Quelques applications des transformations discrètes de Galois-Fourier aux codes de Goppa

On some applications of Galois-Fourier transforms to Goppa Codes

Jean CONAN

École Polytechnique, Département de Génie Électrique, Case Postale 6079, succursale A, MONTREAL, Quebec H3C 3A7, Canada.

Jean Conan est Ingénieur Radioélectricien et Ingénieur en Génie Atomique diplômé de l'Institut Polytechnique de Grenoble (1964, 1965). Il a de plus obtenu une Maîtrise en Sciences (Génie Electrique) de l'Université du Michigan, Ann Arbor, USA en 1971, et un Doctorat es Sciences (Ph. D.) de l'Université McGill, Montréal, Canada en 1981.

Depuis 1972, il enseigne au Département de Génie Electrique de l'Ecole Polytechnique de Montréal où il occupe, depuis 1983, le poste de Professeur Titulaire. En 1985-1986, il fut Professeur Invité au Collège Militaire Royal de Kingston, Ontario. Ses domaines de Recherche portent sur la théorie des communications, la théorie de l'information et du codage, l'analyse et la synthèse des réseaux de transmissions numériques et la Téléinformatique.

M. Conan agit comme consultant auprès d'industries et d'agences gouvernementales canadiennes et est membre de l'IEEE. Il fut membre du comité d'organisation du Symposium International de Théorie de l'Information (Saint-Jovite, Canada, 1983), président du Chapitre de Théorie de l'Information de la Section IEEE de Montréal (1984-1985), et est membre fondateur de la Société Canadienne de Théorie de l'Information (Montréal, 1986).

RÉSUMÉ

Dans cet article, nous présentons une transformation de Galois-Fourier applicable à l'analyse des codes de Goppa et qui possède toutes les propriétés d'une transformée classique de Galois-Fourier discrète bien que n'utilisant pas nécessairement une racine primitive de l'unité. Une application de cette technique nous permet d'identifier de façon unifiée les connexions entre les codes de Goppa et les codes cycliques. D'autre part, lorsque le problème du décodage algébrique de ces codes est exprimé dans l'espace des transformées, l'algorithme correspondant se trouve grandement simplifié et la technique de décodage par transformées de Blahut devient directement applicable. Compte tenu des développements récents en matière de calculs rapides des transformées de Fourier, cette nouvelle approche devrait présenter un intérêt certain pour les applications pratiques.

MOTS CLÉS

Codes de Goppa, transformation discrète de Galois-Fourier, cyclicité, décodage algébrique par transformée.

SUMMARY

In this paper we present a Galois-Fourier transform applicable to the class of Goppa codes. Such a transform presents all the classical properties of a discrete Galois-Fourier transform without being necessarily generated through a primitive root of unity. A direct application of this technique has allowed us to unify the relationship between Goppa and cyclic codes. Furthermore we show how the decoding problem of this class of codes becomes greatly simplified when expressed in the transform domain and demonstrate the applicability of Blahut's decoding technique in the transform domain. Consequently, since efficient and fast procedures are known for the computation of Fourier type transforms, this new approach appears to be of great value for practical applications.

KEY WORDS

Goppa codes, Galois-Fourier transform, cyclic codes, algebraic transform decoding.

1. Introduction

Récemment une classe importante de codes en blocs linéaires applicables à la correction des erreurs de transmission a été introduite par le mathématicien russe V. D. Goppa [1], [2], [3]. Cette famille de codes comprend, parmi d'autres, comme sous-ensembles connus les classes des codes BCH, Reed-Solomon, Srivastava et Gabidulin. Une des propriétés fondamentales de ces codes tient au fait que la sous-classe formée de ceux qui sont dits irréductibles comprend des codes de longueur arbitrairement grande et qui satisfont simultanément à la borne de Varshamov-Gilbert [4].

