Théorie de l'information et codage pour les canaux de Rayleigh MIMO

Philippe Ciblat

École Nationale Supérieure des Télécommunications, Paris, France

Plan

1. Canal de Rayleigh
   - Modèle
   - Diversité
   - Système MIMO
2. Théorie de l'information
   - Canal déterministe (SISO et MIMO)
   - Canal aléatoire (capacité ergodique, probabilité de coupure)
   - Compromis « gain de multiplexage - gain de diversité »
3. Construction de codes
   - Code d'Alamouti
   - Code V-BLAST
   - Code d'Or

Modèle de canal radio-mobile

- Débit < Bande de cohérence
- Temps symbole $\approx$ Temps de cohérence

Canal de Rayleigh

$$y(n) = h(n)x(n) + b(n)$$

avec

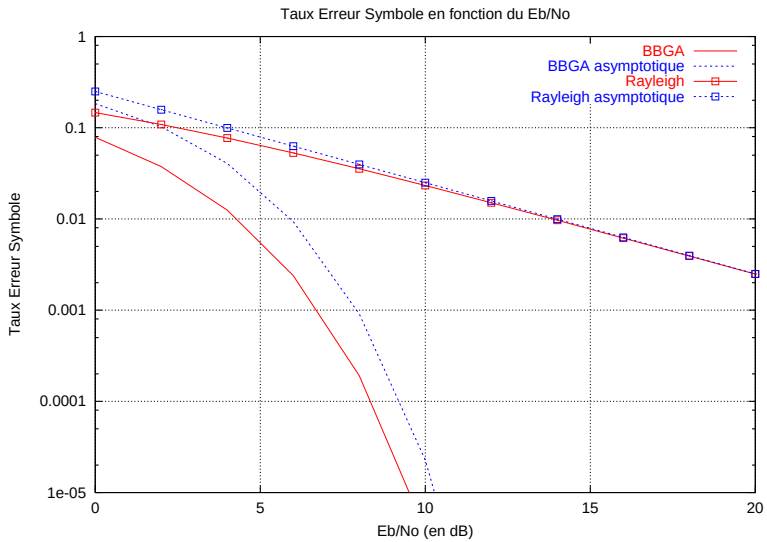
- $y(n)$: signal reçu
- $x(n)$: signal émis
- $h(n)$: canal aléatoire de Rayleigh
- $b(n)$: bruit additif gaussien

- Modèle valide aussi pour l'OFDM

Performances

Probabilité d'erreur

$$P_e = \mathbb{E}[P_e(h)] \propto \frac{1}{E_s/N_0}$$



Canal gaussien

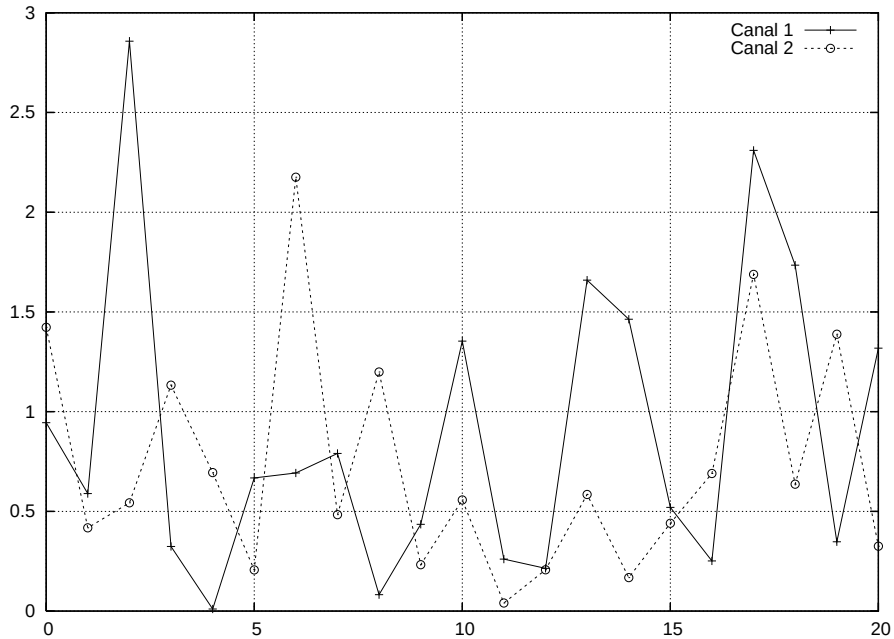
$$P_e \approx e^{-E_s/N_0}$$

Notion de diversité

Problème : lorsque l'évanouissement $h(n)$ est faible, la qualité de la transmission est catastrophique.

Remarque

Si le même signal est reçu par plusieurs canaux indépendants, alors la probabilité d'erreur va diminuer. Le nombre de versions reçues sera appelé *ordre de diversité* ou *diversité*.



