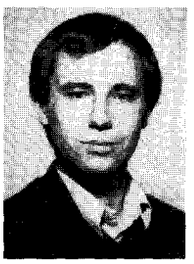
Une nouvelle méthode de décodage des codes de Reed-Solomon

A new method for decoding Reed-Solomon codes



Jean-Louis DORNSTETTER

Laboratoire Central de Télécommunications, 18-20, rue Grange-Dame-Rose, 78140 VÉLIZY-VILLACOUBLAY

Ingénieur au LCT depuis 1982, il a participé à la définition de systèmes de transmissions résistant au brouillage et à la mise au point d'un récepteur de radionavigation GPS/NAVSTAR. Il s'intéresse présentement à la conception de décodeurs algébriques à hautes performances.

RÉSUMÉ

On montre qu'une propriété fondamentale de la matrice de contrôle de parité des codes de Reed-Solomon permet de formuler une équation caractéristique du décodage différente de l'équation classique due à Berlekamp [1].

On présente un algorithme efficace pour la résolution de cette nouvelle équation.

MOTS CLÉS

Codes de Reed-Solomon, équation caractéristique du décodage, décodage algébrique.

SUMMARY

We show that a basic property of the parity check matrix of Reed-Solomon codes yields a new key-equation for the decoding problem that is different from the classical one given by Berlekamp.

We present an efficient algorithm for solving this new key-equation.

KEY WORDS

Reed-Solomon codes, key-equation, algebraic decoding.

TABLE DES MATIÈRES

Introduction

Berlekamp a introduit récemment [2] une nouvelle structure pour réaliser des encodeurs systématiques pour les codes de Reed-Solomon définis sur des corps de caractéristique 2.

Il en résulte que la complexité de l'encodeur, et corrélativement de celle de la partie du décodeur qui calcule le syndrome, peut être rendue très faible.

Il existe plusieurs définitions équivalentes du syndrome d'un mot d'un code de Reed-Solomon entaché d'erreurs.

La plus classique [1] est la suivante:

$$S_i = C(\alpha_i), \qquad i = 0, 1, \ldots, s-1,$$

où $C(X)$ est le polynôme représentant le mot reçu et les α_i sont les racines du polynôme générateur $g(X)$.

On montre alors que la résolution du problème suivant:

Trouver deux polynômes $N(X)$ et $D(X)$ tels que:

$$D(X)\left\{\sum_{i=0}^{s-1} S_i X^i\right\} \equiv N(X)\,[X^s],\ d^0 N < d^0 D \leqq \left[\frac{s}{2}\right]$$

($a \equiv b\ [c]$ pour « a congru à b modulo c ») permet de corriger $[s/2]$ erreurs par des méthodes algébriques de complexité $O(s^2)$.

La résolution de ce problème peut être effectuée à l'aide de l'algorithme de Berlekamp [1] ou à l'aide de l'algorithme d'Euclide étendu [3], les deux méthodes étant virtuellement équivalentes [4].

Si on utilise pour le calcul du syndrome un encodeur ayant la structure suggérée en [2], le syndrome disponible est le polynôme R de degré $< s$ tel que :

$$R(\alpha_i) = S_i, \qquad i = 0, \ldots, s-1.$$

L'utilisation des méthodes classiques impose une première étape qui consiste à calculer, à partir des coefficients du polynôme $R(X)$ les valeurs des S_i.

On présente ici une méthode de décodage qui évite ce calcul, qui grève notablement le budget du temps de décodage dans le cas où le mot reçu est entaché de peu d'erreurs.

L'existence d'une telle méthode a été indiquée par Welch et Berlekamp lors d'un exposé au congrès *IEEE Symposium on Information Theory*, 1983 [5].

Notations

Nous nous restreindrons aux codes de Reed-Solomon définis sur des corps de caractéristique 2, l'extension des résultats du cas général étant directe.

Comme précédemment, on note $a \equiv b\ [c]$ pour « a congru à b modulo c ». F_{2^m} désigne le corps de Galois de cardinalité 2^m.

Soit un code de Reed-Solomon défini sur F_{2^m} de paramètres (n, k, d) avec $n = 2^m - 1$, k la dimension du code et $d = n - k + 1$ sa distance minimale [1, 3].

On note $s = n - k$ et on suppose que le code admet pour polynôme générateur:

$$g(X) = \prod_{i=0}^{s-1} (X + \alpha^{W+i}) = X^s + g_{s-1} X^{s-1} + \ldots + g_0,$$

α étant une racine primitive n-ième de l'unité dans F_{2^m} et W un entier, choisi généralement pour rendre $g(X)$ symétrique:

$$g(X) = X^s g(X^{-1}).$$

On pose $\alpha_i = \alpha^{W+i}$ et on appelle $R(X)$ le reste de la division polynômiale du mot reçu par $g(X)$.

On a donc:

$$\sum_{j \text{ en erreur}} E_j X^j \equiv R(x)\,[g(X)].$$

E_j étant l'amplitude (valeur) de l'erreur affectant la position j.

On désigne par $r_0, \ldots, r_{s-1}$ les coefficients de ce reste:

$$R(X) = r_{s-1} X^{s-1} + \ldots + r_0$$

(comme indiqué dans l'introduction, il existe des méthodes très performantes pour obtenir $r_{s-1}, r_{s-2}, \ldots, r_0$).

Les éléments non nuls de F_{2^m} sont $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ et servent à énumérer les coordonnées des mots de code.

On note enfin $a \mid b$ pour « a divise b ».

1. Factorisation de la matrice de contrôle des codes de Reed-Solomon

On peut montrer [3] que le vecteur colonne $\begin{pmatrix} C_0 \\ \vdots \\ C_{n-1} \end{pmatrix}$ représente un mot du code considéré si et seulement si on a l'égalité matricielle:

$$L\begin{pmatrix} C_0 \\ \vdots \\ C_{n-1} \end{pmatrix} = 0,$$

où L est une matrice à s lignes et n colonnes, dite de contrôle de parité, dont l'élément générique est $L_{ij} = \alpha_i^j$ (L est une matrice de Van der Monde).

