Décodage de certaines classes de codes de Reed-Solomon

Decoding of certains clases of Reed-Solomon codes

Odile PAPINI

GECT, UER de Sciences, Université de Toulon et du Var, CHATEAU-SAINT-MICHEL, 83130 LAGARDE

Chercheur au GECT, docteur 3e cycle, recherche d'algorithmes de décodage de codes de Reed-Solomon.

RÉSUMÉ

Nous présentons une méthode de décodage pour certaines classes de codes de Reed-Solomon sur F_{2^m}, et pour leurs images binaires. La méthode utilise dans certains cas uniquement un décodage par permutations et dans d'autres un décodage par permutations et une lecture de table.

MOTS CLÉS

Code, décodage par permutations.

SUMMARY

We present a decoding procedure for certain classes of Reed-Solomon codes over GF(2^m) *as well as their binary images. The method uses permutation decoding completed in some cases by other techniques for example a short look-up table.*

KEY WORDS

Code, permutation decoding.

TABLE DES MATIÈRES

Introduction

LES CODES DE REED-SOLOMON

Nous utilisons les codes de Reed-Solomon sur F_{2^m}, ces codes étendus ou non sont MDS (Maximum Distance Separable). Notons que les codes de Reed-Solomon étendus sont invariants par le groupe affine quand les composantes des mots du code sont indexées par les éléments de F_{2^m}.

Nous utilisons également l'image binaire de ces codes. Rappelons que l'image binaire d'un code C linéaire sur F_{2^m} de paramètres (n, k, d), par rapport à une base de F_{2^m} sur F_2, est un code linéaire binaire $\mathcal{I}(C)$ de paramètres $(mn, mk, \tilde{d})$ avec $\tilde{d} \geqq d$.

Notons qu'il est quelquefois utile d'utiliser des bases trace orthogonale pour construire des images binaires comme l'ont fait J. Wolfmann [2] et G. Pasquier [3].

LE DÉCODAGE PAR PERMUTATIONS

Cette méthode s'appuie sur le théorème fondamental suivant dû a J. MacWilliams [1].

Soit un code linéaire systématique $C(n, k, d)$ t-correcteur de matrice génératrice $G(I_k | M)$, et de matrice de contrôle $H({}^tM | I_{n-k})$.

Soient y le mot reçu, c le mot transmis, e le mot erreur de poids inférieur ou égal à t, S le syndrome $= H.y^t$.

Théorème : $W(S(y)) \leqq t$ *si et seulement si les symboles d'information,* $(y_1, \ldots, y_k)$ *sont corrects* $c=(y_1, \ldots, y_k).G$.

On désigne par E un ensemble d'erreurs e, inclus dans l'ensemble des erreurs de poids inférieur ou égal à t, de support $s(e)$, $s(e)=\{i, e_i \neq 0\}$, pour tout e appartenant à E.

Définition : On appelle ensemble de permutations de décodage P pour le code C pour les erreurs appartenant à E un ensemble vérifiant :

– P est inclus dans le groupe d'automorphismes du code C;

– $\forall s(e) \subset \{1, \ldots, n\}$,

$\hat{\sigma}_i \in P$, $\hat{\sigma}_i(s(e)) \subset \{k+1, \ldots, n\}$.

Lorsque nous disposons d'un ensemble de permutations de décodage nous avons la méthode de décodage dont l'algorithme est le suivant :

pour i allant de 1 à $|P|$

– calcul de $\hat{\sigma}_i(y)$

– calcul de $S^{(i)} = H(\hat{\sigma}_i(y))^t$

si $W(S^{(i)}) \leqq t$

alors $\hat{\sigma}_i(c) = (\hat{\sigma}_i(y_1), \ldots, \hat{\sigma}(y_k)).G$

et $c = \hat{\sigma}_i(\hat{\sigma}_i(c))$

sinon continuer

Définition : Le code C corrige toutes les erreurs appartenant à E, par les permutations appartenant à P, lorsqu'à partir du mot reçu y, on sait retrouver le mot du code C, par un décodage par permutations.