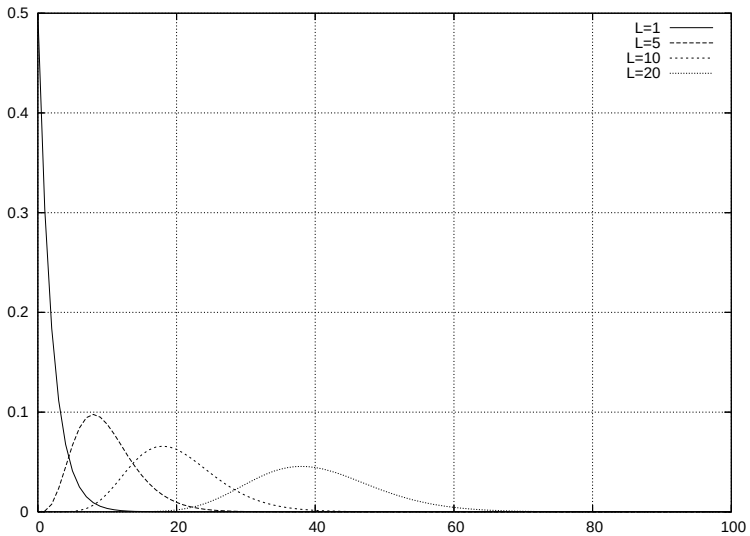
Performances (I)

$$y_\ell(n) = h_\ell(n)x(n) + b_\ell(n), \quad \ell = 1, \cdots, L$$

Récepteur optimal : détecteur à seuil sur la variable

$$z(n) = \sum_{\ell=1}^{L} \overline{h_\ell(n)} y_\ell(n) = \underbrace{\left(\sum_{\ell=1}^{L} |h_\ell(n)|^2 \right)}_{G(n)} x(n) + \sum_{\ell=1}^{L} \overline{h_\ell(n)} b_\ell(n)$$

$G(n)$ suit une loi du χ_2 à $2L$ degrés de liberté.



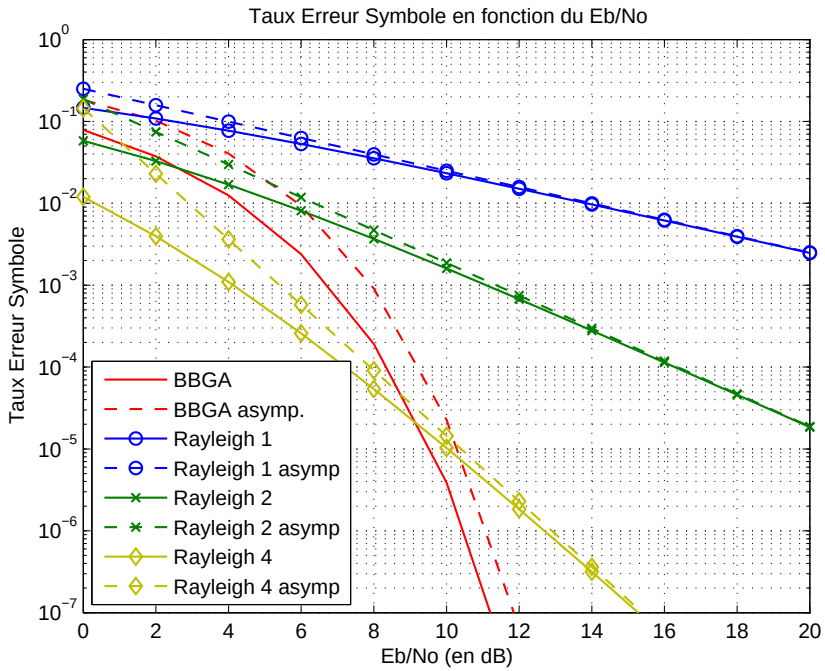
Performances (II)

Probabilité d'erreur

$$P_e \propto \frac{1}{(E_s/N_0)^L}$$

à fort Rapport Signal-à-Bruit.

L = ordre de diversité



Types de diversité

Type 1 : ne nécessite pas de répétition de l'information

- Diversité d'espace en réception (longueur de cohérence : $\lambda/2$)
- Diversité de trajets

Type 2 : nécessite la répétition (ou codage)

- Diversité de fréquence (bande de cohérence)
- Diversité de temps (temps de cohérence)
- Diversité d'espace en émission