Dans le cas d'un codage systématique, les éléments $C_0, \ldots, C_{s-1}$ sont redondants, l'information utile étant $C_s, \ldots, C_{n-1}$.

Il existe une forme équivalente pour la matrice L qui est la suivante:

$$H = (I_s \mid U),$$

où I_s désigne la matrice identité d'ordre s et U est une matrice à s lignes et k colonnes dont l'élément générique U_i^j (i-ième ligne, j-ième colonne) est défini par les relations:

$$X^{j+s} \equiv \sum_{i=0}^{s-1} U_i^j X^i \,[g(X)], \qquad j = 0, \ldots, k-1.$$

Tout mot de code vérifie $H\begin{pmatrix} C_0 \\ \vdots \\ C_{n-1} \end{pmatrix} = 0$ et réciproquement.

Les deux définitions du syndrome évoquées dans l'introduction correspondent respectivement à:

$$\begin{pmatrix} S_0 \\ \vdots \\ S_{s-1} \end{pmatrix} = L\begin{pmatrix} t_0 \\ \vdots \\ t_{n-1} \end{pmatrix},$$

$$\begin{pmatrix} r_0 \\ \vdots \\ r_{s-1} \end{pmatrix} = H\begin{pmatrix} t_0 \\ \vdots \\ t_{n-1} \end{pmatrix},$$

$t_0, \ldots, t_{n-1}$ étant les symboles reçus.

La méthode de décodage proposée repose sur le théorème suivant:

Théorème 1 : *Il existe deux matrices diagonales* D *et* D′ *de dimensions respectives s et k telles que:*

$$U = DCD',$$

où C *est une matrice de Cauchy* (1).

Ceci est une propriété « forte » qui lie la forme canonique réduite d'une matrice de Van der Monde à une matrice de Cauchy. (Ces deux types de matrices sont des exemples classiques de matrices dont tous les déterminants mineurs sont non nuls.)

On remarquera que la j-ième colonne de H représente le reste de la division de X^j par $g(X)$. La démonstration procède par exhibition de D et preuve que $D^{-1}H$ est bien de la forme CD′; elle repose sur le lemme suivant:

Lemme 1: *Soit:*

$$P_j(X) = \sum_{i=0}^{s-1} (\alpha_i + \alpha_{j+s}) U_i^j X^i, \qquad j = 0, \ldots, k-1,$$

alors:

$$P_j(\alpha_i) = 0, \qquad i = 0, 1, \ldots, s-2.$$

Preuve du lemme 1 : On a :

$$X^{j+s} = Q_j(X)\, g(X) + \sum_{i=0}^{s-1} U_i^j X^i$$

pour un certain $Q_j(X)$, d'où :

$$\alpha^{j+s} X^{j+s} = Q_j(\alpha X)\, g(\alpha X) + \sum_{i=0}^{s-1} \alpha^i U_i^j X^i,$$

comme $\alpha_i = \alpha^{W+i}$ on a également:

$$\begin{aligned} P_j(X) &= \alpha_0 \left(\sum_{i=0}^{s-1} \alpha^i U_i^j X^i + \alpha^{j+s} \sum_{i=0}^{s-1} U_i^j X^i \right) \\ &= \alpha_0 \{ \alpha^{j+s} X^{j+s} + Q_j(\alpha X)\, g(\alpha X) \\ &\quad + \alpha^{j+s} X^{j+s} + \alpha^{j+s} Q_j(X)\, g(X) \} \\ &= \alpha_0 Q_j(\alpha X)\, g(\alpha X) + \alpha_{j+s} Q_j(X)\, g(X). \end{aligned}$$

Mais:

$$g(X) = g(\alpha X) = 0 \text{ pour } X = \alpha_0, \alpha_1, \ldots, \alpha_{s-2}. \quad \square$$

(1) Une matrice de Cauchy admet un élément générique de la forme:

$$C_{ij} = \frac{1}{x_i + y_j}.$$

On notera que l'hypothèse « les racines de $g(X)$ sont consécutives » est essentielle dans la dernière étape de la démonstration.

Preuve du théorème 1: Il résulte du lemme 1 que chacun des P_j est un multiple (non trivial) du polynôme:

$$Q(X)=g(X)/(X+\alpha_{s-1}).$$

Il existe donc k constantes non nulles n_j telles que:

$$P_j(X)=n_j Q(X), \qquad j=0, \ldots, k-1.$$

On pose :

$$P_0(X)=\sum_{i=0}^{s-1} p_i X^i \qquad (p_i=g_i(\alpha_i+\alpha_s), i=0, \ldots, s-1).$$

Alors:

$$U_i^j(\alpha_i+\alpha_{j+s})=p_i n_j.$$

On en déduit la factorisation de la matrice U énoncée dans le théorème 1, avec:

$$D_{ii}=p_i,\ D'_{jj}=n_j \qquad \text{et} \qquad C_{ij}=1/(\alpha_i+\alpha_{j+s}).$$

Tous les p_i sont non nuls du fait que $g_i \neq 0$. (Le polynôme générateur $g(X)$ est un mot du code dont le poids est $s+1=d$ car le code est MDS [3].) □

2. La nouvelle équation caractéristique du décodage

On pose :

$$m_i=r_i/p_i, \qquad i=0, \ldots, s-1.$$

Supposons que le mot reçu ne comporte qu'une seule erreur en position l d'amplitude E_l.

cas (1) $0 \leqq l \leqq s-1$ (erreur dans une position de redondance).

Dans ce cas, tous les m_i sont nuls sauf $m_l=E_l/p_l$.

cas (2) $l \geqq s$ (erreur dans une position d'information).

Alors:

$$m_i=n_{l-s}E_l/(\alpha_i+\alpha_l)$$

par le théorème 1.

