

Étude des codes de Hamming sur les corps finis

Andreas Pauper

1 Introduction et définitions

Dans tout le TIPE, si l'on se place sur un corps de cardinal N (où N est la puissance d'un nombre premier), le terme code fera référence à une partie de N^k , où k est un entier considéré comme la taille du code. Les éléments du codes sont en théorie des codes associés à des éléments d'un ensemble plus petit de façon à s'assurer que des messages stockés ou transmis puissent être conservés malgré les erreurs qui peuvent être rencontrées.

Le code correspond alors également à l'injection entre l'ensemble des messages de taille α (c'est-à-dire K^α) et la partie aussi appelée code $C \subset K^\beta$.

Au sein de la famille plus large des codes correcteurs, on s'intéressera ici uniquement à des codes linéaires, c'est-à-dire des codes C qui sont des sous-espaces vectoriels de K^β et où les fonctions de codages peuvent donc êtres linéaires, ce qui simplifie les calculs. Plus exactement si l'on note ϕ l'injection permettant de coder les messages de l'ensemble de départ K^α (ou K est un corps de cardinal p^k) dans l'ensemble d'arrivée C , ϕ est un code linéaire si et seulement si pour tous messages \mathbf{m} et \mathbf{m}' dans K^α , pour tous scalaires λ et μ dans K on a

$$\phi(\lambda\mathbf{m} + \mu\mathbf{m}') = \lambda\phi(\mathbf{m}) + \mu\phi(\mathbf{m}')$$

Dire que le code est linéaire revient donc à dire que ϕ ainsi définie est K -linéaire. Nous utilisons ainsi dans le cadre des codes linéaires plusieurs fonctions qui sont linéaires. Ainsi si ϕ est une application linéaire de K^α dans un espace d'arrivée K^β , en représentant les mots \mathbf{m} au départ et à \mathbf{m} et \mathbf{m}' à l'arrivée par la matrice ligne des coordonnées dans les bases canoniques des deux espaces, on peut représenter ϕ par une matrice Φ dans $\mathcal{M}_{\alpha,\beta}(K)$ avec :

$$\mathbf{m}' = \mathbf{m} \cdot \Phi$$

Il existe de nombreux codes linéaires mais nous nous concentrerons ici sur les codes de Hamming, définis initialement sur le corps F_2 . Nous étudierons ici les codes définis sur F_{2^α} pour des raisons que nous évoquerons d'ici peu.

Distance de Hamming La distance de Hamming permet de mesurer les différences entre deux mots, dans le cas où le corps d'étude est F_2 , il s'agit du nombre de bits qui diffèrent. Si l'on se place sur K^α , la distance de Hamming d entre deux messages $\mathbf{m} = [m_1 \cdots m_\alpha]$ et $\mathbf{m}' = [m'_1 \cdots m'_\alpha]$ de K^α est définie comme suit :

$$d(\mathbf{m}, \mathbf{m}') = |\{1 \leq i \leq \alpha / m_i \neq m'_i\}|$$

Lié à la notion de distance est la notion de poids. Le mot « poids » sera employé à quelques reprises dans la suite du TIPE et correspond pour un mot \mathbf{m} à $d(\mathbf{m}, \mathbf{0})$ avec $\mathbf{0}$ le message nul de K^α .

Distance minimale Si $C \subset K^\alpha$ est un code, $d_{min} = \min_{\mathbf{m}, \mathbf{m}' \in C \setminus \{0\}} d(\mathbf{m}, \mathbf{m}')$ est appelé distance minimale du code C. Il nous intéresse dans la suite du TIPE car avoir une distance minimale de 3 revient à être 1-correcteur, c'est-à-dire pouvoir détecter et corriger une erreur.

Produit scalaire sur K^α Il est important pour la suite de définir un « produit scalaire » (il n'est pas défini) sur K^α , permettant entre autres de définir l'orthogonalité sur cet espace et de vérifier l'appartenance d'un mot \mathbf{m} de K^α au code $C \subset K^\alpha$. En notant $\mathbf{m} = [m_1 \cdots m_n]$ et $\mathbf{m}' = [m'_1 \cdots m'_n]$ deux messages de K^α , on a :

$$\langle \mathbf{m}, \mathbf{m}' \rangle = \sum_{i=1}^{\alpha} m_i m'_i$$

2 Choix de p

Il a été dit plus tôt qu'un corps fini a pour cardinal une puissance d'un nombre premier p . Cependant en pratique le nombre premier 2 est toujours choisi. Cet entier premier permet d'optimiser facilement l'espace mémoire occupé.