Définition : On appelle un code C E-corrigible par permutations, un code qui corrige toutes les erreurs e appartenant à E, par permutations.

1. Décodage de certaines classes de codes de Reed-Solomon et de leurs images binaires

1.1. CAS DES CODES DE REED-SOLOMON ÉTENDUS SUR F_{2^m} DE DIMENSION $k=2^r$

Soit $C(n, k, d)$ un code de Reed-Solomon sur F_{2^m} et $\hat{C}(n+1, k, d+1)$ son étendu avec $k=2^r$, $r<m$.

Soit I l'ensemble des positions d'information de cardinal k, nous supposons que I est un sous-espace vectoriel de dimension r.

Nous utilisons l'espace quotient F_{2^m}/I dont les éléments s'écrivent $I_i = I + a_i$ avec a_i appartenant à F_{2^m}, cet ensemble est une partition de F_{2^m} et nous savons que le groupe des translations opère transitivement sur celui-ci.

Considérons l'ensemble E des erreurs e défini comme suit :

Pour tout e appartenant à E, il existe au moins i tel que $s(e) \cap I_i = \varnothing$.

En d'autres termes il existe une classe sans position d'erreur.

Nous avons le résultat suivant :

Proposition 1 : *Le code* C *est* E*-corrigible par le groupe des translations.*

Preuve : En effet, les codes de Reed-Solomon étendus sont invariants par le groupe des translations, et du fait que celui-ci est transitif s'il existe une classe qui ne contient pas de position d'erreur il existe une translation qui échange celle-ci et l'ensemble des positions d'information.

pour l'image binaire :Proposition 2 : *Tout paquet de longueur l, $l \leqq m(n+1)-2mk$ et poids binaire inférieur ou égal à mt est l'image binaire d'une erreur appartenant à* E.

Preuve : Soit $\mathcal{I}(e)$ l'image binaire d'une erreur appartenant à E, de longueur $m(n+1)$.

Soit l, la longueur du paquet; a, le nombre de composantes précédent le paquet; b, le nombre de composantes suivant le paquet :

$$m(n+1)-l=a+b.$$

Montrer que si $\mathcal{I}(e)$ n'appartient pas à $\mathcal{I}(\mathrm{E})$ alors $l>m(n+1)-2mk$ est équivalent à montrer la proposition 2.

Si $\mathcal{I}(e)$ n'appartient pas $\mathcal{I}(\mathrm{E})$ alors $a<km$ et $b<km$ car sinon $a \geqq km$ et $b \geqq km$ alors au moins une classe de $\mathcal{I}(\hat{\mathrm{C}})$ ne contient pas de position d'erreur et $\mathcal{I}(e)$ appartient à $\mathcal{I}(\mathrm{E})$, donc $m(n+1)-l<2km$, d'où $l>(n+1)m-2km$.

Par conséquent les paquets de longueur l, $l \leqq m(n+1)-2mk$ sont corrigés par permutations.

Pourcentage d'erreurs corrigibles par translations

Proposition 3 : *Soit* C(n, k, d) *t-correcteur,*

$$t=\left[\frac{d-1}{2}\right], \qquad n+1=sk.$$

Le pourcentage d'erreurs corrigibles par translation est :

$$p=\frac{\binom{s}{s-1}\binom{k(s-1)}{t}-\binom{s}{s-2}\binom{k(s-2)}{t}+\ldots+(-1)^{s-1}\binom{s}{1}\binom{k}{t}}{\binom{sk}{t}}.$$

Preuve : Pour évaluer le pourcentage d'erreurs corrigibles par translations, nous devons dénombrer les affectations de t erreurs, où aucune erreur n'apparaît dans au moins une des s classes de k éléments.

Il est plus simple de dénombrer les affectations de t erreurs où au moins une erreur apparaît dans chaque classe.

