DIXIEME COLLOQUE SUR LE TRAITEMENT DU
SIGNAL ET SES APPLICATIONS

NICE du 20 au 24 MAI 1985

LES PERFORMANCES DES CODES DE REED-SOLOMON SUR UN CANAL DISCRET SANS MEMOIRE

Francisco J. GARCIA-UGALDE
Docteur Ingénieur, Ingénieur E.S.E.

División de Estudios de Posgrado, Facultad de Ingeniería, Universidad Nacional Autónoma de México
C. Universitaria, P. O. Box 70-256, C.P. 04510 México, D.F.

RESUME

Pour contrôler les erreurs de transmission dans les systèmes de communication de données, on peut utiliser un code linéaire à bloques, essentiellement de deux manières différentes, à savoir: pour effectuer la correction des erreurs qui détecte, localise et corrige les erreurs. Cette technique est connue comme la Correction Directe des Erreurs (FEC, de l'anglais: "forward-error correction"). La deuxième technique s'utilise uniquement pour détecter les erreurs. Dans les canaux où il est possible une retransmission, le fait d'introduire la détection avec un Repeteur Automatique sur Demande (ARQ: "automatic repeat request"), permet d'obtenir dans l'idéal une transmission de données dépourvues d'erreurs.

Dans cette communication on présente les résultats qui montrent les propriétés des quelques codes de Reed-Solomon (RS), lorsqu'ils sont utilisés pour la correction et pour la détection des erreurs sur un canal discret sans memoire (DMC: "discrete memoryless channel"). On donne les expressions qui permetent le calcul des probabilités des événements qui peuvent se présenter après le décodage. Parmi ces événements, celui qui correspond au cas où le décodeur décode incorrectement avec une probabilité P_{DIC}, permet le calcul du taux d'erreurs résiduel par symbole ε', ensuite celui-là permet de mesurer le gain apporté par le code sur le rapport signal sur bruit. Cette probabilité permet aussi de calculer la distribution d'erreurs après le décodage, c'est-à-dire la probabilité d'avoir plus de Γ erreurs après le decodage ($P(\Gamma)$).

Lorsqu'on utilise les codes RS pour la détection d'erreurs, on peut dénombrer les cas où le décodeur n'est plus capable de détecter les erreurs présentes dans le mot reçu à partir de la probabilité de non-détection, cette quantité permet d'effectuer une comparaison entre différents codes RS lorsqu'on fait varier leurs paramètres (n,k,q).

SUMMARY

To control transmission errors in data communication systems, a linear block code can be bassically used in two different ways. These are: to correct errors, a linear block code can be used to detect, locate and correct errors. This method is known as forward-error correction (FEC). The second method can use a linear block code to detect errors only. In channels where a retransmission is possible; when errors are detected the system requests restransmission. This method is known as automatic-repeat request (ARQ), and it permits an ideal error free data transmission.

In this correspondance we present some results that show some properties of Reed-Solomon codes (RS), when they are used to correct errors and to detect errors, on a discrete memoryless channel (DMC). Expressions to calculate post-decoding error events for non-binary block codes are presented too. Among these events, the one that corresponds to decoding incorrectly with a probability P_{DIC} permits to calculate the post-decoder character error rate ε' and the distribution of post-decoder errors, that is the probability $P(\Gamma)$ of more than Γ post-decoder errors. The post-decoder character error rate permits to measure the code gain on the signal to noise ratio.

For linear block codes for error detection the probability of undetected errors (P_{ND}) for and (n,k, q) code is considered, and it permits to compare several RS codes.

LES PERFORMANCES DES CODES DE REED-SOLOMON SUR UN CANAL DISCRET SANS MEMOIRE

Francisco J. GARCIA-UGALDE
Docteur Ingénieur, Ingénieur E.S.E.

I. INTRODUCTION

Cet étude est basée sur l'analyse de différents événements qui peuvent se présenter après le décodage, lorsqu'on utilise les codes de Reed-Solomon pour diminuer le taux d'erreurs par symbole, sur un canal de communications. On a regroupé le cas où on utilise ces codes en tant que codes correcteurs d'erreurs, avec le cas où on les utilise comme codes détecteurs d'erreurs.

Dans le cas de la correction d'erreurs, quatre paramètres de comparaison ont été selectionés pour être considérés les plus représentatifs des différents événements issus de la décodification, ces paramètres sont: la probabilité de décodage correct (P_{DC}), qui est une quantité facile à calculer pour les codes de RS qui ont un schéma de décodage où la capacité est bornée par la distance du code, et quand le modèle de probabilité qu'on utilise pour décrire le phénomène aléatoire associé au procès de transmission est basé sur les propriétés d'un canal discret sans mémoire (DMC: "discrete memoryless channel"), avec q entrées et q sorties [1]. Le deuxième paramètre de comparaison est la probabilité de décodage incorrect (P_{DIC}), et les deux autres, qui s'obtiennent à partir de cette dernière, sont le taux d'erreurs résiduel par symbole (ε') et la probabilité d'avoir plus de Γ erreurs après le décodage ($P(\Gamma)$).

