

# DIXIEME COLLOQUE SUR LE TRAITEMENT DU SIGNAL ET SES APPLICATIONS

613



NICE du 20 au 24 MAI 1985

---

ÉFFICACITÉ EXPÉRIMENTALE DE CODES CONCATÉNÉS OU NON

A. POLI, M.C. GENNERO, A. RANDRIANANJA

Laboratoire A.A.E.C.C./L.S.I. - Université P. Sabatier - 118 route de Narbonne - 31062 TOULOUSE cédex- FRANCE

---

## RESUME

Nous présentons des résultats de simulation de transmissions, dans les cas où on utilise des codes de Reed Solomon et/ou des codes convolutionnels. Ces codes sont utilisés séparément ou concaténés. Les résultats sont obtenus en utilisant la 'décision dure' (hard decoding).

## SUMMARY

We present simulation results for data transmissions, using Reed Solomon codes and/or convolutional codes. These codes are concatenated or not. We only give results for hard decoding.



## INTRODUCTION

Protéger l'information transmise, au moyen de codes correcteurs, est une technique en plein essor. A côté des nécessités nouvelles imposées par l'enregistrement vertical pour les disques magnétiques, à côté de la technologie mise en œuvre pour les disques optiques, se profile la nécessaire normalisation qui actuellement concerne les codes correcteurs recommandés pour les transmissions par satellites (recommandations CCSDS).

Comme le signale E.R. BERLEKAMP dans son article [1], le choix des codes est souvent délicat, car la modélisation d'un canal de transmission est rarement possible. Il recommande, au delà des choix algébriques de procéder à de nombreuses simulations. Ces simulations sont également nécessaires dans le cas où on voudrait faire des réalisations électroniques.

Dans l'article que nous présentons ici, nous donnons des résultats expérimentaux concernant certains codes (codes de Reed-Solomon sur  $\mathbb{F}_p$ , codes de Reed-Solomon sur  $\mathbb{F}_{2^n}$ , codes convolutionnels) utilisés seuls ou concaténés. Nous donnons également des résultats de simulation de certains types d'erreurs.

Tous ces résultats ont été obtenus à partir de plusieurs logiciels, qui sont en fait des versions différentes issues de LOUSTICC, que nous avons présenté de nombreuses fois [3], [4], [5].

LOUSTICC simule une transmission (half ou full duplex), et simule des erreurs additives (isolées ou en bursts) selon diverses modélisations (bruit blanc, bruits avec loi des écarts normale, géométrique, uniforme). Nous présenterons des résultats expérimentaux concernant une procédure plus complexe de brouillage (module ORAGE), et concernant la génération de bruits blancs ainsi que leur loi d'espacement. LOUSTIC, et ses différentes versions, peuvent mettre en œuvre divers codes (codes de FIRE, codes auto-duaux, code de GOLAY, codes de Reed Solomon, codes convolutionnels).

Nous donnerons ici des résultats sur des codes de Reed Solomon et convolutionnels, entrelacés ou non, concaténés ou non (en hard decoding).

Les principaux résultats sont décrits sous forme de courbes montrant l'efficacité d'un système de codage en fonction du rapport signal à bruit ( $E_b/N_0$ ). D'autres sont donnés sous forme de tableaux. Dans certaines de nos simulations nous ne faisons intervenir des problèmes de perte de synchronisation primaire.

## I) LES CODES DE REED SOLOMON

### 1) Définition

Un code de Reed Solomon (noté RS), de longueur  $N=p^s-1$  ( $p$  premier) est un code cyclique sur un corps de Galois  $\mathbb{F}_{p^s}$ . Son polynôme générateur est de la forme :

$$g(X) = \prod_{i=0}^{D-2} (X - \alpha^{m+i}) = \sum_{i=0}^{D-1} g_i X^i$$

où  $\alpha$  est un élément primitif de  $\mathbb{F}_{2^s}$ .

### 2) Propriétés

La dimension d'un code RS est  $K=N-D+1$ , où  $D$  est la distance minimale du code.

Un code  $(N,K,D)$  est capable de corriger  $t = \left\lfloor \frac{D-1}{2} \right\rfloor$  erreurs. On dit qu'il est  $t$ -correcteur.