Nous avons :

$$u=\sum_{\substack{i_1 \geqq 0, \ldots, i_s \geqq 0 \\ i_1+i_2+\ldots+i_s=t}} \binom{k}{i_1}\binom{k}{i_2}\cdots\binom{k}{i_s}.$$

Le pourcentage est alors :

$$p=1-\frac{u}{\binom{sk}{t}},$$

où $\binom{sk}{t}$ est le nombre total d'affectations de t erreurs.

u est le coefficient de x dans le polynôme $((1+x)^k-1)^s$, or :

$$((1+x)^k-1)^s=\sum_{j \geqq 0}\binom{s}{j}(-1)^{s-j}\sum_{i \geqq 0}\binom{kj}{i}x^i,$$

d'où :

$$u=\sum_{j \geqq 0}\binom{s}{j}(-1)^{s-j}\binom{kj}{t},$$

donc :

$$p=\frac{\binom{s}{s-1}\binom{k(s-1)}{t}-\binom{s}{s-2}\binom{k(s-2)}{t}+\binom{s}{s-3}\binom{k(s-3)}{t}-\ldots-(-1)^{s-1}\binom{s}{1}\binom{k}{t}}{\binom{sk}{t}}.$$

1.2. Cas des codes de Reed-Solomon sur F_{2^m} de dimension k, k divise 2^{m-1}

Soit C(n, k, d), un code de Reed-Solomon de dimension k, k divise 2^m-1, et de capacité de correction t, $t=[(d-1)/2]$.

Supposons que l'ensemble des positions d'information I de cardinal k est un sous-groupe multiplicatif de $F_{2^m}^*$ d'ordre k.

Nous utilisons l'ensemble quotient $F_{2^m}^*/\mathrm{I}$ dont les éléments sont les classes $\mathrm{I}_i=\mathrm{I}.a_i$, avec a_i appartenant à $F_{2^m}^*$.

Cet ensemble est une partition de $F_{2^m}^*$ et nous savons que le groupe des multiplications opère transitivement sur celui-ci.

Dans cette situation nous envisageons un ensemble d'erreurs E défini de la façon suivante :

Pour tout e appartenant à E, il existe au moins i tel que $s(e) \cap I_i = \varnothing$, c'est-à-dire qu'il existe au moins i tel que $s(e) \cap I_i = \varnothing$, c'est-à-dire qu'il existe une classe qui ne contient pas de position d'erreur.

A partir de cette définition, nous avons le résultat suivant :

Proposition 4 : *Le code* C *est* E*-corrigible par multiplications (ou décalages circulaires).*

Preuve : En effet les codes de Reed-Solomon sont invariants par le groupe des multiplications, par le fait que celui-ci est transitif, s'il existe une classe qui ne contient pas de position d'erreur, il existe un multiplication qui échange celle-ci et l'ensemble des positions d'information.

Pour l'image binaire $\mathcal{I}(C)$, nous avons le résultat suivant :

Proposition 5 : *Tout paquet de longueur* l, $l \leqq mn - 2mk$ *et de poids binaire inférieur ou égal à* mt *est l'image binaire d'une erreur appartenant à* E.

La preuve est la même que celle de la proposition 2.

Par conséquent tous les paquets de longueur l, $l \leqq mn - 2\,mk$ sont corrigibles par multiplications.

Pourcentage d'erreurs corrigibles par multiplications.

Proposition 6 : *Soit* $C(n, k, d)$ *t-correcteur,*

$$t = \left[\frac{d-1}{2}\right], \qquad n = s.k,$$

Le pourcentage d'erreurs corrigibles par multiplications est :

$$p = \frac{\binom{s}{s-1}\binom{k(s-1)}{t} - \binom{s}{s-2}\binom{k(s-2)}{t} + \ldots + (-1)^{s-1}\binom{s}{1}\binom{k}{t}}{\binom{sk}{t}}.$$

La preuve est analogue à celle de la proposition 3.

2. Un exemple : le décodage du code de Reed-Solomon (16, 8, 9) et de son image binaire le (64, 32, 12)

INTRODUCTION

Soit le code de Reed-Solomon C (15, 8, 8) sur F_{2^4} et son étendu $\hat{C}(16, 8, 9)$. L'image binaire de C par rapport à la base TOB de F sur F (α^3, α^7, α^{12}, α^{13}) est le code $\mathcal{I}(\hat{C})$ (64, 32, 12) autodual, extrémal, à poids multiple de 4, comme l'a montré G. Pasquier [3].