Parmi ces paramètres, le taux d'erreurs résiduel par symbole, c'est-à-dire, le taux d'erreurs par symbole après le décodage est un paramètre très important dans des applications où par des critères quantitatifs ou qualitatifs, il a été possible d'établir une borne supérieure à ne pas dépasser. Dans ce sens on peut mesurer le gain apporté par le code.

Dans le cas de la détection d'erreurs le paramètre de comparaison qu'on utilise traditionnellement, est la probabilité que le décodeur échoue dans la détection des erreurs présentes dans le mot reçu, cette probabilité est connue comme la probabilité d'erreurs non détectées (P_{ND}). Elle a été calculée pour le même modèle de canal utilisé dans le cas de la correction d'erreurs.

II. GENERALITES

Un code linéaire des paramètres (n,k,q) qui utilise les symboles d'un corps fini à q élément, CG(q), est connu sous le nom de code de Reed-Solomon de longueur de bloque n=q-1, et de distance minimale au sens de Hamming d=n-k+1, où k est le nombre de symboles d'information [1], [2]. Le codeur traite l'information d'une manière discontinue par bloques de k symboles, auquels on associe n-k symboles redondants. Ces symboles redondants permetent au décodeur, lorsqu'il est utilisé comme correcteur, de détecter, localiser et corriger les erreurs. Lorsqu'il, est utilisé comme détecteur, ces mêmes symboles permetent d'effectuer la détection. Les règles qui permetent au codeur de calculer les symboles redondants à partir de symboles d'information, sont l'ensemble de relations linéaires contenues dans la matrice génératrice du code, G[kxn]. Ces relations sont aussi contenues dans le polynôme générateur du code g(x).

Les lignes de la matrice G étant les vecteurs de base d'un sous-espace vectoriel linéaire de $R^{(n)}$, C, de dimension k. Il existe une matrice H[(n-k)xn] où les lignes sont les vecteurs de base d'un sous-espace vectoriel linéaire de $R^{(n)}$, $C^{\perp}$, de dimension n-k, qui est orthogonal au premier [1], [2], [3]. Ainsi le produit,

$$G \cdot H^T = H \cdot G^T = 0 \qquad (1)$$

La matrice H, génératrice du code $C^{\perp}$ (dual de C) est appelée matrice de vérification de parité ou matrice de contrôle de C.

Et puisque tout mot du code est une combinaison linéaire des lignes de G, il est orthogonal à toutes les lignes de H, c'est-à-dire:

$$c \in C \iff c \cdot H^T = 0 \qquad (2)$$

On appelle syndrôme de x le produit:

$$S(x) = x \cdot H^T \quad ; \quad \forall\, x \in R^{(n)} \qquad (3)$$

Alors $x \in C$ si et seulement si $S(x) = 0$. Si $x = c + e$ avec $c \in C$:

$$S(x) = x \cdot H^T = e \cdot H^T \qquad (4)$$

Le syndrôme dépend donc uniquement de l'erreur e.

De plus, un code dont la distance minimale atteint la borne n-k+1 est appelé code avec Distance Maximale de Séparation (MDS: "maximum-distance-separable"). Utilisé comme code correcteur, un tel code est susceptible de corriger t erreurs, où $t \leq \left[\frac{d-1}{2}\right]$, le symbole [x] représente la partie entière de x. A la fois, utilisé comme code détecteur, il permet la détection, au plus, de d-1 erreurs. Du point de vue du fonctionement du décodeur le choix entre code correcteur ou code détecteur est basé sur l'algorithme sélectioné.

Les codes de RS (ou raccourcis de RS) s'utilisent largement pour le contrôle des erreurs dans les systèmes de communication et stockage de données. On peut les utiliser soit pour la correction des symboles d'erreurs aléatoires, ou pour la correction de paquets d'erreurs multiples, ou encore pour la correction d'un paquet d'erreurs unique dans le bloque codé. Dans le cadre de cette communication, on analyse leurs performances vis-à-vis des symboles d'erreurs aléatories. Il faut souligner aussi que par le fait d'être des codes MDS, ils gardent toutes leurs caractéristiques après le raccourcissement, c'est-à-dire qu'un code raccourci de RS est aussi un code MDS [1].