### 3) Codes de RS utilisés dans les simulations

#### ◦ codes RS sur $\mathbb{F}_{2^s}$

- Le polynôme générateur  $g(X)$  est choisi palindrome et unitaire :

$$\begin{cases} g_i = g_{D-(i+1)} \\ g_0 = 1 \end{cases}$$

- Le codage met en œuvre l'algorithme proposé par E.R. BERLEKAMP dans [9].
- Le décodage utilise le calcul des polynômes localisateur et évaluateur de l'erreur selon J.L. DORNSTETTER [10]. Le calcul des racines du polynôme localisateur de l'erreur consiste en une recherche de CHIEN.

#### ◦ Codes RS sur $\mathbb{F}_p$ ( $p$ premier de la forme $2^M \pm 1$ )

- Le codage est classique, il simule le fonctionnement d'un registre à décalages, calculant le reste de division du produit de deux polynômes par le polynôme  $g(X)$ .
- Le décodage utilise l'algorithme des fractions continues pour le calcul du polynôme localisateur d'erreurs, proposé par REED, MILLER et al [7]. On utilise la transformée inverse de FOURIER pour la correction des erreurs.

## II) LES CODES CONVOLUTIONNELS

### 1) Le codage

Un code convolutionnel binaire de taux  $1/v$ , et de longueur de contrainte  $K$ , peut être généré par un registre à décalages à  $K$  bascules, dont certaines sont connectées à au plus  $v$  additionneurs (modulo 2).

Les connexions des  $K$  bascules aux  $v$  addition-



## EFFICACITÉ EXPÉRIMENTALE DE CODES CONCATÉNÉS OU NON

neurs sont représentées par  $v$  vecteurs  $u_1, u_2, \dots, u_v$  de longueur  $K$ , tels que :

$$u_i(j) = \begin{cases} 1 & \text{si la } j^{\text{ème}} \text{ bascule est connectée au} \\ i^{\text{ème}} & \text{additionneur} \\ 0 & \text{sinon} \end{cases}$$

### 2) Le décodage

Nous avons mis en œuvre un décodage dérivé de celui de VITERBI, qui est un décodage par maximum de vraisemblance. Il détermine récursivement, à partir de la séquence d'information reçue, la séquence la plus probablement émise.

### III) LE BROUILLAGE

#### 1) Erreurs de coupure, erreurs isolées

Nous avons réalisé un module de génération d'erreurs de coupure (bursts) ou d'erreurs isolées, dont l'espacement est modélisé par variables aléatoires de la forme :

$$Y = aX^1 + T$$

(où  $T$  est une v.a. certaine,  $X$  est une V.A. qui suit une loi normale  $(\mu, \sigma)$ , ou une loi uniforme définie sur  $[0, 63]$ , ou encore une loi géométrique de paramètre  $1/2$ ).

Nous avons montré [3], que le taux binaire d'erreur est alors donné par :

$$\tau = \frac{1/2}{(1+aE(X^1)+t)} \quad \text{où } l \text{ est la longueur maximale des erreurs.}$$

Un deuxième module de brouillage simule des "orages" lors de transmissions, c'est à dire une forte densité d'erreurs pendant un temps très court, et très peu d'erreurs le reste du temps. Dans ce cas le taux d'erreurs est modélisé par :

$$\tau = \frac{a' E(Y^j) + t'}{2(1+aE(X^1)+t)}$$

où  $Y$  est une v.a. qui suit une loi normale  $(\mu, \sigma)$ , et  $X$  est une v.a. qui suit une loi uniforme sur  $[0, 63]$

#### exemples

|          |                      |                      |                      |                      |
|----------|----------------------|----------------------|----------------------|----------------------|
| $\tau_t$ | $41.4 \cdot 10^{-3}$ | $7.55 \cdot 10^{-3}$ | $45.7 \cdot 10^{-3}$ | $7.02 \cdot 10^{-3}$ |
| $\tau_e$ | $40.4 \cdot 10^{-3}$ | $7.12 \cdot 10^{-3}$ | $47.3 \cdot 10^{-3}$ | $6.91 \cdot 10^{-3}$ |

|          |                      |                      |                      |                      |
|----------|----------------------|----------------------|----------------------|----------------------|
| $\tau_t$ | $82.8 \cdot 10^{-3}$ | $14.0 \cdot 10^{-3}$ | $11.3 \cdot 10^{-3}$ | $3.77 \cdot 10^{-3}$ |
| $\tau_e$ | $86.0 \cdot 10^{-3}$ | $16.7 \cdot 10^{-3}$ | $13.3 \cdot 10^{-3}$ | $3.42 \cdot 10^{-3}$ |

$\tau_t$  est le taux théorique,  $\tau_e$  est le taux expérimental

### 2) Bruit blanc

Nous avons introduit dans LOUSTICC, un module qui génère des erreurs isolées, simulant un bruit blanc. La probabilité d'apparition d'une erreur (par symbole binaire) peut être au choix gaussienne ou uniforme.