Nous choisissons comme ensemble de positions d'information I, un hyperplan de F_{2^4}.

La matrice de $\hat{C}$ s'écrit $G = (I \mid M)$, avec :

$$H = \{0, 1, \alpha, \alpha^4, \alpha^2, \alpha^8, \alpha^5, \alpha^{10}\},$$

$$H = \{\alpha^3, \alpha^{14}, \alpha^9, \alpha^7, \alpha^6, \alpha^{13}, \alpha^{11}, \alpha^{12}\}.$$

ENSEMBLE DE PERMUTATIONS DE DÉCODAGE

Les codes de Reed-Solomon sont invariants par le groupe affine, l'ensemble de permutations de décodage de $\hat{C}$ est l'ensemble de 30 permutations de la forme suivante :

$$P = \{s^i \circ t^j;\ i \in [0, 14];\ j = 0, 1\},$$

où s est la translation par un élément du complémentaire de l' hyperplan (elle échanger un hyperplan et son complémentaire).

ENSEMBLE DE PERMUTATIONS DE DÉCODAGE POUR $\mathcal{I}(\hat{C})$

L'ensemble des permutations de décodage pour $\hat{C}$ induit les permutations de 1-64 pour $\mathcal{I}(\hat{C})$.

L'ensemble de ces 30 permutations est de la forme suivante :

$$\tilde{P} = \{\tilde{s}^i \circ \tilde{t}^j;\ i \in [0, 14];\ j = 0, 1\},$$

ots et $\tilde{t}$ sont induites respectivement par s et t, on montre que :

$\tilde{s}$: (1) (2) (3) (4) (5, 9, 17, 33, 13, 25, 49, 45, 21, 41, 29, 57, 61, 53, 37)

(6, 10, 18, 34, 14, 26, 50, 46, 22, 42, 30, 58, 62, 54, 38)

(7, 11, 19, 35, 15, 27, 51, 47, 23, 43, 31, 59, 63, 55, 39)

(8, 12, 20, 36, 16, 28, 52, 48, 24, 44, 32, 60, 64, 56, 40),

$\tilde{t}$: (1, 33) (2, 34) (3, 35) (4, 36) (5, 37) (6, 38) (7,39) (8,40) (9,41)

(10, 42) (11, 43) (12, 44) (13, 45) (14, 46) (15, 47) (16, 48) (17, 49)

(18, 50) (19, 51) (20, 52) (21, 53) (22, 54) (23, 55) (24, 56) (25, 57)
(26, 58) (27, 59) (28, 60) (29, 61) (30, 62) (31, 63) (32, 64).

DÉCODAGE DE $\hat{C}$ ET DE $\mathcal{I}(\hat{C})$

Pour le décodage du code de Reed-Solomon, nous avons le résultat suivant :

Proposition : *Il existe toujours une permutaton* $\hat{\sigma}_i$ *appartenant à* P *telle que* $W(S^{(i)}) \leqq 4$, *et toutes les erreurs sur* $\hat{C}$ *peuvent être corrigées par permutations :*

$$S^{(i)} = H(\hat{\sigma}_i(y))^t.$$

Preuve : Elle est basée sur le rang des positions de l'erreur (en tant qu'élément de l'EVF_{2^4}) :

– Si le rang des positions est inférieur ou égal à 4 alors il existe toujours un hyperplan qui les contient, donc il existe au moins une permutation de l'ensemble de permutations de décodage qui envoie les positions à l'extérieur des positions d'information.

– Si le rang des positions est égal à 4 : soit $\langle x, y \rangle$ le produit scalaire de x par y sur F_{2^4}.

L'équation du complémentaire d'un hyperplan étant $\langle a, x \rangle = 1$, nous obtenons un système de quatre équations à quatre inconnues de rang 4, il a une solution unique. Il existe donc un complémentaire d'hyperplan qui contient ces quatre positions et il existe toujours une permutation de l'ensemble des permutations de décodage qui envoie ces positions à l'extérieur des positions d'information.