III. PRESENTATION DU PROBLEME

Le modèle associé au canal est basé sur l'hypothèse d'indépendance entre symboles, où la probabilité qu'un symbole soit reçu correctement est $1-\varepsilon$, et en considérant que lorsqu'un symbole est affecté par le bruit, ce symbole peut se transformé en un des q-1 symboles restants de l'alphabet, avec une probabilité $\frac{\varepsilon}{q-1}$. Ce modèle d'erreurs est représenté par la figure suivante:

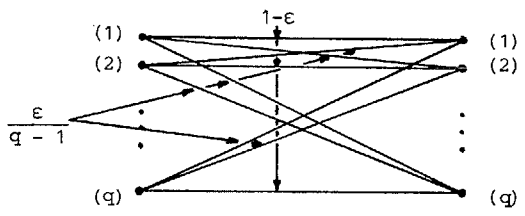

Fig. 1. Canal discret sans mémoire, DMC, avec q entrées et q sorties.

Ainsi puisque les erreurs à l'entrée du décodeur ont une loi binomiale, la probabilité de décodage correct, sachant que le code est capable de corriger t erreurs, est donnée par:

$$P_{DC} = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \left(\frac{\varepsilon}{q-1}\right)^i (1-\varepsilon)^{n-i} =$$

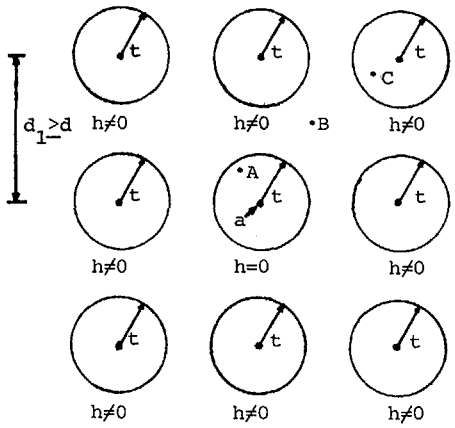

Fig. 2. Représentation schématique d'un décodage incorrect.
a. Mot transmis, A. mot reçu qui donne un décodage correct, B. mot reçu qui donne un décodage impossible, C. mot reçu qui donne un décodage incorrect.

$$P_{DC} = \sum_{i=0}^{t} \binom{n}{i} \varepsilon^i (1-\varepsilon)^{n-i}, \quad 0 \leq \varepsilon \leq 1 \tag{5}$$

Cependant lorsque le nombre d'erreurs dépasse la capacité de correction du code (t), deux situations peuvent se présenter: le décodeur décode incorrectement avec une probabilité P_{DIC} [3], [4], ce qui donne comme résultat un patron d'erreurs après le décodage. Ou alors le décodeur reconnaît une situation anormale lors de différentes étapes de l'algorithme de décodage, manifestant dans ce cas la présence d'une erreur détectée mais impossible de corriger, avec une probabilité P_D. On a en effet:

$$P_{DC} + P_{DIC} + P_D = 1 \tag{6}$$

Le problème du calcul de P_{DIC} consiste à pouvoir, dénombrer toutes les situations qui peuvent contribuer à un décodage incorrect. Le taux d'erreurs résiduel par symbole ε', ainsi que la distribution d'erreurs après le décodage $P(\Gamma)$, se calculent à partir de P_{DIC}.

Dans les canaux où il est possible une retransmission, on peut utiliser les codes linéaires comme détecteurs d'erreurs. L'algorithme de détection consiste à calculer côté recepteur, les symboles redondants, de la même manière que l'a fait le codeur, et de les comparer avec les symboles redondants reçus. Lorsqu'ils sont différents, le décodeur a détecté des erreurs. Lorsqu'ils son égaux deux cas peuvent se présenter: soit qu'il n'y a pas d'erreurs, soit que les erreurs se sont présentées d'une telle manière qu'il est impossible de les détecter. Il est intéressant de pouvoir mesurer la probabilité qu'un décodage donné soit dans ce dernier cas, cette probabilité est appelé probabilité de non-détection P_{ND} [5]. Pour la calculer exactement, on utilise le modèle de canal de transmission décrit au début du paragraphe. Et le problème du calcul est aussi un problème de dénombrement, qui se simplifie lorsqu'on travaille avec des codes où la distribution des poids des mots est connue. C'est le cas des codes de Reed-Solomon.

IV. CALCUL DE LA PROBABILITE DE DECODAGE INCORRECT.

Le calcul de P_{DIC} s'effectue en considérant les propriétés linéaires des codes de RS, en supposant qu'on transmet le mot de poids zéro, au sens de Hamming sur un canal DMC [1].

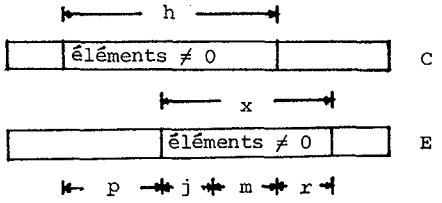

Fig. 3. Représentation schématique du mot de code C et du patron d'erreurs E.