Démonstration. Attribuer une certaine quantité de mémoire pour représenter un élément du corps K de cardinal p^l revient à y attribuer un certains nombres de bits l' . Autrement dit, il serait souhaitable d'avoir $p^l = 2^{l'}$, c'est-à-dire qu'à chaque combinaison d'états de bits possible corresponde un unique élément de K . Alors $2|p^l$, ce qui n'est possible que si $p = 2$. \square

Nous nous placerons dans le cas où $p = 2$ dans toute la suite du TIPE.

3 Représentation des erreurs

Pour qu'il y ait détection et correction d'erreurs, il faut d'abord qu'erreurs il y ait. Pour cela il convient de déterminer la probabilité qu'un bit soit erroné. Deux modèles seront étudiés ici : un premier modèle permet de représenter les erreurs affectant chaque bit individuellement et un autre permet de modéliser

les cas de corruptions de plusieurs bits à la suite, les « bouffées d'erreurs », qui peuvent survenir par exemple lorsqu'on raye un CD. Nous considérons dans toute cette partie des messages de $l > 0$ bits.

Il est sous entendu dans les deux sous sections suivantes et dans la suite du TIPE que si 2^α est l'ensemble des messages de longueur α sur le corps F_2 , alors une suite d'erreurs sur un message est représenté de manière générale par une variable aléatoire de Ω à valeurs dans F_2^α , où Ω est un espace probabilisable. La présence d'un 1 à la i -ème composante d'une erreur représente une erreur au i -ème bit d'un message.

3.1 Premier modèle : erreurs indépendantes

Considérons $\mathbf{m} = [m_1 \cdots m_l] \in (F_2)^l$, dans ce modèle les lettres m_i sont indépendantes deux à deux et pour $1 \leq i \leq l$, m_i suit une loi de Bernoulli de paramètre $0 < \rho < 1/2$.

En effet certains cas sont inutiles à considérer. Le cas $\rho = 0$ n'est pas intéressant car il n'y aurait dans ce cas pas d'erreurs à corriger, le cas $\rho > 1/2$ est peu probable et pourrait se déduire en inversant tous les bits en plus de l'utilisation de codes de Hamming. Dans le cas où $\rho = 1/2$ il devient tout bonnement impossible de corriger les erreurs.

En notant X le nombre de bits erronés sur un message de taille l , X suit donc une loi binômiale de paramètres ρ et l .

Ce modèle est intéressant en première approximation pour traiter le cas d'un bruit uniformément réparti, mais ne rend pas compte de phénomènes de « bouffées d'erreurs », qui peuvent corrompre un ensemble de bits qui se suivent.

3.2 Modélisation des bouffées d'erreurs

Une illustration simple de ce type d'erreur est le CD rayé. Lorsque l'on raie un CD, plutôt que de corrompre quelques bits épars sur toute la surface du CD, un certain nombre de bits sont corrompus à la suite. D'une certaine façon l'on pourrait donc dire que le fait qu'un bit soit erroné renforce la probabilité que le bit suivant le soit également.

J'ai donc choisi de modéliser ce type d'erreurs par une chaîne de Markov avec deux états « E » et « C », pour erroné et correct, avec une probabilité ρ_1 d'avoir un bit correct lorsque le bit précédent l'est, et une probabilité ρ_2 d'avoir un bit erroné lorsque le bit précédent est erroné.

Encore une fois, pour garder un modèle cohérent avec la réalité, choisissons $1/2 < \rho_1 < 1$ et $1/2 < \rho_2 < 1$. Admettons aussi que l'état de départ de la chaîne soit correct, afin d'éviter d'ajouter une loi supplémentaire sur le premier bit.

Dans ce cas en considérant un message de taille l et en notant pour $1 \leq i \leq l$, X_i l'événement *le i -ème bit du message est erroné*, la loi des probabilités totales donne :

$$\forall i \in \{1, \dots, l-1\}, P(X_{i+1}) = \rho_2 P(X_i) + (1 - \rho_1) P(\overline{X_i})$$

Soit encore

$$P(X_{i+1}) = (\rho_2 + \rho_1 - 1)P(X_i) + 1 - \rho_1$$

Cela nous donne pour $1 \leq i \leq l$, $P(X_i) = (1 - \rho_1)^{\frac{1 - (\rho_1 + \rho_2 - 1)^i}{2 - \rho_1 - \rho_2}}$ avec la condition initiale. Encore une fois, on veut un modèle pour lequel il est plus probable d'avoir un bit correct qu'un bit erroné, pour cela il suffit que $\rho_2 < \rho_1$.

