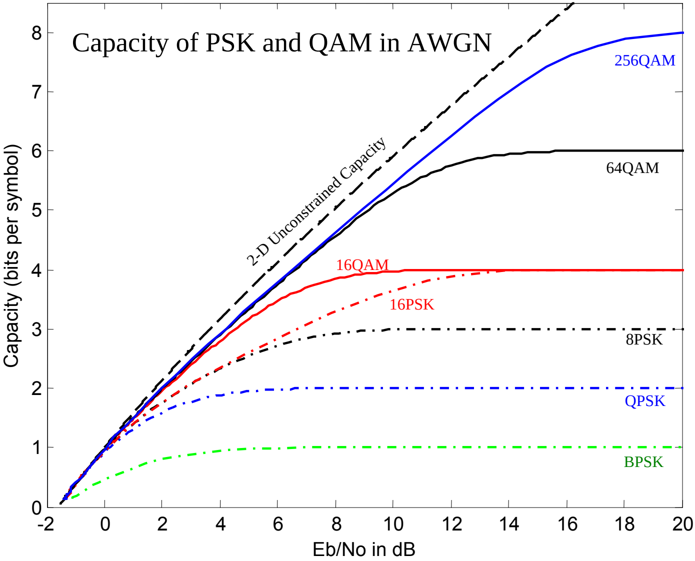
Canal additif gaussien à entrées M-aire (CM-AWGN)

Influence du nombre d'échantillons

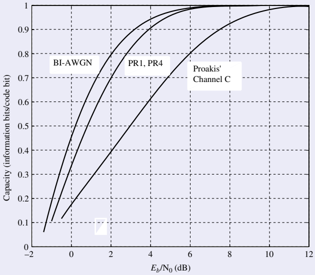


Canal additif gaussien à entrées M-aire (CM-AWGN)

Exemples



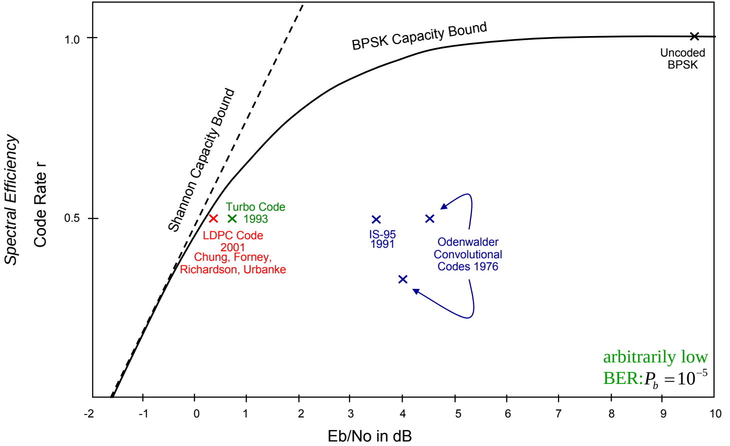
Canaux sélectif en fréquence à entrées binaires(BI-ISI)



$$y[n] = \sum_{k=0}^{L-1} h[k]x[n-k] + b[n] \quad (12)$$

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

Comparer l'efficacité des systèmes de codage grâce à la capacité.



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 **u** un mot de code **c**.

$$\begin{aligned} g : \mathbb{F}_2^K &\rightarrow \mathbb{F}_2^N \\ \mathbf{u} &\mapsto \mathbf{c} = g(\mathbf{u}) \end{aligned} \tag{13}$$

- $\#$ 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 $\mathbf{c} = [c_0, \dots, c_{N-1}]$ et $\mathbf{u} = [u_0, \dots, u_{K-1}]$
- 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 **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 :

$$\begin{aligned} d_{\min} &= \min\{d_H(c_i, c_j) | c_i, c_j \in \mathcal{C}(N, K); c_i \neq c_j\} \\ &= \min\{\boldsymbol{w}(c) | c \in \mathcal{C}(N, K), c \neq 0\} \end{aligned} \quad (14)$$

- Spectre de distance d'un code :

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

  $\{A_0, A_1 \dots A_N\}$ 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.

Critères de décodage

Décodage par Maximum a Posteriori (MAP)

$$\hat{\mathbf{c}} = \arg\max_{\mathbf{c}'} p(\mathbf{c}'|\mathbf{y}) \quad (15)$$

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

Décodage par Maximum de Vraisemblance (ML)

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

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. Comment déterminer les performances asymptotiques d'un système ?
   - Rappels de théorie de l'information
   - Capacité d'un canal discret sans mémoire
   - Capacité d'un canal à entrées et/ou sorties continues
2. Rappel sur le codage de canal
   - Quelques définitions
3. Notion de décodage souple et utilisation de LLR
   - Décodage souple
   - 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

$$\begin{aligned}\hat{c}_n &= \arg\max_{c_n} p(c[n]|y[n]) \\ &= \mathrm{signe}(L(c_n))\end{aligned} \tag{18}$$

Décodage par Maximum de Vraisemblance révisité

BI-AWGN sans a priori : décodeur par corrélation

$$\begin{aligned} \hat{\mathbf{c}} &= \arg\min_{\mathbf{c}'} \sum_n (y_n - c'_n)^2 \\ &= \arg\max_{\mathbf{c}'} \sum_n I(c'_n)c'_n \end{aligned} \tag{19}$$

où

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

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

$$\hat{\mathbf{c}} = \arg\max_{\tilde{\mathbf{c}}'} \sum_n I(\tilde{c}'_n)\tilde{c}'_n \tag{20}$$

où

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

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 :

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

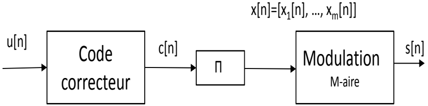
MAP bit

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

Plan

Analyse EXIT charts

Modulations codées à bits entrelacés



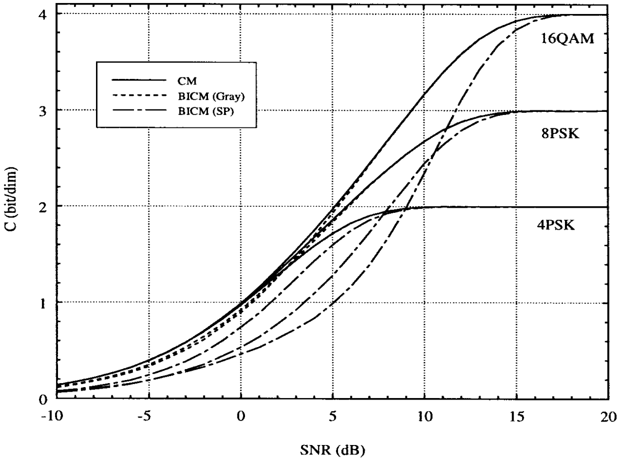
Bit-Interleaved Coded Modulation

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

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

Analyse EXIT charts

Modulations codées à bits entrelacés



Analyse EXIT charts

Modulations codées à bits entrelacés