Nous ramenons l'étude du décodage de l'image binaire $\mathcal{I}(\hat{C})$ qui est 5-correcteur à celle du décodage de $\hat{C}$. Remarquons que cinq positions sur le code $\mathcal{I}(\hat{C})$ correspondent au plus à cinq positions sur le code $\hat{C}$.

Proposition : *Toutes les erreurs sur l'image bianaire* $\mathcal{I}(\hat{C})$ *peuvent être corrigées soit par permutations, soit en utilisant une rapide lecture de table.*

Preuve : Si le rang des positions de l'erreur est inférieur ou égal à 4, par le même argument que précédemment il existe au moins un hyperplan qui les contient et les erreurs sont corrigées par permutations.

– Si le rang des positions de l'erreur est égal à 4 : cinq positions dans un espace vectoriel de dimension 4 ont pour rang maximal 4. L'équation du complémentaire d'un hyperplan est $\langle a, x \rangle = 1$. Nous obtenons un système de cinq équations à cinq inconnues de rang 4, deux cas se présentent :

– Il y a compatibilité de la cinquième équation avec les quatre précédentes, dans ce cas il existe un complémentaire d'hyperplan qui contient ces positions et il existe une permutation de l'ensemble de permutations de décodage qui envoie les positions erronées hors des positions d'information.

– Il y a incompatibilité de la cinquième équation avec les précédentes dans ce cas il existe un complémentaire d'hyperplan qui contient quatre positions et un hyperplan qui en contient une.

Dans ce cas nous utilisons une lecture de table comme suit :

Soit e le mot erreur $e = (e_1 \mid e_2)$ avec poids binaire de e_1 est égal à 4 et poids binaire de e_2 est égal à 1.

Le syndrome :

$$S = (e_1 \mid e_2).G = (e_1 \mid e_2).(I \mid M) = e_1 + e_2.M.$$

e est le seul vecteur de poids binaire 5 tel que $S = e_1 + e_2.M$.

Nous tabulons tous les vecteurs u de longueur $n/2$ et de poids bianaire 1, et tous les produits $u.M$.

Dans la table $(u \mid u.M)$, nous cherchons u tel que $d(u.M, S) = 4$.

Cette table ne comporte que 32 vecteurs (annexe).

ALGORITHME DE DÉCODAGE

pour i allant de 1 à 30
  – calcul du syndrome $S^{(i)} = H(\hat{\sigma}_i(y))^t$
    si $W(S^{(i)}) \leqq 4$
    alors $c = \hat{\sigma}_i^{-1}(\hat{\sigma}_i(y) + (0, S^{(i)}))$
  sinon continuer
pour i allant de 1 à 30
  – calcul de $D = d(u_1.M, S)$
  si $D = 4$
    alors $u_1 = S + u_2.M$
      et $e = \hat{\sigma}_i^{-1}(u_1 \mid u_2)$
    sinon continuer.

si D n'est jamais égal à 4 alors une erreur non corrigible est détectée.

Conclusion

Nous avons montré que certains codes de Reed-Solomon étendus ou non sont décodables par permutations, en utilisant pour l'ensemble des positions d'information une structure de sous-espace vectoriel ou de sous-groupe multiplicatif. Cette étude pourrait être poursuivie dans le cas d'autres structures.

Une application pourrait être la réalisation d'un décodeur utilisant parallèlement un décodage par permutations et un autre décodage.

BIBLIOGRAPHIE

[1] 1] J. MacWilliams et Sloane, *The theory of error coreecting codes*, North Holland, Amsterdam, 1977.

[2] J. Wolfmann, A permutation decoding of the (24, 12, 8) Golay code, *IEEE on information theory*, 19, n° 5, septembre 1983.

[3] G. Pasquier, Binaryimages of some self dual codes over GF(2) with respect to trace orthogonal basis, *IEEE on information theory*, 37, n° 1, 1981.