Dans tous les cas, si on pose $D(X)=X+\alpha_l$, on a les relations:

$$m_i D(\alpha_i)=\text{Cte}, \qquad i=0, \ldots, s-1,$$

la valeur de la constante étant zéro dans le cas (1), $n_{l-s}E_l$ dans le cas (2).

On peut réécrire les relations précédentes sous la forme:

$$m_i D(X) \equiv N(X)\,[X+\alpha_i],\ i=0, \ldots, s-1,$$

avec $d^0 D=1$, $d^0 N<1$.

La généralisation de cette équation est donnée par le résultat suivant:

Théorème 2: *Si le mot reçu est entaché de t erreurs, avec* $2t \leqq s$, *alors le problème suivant:*

Trouver un couple de polynômes $N(X)$, $D(X)$ *tel que:*

- $m_i D(X) \equiv N(X)\,[X+\alpha_i]$, $i=0, \ldots, s-1$;
- Sup $(d^0 D, 1+d^0 N)$ *minimal.*

possède une solution unique (à une constante près) qui vérifie $d^0 D=t$ *et* $D(\alpha_l)=0$ *si et seulement si le l-ième symbole reçu est erronné.*

La preuve du théorème 2 est basée sur deux lemmes. On suppose que les t erreurs affectent les symboles correspondant à $\alpha_{k_1}, \ldots, \alpha_{k_t}$ avec des amplitudes $E_1, \ldots, E_t$.

Lemme 2: *Le problème du théorème* 2 *privé de la contrainte de minimalité de degré admet une solution pour laquelle:*

$$D(X)=\prod_{i=1}^{t}(X+\alpha_{k_i})$$

Preuve du lemme 2: Par récurrence sur t. Le cas $t=1$ a déjà été prouvé.

Si la propriété est vraie pour $t \leqq h-1<[s/2]$ et que l'on rajoute une h-ième erreur en α_{k_h} de valeur E_h, il est simple de vérifier que le couple:

$$(X+\alpha_{k_h})N+aD, \qquad (X+\alpha_{k_h})D,$$

vérifie les conditions requises avec $a=0$ si $k_h<s$, $a=E_h n_{k_h-s}$ sinon, (N, D) étant le couple de polynômes déduit de l'hypothèse de récurrence pour les $h-1$ premières erreurs. □

Une expression explicite du polynôme $N(X)$ que la construction précédente fournit est:

$$N(X)=\prod_{k_i<s}(X+\alpha_{k_i})\Big(\sum_{k_i \geqq s} n_{k_i-s}.E_i.\prod_{j\neq i}(X+\alpha_{k_j})\Big).$$

On note E_l l'ensemble des couples $(N(X), D(X))$ qui vérifient:

$$\{D \neq 0, m_i D(X) \equiv N(X)\,[X+\alpha_i],\ i=0, \ldots, l-1\}$$

sans autre restriction.

On définit:

$$d^0(N, D)=\text{Sup}(d^0 D, 1+d^0 N).$$

Par convention, on notera $(N, D) /\!/ (N', D')$ si $ND'=N'D$ et $(N, D) \not/\!/ (N', D')$ sinon.

Lemme 3: *Si:*

$$(N, D) \in E_l,$$
$$(N', D') \in E_l \qquad \textit{et} \qquad (N, D) \not/\!/ (N', D'),$$

alors on a:

$$d^0(N, D)+d^0(N', D') \geqq l+1.$$

Preuve du lemme 3: On considère le polynôme $ND' + N'D$. Sous les hypothèses du lemme 3, ce polynôme est congru à zéro modulo $(X+\alpha_i)$, $i=0, \ldots, l-1$. C'est donc un multiple non trivial de $\prod_{i=0}^{l-1} (X+\alpha_i)$ et le résultat découle de simples considérations de degré; [il y a plusieurs cas à distinguer, vu la définition de $d^0(N, D)$].

Preuve du théorème 2: Il suffit de montrer que le couple (N, D) indiqué par le lemme 2 est bien la solution de degré minimal, à une constante près, si $2t \leqq s$.

On a $d^0(N, D) = t$. Supposons qu'une autre solution (A, B) de degré $\leqq t$ existe pour le problème du théorème 2.

Alors le lemme 3 implique que l'on a $(A, B) /\!\!/ (N, D)$ car $2t \leqq s$ et les deux couples sont éléments de E_s.

On peut alors écrire:

$$A = u N_0, \qquad B = u D_0,$$
$$N = v N_0, \qquad D = v D_0,$$

avec PGCD $(N_0, D_0) = 1$ et $d^0 u \leqq d^0 v$.

Le théorème 2 est établi si l'on parvient à montrer $u = v$ à une constante près. Pour cela il suffit de montrer que $v \mid u$.

Par construction, D est un diviseur de X^n+1 et n'admet donc que des racines simples dans F_{2^m}.

On sait également [*voir* l'expression explicite de N(X)] que:

$$v(X) = \prod_{k_i < s} (X + \alpha_{k_i}).$$

Le polynôme v admet donc toutes ses racines (simples) dans l'ensemble $\alpha_0, \ldots, \alpha_{s-1}$. On va montrer que toute racine α_l de v est également une racine de u.

D n'ayant que des racines simples,

$$v(\alpha_e) = 0 \quad \Rightarrow \quad D_0(\alpha_l) \neq 0.$$

Considérons la configuration de $t-1$ erreurs déduite de la précédente par suppression de l'erreur en α_l, qui correspond à une erreur dans une position de redondance. Toutes les valeurs des m_i restent inchangées sauf pour $i = l$.

Le couple (N', D') déduit de (N, D) par suppression du facteur commun $(X+\alpha_l)$ vérifie:

$$N'(\alpha_i) = m'_i D'(\alpha_i), \qquad i = 0, \ldots, s-1,$$

avec $m'_i = m_i$ sauf pour $i = l$.