4 Construction et représentation de K

Si p est premier il est évident d'après le petit théorème de Fermat que $\mathbb{Z}/p\mathbb{Z}$ est un corps, cherchons maintenant à construire un corps de cardinal p^α avec α naturel non nul. Même si nous notons occasionnellement ici le corps F_{p^α} il faut prendre garde au fait que ce corps n'est pas unique à isomorphisme près. Une fois le corps construit nous nous permettrons tout de même de le noter ainsi sans ambiguïté.

Une approche simple de construction d'un tel corps consiste à utiliser un polynôme P irréductible de degré α et de prendre $F_{p^\alpha} = F_p/(P)$ une extension de corps de F_p de cardinal p^n .

Il est démontré dans *Algèbre* de Demazure que pour tout entier non nul α l'on peut trouver un polynôme irréductible de F_p . C'est sur cela que nous nous appuierons pour construire en particulier des corps de taille 2^α . Notons dans la suite de cette partie $F_2[X]/(P)$ l'ensemble quotient formé des classes d'équivalences de polynômes de $F_2[X]$ modulo le polynôme P .

Proposition Si P est un polynôme de $F_2[X]$ et de degré α non nul, $F_2[X]/(P)$ est un corps si et seulement si P est irréductible dans $F_2[X]$.

Démonstration. Le fait que $F_2[X]/(P)$ soit un anneau est immédiat et indépendant du fait que P soit ou non irréductible.

Si P n'est pas irréductible, il existe deux polynômes A et B tous deux de degrés inférieur à α tels que $AB = P$. Or dans $F_2[X]/P$, cela revient à dire que $AB = 0$, A et B étant tous deux non nuls cela implique que $F_2[X]/(P)$ n'est pas un corps.

Si P est irréductible, prenons A un élément de $F_2[X]/(P)$ non nul. En identifiant encore une fois le polynôme et sa classe d'équivalence, on peut affirmer que A et B sont premiers entre eux (A est de degré strictement inférieur à n).

Le théorème de Bézout nous permet de trouver deux polynômes U et V dans $F_2[X]/(P)$ tels que $AU + BV = 1$. $F_2[X]/(P)$ est donc un corps. \square

En choisissant P un polynôme irréductible de degré α nous noterons $F_{2^\alpha} = F_2[X]/(P)$. La forme précise du corps choisi n'a donc pas d'importance pour la suite.

Sur un ordinateur nous considérerons qu'utiliser des éléments du corps F_{2^α} revient à regrouper les bits par groupe de α bits.

5 Construction des matrices génératrices et vérificatrices

5.1 Lien entre matrice génératrice et vérificatrices

Si Φ est une matrice vérificatrice d'un code C de paramètres $(2^\alpha; n, k, 3)$ sous la forme :

$$G = \begin{bmatrix} B \\ I_{n-k} \end{bmatrix}$$

alors la matrice génératrice du code (à opérations sur les lignes prêt) est de la forme :

$$\Phi = [I_k \quad -B]$$

Michel DEMAZURE donne dans son livre *Algèbre* aux éditions Cassini une méthode de construction par récurrence des matrices vérificatrices des codes de Hamming. La sous-section suivante traite une généralisation de cette méthode pour tout corps de taille 2^α

5.2 Construction de H_r par récurrence

Posons $N = 2^\alpha$, où $\alpha > 0$, et notons pour $r \geq 2$ H_r le code de Hamming de paramètres $(N; n_r = \frac{N^r-1}{N-1}, k_r = \frac{N^r-1}{N-1} - r, 3)$ Nous considérons dans cette partie que les polynômes du corps F_N tel que construit précédemment sont représentés par simplicité dans cette partie par des entiers, ce qui ne crée pas d'ambiguïté ici. Si $b_{\alpha-1}X^{\alpha-1} + b_{\alpha-2}X^{\alpha-2} + \dots + b_1X + b_0$ est un élément de F_N , il est représenté ici par $n = \sum_{i=0}^{\alpha-1} b_i 2^i \in \{0, \dots, N-1\}$.