Exemples de diversité temporelle

- La répétition revient à utiliser un code à répétition de rendement $1/n$. Cela induit une faible efficacité spectrale.
  Il convient d'employer un code de rendement k/n et de distance minimale $d_{\min}$. On aura

$$P_e \propto \frac{1}{(E_s/N_0)^{d_{\min}}}$$

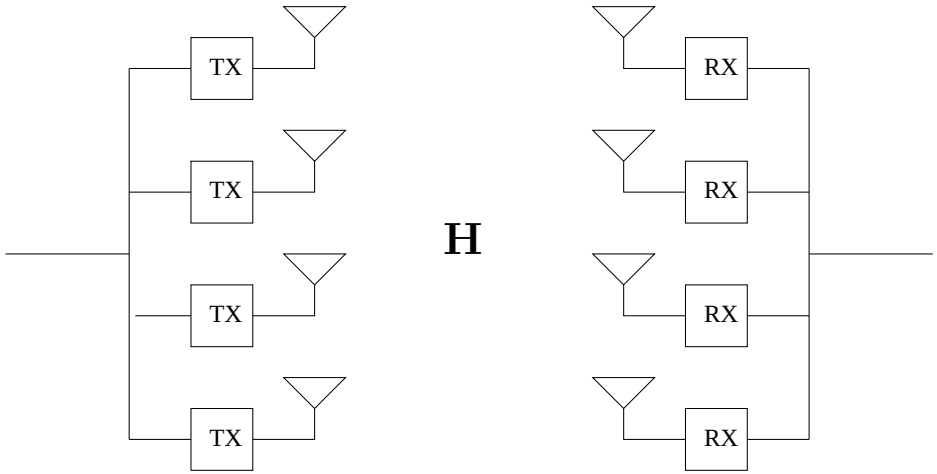
- Observons $y(1) = h(1)x(1) + b(1)$ et $y(2) = h(2)x(2) + b(2)$, avec $x(1)$ et $x(2)$ des données indépendantes appartenant à une MDP-2. On a

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{b}$$

  avec $\mathbf{y} = [y(1), y(2)]^{\mathrm{T}}$, $\mathbf{H} = \mathrm{diag}(h(1), h(2))$.

  - Système à diversité de 1.
  - En lieu et place de $\mathbf{x}$, transmettons $\mathbf{Wx}$ avec $\mathbf{W}$ une rotation.
    Système à diversité de 2 et pourtant code de rendement 1.

Système MIMO



Signal reçu

$$\mathbf{Y}_{n_r \times T} = \mathbf{H}_{n_r \times n_t} \mathbf{X}_{n_t \times T} + \mathbf{B}_{n_r \times T}$$

avec

- **H** parfaitement connu au récepteur.
- le canal à évanouissement par bloc
- T la longueur temporelle du bloc ($T > 1$ nécessaire en MIMO !)

Performances (I)

Probabilité d'erreur par paire

A fort Rapport Signal-à-Bruit, le maximum de vraisemblance donne

$$P(\mathbf{X} \to \mathbf{X}') \approx \left(\prod_{k=1}^{r} \lambda_k \right)^{-n_r} \left(\frac{1}{E_s/N_0} \right)^{rn_r}$$

avec λ_k les v.a.p. et r le rang de la matrice $(\mathbf{X} - \mathbf{X}').(\mathbf{X} - \mathbf{X}')^{\mathrm{H}}$.

Pseudo-distance :

- Gaussien : distance euclidienne
- Canal binaire symétrique : distance de Hamming
- Canal de Rayleigh : distance produit

Diversité et gain de codage

$$d = rn_r \quad \gamma = \left(\prod_{k=1}^{r} \lambda_k \right)^{n_r}$$

Performances (II)

Construction de codes :

- La diversité à la réception est acquise (n_r)
- La diversité à l'émission (n_t) est à récupérer

Critère du rang

Afin d'atteindre la diversité maximale $n_t n_r$, la matrice $(\mathbf{X} - \mathbf{X}').(\mathbf{X} - \mathbf{X}')^{\mathrm{H}}$ doit être de rang plein ($\Rightarrow T > 1$ si $n_t > 1$).

Critère du déterminant

Afin de maximiser le gain de codage, le déterminant minimal de la matrice $(\mathbf{X} - \mathbf{X}').(\mathbf{X} - \mathbf{X}')^{\mathrm{H}}$ doit être maximiser.

Débit :

- Rendement du code : nombre de symboles émis par temps-symbole (max. n_t)
- Performances à débit fixé bien connues
- Quid du débit admissible ?

Théorie de l'information : canal déterministe

Canaux discrets stationnaires sans mémoire

Entropie :

$$H(Z) = -\sum_k \Pr(Z = z_k) \log_2(\Pr(Z = z_k))$$

Information mutuelle :

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

- Exemple :
  Si $Y = X$, alors $I(X,Y) = H(X)$
  Si Y et X ind., alors $I(X,Y) = 0$