Cet article traite d'une étude des propriétés de ces codes par le biais d'une transformation discrète de Galois-Fourier. Après avoir brièvement rappelé la définition des paramètres constitutifs de ces codes et revu leurs propriétés fondamentales, nous introduisons une transformation discrète de Galois-Fourier qui s'avère appropriée à leur étude et dont la définition originelle apparaît dans les références [5] et [6]. Nous démontrons par la suite comment l'utilisation de cette transformation permet de retrouver aisément toutes leurs propriétés classiques. Une extension de la méthode nous permet alors d'identifier une sous-classe de codes de Goppa potentiellement cycliques. Enfin, nous concluons par une section qui traite dans un cadre unifié du problème du décodage algébrique de ces codes. L'approche qui y est proposée est basée sur le décodage dans l'espace des transformées et nous conduit essentiellement à généraliser aux codes de Goppa la méthode de décodage par transformation discrète de Fourier des codes BCH due à Blahut [7].

2. Rappel sur les propriétés des codes de Goppa

De façon générale, les codes de Goppa classiques peuvent se définir à partir des paramètres et entités mathématiques dont la présentation suit.

Soient q une puissance d'un nombre premier p (la caractéristique du corps de Galois F_q sous-jacent) et m un entier positif. Étant donnés un ensemble de localisation $L=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ formé de n éléments distincts du corps de Galois F_{q^m} et $G(z)$ un polynôme de degré r à coefficients dans F_{q^m}, appelé le polynôme de Goppa et ne possédant aucune racine dans L; nous définirons le code de Goppa associé comme l'ensemble $\Gamma(L, G)$ des n-uples $\mathbf{a}=(a_1, a_2, \ldots, a_n)$ à composantes dans F_q et satisfaisant à la relation :

$$(1) \qquad R^a(z)=\sum_{i=1}^{n}\frac{a_j}{(z-\alpha_i)}=0 \text{ modulo } G(z).$$

Du fait que le polynôme $G(z)=\sum_{k=0}^{r} g_k z^k$ de degré $r (g_r \neq 0)$ ne possède aucune racine sur l'ensemble L et que l'identité

$$G(z)-G(\alpha_i)=(z-\alpha_i).\sum_{k=1}^{r} g_k \sum_{j=0}^{k-1} z^{k-1-j}\alpha_i^j$$

est satisfaite pour toutes les valeurs de l'indice i, il apparaît que l'élément $(z-\alpha_i)^{-1}$ existe dans l'algèbre des séries en z modulo $G(z)$ et prend la valeur :

$$\frac{1}{(z-\alpha_i)} \bmod G(z)$$

$$=-\frac{1}{G(\alpha_i)}.\sum_{k=1}^{r} g_k \sum_{j=0}^{k-1} z^{k-1-j}\alpha_i^j$$

$$=-\frac{1}{G(\alpha_i)}.\sum_{k=0}^{r-1} z^k \sum_{j=0}^{r-1-k} g_{j+1+k}\alpha_i^j.$$

Reportant ces relations dans (1), il apparait que le n-uple $\mathbf{a}$ appartient à $\Gamma(L, G)$ si et seulement si :

$$(2) \qquad \sum_{k=0}^{r-1} z^k \sum_{j=0}^{r-1-k} g_{j+1+k} \sum_{i=1}^{n}\frac{a_i\alpha_i^j}{G(\alpha_i)}=0.$$

Cette dernière relation est évidemment satisfaite lorsque :

$$(3) \qquad \sum_{i=1}^{n}\frac{a_i\alpha_i^j}{G(\alpha_i)}=0, \qquad j=0, 1, \ldots, r-1.$$

Réciproquement, lorsque (3) est vérifiée, les identités

$$(4) \qquad \sum_{j=0}^{r-1-k} g_{j+1+k} \sum_{i=1}^{n} \frac{a_i \alpha_i^j}{G(\alpha_i)} = 0,$$

sont satisfaites pour toutes les valeurs de l'indice k entre 0 et $r-1$. Ceci implique pour $k=r-1$:

$$g_r \cdot \sum_{i=1}^{n} \frac{a_i}{G(\alpha_i)} = 0$$

d'où

$$\sum_{i=1}^{n} \frac{a_i}{G(\alpha_i)} = 0$$

puisque $g_r \neq 0$.