Dans ce cas on a le mot de code $C=(C_o,C_1,C_2,\ldots,C_{n-1})$, où $C_i=0$, $i \in [0, n-1]$. Un patron d'erreurs de poids x, $E=(E_o,E_1,E_2,\ldots,E_{n-1})$, donne un décodage incorrect, si lorsqu'il passe par le décodeur, celui-ci l'identifie comme un mot de code de poids différent de zéro. Ceci est possible lorsque le patron d'erreurs se trouve à una distance $\ell \leq t$, d'un mot de code de poids h, $h \neq 0$. Par le principe de fonctionnement du décodeur qui est basé sur un critère maximum de vraisemblance, le patron d'erreurs est décodé précisément comme ce mot de poids h, situé dans le centre d'une sphère de rayon t dans un espace à n dimensions. En conséquence le poids du patron d'erreurs après le décodage est aussi h. La figure 2 schématise un décodage incorrect.

Si on définit $P_{DIC}(h)$ comme la probabilité d'un décodage incorrect [4] lorsque le patron d'erreurs est décodé comme le mot de code de poids h, la probabilité totale de décodage incorrect est donnée par:

$$P_{DIC} = \sum_{h=d}^{n} P_{DIC}(h) \tag{7}$$

Pour calculer $P_{DIC}(h)$ il faut pouvoir calculer le nombre de patrons d'erreurs de poids x situés à une distance $\ell \leq t$ d'un mot de code de poids h, ce nombre noté par la lettre $n(h,x,\ell)$, sera différent de zéro pour $h-\ell \leq x \leq h+\ell$. Et les patrons d'erreurs seront décodés comme le mot de poids h.

Le nombre $n(h,x,\ell)$ sera calculé en considérant le mot de code C de poids h avec C_i éléments, $i \in [0, n-1]$, et le patron d'erreurs E de poids x avec E_i éléments, $i \in [0, n-1]$. Ces mots sont représentés schématiquement sur la figure 3.

A partir de cette représentation, ou peut définir les ensembles suivants:

$$h = \xi\{i: C_i \neq 0\}$$
$$x = \xi\{i: E_i \neq 0\}$$
$$j = \xi\{i: C_i = E_i,\ C_i \neq 0,\ E_i \neq 0\}$$
$$m = \xi\{i: C_i \neq E_i,\ C_i \neq 0,\ E_i \neq 0\}$$
$$p = \xi\{i: C_i \neq 0,\ E_i = 0\}$$
$$r = \xi\{i: C_i = 0,\ E_i \neq 0\}$$

Grâce auquels on peut établir les relations:

$$h = p+j+m \tag{8}$$
$$x = j+m+r \tag{9}$$

La distance entre le mot de code C et le patron d'erreurs E est donnée par:

$$\ell = p+m+r \tag{10}$$

Et le nombre $n(h,x,\ell)$, est donné par:

$$n(h,x,j,r,m) = \binom{h}{j}(1)^j \binom{n-h}{r}(q-1)^r \binom{h-j}{m}(q-2)^m \tag{11}$$

On peut regrouper les équations pour avoir:

$$j = h-\ell+r \tag{12}$$

$$m = x-h+\ell-2r \tag{13}$$

En conséquence, le nombre de patrons d'erreurs de poids x situés à une distance ℓ d'un mot de code de poids h, est donné par:

$$n(h,x,\ell)=\sum_{r}\binom{h}{h-\ell+r}\binom{n-h}{r}(q-1)^{r}\binom{\ell-r}{x-h+\ell-2r}(q-2)^{x-h+\ell-2r} \tag{14}$$

pour $h-\ell\leq x\leq h+\ell$. La somme sur r doit se calculer dans les limites de $r_1 = \max\{0, x-h\}$ à $r_2 = \frac{x-h+\ell}{2}$, le symbole $\lfloor x_1 \rfloor$ représente la partie entière de x_1, soit:

$$n(h,x,\ell)=\sum_{r=r_1}^{r_2}\binom{h}{h-\ell+r}\binom{n-h}{r}(q-1)^{r}\binom{\ell-r}{x-h+\ell-2r}(q-2)^{x-h+\ell-2r} \tag{15}$$

Sachant que pour une distribution binomiale à l'entrée du décodeur, la probabilité d'un mot de poids x sur un CG(q), est donnée par:

$$P_x = \left(\frac{\varepsilon}{q-1}\right)^{x}(1-\varepsilon)^{n-x}, \quad 0\leq\varepsilon\leq 1 \tag{16}$$

La probabilité d'un décodage incorrect [4] lorsque le patron d'erreurs est décodé comme le mot de poids h, est:

$$P_{DIC}(h)=W_h\sum_{\ell=0}^{t}\sum_{x=h-\ell}^{h+\ell} n(h,x,\ell)\,P_x, \quad h \geq d \tag{17}$$