Capacité de canal

Définition mathématique

Soit C la capacité d'un canal, alors

$$C = \max_{p(X)} I(X, Y)$$

Théorème de la capacité

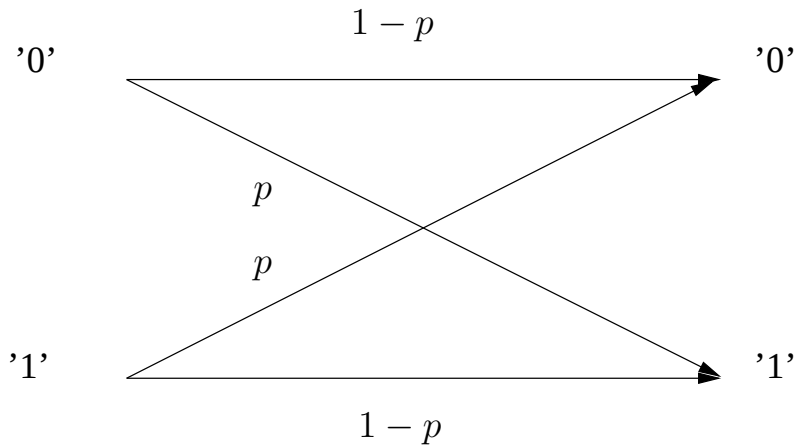
Il existe un codage de taux d'information T et de longueur N tel que $T < C$ pour lequel

$$\lim_{N \to \infty} P_e = 0$$

- La limite fondamentale est le débit et non la performance
- Théorème non constructif (*a priori* entrelacement long nécessaire)

Exemple : canal BSC (I)

Canal binaire symétrique

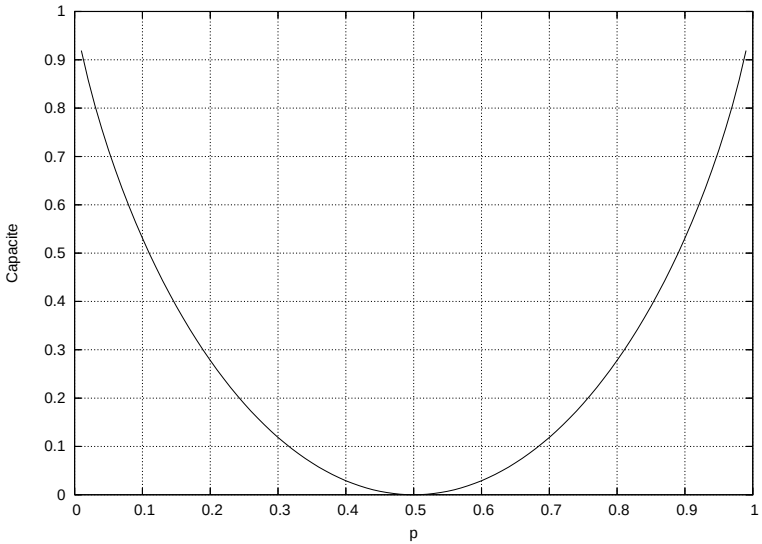


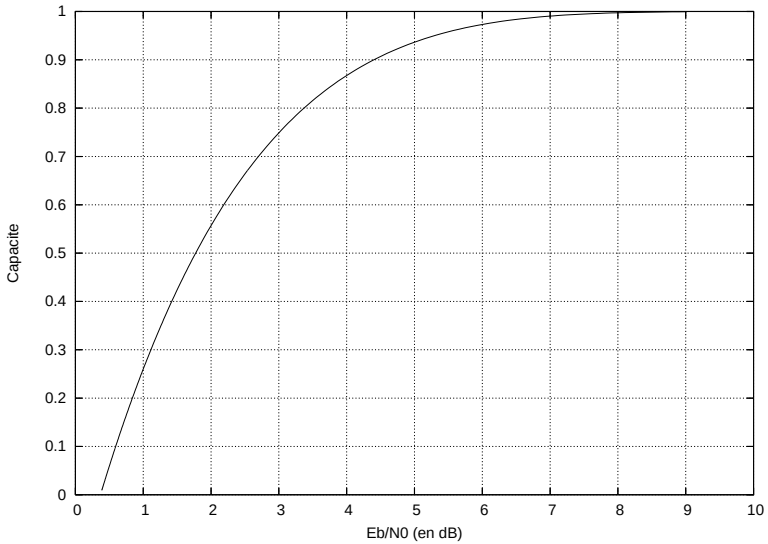
$$C = 1 - H(p)$$

- Canal représentant une transmission binaire avec décision dure
- Si le canal physique est gaussien, alors

$$p = Q\left(\sqrt{\frac{2E_c}{N_0}}\right) = Q\left(\sqrt{\frac{2E_bC}{N_0}}\right) \approx \frac{1}{2}e^{-E_bC/N_0}$$

Exemple : canal BSC (II)





- Capacité nulle pour $p = 1/2$.
- Capacité nulle en dessous de $E_b/N_0 = 0,4\text{dB}$

Capacité du canal gaussien

Canal gaussien à entrées et sorties continues :

$$y = x + b$$

avec

- la contrainte $\mathbb{E}[|x|^2] \leq P_x$
- b un bruit gaussien centré de variance $2N_0$ (par dim. complexe).