Annexe I

Codes de Reed-Solomon étendus sur F_{2^m}

n	k	d	t	$\frac{p}{(\%)}$
8	2	7	3	100
8	4	5	2	43
16	2	15	7	100
16	4	13	6	45, 10
16	8	9	4	2
32	2	31	15	100
32	4	29	14	56, 88

Annexe II

Table (U/U.M)

U 10	U.M 10
α^3 0 0 0 0 0 0 0	1 α^4 α^9 α^{11} α^{12} α^5 α^7 α^6
0 α^3 0 0 0 0 0 0	α^4 1 α^{11} α^9 α^5 α^{12} α^6 α^7
0 0 α^3 0 0 0 0 0	α^9 α^1 1 α^4 α^7 α^6 α^{12} α^5
0 0 0 α^3 0 0 0 0	α^{11} α^9 α^4 1 α^6 α^7 α^5 α^{12}
0 0 0 0 α^3 0 0 0	α^{12} α^5 α^7 α^6 1 α^4 α^9 α^{11}
0 0 0 0 0 α^3 0 0	α^5 α^{12} α^6 α^7 α^4 1 α^{11} α^9
0 0 0 0 0 0 α^3 0	α^6 α^7 α^{12} α^5 α^9 α^{11} 1 α^4
0 0 0 0 0 0 0 α^3	α^6 α^7 α^5 α^{12} α^{11} α^9 α^4 1
α^7 0 0 0 0 0 0 0	α^4 α^8 α^{13} 1 α α^9 α^{11} α^{10}
0 α^7 0 0 0 0 0 0	α^8 α^4 1 α^{13} α^9 α α^{10} α^{11}
0 0 α^7 0 0 0 0 0	α^{13} 1 α^4 α^8 α^{11} α^{10} α α^9
0 0 0 α^7 0 0 0 0	1 α^{13} α^8 α^4 α^{10} α^{11} α^9 α
0 0 0 0 α^7 0 0 0	α α^9 α^{11} α^{10} α^4 α^8 α^{13} 1
0 0 0 0 0 α^7 0 0	α^9 α α^{10} α^{11} α^8 α^4 1 α^{13}
0 0 0 0 0 0 α^7 0	α^{11} α^{10} α α^9 α^{13} 1 α^4 α^8
0 0 0 0 0 0 0 α^7	α^{10} α^{11} α^9 α 1 α^{13} α^8 α^4
α^{12} 0 0 0 0 0 0 0	α^9 α^{13} α^3 α^5 α^6 α^{14} α 1
0 α^{12} 0 0 0 0 0 0	α^{13} α^9 α^5 α^3 α^{14} α^6 1 α
0 0 α^{12} 0 0 0 0 0	α^3 α^5 α^9 α^{13} α 1 α^6 α^{14}
0 0 0 α^{12} 0 0 0 0	α^5 α^3 α^{13} α^9 1 α α^{14} α^6
0 0 0 0 α^{12} 0 0 0	α^6 α^{14} α 1 α^9 α^{13} α^3 α^5
0 0 0 0 0 α^{12} 0 0	α^{14} α^6 1 α α^{13} α^9 α^5 α^3
0 0 0 0 0 0 α^{12} 0	α 1 α^6 α^{14} α^3 α^5 α^9 α^{13}
0 0 0 0 0 0 0 α^{12}	1 α α^{14} α^6 α^5 α^3 α^{13} α^9
α^{13} 0 0 0 0 0 0 0	α^{10} α^{14} α^4 α^6 α^7 1 α^2 α
0 α^{13} 0 0 0 0 0 0	α^{14} α^{10} α^6 α^4 1 α^7 α α^2
0 0 α^{13} 0 0 0 0 0	α^4 α^6 α^{10} α^{14} α^2 α α^7 1
0 0 0 α^{13} 0 0 0 0	α^6 α^4 α^{14} α^{10} α α^2 1 α^7
0 0 0 0 α^{13} 0 0 0	α^7 1 α^2 α α^{10} α^{14} α^4 α^6
0 0 0 0 0 α^{13} 0 0	1 α^7 α α^2 α^{14} α^{10} α^6 α^4
0 0 0 0 0 0 α^{13} 0	α^2 α α^7 1 α^4 α^6 α^{10} α^{14}
0 0 0 0 0 0 0 α^{13}	α α^2 1 α^7 α^6 α^4 α^{14} α^{10}