On vérifie expérimentalement l'adéquation de nos résultats à la courbe théorique des espacements (cf. figure 4).

### IV) RESULTATS EXPERIMENTAUX

Les figures 1 à 3 (page suivante) montrent l'efficacité d'un code de Reed Solomon (RS) et d'un code convolutionnel, en fonction du rapport signal à bruit.

Les tableaux 1 et 2 ci-dessous donnent quelques résultats expérimentaux sur la concaténation d'un code de Reed Solomon (entrelacé ou non) (127,119) avec un code convolutionnel de taux  $1/2$  (longueur de contrainte 7)

| $\tau_1$ | $\tau_2$ | $E_b/N_0$ (dB) |                                                                |
|----------|----------|----------------|----------------------------------------------------------------|
| 0.0530   | 0.0173   | 1.432          | $\tau_1$ : taux binaire d'erreurs (en entrée)                  |
| 0.0435   | 0.0075   | 1.941          |                                                                |
| 0.0345   | 0.0019   | 2.468          | $\tau_2$ : taux binaire d'erreurs résiduelles (après décodage) |
| 0.0299   | 0.0012   | 2.763          |                                                                |

tableau 1 : concaténation d'un code RS(127,119) avec un code convolutionnel (7,1/2) (hard décodage - pas d'entrelacement)

| $\tau_1$ | $\tau_2$ | $E_b/N_0$ (dB) |                                                                |
|----------|----------|----------------|----------------------------------------------------------------|
| 0.0530   | 0.0172   | 1.434          | $\tau_1$ : taux binaire d'erreurs (en entrée)                  |
| 0.0476   | 0.0088   | 1.722          |                                                                |
| 0.0435   | 0.0039   | 1.940          | $\tau_2$ : taux binaire d'erreurs résiduelles (après décodage) |
| 0.0398   | 0.0019   | 2.152          |                                                                |

tableau 2 : concatenation d'un code RS(127,119) (entrelacement de profondeur 3), avec un code convolutionnel (7,1/2) (hard décodage)

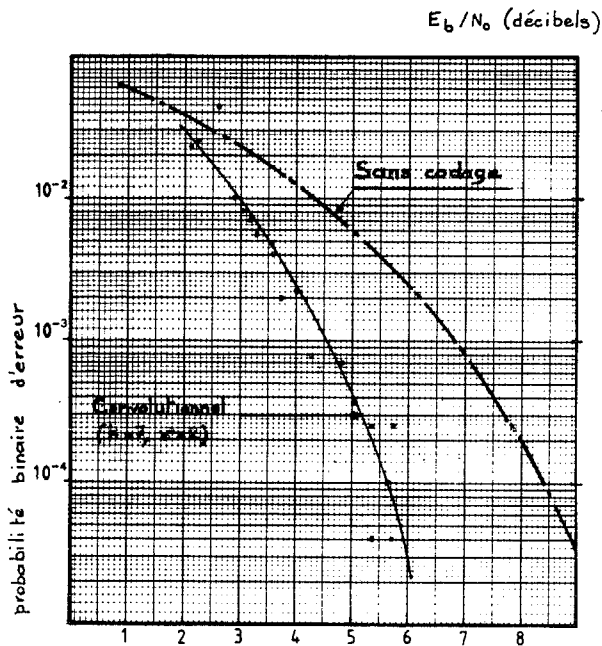


FIGURE 1: CODE CONVOLUTIONNEL ( $k=7$ , taux  $1/2$ )  
(utilisé seul, avec un hard décodage)

Pour ces simulations, nous avons utilisé un code convolutionnel de taux  $1/2$ , de longueur de contrainte 7.

Le brouillage simule un bruit blanc. La probabilité d'apparition d'une erreur (par symbole binaire) est gaussienne.

On voit sur la courbe que pour une probabilité binaire d'erreur de  $10^{-4}$  on obtient un gain de 2.7 décibels. Ce résultat est tout à fait conforme aux résultats classiques.