Information mutuelle

- L'entropie de x et y est infinie.
- On définit de manière plus générale l'information mutuelle

$$I(X;Y) = \int p(X,Y) \log_2 \left(\frac{p(X,Y)}{p(X)p(Y)} \right) dXdY$$

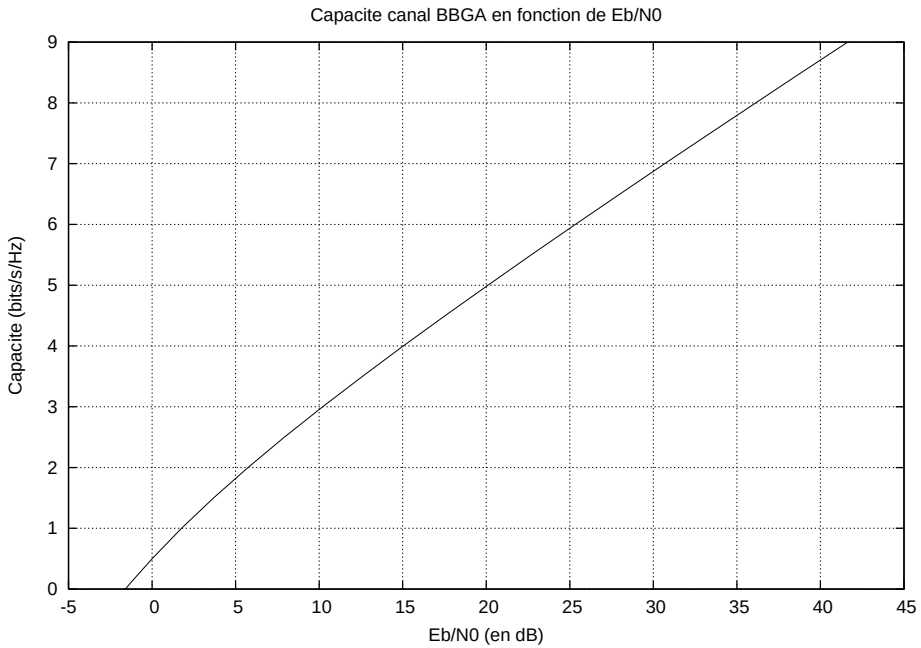
Exemple

Capacité

$$C = \log_2\left(1 + \frac{E_s}{2N_0}\right)$$

Comme $E_s/2 = T \times E_b$ et $T < C$,

$$E_b/N_0 \geq (2^T - 1)/(T) \overset{T\to 0}{\geq} \ln(2) \quad (-1.6\text{dB})$$



Canal MIMO

Soit X et Y deux processus gaussiens

Information mutuelle

$$I(X;Y) \propto \log_2 \det\left(\mathbf{Id} + \frac{1}{2N_0}\mathbf{HQH}^{\mathrm{H}}\right)$$

avec

$$\mathbf{Q} = \mathbb{E}[\mathbf{X}\mathbf{X}^{\mathrm{H}}]$$

Cas particulier :

Si

$$\mathbf{Q} = \frac{P_{\mathbf{X}}}{n_t}\mathbf{Id}_{n_t} \quad (\mathbb{E}[\mathrm{Tr}(\mathbf{X}\mathbf{X}^{\mathrm{H}})] \leq P_{\mathbf{X}})$$

alors

$$I(X;Y) \propto \log_2 \det\left(\mathbf{Id} + \frac{P_{\mathbf{X}}}{n_t 2N_0}\mathbf{H}\mathbf{H}^{\mathrm{H}}\right)$$

Théorie de l'information : canal aléatoire

Canal inconnu à l'émetteur (car canal variant dans le temps)

Capacité ergodique

Si un mot de code visite toutes les réalisations du canal, alors

$$C = \mathbb{E}_{\mathbf{H}} \left[\log_2 \det \left(\mathbf{Id} + \mathrm{RSB} \mathbf{H} \mathbf{H}^{\mathrm{H}} \right) \right]$$

A fort Rapport Signal-à-Bruit, si **H** est i.i.d., alors

$$C = \min(n_t, n_r) \log_2(\mathrm{RSB}) + \mathcal{O}(1)$$

Remarques :

- Gain de multiplexage : $\min(n_t, n_r)$
- le canal doit être de rang plein ($\min(n_t, n_r)$)
- le canal doit varier très rapidement
- le code ne doit pas avoir de contraintes de latence

Probabilité de coupure

Canal supposé constant sur un bloc

- Equivalent à des contraintes de latence
- Modèle plus proche des systèmes pratiques

Probabilité de coupure

L'information mutuelle

$$I(\mathbf{H}) = \log_2 \det\left(\mathbf{Id} + \mathrm{RSB}\mathbf{H}\mathbf{H}^{\mathrm{H}}\right)$$

est vue comme une variable aléatoire.
Les blocs pour lesquels l'information mutuelle $I(\mathbf{H})$ est inférieure au rendement R du système sont dits en « coupure ».

$$P_{\text{out.}} = \Pr(I(\mathbf{H}) < R)$$

Remarque : la meilleure P_e est « équivalente » à $P_{\text{out.}}$

Remarque (I)