La démonstration relative à la nécessité des relations (3) procède alors aisément par récurrence. Nous venons juste de démontrer leur nécessité pour $j=0$. Supposons donc qu'elles soient nécessaires pour $j=0, 1, \ldots, s$ $(s<r-1)$. Il s'ensuit que la relation (4) conduit, pour la valeur d'indice $k=r-s-2$, à l'identité :

$$\sum_{j=0}^{s+1} g_{j+r-s-1} \sum_{i=1}^{n} \frac{a_i \alpha_i^j}{G(\alpha_i)} = 0.$$

Conformément aux hypothèses on doit donc satisfaire :

$$g_r \sum_{i=1}^{n} \frac{a_i \alpha_i^{s+1}}{G(\alpha_i)} = 0,$$

ce qui implique

$$\sum_{i=1}^{n} \frac{a_i \alpha_i^{s+1}}{G(\alpha_i)} = 0$$

puisque $g_r \neq 0$.

La récurrence s'arrête lorsque $s=r-1$ faute d'équations supplémentaires dans (4).

C.Q.F.D.

Les équations (3) constituent les relations de vérification de parité associées au code. La matrice de contrôle de parité correspondante peut donc s'écrire sous la forme alternante suivante :

$$(5) \quad H = \begin{vmatrix} \alpha_1^0 & \alpha_2^0 & \ldots & \alpha_n^0 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \ldots & \alpha_n^{r-1} \end{vmatrix} \times \begin{vmatrix} G(\alpha_1)^{-1} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & G(\alpha_n)^{-1} \end{vmatrix}.$$

Il résulte de l'analyse précédente que le code de Goppa $\Gamma(L, G)$ peut être redéfini comme :

$$(6) \qquad \Gamma(L, G) = \{ \mathbf{a} \in (F_q)^n / \mathbf{a} H^T = \mathbf{0} \}.$$

On reconnait dans la composante de gauche du produit associé à H une matrice de Vandermonde de rang r qui peut être considérée comme la matrice de contrôle de parité d'un code de Reed-Salomon Γ' sur F_{q^m} éventuellement perforé $(n \leqq q^m - 1)$. Il s'ensuit que tout n-uple non nul appartenant à Γ' ne peut avoir moins de $r+1$ composantes non nulles (i. e. son poids de Hamming est au moins $r+1$). Comme pour tout $\mathbf{a}=(a_1, \ldots, a_n)$ dans $\Gamma(L, G)$, le n-uple correspondant $\mathbf{b}=(a_1 . G(\alpha_1)^{-1}, \ldots, a_n . G(\alpha_n)^{-1})$ appartient à Γ' et possède le même poids que $\mathbf{a}$, il est clair que la distance minimale d_{min} de $\Gamma(L, G)$ ne peut être inférieure à $r+1$. D'autre part, comme la matrice H dans (6) fournit un maximum de $m \times r$ équations de vérification de parité indépendantes sur F_q, il s'ensuit que la dimension de $\Gamma(L, G)$ est au moins $n - m \times r$. Toutes ces remarques nous conduisent à énoncer la proposition suivante :

Proposition 1 : *Tout code de Goppa $\Gamma(L, G)$ de longueur n et dont le polynôme de Goppa $G(z)$ est de degré r peut être défini à partir de la matrice de contrôle de parité alternante* (5). *Sa dimension est $k \geqq n - m \times r$ et la borne de Goppa stipule que sa distance minimale est bornée inférieurement par sa* distance a priori $\delta = r+1$.

Pour trouver la dimension vraie de $\Gamma(L, G)$, il est nécessaire de déterminer le rang sur F_q de la matrice de contrôle de parité associée. La procédure correspondante est relativement simple et consiste, tout d'abord, à convertir chacun des éléments de H dans F_{q^m} en un vecteur colonne à m composantes dans F_q prises par rapport à une base naturelle $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$. Après réduction de la matrice résultante sous forme canonique, suppression des rangées nulles et un éventuel réarrangement des colonnes, on obtient une matrice $k \times n$ équivalente :

$$H' = |I_{k'} P|.$$

La dimension effective du code est alors k' et la matrice génératrice canonique qui lui est associée s'écrit simplement :