Dans cette expresion W_h est la distribution des poids des mots de code [1] c'est-à-dire que dans un code de Reed-Solomon de distance minimale d, le nombre des mots de code de poids h est donné par:

$$W_h=\binom{n}{h}(q-1)^{h}\sum_{i=0}^{h-d}(-1)^{i}\binom{h-1}{i}q^{h-d-i}, \quad d\leq h\leq n \tag{18}$$

Connaisant $P_{DIC}(h)$, le taux d'erreus résiduel par symbole ε', est défini comme l'espérance d'un nombre d'erreurs dans un mot après le décodage:

$$\varepsilon' = \frac{1}{n}\sum_{h=d}^{n} h\,P_{DIC}(h) \tag{19}$$

Finalement, la probabilité d'avoir plus de Γ erreurs après le décodage $P(\Gamma)$, est donnée par:

$$P(\Gamma) = \sum_{h=\Gamma+1}^{n} P_{DIC}(h) \tag{20}$$

V. CALCUL DE LA PROBABILITE DE NON-DETECTION

De la même manière que pour le calcul de P_{DIC}, le calcul de P_{ND} [5] s'effectue en considérant les propriétés linéaires des codes de RS, et en supposant également qu'on transmet le mot de poids zéro, au sens de Hamming, sur un canal DMC. Cependant les résultats sont tout à fait généraux dû aux propriétés linéaires des codes.

La clé du problème consiste à affirmer qu'il est impossible de détecter un patron d'erreurs lorsqu'il est égal à un mot de code.

D'après le paragraphe II, pour un code linéaire des paramètres (n,k,q), de matrice de parité H, le produit de tout mot de code $c \in C$, par H transposée, appelé le syndrôme de c, est égal à zéro, et s'écrit:

$$S(c) = c\cdot H^{T} = 0 \tag{21}$$

Lorsque le mot reçu Y a été perturbé par le bruit E, le produit $Y\cdot H^T$ n'est plus égal à zéro [1], [2] [3]:

$$Y = c + E \tag{22}$$

$$S(Y) = E\cdot H^{T} \neq 0 \tag{23}$$

En considérant une distribution binomiale à l'entrée du décodeur, la probabilité d'un mot de poids x sur un CG(q) est donnée par:

$$P_x = \left(\frac{\varepsilon}{q-1}\right)^{x}(1-\varepsilon)^{n-x}, \quad 0\leq\varepsilon\leq 1 \tag{24}$$

On peut calculer la probabilité d'avoir un syndrôme nul, comme la probabilité de tous les mots de code:

$$P(S(c)=0)=\sum_{h=0}^{n} W_h\left(\frac{\varepsilon}{q-1}\right)^{h}(1-\varepsilon)^{n-h}=(1-\varepsilon)^{n}\sum_{h=0}^{n} W_h\left(\frac{\varepsilon}{(q-1)(1-\varepsilon)}\right)^{h}$$

$$= (1-\varepsilon)^{n}\,W(z) \tag{25}$$

Où W_h est la distribution des poids des mots de code [1], et W(z) est définie comme la fonction de dénombrement des poids du code. A partir de cette expresion, la probabilité de non-détection [5], [6], [7] s'obtient directement. En rappelant que lorsqu'on transmet le mot de code de poids nul, les erreurs seront non-détectées, si et seulement si, le patron des erreurs est égal à un autre mot de code de poids différent de zéro [5], [8], [9]. En conséquence:

$$P_{ND} = \sum_{h=1}^{n} W_h\left(\frac{\varepsilon}{q-1}\right)^{h}(1-\varepsilon)^{n-h}, \quad 0\leq\varepsilon\leq 1 \tag{26}$$

En considérant l'identité de Mac Williams, [1], [10], qui établit le rapport entre la distribution des poids des mots de code, et la distribution des poids des mots du code dual. On peut établir une expression parallèle pour le calcul de P_{ND}.

L'identité de Mac Williams est donnée par:

$$q^{n-k}\,W(z) = (1+(q-1)z)^{n}\,M\left(\frac{1-z}{1+(q-1)z}\right) \tag{27}$$

Où M(z) est la fonction de dénombrement des poids du code dual. Dans l'expression précédente, $z = \frac{\varepsilon}{(q-1)(1-\varepsilon)}$, ainsi:

$$(1-\varepsilon)^{n}\sum_{h=0}^{n} W_h\left(\frac{\varepsilon}{(q-1)(1-\varepsilon)}\right)^{h}=q^{-(n-k)}\sum_{h=0}^{n} M_h\left(1-\varepsilon\frac{q}{q-1}\right)^{h} \tag{28}$$

La probabilité de non-détection [5], [9] est maintenant donnée par:

$$P_{ND} = q^{-(n-k)}\sum_{h=0}^{n} M_h\left(1-\varepsilon\frac{q}{q-1}\right)^{h} - (1-\varepsilon)^{n} \tag{29}$$

Le terme $(1-\varepsilon)^n$ est la probabilité du mot de poids zéro, c'est-à-dire la probabilité qu'il n'y ait pas d'erreurs:

$$(1-\varepsilon)^{n}\,W_o\left(\frac{\varepsilon}{(q-1)(1-\varepsilon)}\right)^{0} = (1-\varepsilon)^{n} \tag{30}$$

puisque $W_o=1$.