- Canal SISO
- Constellation MAQ à M états

Probabilité d'erreur

$$P_e = \frac{1}{2} - \frac{1}{2} \frac{1}{\sqrt{1 + \frac{4}{3} \frac{M-1}{\mathrm{RSB}}}}$$

A fort Rapport Signal-à-Bruit,

$$P_e = \frac{M-1}{3\mathrm{RSB}}$$

Remarque : A débit fixé, la diversité vaut $d = 1$

Remarque (II)

Remarque

- Lorsque le RSB augmente, la capacité de Shannon d'une communication SISO se comporte en $\log_2(\mathrm{RSB})$.
- Ainsi, on augmente la taille de la MAQ dans la même proportion, c'est-à-dire, $m = r \log_2(\mathrm{RSB})$ avec $m = \log_2(M)$.

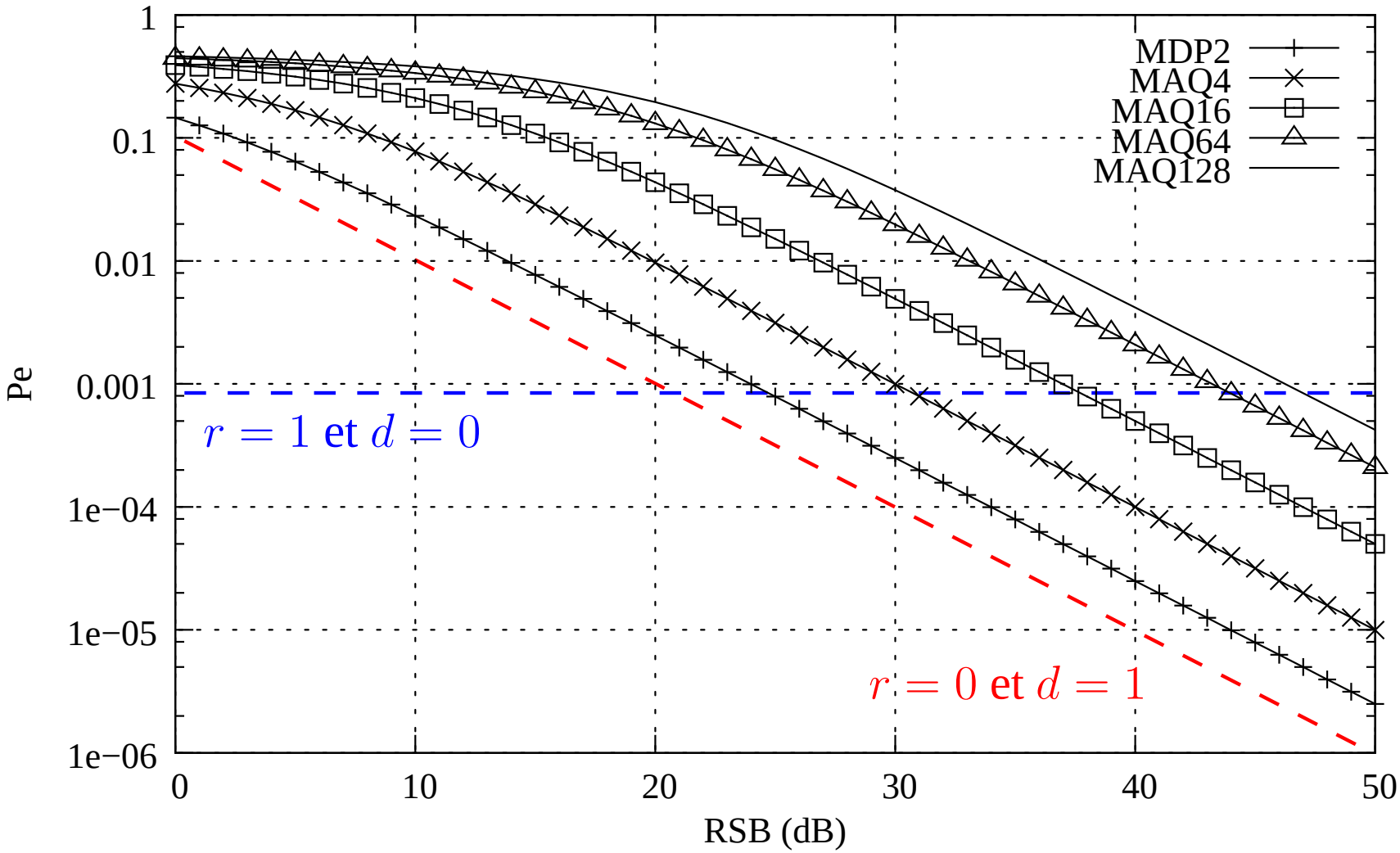
A fort Rapport Signal-à-Bruit,

$$P_e \propto \frac{1}{\mathrm{RSB}^{1-r}}$$

Résultat : la diversité vaut $d = 1 - r$

Compromis entre la fiabilité (d) et le débit (r)