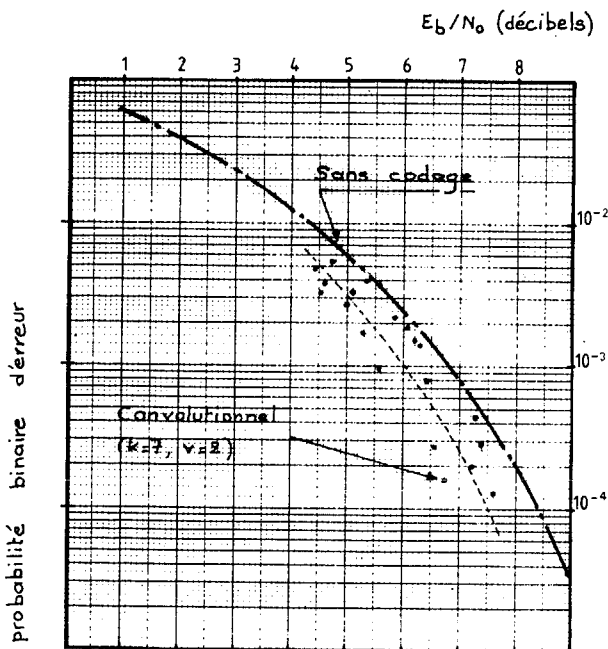


FIGURE 2: CODE CONVOLUTIONNEL ( $k=7$ , taux  $1/2$ )  
(utilisé seul, avec un hard décodage)

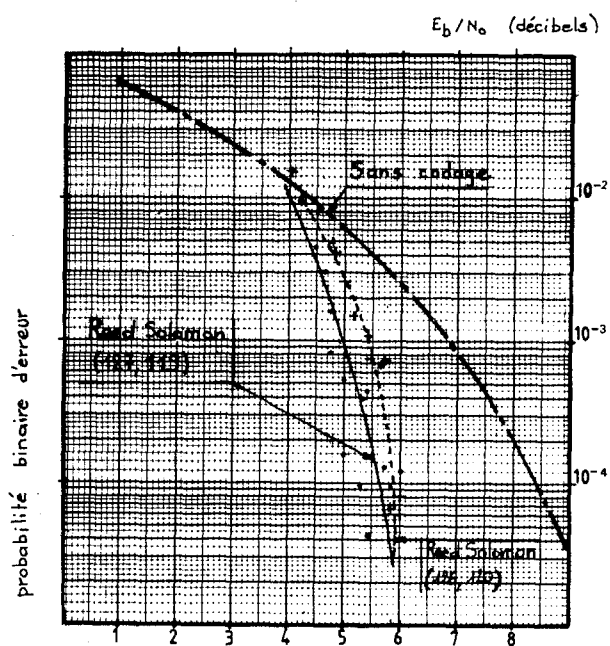
Pour ces simulations nous avons utilisé le même code convolutionnel que pour la figure 1 (taux  $1/2$ , longueur de contrainte 7).

Dans ce cas nous avons simulé l'arrivée d'erreurs de coupure (bursts), dont l'espacement est modélisé par une variable aléatoire qui suit une loi normale. La longueur maximale des bursts est de 8.

On voit sur la courbe que le gain est d'environ 0.7 décibels.

Ces résultats montrent, comme l'a indiqué E.R. BERLEKAMP, la nécessité de réaliser des simulations des bruits (sur un canal) avant de choisir un code correcteur.

## EFFICACITÉ EXPÉRIMENTALE DE CODES CONCATÉNÉS OU NON



Sur la figure 3, nous avons tracé le gain de codage de deux codes de Reed Solomon :

- \* (127,119) définis sur  $\mathbb{F}_{27}$ , correcteur de 4 erreurs
- \* (126,120) défini sur  $\mathbb{F}_p$  ( $p=2^7-1$ ,  $p$  premier). ce code corrige 3 erreurs.

Les erreurs sont des bursts de longueur maximale 8 (éléments binaires).

L'espace entre deux bursts consécutifs suit une loi normale.