$$G = | -P^T I_{n-k'} |.$$

Exemple 1 : Considérons le code de Goppa sur F_2 construit à partir du polynôme $G(z)=z^2+z+\alpha^3$ et du sous-ensemble de F_{2^4} $L=\{\{\alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{13}, \alpha^{14}\}$ pour α un élément primitif de F_{2^4} satisfaisant à l'équation $\alpha^4+\alpha+1=0$. La matrice de contrôle H correspondante s'écrit :

$$H = \begin{vmatrix} \alpha^3 & \alpha^9 & \alpha^4 & \alpha & \alpha^8 & \alpha^3 & \alpha^6 & \alpha & \alpha^2 & \alpha^8 & \alpha^9 \\ \alpha^5 & \alpha^{12} & \alpha^8 & \alpha^6 & \alpha^{14} & \alpha^{11} & 1 & \alpha^{11} & \alpha^{13} & \alpha^6 & \alpha^8 \end{vmatrix}.$$

On trouve alors aisément :

$$H' = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{vmatrix}$$

et

$$G = \begin{vmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

qui définissent un code (11, 4, 5) correcteur d'erreurs doubles. Il est aisé de vérifier que ce code peut être construit à partir du polynôme $G(z)^2$ de degré 4 de sorte que, dans ce cas, la borne de Goppa est atteinte.

3. Transformées de Galois-Fourier des mots de code

Étant donné un code de Goppa $\Gamma(L, G)$ sur F_q de longueur n et caractérisé par le sous-ensemble de F_{q^m} $L=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, duquel nous excluons momentanément la valeur 0, et le polynôme de Goppa $G(z)$ de degré r dont les racines n'appartiennent pas à L; nous définirons N comme :

$$(7) \qquad N = \underset{L}{\text{ppcm}} \{ \text{ordre multiplicatif de } \alpha_i \}.$$

Si **a** est un n-uple d'éléments de F_q, nous introduisons, conformément à [5], la transformée discrète de Galois-Fourier correspondante comme le N-uple $(A_0, A_1, \ldots, A_{N-1})$ sur F_{q^m} satisfaisant à la relation de définition :

$$(8) \qquad A_j = \sum_{i=1}^{n} a_i \alpha_i^j, \qquad j=0, 1, \ldots, N-1.$$

Nous y associons d'autre part la transformée de Galois-Fourier polynômiale :

$$(9) \qquad A(z) = \sum_{j=0}^{N-1} A_j z^{N-1-j}.$$

Il pourra être souhaitable, dans certaines applications, d'utiliser une valeur de N qui soit un multiple de la valeur minimale apparaissant dans (7), soit par exemple $N = q^m - 1$. Dans ce cas les coefficients de Galois-Fourier satisfont, compte tenu de la notation $\langle j \rangle N = j$ modulo N, à la relation :

$$A'_j = A_{\langle j \rangle N}, \qquad j=0, 1, \ldots, N'-1.$$

de sorte que la transformée polynômiale correspondante devient simplement :

$$(10) \quad A'(z) = \sum_{j=0}^{N'-1} A_{\langle j \rangle N} z^{N'-1-j} = A(z) \cdot \left(\sum_{j=0}^{N'/N-1} z^{jN} \right),$$

où $A(z)$ représente la transformée restreinte donnée en (9).

On démontre aisément que la transformation considérée ci-dessus possède les caractéristiques classiques suivantes d'une transformation de Fourier en champ fini.

(1) Inversibilité

Les composantes de **a** s'obtiennent par les relations :

$$(11) \qquad a_i = N^{-1} . \alpha_i . A(\alpha_i), \qquad i=1, 2, \ldots, n,$$

où N^{-1} représente l'inverse multiplicatif de N sur le sous corps des entiers de F_q.

(2) Contraintes de conjugaison

Les composantes de N-uple **A** satisfont aux relations dites de conjugaison :

$$(12) \qquad (A_j)^q = A_{\langle jq \rangle N}, \qquad j=0, 1, \ldots, N-1$$

pour tenir compte du fait que les composantes de **a** prennent leur valeur dans F_q.