Remarque (III)



Compromis

On définit une séquence de codes vérifiant

- *Gain de multiplexage :*

$$r = \lim_{\mathrm{RSB}\to\infty} \frac{R(\mathrm{RSB})}{\log_2(\mathrm{RSB})}$$

- *Diversité :*

$$d = -\lim_{\mathrm{RSB}\to\infty} \frac{\log P_e(\mathrm{RSB})}{\log(\mathrm{RSB})}$$

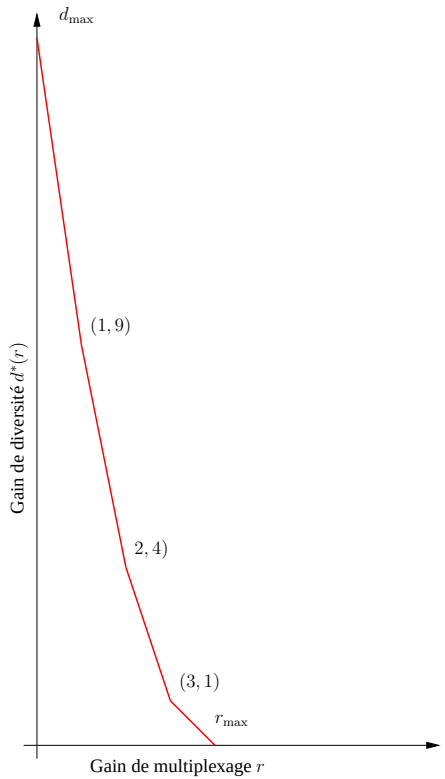
Théorème

On suppose $T \geq n_t + n_r - 1$. La courbe de compromis optimal $d^*(r)$ est une fonction linéaire par morceaux avec les points de rupture $d^*(k)$ pour $k = 0, 1, \cdots, \min(n_t, n_r)$ et où

$$d^*(k) = (n_t - k)(n_r - k)$$

Illustrations

Exemple : $n_t = n_r = 4$



$$d_{\max} = n_t n_r \quad \text{et} \quad r_{\max} = \min(n_t, n_r)$$

Construction des codes

Constat

Des codes admettant la même diversité maximale (débit fixe)

- ne gèrent pas nécessairement l'augmentation en débit de la même manière
- et donc n'admettent pas nécessairement le même gain de multiplexage

- Critères de rang et du déterminant : débit fixe
- « Critère » du compromis : débit variable

Critères de rang et du déterminant pas suffisant

Code d'Alamouti (I)

Considérons $n_t = 2$

- Si $T = 1$, il n'y a aucun gain de diversité d'émission
- Alors $T > 1$

$$\mathbf{X} = \begin{bmatrix} s_1 & s_2 \\ -\overline{s_2} & \overline{s_1} \end{bmatrix}$$

avec s_1 et s_2 deux symboles complexes

Décodage : exemple $n_r = 1$

Si

$$\begin{cases} r(1) &= \overline{h(1)}y(1) + h(2)\overline{y(2)} \\ r(2) &= -h(2)\overline{y(1)} + \overline{h(1)}y(2) \end{cases}$$

Alors

$$\begin{cases} r(1) &= (|h(1)|^2 + |h(2)|^2)s_1 \\ r(2) &= (|h(1)|^2 + |h(2)|^2)s_2 \end{cases}$$

Ce décodage est en fait optimal (car $\mathbf{X}\mathbf{X}^{\mathrm{H}} \propto \mathbf{Id}$).

Code d'Alamouti (II)

- linéaire en fonction des symboles
- rendement de 1 symbole par temps-symbole

$$d_{\text{Alamouti}}(r) = 2n_r(1-r)^+$$

- Diversité maximale : $2n_r$
- Rendement maximal : 1

Code d'Alamouti vérifie le compromis optimal ssi $n_r = 1$

Code V-BLAST

- $n_r \geq n_t$.
- Principe de multiplexage spatial

$$\mathbf{X} = \begin{bmatrix} s_1 & s_{n_t+1} & s_{2n_t+1} & \cdots \\ \vdots & & & \\ s_{n_t} & s_{2n_t} & s_{3n_t} & \cdots \end{bmatrix}$$

- linéaire en fonction des symboles
- rendement de n_t symboles par temps-symbole (plein)

$$d_{\mathrm{V-BLAST}}(r) = (2-r)^+, \quad \text{si} \quad (n_t = n_r = 2)$$

- Diversité $d_{\max}$ maximale : n_r
- Rendement $r_{\max}$ maximal : $n_t \quad (\leq n_r)$

Le code V-BLAST ne vérifie jamais le compromis optimal

Codes orthogonaux

- Codes tels que $\mathbf{X}\mathbf{X}^{\mathrm{H}} \propto \mathbf{Id}$
- Décodage ML possible par transformation linéaire
- Compromis « mauvais » (sauf Alamouti(1,2))