VI. CODES RACCOURCIS DE REED-SOLOMON

Le raccourcissement des codes de Reed-Solomon permet la construction d'un code de paramètres (n-I, k-I, q) à partir d'un code (n,k,q); on parle alors d'un

code raccourci [1], [2], [3] d'ordre I avec la même capacité de correction que le code d'origine, dans ce cas les I premiers symboles d'information sont considérés comme nuls et non transmis.

La probabilité de décodage incorrect P_{DIC} s'obtient en remplaçant n par n-I dans les équations: (15), (16) et (18) et ensuite en remplaçant les valeurs modifiées dans l'équation (17). Pour avoir:

$$P_{DIC} = \sum_{h=d}^{n-I} P_{DIC}(h) \qquad (31)$$

Le taux d'erreurs résiduel par symbole ε' se calcule aussi en utilisant l'équation (17) modifiée, et en remplaçant n par n-I sur (19).

Finalement, la probabilité de non-détection P_{ND} s'obtient en faisant la même modification sur (26) avec une distribution des poids des mots de code W_h où on a remplacé n par n-I sur (18).

VII. PRESENTATION DES RESULTATS

Les expresions pour le calcul des probabilités utilisées dans le cas de la correction d'erreurs, ainsi que celles utilisées dans le cas de la détection d'erreurs, sont bien connues dans la littérature specialisée [4], [5] et leur calcul est exact lorsqu'on connaît la distribution des poids des mots de code, tel est le cas des codes de Reed-Solomon. Dans cette communication on présente les résultats obtenus pour les codes de Reed-Solomon où la longueur de bloque n n'est pas trop grande, puisqu'il faut faire remarquer que les calculs deviennent très rapidement une tâche assez lourde pour un ordinateur. Les résultats obtenus ont été calculés sur un micro-ordinateur APPLE IIe. Dans le cas où on decide de calculer ces paramètres, pour des longueurs de code où le calcul exact est pratiquement impossible, on peut calculer des seuils approximatifs [5], [8], [9] d'utilité pratique.

Sur la figure 4 on a tracé les courbes du taux d'erreurs résiduel par symbole ε', en fonction du taux d'erreurs par symbole à l'entrée du décodeur ε, pour les codes de Reed-Solomon de longueur de bloque n=31, et des capacités de correction t=1, t=2 et t=3. On constate une diminution du taux d'erreurs résiduel par symbole au fur et à mesure qu'on augmentela capacité de correction.

Sur la figure 5, on a étudié l'effet du raccourcissement pour un code RS de longueur de bloque n=7. En effectuant le raccourcissement sur les symboles d'information, la capacité de correction du code ne change pas, cependant le taux d'erreurs résiduel par symbole diminue pour les codes raccourcis, vis-à-vis du code non-raccourci. Ce gain s'interprète par le fait que les codes raccourcis utilisent un pourcentage plus grand de la largeur de bande, pour transmettre la redondance. En effet, le taux de redondance donné par $\frac{(n-I)-(k-I)}{(k-I)}$, où I est l'ordre de raccourcissement, augmente lorsque I augmente.

Finalement, sur la figure 6. On a tracé les courbes de probabilité de non-détection P_{ND} pour des codes de RS de longueur de bloque n=63, et des distances d=3, d=4 et d=5. La probabilité de non-détection diminue lorsqu'on augmente la distance entre les mots du code.

Dans l'ensemble des courbes, lorsque le taux de redondance augmente, les performances du code augmentent, mais le pourcentage de la largeur de bande alloué aux symboles de redondance est aussi en augmentation. En conséquence, pour transmettre la même quantité d'information pendant la même durée de temps