Mais $N_0 \mid N'$, $D_0 \mid D'$ et comme $D'(\alpha_l) \neq 0$ on a:

$$N_0(\alpha_l) = m'_l D_0(\alpha_l).$$

Maintenant, si α_l n'est pas un zéro de u, on a aussi $N_0(\alpha_l) = m_l D_0(\alpha_l)$, une contradiction qui prouve que v divise u et le théorème 2 est établi. □

Nous allons développer un algorithme qui permet de résoudre efficacement le problème mentionné dans l'énoncé du théorème 2, qui est la nouvelle équation caractéristique du décodage.

3. Algorithme de résolution de l'équation caractéristique

Le problème est de trouver deux polynômes N(X), D(X) tels que:

$$m_i D(\alpha_i) = N(\alpha_i), \qquad i = 0, \ldots, s-1,$$

en minimisant $\mathrm{Sup}(d^\circ D, 1 + d^\circ N)$.

Une première approche consiste à poser [2]:

$$T(X) = \sum_{i=0}^{s-1} \left\{ m_i \cdot \prod_{\substack{j=0 \\ j \neq i}}^{s-1} (X+\alpha_j) \Big/ \prod_{\substack{j=0 \\ j \neq i}}^{s-1} (\alpha_j + \alpha_i) \right\}$$

et à chercher à résoudre la congruence:

$$T(X) D(X) \equiv N(X) [g(X)],$$

avec $d^0(N, D)$ minimal.

Cette congruence peut être résolue à l'aide de l'algorithme d'Euclide étendu avec l'initialisation $R_{-1} = g$, $R_0 = T$.

Cette approche est correcte mais ne présente pas d'avantages majeurs par rapport à la méthode traditionnelle car le passage des valeurs de m_i aux coefficients de T(X) nécessite un calcul au moins aussi coûteux que le calcul du syndrome classique:

$$S_i = \sum_{j=0}^{s-1} r_j \alpha_i^j, \qquad i = 0, \ldots, s-1.$$

Il existe une approche plus efficace que nous allons introduire maintenant.

On pose :

$$d_j = \min_{(A, B) \in E_j} d^0(A, B),$$
$$H_j(X) = \prod_{i=0}^{j-1} (X + \alpha_i),$$
$$\bar{E}_j = \{ (A, B) \in E_j / d^0(A, B) = d_j \}.$$

On remarque que d_j est une fonction non décroissante de j et que l'on a les inclusions $\bar{E}_j \subset E_j$, $E_{j+1} \subset E_j$.

Lemme 4: *Si* $(N, D) \in \bar{E}_j$ *et* $2d_j \leqq j$, *alors l'ensemble* $\bar{E}_j$ *est formé des multiples de* (N, D) *par un élément non nul de* F_{2^m}.

---

[2] T(X) est simplement l'interpolateur de Lagrange associé aux points $(\alpha_0, \ldots, \alpha_{s-1})$ et aux valeurs $(m_0, \ldots, m_{s-1})$: $T(\alpha_i) = m_i$.

Preuve du lemme 4: Soient (A, B) et (C, D) deux éléments de $\bar{E}_j$.

Le lemme 3 et la condition $2d_j \leqq j$ entraînent alors $AD = BC$.

On peut donc écrire:

$$A = u N_0, \qquad B = u D_0, \qquad C = v N_0, \qquad D = v D_0,$$

avec PGCD $(N_0, D_0) = 1$.

(A, B) étant de degré minimal, on a $u \mid H_j$. De même $v \mid H_j$.

Soit α_l une racine de u; alors $N_0(\alpha_l) \neq m_l D_0(\alpha_l)$ sans quoi on pourrait obtenir une solution de plus petit degré en divisant A et B par $(X + \alpha_l)$.

Celà entraîne $v(\alpha_l) = 0$, et donc $u \mid v$. Par les mêmes arguments $v \mid u$, d'où le résultat. □

La condition $2d_j \leqq j$ suffit donc à garantir l'unicité de la solution partielle au rang j à une constante près.

Lemme 5: *Si* $(N, D) \in \bar{E}_j$, $(N, D) \notin E_{j+1}$ *et* $2d_j \leqq j$, *alors:*

$$d_{j+1} = d_j + 1.$$

Preuve du lemme 5: On a $d_{j+1} \leqq d_j + 1$ car le couple $((X + \alpha_j) N, (X + \alpha_j) D)$ est bien élément de E_{j+1}.

Il reste à exclure $d_{j+1} = d_j$.

Si l'on suppose $d_{j+1} = d_j$, alors tout élément (A, B) de $\bar{E}_{j+1}$ est aussi dans E_j. Le lemme 4 entraîne alors $(A, B) = (N, D)$ à une constante près, ce qui contredit l'hypothèse $(N, D) \notin E_{j+1}$. □

On remarque que, sous les hypothèses du lemme 5, la condition $2d_j < j$ entraîne (*cf.* lemme 4) que $((X + \alpha_j) N, (X + \alpha_j) D)$ est le seul élément de $\bar{E}_{j+1}$.

On va maintenant montrer qu'il est simple de construire une suite de solutions partielles optimales (dans $\bar{E}_j$) à l'aide d'une suite de solutions auxilliaires (non optimales).

Théorème 3: *L'algorithme suivant permet de construire deux suites de couples éléments de* $E_j (j = 0, 1, \ldots, s)$ *qui vérifient:*

$$(N_j, D_j) \in \bar{E}_j, \qquad (N'_j, D'_j) \in E_j,$$
$$d^0(N'_j, D'_j) = j + 1 - d_j,$$
$$N_j D'_j + N'_j D_j = H_j.$$

Algorithme: *Initialisation:* $j = 0$: $N_0 = D'_0 = 0$, $D_0 = N'_0 = 1$, $d_0 = 0$.