Posons :

$$\Phi_2 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \\ \vdots & \vdots \\ N-1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Et pour $r \geq 2$:

$$\Phi_{r+1} = \begin{bmatrix} \mathbf{1} & \Phi_r \\ \mathbf{2} & \Phi_r \\ \vdots & \vdots \\ \mathbf{N-1} & \Phi_r \\ 1 & \mathbf{0} \\ \mathbf{0} & \Phi_r \end{bmatrix}$$

Démontrons par récurrence sur $r \geq 2$ que le noyau de Φ_r définit un code H_r .

Démonstration. **Cas $r = 2$:** la matrice de Φ_2 a $N + 1 = \frac{N^2-1}{N-1}$ lignes, donc $\text{Ker } \Phi_2 \subset F_N^{n_2}$. De plus il est apparent que $\text{rg } \Phi_2 = 2$, ainsi d'après le théorème du rang, $\dim \text{Ker } \Phi_2 = N - 1 = k_2$.

Si $\mathbf{m} = [m_1 \cdots m_{n_2}] \in \text{Ker } \Phi_2$, supposons que $d(\mathbf{m}, \mathbf{0}) \leq 2$. Si $d(\mathbf{m}, \mathbf{0}) = 1$ comme $m_1 + m_2 + \cdots + m_{N-1} + m_{N+1} = 0$, on a $m_N \neq 0$ et pour $i \neq N$, $m_i = 0$. D'autre part, $m_N = 0$, ce qui est absurde. Si $d(\mathbf{m}, \mathbf{0}) = 2$, il existe $i \neq N$ et $j \neq N$ tels que $i \neq j$ et $m_i \neq 0$ et $m_j \neq 0$ et $m_i + m_j = 0$. D'autre part $im_i = jm_j$ donc $-m_j/m_i = i/j = 1$ ce qui est impossible car $i \neq j$. Il vient que soit $\mathbf{m} = \mathbf{0}$ soit $d(\mathbf{m}, \mathbf{0}) \geq 3$. De plus $\mathbf{m} = [1 \ 0 \ \cdots \ 0 \ 1 \ 1] \in \text{Ker } \Phi_2$ et est de poids 3, la distance minimale est donc de 3. H_2 peut donc être défini comme le noyau de Φ_2 .

Cas $r > 2$: Supposons que H_{r-1} peut être défini comme étant le noyau de Φ_{r-1} . Alors la définition de Φ_r donne que le nombre de lignes de Φ_r est $Nn_{r-1} + 1$ par hypothèse de récurrence. Il s'agit bien de n_r . On a :

$$\text{rg } \Phi_r = \text{rg} \begin{bmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \Phi_{r-1} \end{bmatrix}$$

Donc $\text{rg } \Phi_r = \text{rg } \Phi_{r-1} + 1 = r$, et par théorème du rang $\dim \text{Ker } \Phi_r = n_r - r = k_r$.

Enfin si $\mathbf{m} \in \text{Ker } \Phi_r$, posons $\mathbf{m}_1, \dots, \mathbf{m}_N \in F_N^{n_{r-1}}$ et $a \in F_N$ tels que $\mathbf{m} = [\mathbf{m}_1 \ \cdots \ \mathbf{m}_{N-1} \ a \ \mathbf{m}_N]$, alors par définition de Φ_r on a :

$$\mathbf{m}_1 \cdot \Phi_{r-1} + \cdots + \mathbf{m}_N \cdot \Phi_{r-1} = \mathbf{0} \quad (1)$$

$$\langle \mathbf{m}_1, \mathbf{1} \rangle + \cdots + \langle \mathbf{m}_{N-1}, \mathbf{N-1} \rangle + a = 0 \quad (2)$$

Supposons que \mathbf{m} est non nul et que $d(\mathbf{m}, \mathbf{0}) \leq 2$. Si $d(\mathbf{m}, \mathbf{0}) = 1$, soit un seul des \mathbf{m}_i est non nul ce qui contredit (1) comme H_{r-1} est de distance minimale 3 par hypothèse de récurrence, soit $a \neq 0$ et les \mathbf{m}_i sont tous nuls ce qui contredit (2).