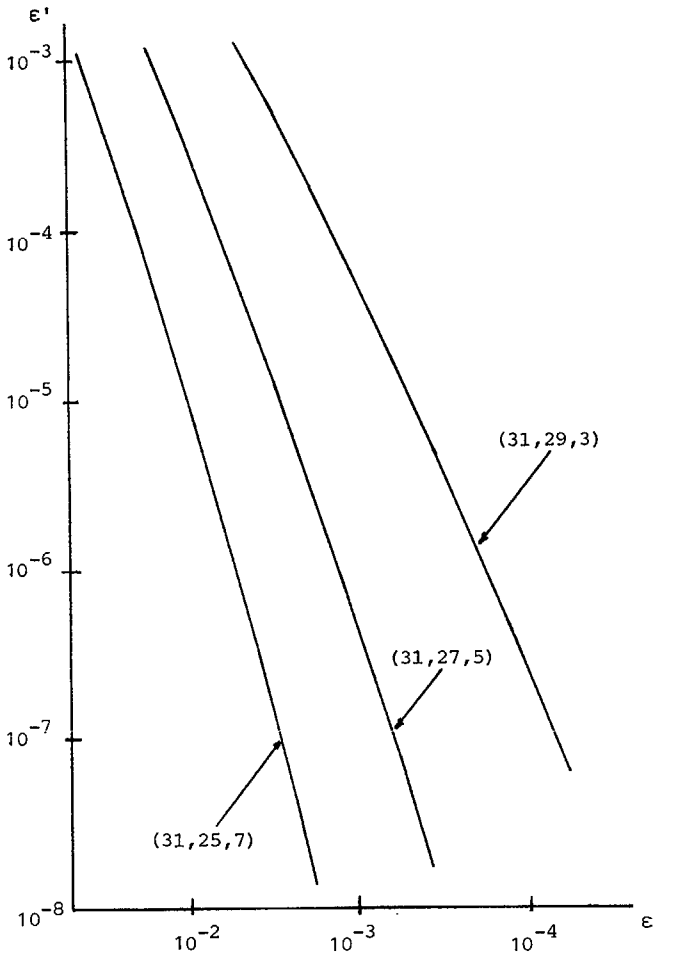

Fig. 4. Taux d'erreurs par symbole après le décodage ε' en fonction du taux d'erreurs par symbole à l'entrée du décodeur ε pour codes RS de longueur n=31 et des distances d=3, d=5 et d=7.

il faudra augmenter la rapidité de transfert des symboles par unité de temps. Il est évident que par les caractéristiques physiques du canal de transmission, il y a une limite à sa propre capacité, il faut donc trouver un compromis entre l'amélioration des performances du code et la quantité d'information transmise.

VIII. CONCLUSIONS

On a présenté une analyse des expressions qui permetent le calcul des probabilités des événements qui peuvent se présenter après le décodage lorsqu'on utilise les codes de Reed-Solomon (RS) pour diminuer le taux d'erreurs par symbole sur un canal de communications. On a considéré le cas où on utilise les codes RS pour la correction d'erreurs, et le cas où on les utilise pour la détection d'erreurs. Dans les deux cas on considère l'hypothèse d'un canal discret sans mémoire avec q entrées et q sorties, où il y a indépendance entre symboles, et lorsqu'un symbole est affecté par le bruit, il peut prendre la valeur d'un des q-1 symboles différents avec la même probabilité.

Les courbes tracées montrent le comportement des codes RS, lorsque le pourcentage de la largeur de bande du canal de transmission consacré aux symboles de redondance augmente; permetant une réduction du taux d'erreurs résiduel par symbole.

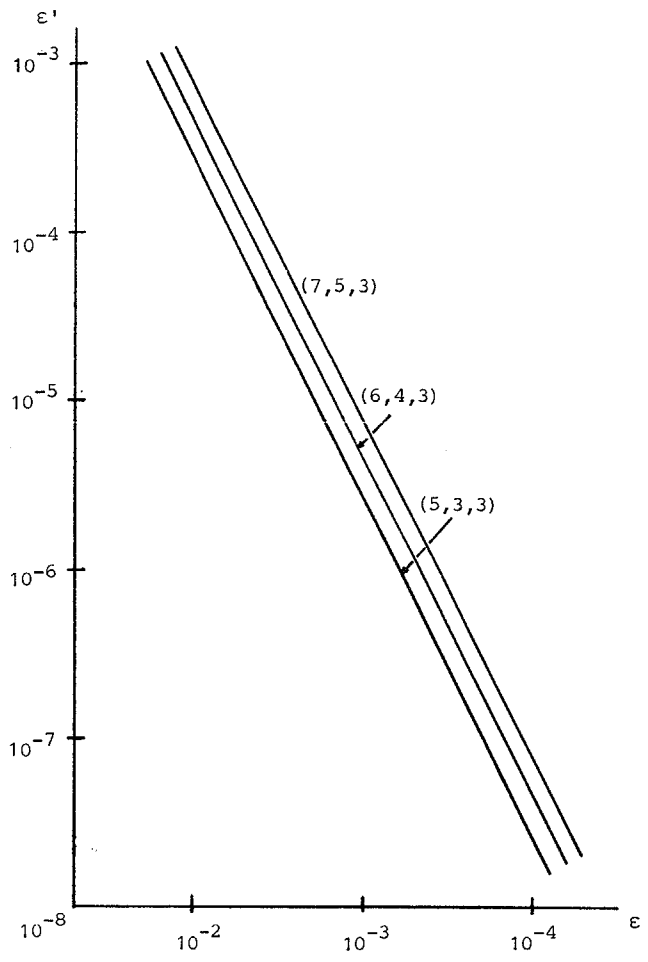

Fig. 5. Taux d'erreurs résiduel par symbole ε'en fonction du taux d'erreurs par symbole à l'entrée du décodeur ε pour le code non-raccourci de RS (7,5,3) et les codes raccourcis de RS (6,4,3) et (5,3,3).