Procéder ensuite de proche en proche, $j = 0, 1, \ldots, s-1$: *on pose:*

$$s_j = m_j D_j(\alpha_j) + N_j(\alpha_j),$$
$$t_j = m_j D'_j(\alpha_j) + N'_j(\alpha_j),$$

trois cas sont à distinguer:

(*a*) $s_j = 0$: $d_{j+1} = d_j$:

$$(N_{j+1}, D_{j+1}) = (N_j, D_j),$$
$$N'_{j+1} = (X + \alpha_j) N_j, \qquad D'_{j+1} = (X + \alpha_j) D_j.$$

(*b*) $s_j \neq 0$ et $2d_j \leqq j$: $d_{j+1} = d_j + 1$:

$$N_{j+1} = (X + \alpha_j) N_j, \qquad D_{j+1} = (X + \alpha_j) D_j,$$
$$N'_{j+1} = N'_j + t_j s_j^{-1} N_j,$$
$$D'_{j+1} = D'_j + t_j s_j^{-1} D_j.$$

(*c*) $s_j \neq 0$ et $2d_j = j + 1$: $d_{j+1} = d_j$:

$$N_{j+1} = N'_j + t_j s_j^{-1} N_j,$$
$$D_{j+1} = D'_j + t_j s_j^{-1} D_j,$$
$$N'_{j+1} = (X + \alpha_j) N_j, \qquad D'_{j+1} = (X + \alpha_j) D_j.$$

Il n'est pas nécessaire de calculer t_j si $s_j = 0$; de même on peut vérifier que le calcul de N'_{j+1} et D'_{j+1} peut être omis dès que $2d_j \leqq 2j - s$.

Ces simplifications, importantes quand il y a peu d'erreurs, n'ont pas été incluses dans l'énoncé de l'algorithme par souci de clarté.

Preuve du théorème 3: Il convient de montrer qu'après chaque étape on a bien les propriétés annoncées quel que soit le choix (*a*), (*b*) ou (*c*) effectué.

On vérifie aisément que:

$$(N'_j + t_j s_j^{-1} N_j, D'_j + t_j s_j^{-1} D_j) \in E_{j+1}$$

et que $N_j D'_j + N'_j D_j = H_j$ (récurrence sur j).

Il faut prouver que la quantité d_j calculée par l'algorithme précédent est correcte. Là encore, on montre ceci par récurrence sur j. Seule l'étape (*b*) conduisant à une augmentation de d_j, la propriété est vraie au rang $j+1$ si elle l'est au rang j et si l'on effectue les choix (*a*) ou (*c*); le lemme 5 montre qu'elle l'est également lorsque l'on effectue le choix (*b*). Le reste de la preuve découle alors de simples considérations de degrés. □

La méthode de décodage proposée pour les codes de Reed-Solomon est donc la suivante:

(1) Calculer le syndrome $r_0, r_1, \ldots, r_{s-1}$.

(2) Poser:

$$m_i = r_i / g_i(\alpha_i + \alpha_s), \qquad i = 0, \ldots, s-1.$$

(3) Utiliser l'algorithme précédent pour trouver un couple (N_s, D_s) de $\bar{E}_s$.

(4) Calculer $f(X) = \text{PGCD}\ (N_s, D_s)$.

Par construction, $f(X)$ divise $g(X)$. Soit $l = d^0 f$ et soient $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_l}$ les racines de f. Il y a eu l erreurs dans les positions de redondance $i_1, \ldots, i_l$.

(5) Soit $N_s = f N$, $D_s = f D$.

Calculer les racines de D parmi les éléments $\alpha_s, \ldots, \alpha_{n-1}$.

Si le nombre de racines distinctes trouvées dans $\alpha_s, \ldots, \alpha_{n-1}$ est inférieur à $d_s - l$, on détecte l'occurence de plus de $[s/2]$ erreurs.

Dans le cas contraire $D = \prod_{j=1}^{e} (X + \alpha_{i_j})$ avec $i_j \geqq s$ et $e = d^0 D = d_s - l$.

(6) Décomposer la fraction $N(X)/D(X)$ en éléments simples :

$$\frac{N(X)}{D(X)} = \sum_{j=1}^{e} \frac{a_j}{X+\alpha_{i_j}}.$$

$D'(X)$ désignant la dérivée formelle de $D(X)$, on peut calculer les a_j par la formule :

$$a_j = \frac{N(\alpha_{i_j})}{D'(\alpha_{i_j})}.$$

La valeur de l'erreur en position α_{i_j} est alors donnée par :

$$E_j = a_j n_{i_j-s}^{-1}.$$

Si on désire connaître la valeur des erreurs dans les positions de redondance on peut les calculer par la formule :

$$E_j = r_j + g_j(\alpha_j+\alpha_s)\frac{N(\alpha_j)}{D(\alpha_j)},$$
$$j = i_1, \ldots, i_l.$$

Exemple : Nous allons illustrer ce qui précède sur un exemple.

$m=4$, $n=15$, $s=8$, $W=2$.

α désigne une racine primitive 15e de l'unité dans F_{16} vérifiant $\alpha^4=\alpha+1$.

On a donc :

$$g(X)=(X+\alpha^2)(X+\alpha^3)\ldots(X+\alpha^9).$$

Ce code a pour paramètres (15, 7, 9) et corrige quatre erreurs.

On a :

$$g(X)=X^8+X^7+\alpha^4X^6+\alpha^7X^5 + \alpha^6X^4+\alpha^3X^3+\alpha^{11}X^2+\alpha^3X+\alpha^{14}.$$

Les matrices D et D′ du théorème 1 admettent respectivement comme coefficients diagonaux (α^3, 1, α^{13}, α^3, α^{13}, α^{13}, α^5, α^{13}) et (1, α^5, α^4, α^4, α, α^{14}, α^6).

On suppose que le polynôme d'erreurs est donné par :

$$E(X)=\alpha X^{14}+\alpha^7X^{10}+\alpha^2X+\alpha^{13}$$

(ce qui correspond à des erreurs en α_{14}, α_{10}, α_1, α_0, soit α, α^{12}, α^3 et α^2).

Le décodage procède donc comme suit :

(1) Le reste de la division de E par g est :

$$R(X)=\alpha^5X^7+\alpha^{12}X^6+\alpha^{10}X^5 + \alpha^6X^4+\alpha^2X^3+\alpha^{11}X^2+\alpha^7X.$$

(2) On calcule $m_0, \ldots, m_7=0$, α^7, α^{13}, α^{14}, α^8, α^{12}, α^7, α^7.