Résultats

- $n_t = 2$:
  - $n_r = 1$: optimal
  - $n_r > 1$: pas optimal
- $n_t > 2$:
  - rendement de 1 maximum
  - diversité maximale de $n_t n_r$

Code d'Or

Pour $n_t = n_r = 2$, on a

$$\mathbf{X} = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(s_1 + s_2\theta) & \alpha(s_3 + s_4\theta) \\ i\overline{\alpha}(s_3 + s_4\overline{\theta}) & \overline{\alpha}(s_1 + s_2\overline{\theta}) \end{bmatrix}$$

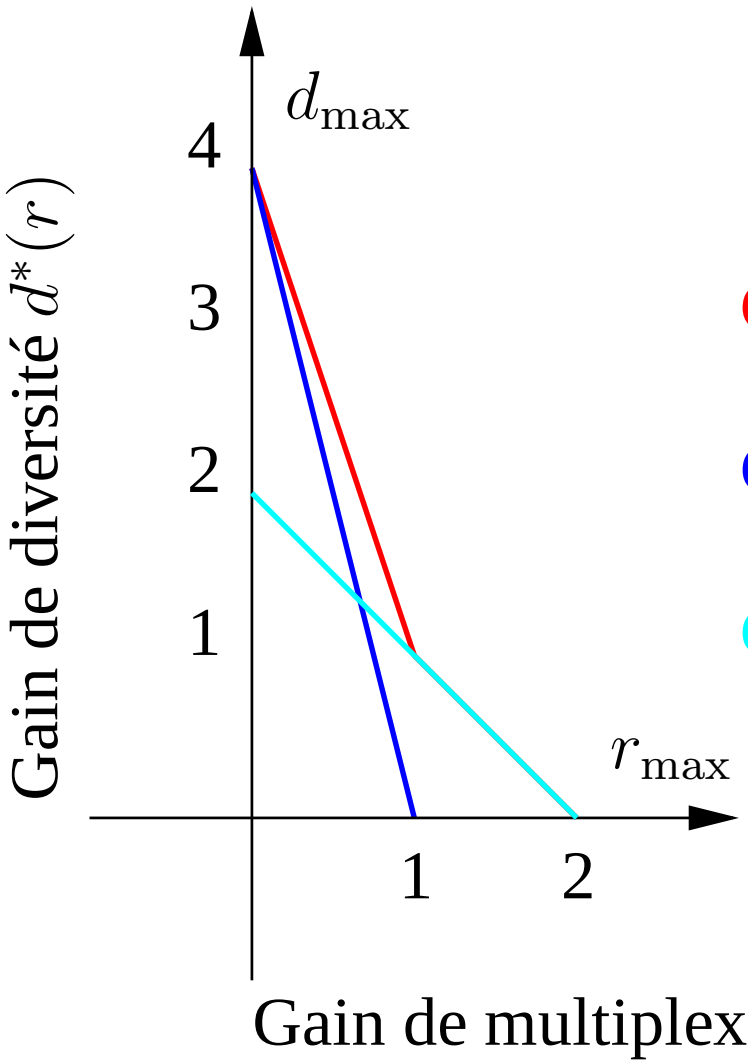
avec

- $\theta = (1 + \sqrt{5})/2$ et $\overline{\theta} = (1 - \sqrt{5})/2$
- $\alpha = 1 + i - i\theta$ et $\overline{\alpha} = 1 + i - i\overline{\theta}$

- Extension possible pour $n_t = 3, 4$ et 6 (codes parfait)
- Adaptable aux cas $n_r > n_t$
- Le code d'Or atteint le *compromis optimal*

Performances : compromis

Exemple : $n_t = 2, n_r = 2$



Compromis optimal + code d'Or

Code d'Alamouti

Code V-BLAST

Bibliographie

- *Théorie de l'information* :
  - L. Zheng, D. Tse, "Diversity ans Multiplexing : a fundamental trade-off in multiple antennas channels", *IEEE Trans. on Information Theory*, Mai 2003.
  - E. Biglieri, J. Proakis, S. Shamai, "Fading channels : information-theoretic and communications aspects", *IEEE Trans. on Information Theory*, Oct. 1998.
  - I. Telatar, "Capacity of multi-antenna Gaussian channels", *ETT*, Nov. 1999.
- *Construction de code* :
  - V. Tarokh, N. Shesadri, A. Calderbank, "Space-time codes for high data rate wireless communication : performance criterion ans code construction", *IEEE Trans. on Information Theory*, Mars 1998.
  - S. Alamouti, "Space-time block coding : a simple transmitter diversity technique for wireless communications, *IEEE JSAC*, Oct. 1998.
  - G. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multiple antennas", *Bell Labs Technical Journal*, 1996.
  - J.C Belfiore, G. Rekaya, E. Viterbo, "The Golden code : a 2×2 full rate space time code with non vanishing determinants", *IEEE Trans. on Information Theory*, Avril 2005.