FIGURE 3 : CODES DE REED SOLOMON SUR  $\mathbb{F}_{27}$  (127,119), ET SUR  $\mathbb{F}_{127}$  (127,120)

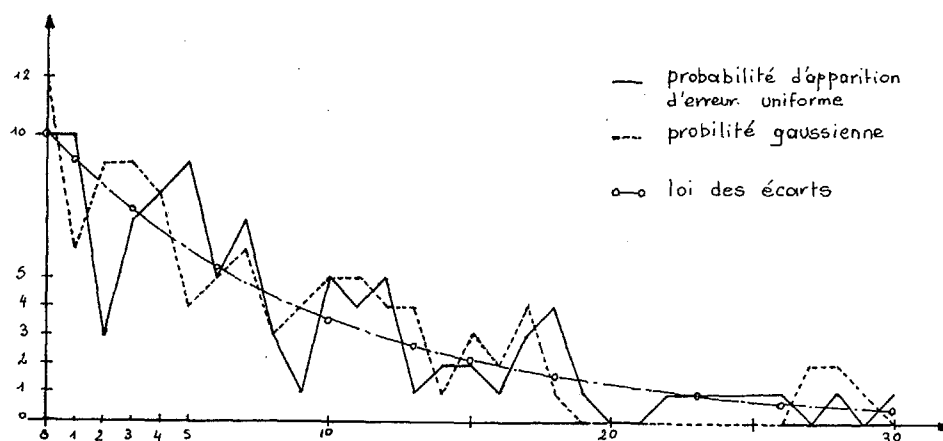


FIGURE 4 : ESPACEMENT DES ERREURS

CONCLUSION

Le choix d'un code correcteur nécessite une option algébrique, suivie de simulations informatiques. La validation d'un système de codage adapté aux images et à la parole exige également des simulations.

Le A.A.E.C.C. est spécialisé, d'une part dans l'étude théorique des codes correcteurs, et d'autre part dans la réalisation de logiciels très performants. Nous avons réalisé des logiciels de construction de codes, et de codage/décodage sur des matériels aussi variés que : TRS 80, APPLE III, VICTOR S1, BURROUGHS 6700, CDC 750, CRAY I.

Nous avons donné dans cet article, des résultats expérimentaux concernant une version de LOUSTICC. Une autre version du logiciel permet de traiter (codage, brouillage, décodage) rapidement (moins de 40 secondes) une image de 1.1 M symboles binaires, sur un CDC 750. Cette version a été spécialement conçue et optimisée pour le codage et le décodage des codes de FIRE.

La version complète de LOUSTICC (codes de FIRE, codes de REED SOLOMON, code de GOLAY binaire, code autodual (64,32,12)) est accessible sur le DPS 8/70 du centre de calcul de l'Université P. Sabatier, via TRANSPAC ou le réseau commuté.

BIBLIOGRAPHIE

- 1 - E.R. BERLEKAMP  
"The technology of error correcting codes"  
The proceedings of IEEE vol 68 n°5, may 1980
- 2 - G.C. CLARK, J.B. CAIN  
"Error-correction coding for digital communication"  
Plenum press - New York ISBN : 0-306-40615-2 (1981)
- 3 - M.C. GENNERO  
"Un logiciel de simulation de transmission d'information : LOUSTICC"  
Mémoire d'ingénieur CNAM (Informatique) Octobre 1983 - Toulouse
- 4 - M.C. GENNERO  
"LOUSTICC software program : experimental results"  
soumis pour publication
- 5 - M.C. GENNERO, O. PAPINI  
"Utilization of error correcting codes for data transmission simulations"  
(à paraître dans DISCRETE MATH., Actes du 1<sup>er</sup> colloque International AAECC)
- 6 - F.J. MacWILLIAMS, N.J.A. SLOANE  
"The theory of error correcting codes"  
North Holland publishing Company - 1977
- 7 - I.S. REED, T.K. TRUONG, R.L. MILLER  
"The fast decoding of Reed Solomon codes using Fermat theoretic transforms, and continued fraction"  
IEEE Transactions on information theory vol 24 n°1, - 1978
- 8 - A. POLI  
"Idéaux principaux nilpotents de dimension maximale dans l'algèbre  $\mathbb{F}_q[G]$  d'un groupe abélien fini G"  
Communications in Algebra 12(4), p391-401 - 1984
- 9 - E.R. BERLEKAMP  
"Bit-sérial Reed Solomon encoders"  
IEEE Transactions on Information Theory vol IT-28 p 869-874 (1982)
- 10 - J.L. DORNSTETTER  
(correspondance privée)