(3) L'algorithme de résolution de l'équation caractéristique donne les résultats partiels suivants :

j	0	1	2	3	4	5
d_j	0	0	1	2	2	3
N_j	0	0	0	0	$X+\alpha^2$	$X^2+\alpha^3X+\alpha^8$
D_j	1	1	$X+\alpha^3$	$X^2+\alpha^7X+\alpha^7$	$\alpha^6X^2+\alpha^5$	$\alpha^6X^3+\alpha^{12}X^2+\alpha^5X+\alpha^{11}$
s_j	0	α^7	α^5	α^3	α^7	α^7
N'_j	1	$X+\alpha^2$	$X+\alpha^2$	$X+\alpha^2$	0	$\alpha^9X+\alpha^{11}$
D'_j	0	0	α^{14}	$\alpha^{13}X+\alpha^7$	$X^3+\alpha^{13}X^2+\alpha^2X+\alpha^{12}$	$X^3+\alpha^6X^2+\alpha^2X+\alpha^5$
t_j		α^6	α^3	α^9	α	α^3

j	6	7	8
d_j	3	4	4
N_j	$\alpha^{11}X^2+\alpha^4X+\alpha^{13}$	$\alpha^{11}X^3+\alpha X+\alpha^6$	$\alpha^2X^3+\alpha^2X^2+\alpha^{10}X+\alpha^5$
D_j	$\alpha^8X^3+\alpha^{14}X^2+\alpha^5X+\alpha^{13}$	$\alpha^8X^4+\alpha^7X^3+\alpha^{13}X^2+\alpha^6$	$\alpha^9X^4+\alpha^9X^3+\alpha^{12}X^2+\alpha X+\alpha^{12}$
s_j	α^6	α^2	
N'_j	$X^3+\alpha^4X^2+\alpha X+1$	$X^3+\alpha^2X^2+\alpha^9X+\alpha^{11}$	
D'_j	$\alpha^6X^4+\alpha X^3+\alpha^8X^2+X+\alpha^3$	$\alpha^6X^4+\alpha^{14}X^3+\alpha^3X^2+\alpha X+\alpha^{10}$	
t_j	α^5	α^{14}	

(4) On a:

$$\mathrm{PGCD}(N_8, D_8) = (X^2+\alpha^6 X+\alpha^5) = (X+\alpha^3)(X+\alpha^2),$$

qui indique la présence de deux erreurs en positions α_0 et α_1.

$$N(X) = \alpha^2 X + 1, \qquad D(X) = \alpha^9 X^2 + \alpha^7 X + \alpha^7. \tag{5}$$

$D(X)=0$ pour $X=\alpha^{12}$, $X=\alpha$, ce qui révèle la présence de deux autres erreurs en positions α_{10} et α_{14}.

$$\frac{N(X)}{D(X)} = \frac{\alpha^{11}}{X+\alpha^{12}} + \frac{\alpha^7}{X+\alpha}, \tag{6}$$

on a donc:

$$E_{10} = \frac{\alpha^{11}}{n_2} = \alpha^7, \qquad E_{14} = \frac{\alpha^7}{n_6} = \alpha,$$

enfin:

$$E_0 = r_0 + \frac{N(\alpha^2)}{D(\alpha^2)} g_0(\alpha_0+\alpha_8) = 0 + \frac{\alpha}{\alpha^6}\alpha^3 = \alpha^{13}$$

et $E_1 = \alpha^2$.

4. Décodage en présence d'effacements

Nous allons montrer comment adapter tout ce qui précède dans le cas où l'on peut recevoir un signal auxilliaire d'effacement indiquant qu'un symbole donné est susceptible d'être erroné. (Un effacement est en quelque sorte une erreur de position connue et de valeur inconnue, éventuellement nulle si le symbole effacé est juste.) Il semble malheureusement que l'on ne puisse échapper à un alourdissement des notations car il est nécessaire de distinguer les effacements dans les positions de redondance.

Notations: On suppose que $l \leqq s$ symbole sont effacés.
On pose:

$$E_f = \{ j \in [0, \ldots, n-1] / \text{ le } j\text{-ième symbole est effacé} \},$$

$$I = E_f \cap [0, \ldots, s-1],$$
$$J = E_f \cap [s, \ldots, n-1],$$
$$I(X) = \prod_{j \in I} (X+\alpha_j),$$
$$J(X) = \prod_{j \in J} (X+\alpha_j).$$

Le polynôme I.J est le localisateur d'effacements classique.

Dans le cas où $J(X)=1$, il n'y a rien à modifier à l'algorithme précédent si ce n'est que l'on s'abstient d'exécuter les itérations correspondant à $j \in I$.
La situation n'est pas aussi simple si $J(X) \neq 1$.
On pose:

$$i_0 = d^0 I, \qquad j_0 = d^0 J, \qquad s' = s - i_0,$$

s' est le nombre de coefficients du reste $R(X)$ qui ne sont pas effacés. On ne considérera pas les coefficients r_i effacés et on supposera pour alléger les notations que les indices correspondants sont $i = s', \ldots, s-1$. (Il n'y a pas de perte de généralité car tout ce qui va être fait par la suite ne dépend pas de l'ordre dans lequel on considère les m_i.)
Dans toute la suite on ne donnera que les différentes par rapport aux preuves précédentes, l'essentiel de l'argumentation restant identique.