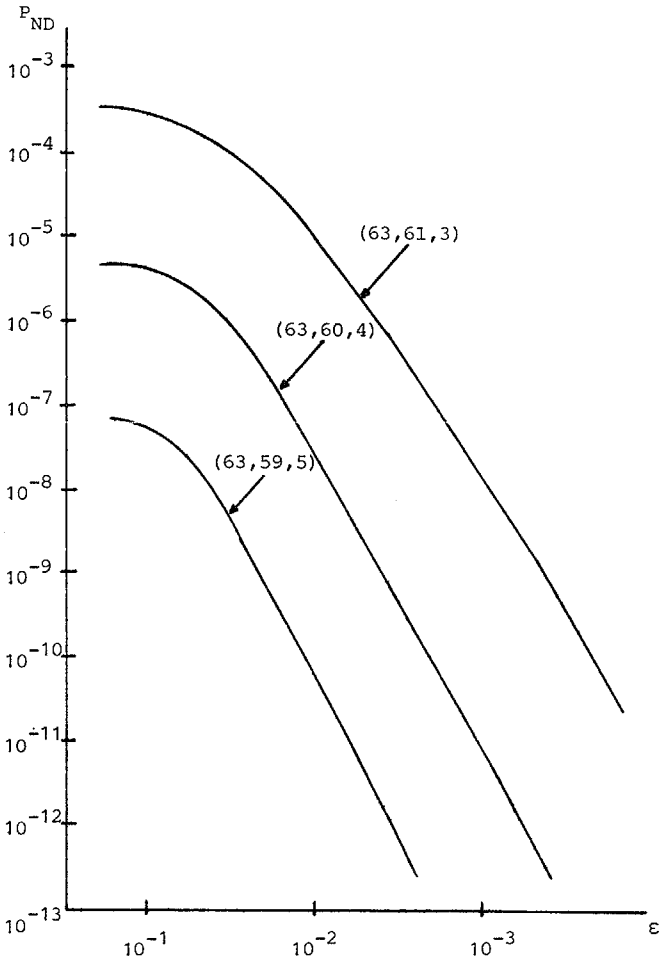

Fig. 6. Probabilité de non-détection P_{ND} en fonction du taux d'erreurs par symbole à l'entrée du décodeur ε pour des codes RS de longueur de bloque n=63 et des distances d=3, d=4 et d=5.

Les courbes de probabilité de non-détection P_{ND}, montrent une tendance asymptotique vers un seuil supérieur lorsque le taux d'erreurs par symbole à l'entrée du décodeur augmente.

REFERENCES

[1] F.J. Mac Williams and N.J.A. Sloane, "The theory of Error-Correcting Codes", New York, North Holland, 1977.

[2] W.W. Peterson and E.J. Weldon, "Error Correction Codes", 2nd. ed. Cambridge, MA, MIT Press, 1972.

[3] E.R. Berlekamp, "Algebraic Coding Theory", New York, Mac Graw-Hill, 1968.

[4] Z. Mc C. Huntoon and A.M. Michelson, "On the Computation of the Probability of Post-Decoding Error Events for Block Codes", IEEE Trans. Inform. Theory, Vol. IT-23, pp. 399-403, May 1977.

[5] J.K. Wolf, A.M. Michelson and A.H. Levesque, "On the Probability of Undetected Error for Linear Block Codes", IEEE Trans. Commun. Vol. COM-30, No. 2, pp. 317-324, Feb. 1982.

[6] T. Kløve, "The Probability of Undetected Error When a Code is Used for Error Correction and Detection", IEEE Trans. Inform. Theory, Vol. IT-30 No. 2, pp. 388-392, March 1984.

[7] T. Kløve and M. Miller, "The Detection of Errors After Error-Correction Decoding", IEEE Trans. Commun, Vol. COM-32, No. 5, pp. 511-517, May 1984.

[8] T. Kasami, T. Kløve and S. Lin, "Linear Block Codes for Error Detection", IEEE Trans. Inform. Theory, Vol. IT-29, No. 1, pp. 131-136, Jan, 1983

[9] T. Kasami and S. Lin, "On the Probability of Undetected Error for the Maximum Distance Separable Codes", IEEE Trans. Commun., Vol. COM-32, No. 9, pp 998-1006, Sept. 1984.

[10] S.C. Chang and J.K. Wolf, "A Simple Derivation of the Mac Williams' Identity for Linear Codes", IEEE Trans. Inform. Theory, Vol. IT-26, No. 4, pp. 476-477, July, 1980.