Si $d(\mathbf{m}, \mathbf{0}) = 2$, soit un seul des \mathbf{m}_i est non nul, avec $d(\mathbf{m}_i, \mathbf{0}) = 2$, ce même cas contredit (1) pour la même raison évoquée ci-dessus. Si un des \mathbf{m}_i est non nul et $a \neq 0$, cela contredit toujours (1). Sinon il existe $i \neq j$ tels que \mathbf{m}_i et \mathbf{m}_j sont tous deux non nuls, avec $d(\mathbf{m}_i, \mathbf{0}) = 1$ et $d(\mathbf{m}_j, \mathbf{0}) = 1$. D'après (1) $\mathbf{m}_i + \mathbf{m}_j \in \text{Ker } \Phi_{r-1}$, comme leur poids est plus petit que 2 il est nécessairement nul.

Donc $\mathbf{m}_i = \mathbf{m}_j$ ce qui d'après (2) est absurde.

Par hypothèse de récurrence, il existe un mot $\mathbf{m}_{r-1} \in H_{r-1}$ de poids 3. Alors en posant $\mathbf{m} = [\mathbf{0} \ \mathbf{m}_{r-1}] \in F_N^{n_r}$ est un élément de $\text{Ker } \Phi_r$ de poids 3.

Donc la distance minimale est de 3 et l'on peut définir H_r comme le noyau de P_r . \square

6 Intérêts

6.1 Modèle des erreurs isolées

Considérons d'abord le cas où les erreurs sont représentées comme indépendantes les unes des autres et suivant chacune une loi de Bernoulli de probabilité $0 < \rho < 1/2$. Commençons par étudier le choix de la taille du corps sur le *taux de transmission* du code correcteur, c'est-à-dire pour un code de paramètres (n, k, d) le rapport k/n qui correspond à l'information utile sur l'information stockée.

Choisissons $\alpha > 0$ et $\beta > 0$ tels que $\alpha < \beta$ deux entiers, et notons pour $r \geq 2$ entier H_r^α et H_r^β définis comme H_r en 5.2 dans le cas où $N = 2^\alpha$ et $N = 2^\beta$. Notons alors $R^{(\alpha)} = k_r^{(\alpha)} / n_r^{(\alpha)}$ et $R^{(\beta)} = k_r^{(\beta)} / n_r^{(\beta)}$. Alors pour $r \geq 2$:

$$\forall k \in \{0, \dots, r-1\}, 2^{\alpha k} < 2^{\beta k}$$

Donc $\frac{2^{\alpha r}-1}{2^\alpha-1} < \frac{2^{\beta r}-1}{2^\beta-1}$.
Or :

$$\begin{aligned} R^{(\alpha)} &= \frac{\frac{2^{\alpha r}-1}{2^\alpha-1} - r}{\frac{2^{\alpha r}-1}{2^\alpha-1}} \\ &= 1 - r \frac{2^\alpha - 1}{2^{\alpha r} - 1} \end{aligned}$$

Et $R^{(\beta)} = 1 - r \frac{2^\beta - 1}{2^{\beta r} - 1}$

Donc $R^{(\alpha)} < R^{(\beta)}$, autrement dit pour corriger autant d'erreurs l'espace accordé à la redondance sera proportionnellement plus petit pour des corps de cardinal plus grand. En terme de stockage utiliser un corps caractéristique de taille plus grande est donc plus avantageux.

Comparons maintenant l'efficacité des deux codes pour corriger un certain nombre d'erreurs. Considérons alors N la variable aléatoire réelle qui compte le nombre d'erreurs sur un message de $F_2^{\alpha n_r}$, qui pour les calculs de correction est considéré comme un message de $F_2^{n_r}$. Soit alors $k \geq 0$ un entier. Notons χ l'événement « l'erreur (si elle existe) est détectée et corrigée ».

Le code H_r^α est 1-correcteur sur le corps F_{2^α} , donc il ne peut corriger qu'au plus α erreurs dans le cas où elles se situent dans le même « paquet » permettant de coder un élément de F_{2^α} , comme illustrer ci-dessous.