Théorème 2 *bis*: *Si le mot reçu est entaché de t erreurs et de l effacements avec* $2t+l \leqq s$, *alors le problème suivant:*
Trouver un couple de polynômes $N(X)$, $D(X)$ *tels que:*
- $m_i D(X) \equiv N(X)\ [X+\alpha_i]$, $i=0, \ldots, s'-1$;
- $J(X) \mid D(X)$;
- $d^0(N, D)$ *minimal;*

possède une solution unique à une constante près qui vérifie $d^0 D = t + j_0$, $D(\alpha_l) = 0$ *si et seulement si le l-ième symbole reçu est affecté d'une erreur, ou d'un effacement si c'est une position d'information.*

Lemme 2 *bis*: *Le problème du théorème 2 bis privé de la contrainte de minimalité pour* $d^0(N, D)$ *admet une solution avec:*

$$D = J \cdot \prod_{i=1}^{t} (X+\alpha_{k_i}).$$

Preuve du lemme 2 bis: La preuve est similaire à celle du lemme 2 et on obtient comme expression explicite de $N(X)$:

$$N(X) = \prod_{k_i < s} (X+\alpha_{k_i}) \Big\{ \sum_{j \in K} n_{j-s} E_j \prod_{\substack{l \neq j \\ l \in K}} (X+\alpha_l) \Big\}.$$

E_j désignant la valeur de l'erreur ou de l'effacement affectant la position k_j et

$$K = J \cup \{ k_j / k_j \geqq s \}$$

(soit l'ensemble des indices correspondant aux erreurs et effacements dans les positions d'information). □
On note E_l l'ensemble des couples (N, D) qui vérifient:

$$D \neq 0, \qquad J \mid D$$

et

$$m_i D(X) \equiv N(X)\,[X+\alpha_i],$$
$$i=0, \ldots, l-1.$$

Lemme 3 *bis*:
Si:

$$(N, D) \in E_l,$$
$$(N', D') \in E_l \quad \textit{et} \quad (N, D) \not\times (N', D')$$

alors on a:

$$d^0(N, D) + d^0(N', D') \geqq l+1+j_0.$$

Preuve du lemme 3 bis: Là encore on considère $N'D+ND'$, qui est un multiple de H_l. Soit $D=D_0 J$, $D'=D_0 J$.
Alors $J(N'D_0+ND_0')=QH_l$ avec $Q\neq 0$. Par construction de J et de H_l, PGCD $(J, H_l)=1$ et donc $J \mid Q$, le résultat est établi car $j_0=d^0 J$. □
La preuve du théorème 2 *bis* est alors similaire à celle du théorème 2 à ceci près, lors de la preuve du fait que $v \mid u$, qu'une complication apparaît car v peut avoir des racines dans $\alpha_s, \ldots, \alpha_{n-1}$ si il existe des effacements de valeur nulle. Mais dans ces conditions, une telle racine est racine de J et donc de u car on contraint B à être divisible par J. □

Lemme 4 *bis*: *Si* $(N, D) \in \bar{E}_j$ *et* $2d_j \leqq j+j_0$ *alors* $\bar{E}_j$ *est formé des multiples de* (N, D) *par un élément non nul de* F_{2^m}.

Preuve du lemme 4 bis: Identique à celle du lemme 4 sauf que l'on n'a pas nécessairement $a \mid H_j$: $u(\alpha_j)=0$ si $j \in J$ et $E_j=0$.
Deux cas sont à distinguer.

(1) $D_0(\alpha_j)\neq 0$: on a alors $(X+\alpha_j) \mid J \mid D$, mais $D=vD_0$ et α_j est racine de v.

(2) $D_0(\alpha_j)=0$. Dans ce cas, $(X+\alpha_j)^2 \mid D$ et $(X+\alpha_j) \mid C$; le couple $C'=C/(X+\alpha_j)$, $D'=D/(X+\alpha_j)$ serait alors dans E_j car D' serait encore divisible par J, ce qui contredirait la minimalité de (C, D). □

Lemme 5 *bis*: *Si:*

$$(N, D) \in \bar{E}_j,$$
$$(N, D) \in \bar{E}_{j+1} \quad \textit{et} \quad 2d_j \leqq j+j_0,$$

alors:

$$d_{j+1}=d_j+1.$$

Preuve du lemme 5 bis: Identique à celle du lemme 5 à partir du lemme 4 *bis*.

Théorème 3 *bis*: *L'algorithme suivant permet de construire deux suites de couples éléments de* $E_j (j=j_0, \ldots, s')$ *qui vérifient:*

$$(N_j, D_j) \in \bar{E}_j, \qquad (N_j', D_j') \in E_j,$$
$$d^0(N_j', D_j') = j+1-d_j+j_0,$$
$$N_j D_j' + N_j' D_j = J.H_j.$$

Algorithme de construction: *On considère le polynôme* $Z(X)$ *de degré* $<j_0$ *tel que:*

$$m_i J(\alpha_i) = Z(\alpha_i), \qquad i=0, \ldots, j_0^{-1}.$$

Initialisation:

$$N_{j_0}=Z, \qquad D_{j_0}=J,$$
$$N_{j_0}'=H_{j_0}, \qquad D_{j_0}'=0,$$
$$d_{j_0}=j_0.$$

Procéder ensuite de proche en proche, $j=j_0, \ldots, s'-1$, *on pose:*

$$s_j = m_j D_j(\alpha_j) + N_j(\alpha_j),$$
$$t_j = m_j D_j'(\alpha_j) + N_j'(\alpha_j),$$

trois cas sont à distinguer:

(a) $s_j=0$; ..... } *Cf. l'énoncé du théorème* 3.
(b) $s_j\neq 0$ *et* $2d_j \leqq j+j_0$; ..... } *Cf. l'énoncé du théorème* 3.
(c) $s_j\neq 0$ *et* $2d_j = j+j_0+1$ ..... } *Cf. l'énoncé du théorème* 3.

Preuve du théorème 3 bis: Il est clair que le polynôme Z considéré existe et est unique. Le couple (Z, J) est bien élément de E_{j_0} mais aussi de $\bar{E}_{j_0}$ du fait de la contrainte de divisibilité par J.

Le reste de la preuve est similaire à celle du théorème 3.

L'initialisation choisie permet de prouver simplement que l'algorithme ci-dessus est correct. Elle introduit une étape de calcul « indépendante » pour Z(X) qui peut facilement être incluse dans la suite des opérations comme suit: on modifie l'initialisation $j=0$: $d_0=j_0$, $N_0=0$, $D_0=J(X)$, $N_0'=1$, $D_0'=0$ et on effectue ensuite les itérations correspondant à $j=0, 1, \ldots, s'-1$.
On vérifie alors que l'on a bien $D_{j_0}=J$, $d_{j_0}=j_0$, $N_{j_0}=Z$ [3] et l'on est ramené au cas précédent.

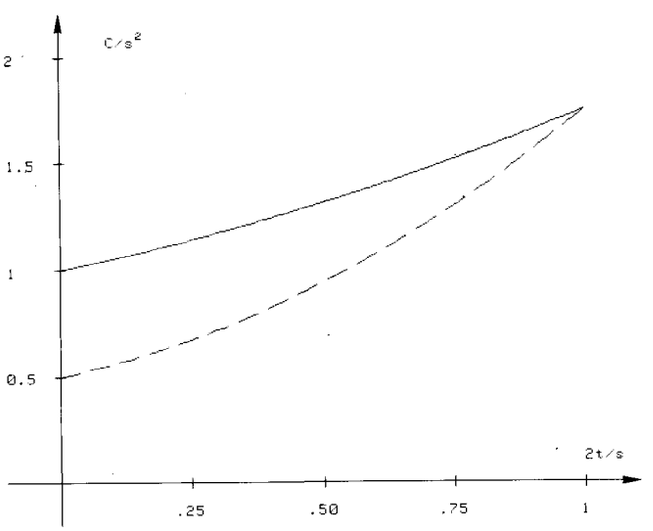
5. Complexité

Nous allons comparer brièvement la complexité de l'algorithme proposé à celle de l'algorithme classique de Berlekamp dans le cas où il n'y a pas d'effacements et où le mot reçu comporte t erreurs, $2t \leqq s$.

([3]) Z est l'interpolateur de Lagrange relatif aux points $\alpha_0, \ldots, \alpha_{j_0-1}$ et aux valeurs $m_0 J(\alpha_0), \ldots, m_{j_0-1} J(\alpha_{j_0-1})$: on constate que les j_0 premières itérations n'effectuent jamais le choix (c) et que la construction résultante de Z est exactement celle de Newton.

Les deux algorithmes comportent des étapes communes (recherche des racines du localisateur d'erreurs, décomposition en éléments simples) que l'on s'abstiendra donc de comptabiliser. Pour simplifier, on ne considérera que le cas « typique » où les $s-2t$ dernières valeurs de s_j sont nulles (ce n'est pas toujours le cas si il y a des erreurs dans les $s-2t$ dernières positions de redondance...).

Dans ces conditions, les $2t$ premières itérations nécessitent $6t^2$ opérations élémentaires {addition, multiplication}. Parmi les $s-2t$ itérations suivantes, aucune ne nécessite le calcul de t_j et seulement la moitié d'entre elles nécessitent la réactualisation de N′ et D′: le calcul des s_j demande $t(s-2t)$ opérations et la réactualisation de N′ et D′ pour les $(s/2)-t$ premières demande $((s^2/2)-t^2)$ opérations. La méthode classique de Berlekamp en demande s^2 pour le passage de (r_i) à (S_i), $3t^2$ pour les $2t$ premières itérations et enfin $t(s-2t)$ pour vérifier $\Delta_j=0$, $j=2t, \ldots, s-1$ (avec les notations de [1]) (4).



La complexité C des deux méthodes peut s'exprimer en fonction du paramètre $x=2t/s$ comme suit:

Méthode classique:

$$C=s^2(1+x/2+x^2/4).$$

Méthode présentée précédemment:

$$C=s^2(1/2+x/2+3x^2/4).$$

La figure présente le graphe de ces deux fonctions pour x allant de zéro à un.

(4) On a omis pour simplifier les termes linéaires en s et t pour ne retenir que les termes quadratiques en t^2, s^2 et ts.

Pour les très petites valeurs de t, le gain représente quasiment un rapport 2 dans les temps d'exécution. C'est donc un avantage important lorsque l'on réalise des systèmes de décodage utilisant un décodeur plus lent que le débit nominal du canal avec des « mémoires tampon » pour tirer profit du décodage rapide des mots comportant peu d'erreurs.

Si l'on s'abstient de comptabiliser les s^2 opérations correspondant au passage des (r_i) aux (S_i) dans l'estimation de la complexité de l'algorithme classique (ce qui est légitime si le décodeur possède un auxilliaire câblé permettant ce calcul, par exemple), la conclusion se trouve inversée, et la méthode proposée devient alors moins performante que la méthode classique.

Cependant, en l'état actuel de l'art, la réalisation de tels auxilliaires câblés est plus complexe que celle d'encodeurs ayant la structure indiquée en [2].

Conclusion

On a montré l'existence d'une équation caractéristique du décodage des codes de Reed-Solomon différente de l'équation classiquement utilisée. On a également montré que la résolution de la congruence qui en résulte peut être effectuée à l'aide d'un algorithme différent de l'algorithme d'Euclide et de ses variantes.

La méthode proposée permet de réaliser des décodeurs dont le débit moyen est supérieur d'un facteur compris entre 1 et 2 à celui des décodeurs exploitant les méthodes précédemment connues.

Le gain réel dépend de la statistique du nombre d'erreurs affectant les mots reçus.

BIBLIOGRAPHIE

[1] E. R. Berlekamp, *Algebraic Coding Theory*, Mac Graw Hill, 1968.

[2] E. R. Berlekamp, Bit serial Reed-Solomon Encoders, *IEEE Trans. Information Theory*, IT-28, n° 6, Novembre 1982.

[3] F. J. MacWilliams et N. J. A. Sloane, *The Theory of Error correcting Codes*, North Holland Math. Lib., 1977.

[4] J. L. Dornstetter, *Équivalence de l'algorithme de Berlekamp a un développement en fractions continues*, en préparation.

[5] L. R. Welch et E. R. Berlekamp, dans «Abstracts of Papers», *IEEE International Symposium on Information Theory*, Saint-Jovite, Québec, 1983.