0		X + 1		0		0		0	
0	0	1	1	0	0	0	0	0	0

Exemple pour H_2^2 d'une erreur qui peut être corrigée. (une seule erreur dans F_4)

0		1		X		0		0	
0	0	0	1	1	0	0	0	0	0

Exemple pour H_2^2 d'une erreur qui ne peut pas être corrigée. (deux erreurs dans F_4)

Alors si $k > \alpha$, $P(\chi|N = k) = 0$ et si $0 < k \leq \alpha$, par dénombrement :

$$P(\chi|N = k) = \frac{n_r \binom{\alpha}{k}}{\binom{n_r \alpha}{k}}$$

Et si $k = 0$:

$$P(\chi|N = 0) = 1$$

N suivant une binomiale de paramètres $(n_r \alpha, \rho)$ il vient d'après la loi des probabilités totales :

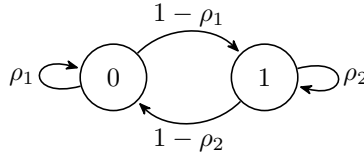
$$\begin{aligned} P(\chi) &= \sum_{k=0}^{n_r \alpha} P(\chi|N = k) P(N = k) \\ &= \sum_{k=1}^{n_r \alpha} n_r \binom{\alpha}{k} \rho^k (1 - \rho)^{n_r \alpha - k} + (1 - \rho)^{n_r \alpha} \\ &= n_r (1 - \rho)^{(n_r - 1) \alpha} + (1 - n_r) (1 - \rho)^{n_r \alpha} \end{aligned}$$

Asymptotiquement, $\lim_{\alpha \rightarrow +\infty} P(\chi) = 0$. Si l'on prend $r = 2$ on constate pour les premiers termes que $P(\chi)$ décroît. Dans ce modèle l'utilisation de corps de cardinal plus grand tend à rendre la correction un peu moins précise dans ce modèle d'erreurs.

6.2 Les bouffées d'erreurs

Reprenons les notations de la partie précédente, et notons \mathbf{E} une suite d'erreurs dans $F_2^{n_r \alpha}$. Comme dans la partie précédente $P(\chi|N = 0) = 1$.

Construire une suite d'erreur revient à parcourir le graphe de la chaîne de Markov suivant, en partant de l'état 0 qui correspond à un bit correct :



Notons A_i pour $1 \leq i \leq n_r$ l'événement « l'erreur formée $\mathbf{E} = [E_1 \cdots E_{\alpha n_r}]$ est de la forme $E_l = 0$ si $l \notin \{(i - 1)\alpha + 1, \dots, i\alpha\}$ et E_l est quelconque sinon ». Autrement dit toutes les erreurs sont regroupées dans un paquet de α termes.

Alors :

$$P(\chi) = P\left(\bigcup_{i=1}^{n_r} A_i\right)$$

Et :

$$\begin{aligned} P(A_i) &= \rho_1^{\alpha(i-1)} P(\overline{X_{\alpha+1}}) \rho_1^{(n_r-i)\alpha-1} \\ &= \rho_1^{(n_r-1)\alpha-1} \left[1 - (1 - \rho_1)^{\frac{1-(\rho_1+\rho_2-1)^{\alpha+1}}{2-\rho_1-\rho_2}}\right] \\ &= \rho_1^{(n_r-1)\alpha-1} \frac{1-\rho_2+(1-\rho_1)(\rho_1+\rho_2-1)^{\alpha+1}}{2-\rho_1-\rho_2} \end{aligned}$$

Comme $A_i \cap A_j = \{E = [0 \cdots 0]\}$ pour $i \neq j$, alors

$$\begin{aligned} P(\chi) &= \sum_{i=1}^{n_r} P(A_i) - (n_r - 1)P(\mathbf{E} = [0 \cdots 0]) \\ &= n_r \rho_1^{(n_r-1)\alpha-1} \frac{1-\rho_2+(1-\rho_1)(\rho_1+\rho_2-1)^{\alpha+1}}{2-\rho_1-\rho_2} - (n_r - 1)\rho_1^{\alpha n_r} \end{aligned}$$

Comme pour le premier modèle $P(\chi)$ décroît selon α , mais en pratique dans les calculs l'on peut trouver avec des corps de cardinal plus grand des valeurs de r pour lesquelles l'on peut obtenir des valeurs de $P(\chi)$ et des taux de transmission plus grands. En prenant $\rho_1 = 0.999$ et $\rho_2 = 0.6$, par exemple, on a pour $\alpha = 1$ et $r = 8$, $P(\chi) \approx 0.854034$, $R^{(1)} \approx 0.968627$, alors que pour $\alpha = 6$ et $r = 2$ l'on a $P(\chi) \approx 0.878731$, $R^{(8)} \approx 0.969231$. Il peut donc être intéressant même dans le cas des codes de Hamming de considéré des corps finis différents de F_2 , et au-delà des codes de Hamming c'est déjà le cas avec par exemple le corps F_{256} et les codes de Reed-Solomon sur les CD.