(3) Correspondance produit direct-convolution

Étant donné le n-uple **c**, dit produit direct de **a** par **b**, dont les composantes sont $c_i = N . \alpha_i^{-1} . a_i . b_i$; la transformée de Galois-Fourier **C** associée est donnée par la convolution cyclique de période N de **A** et **B** :

$$(13) \qquad C(z) = [A(z) . B(z)]_N,$$

où nous utilisons la notation $[A(z) . B(z)]_N$ pour représenter le produit des deux polynômes $A(z)$ et $B(z)$ modulo $z^N - 1$. De façon équivalente on peut écrire :

$$C_j = \sum_{i=0}^{N-1} A_i . B_{\langle j-i \rangle N} \qquad \text{pour} \quad j=0, 1, \ldots, N-1.$$

Réciproquement, si **A** et **B** sont les transformées de **a** et **b**; le vecteur dont la transformée possède les composantes $C_i = A_i . B_i$ pour $i=0, 1, \ldots, N-1$ peut se caractériser comme :

$$(14) \quad c_i = \sum_{k=1}^{n} \sum_{j=1}^{n} a_k . b_j . \delta^i_{k,j}, \qquad i=1, 2, \ldots, n$$

où $\delta^i_{k,j}$ vaut zéro sauf sur l'ensemble des valeurs d'indices k et j tel que $\alpha_k . \alpha_j = \alpha_i$ où sa valeur est 1.

Les propriétés énonçées ci-dessus suggèrent les remarques suivantes :

Remarque 1 : Le calcul des composantes (8) de la transformée ne sont nécessaires que pour un représentant de chacune des q-orbites de Z_N (l'ensemble des entiers modulo N). Les autres composantes relatives à la même orbite s'obtiennent alors simplement à partir de la relation (12).

Remarque 2 : Si $N=n$ et $L=\{1, \gamma, \ldots, \gamma^{n-1}\}$ pour γ une racine primitive n-ième de l'unité; la transformée polynomiale (9) dans l'algèbre modulo z^n-1 est reliée au polynôme classique de Mattson-Solomon [8] par l'identité :

$$P_{MS}(z)=[z \,.\, A(z)]_n. \tag{15}$$

Dans ce cas particulier, la relation (14) prend la forme élémentaire bien connue :

$$c_i=\sum_{j=1}^{n} a_j \,.\, b_{\langle i-j\rangle_n}=\sum_{j=1}^{n} b_j \,.\, a_{\langle i-j\rangle_n}. \tag{16}$$

Le lien étroit entre la transformation définie par (9) et les codes de Goppa apparaît dans l'énoncé du lemme suivant dont la démonstration est immédiate.

Lemme 2 : *La transformée* $C(z)$ *du vecteur* $(c_1, \ldots, c_n)$ *par rapport à l'ensemble* L *à n éléments excluant* 0 *satisfait à l'identité :*

$$\sum_{L} \frac{c_i}{(z-\alpha_i)}=\frac{C(z)}{(z^N-1)}. \tag{17}$$

Compte tenu du résultat de ce lemme, la définition du code de Goppa $\Gamma(L, G)$ peut se récrire :

$$\Gamma(L, G)=\{\mathbf{c}/G(z) \mid C(z) \text{ et } (C_j)^q=C_{\langle jq\rangle_N},\ j=0, \ldots, N-1\}. \tag{18}$$

où la notation $G(z) \mid C(z)$ signifie que $G(z)$ divise $C(z)$.

Cette nouvelle interprétation du code permet aisément de dériver ses équations de vérification de parité. A cet effet, considérons le polynôme $B(z)$ défini comme :

$$B(z)=\frac{C(z)}{G(z)}. \tag{19}$$

La transformation inverse de Galois-Fourier lui associe le vecteur **b** dont les composantes sont :

$$b_i=N^{-1} \,.\, \alpha_i \,.\, C(\alpha_i)/G(\alpha_i)=c_i/G(\alpha_i).$$

Comme le degré de $B(z)$ ne peut dépasser $N-r-1$; on a donc $B_j=0$ $j=0, 1, \ldots, r-1$, et les composantes de tout mot code satisfont aux identités :

$$\sum_{L} \frac{c_i \,.\, \alpha_i^j}{G(\alpha_i)}=0 \qquad \text{pour} \quad j=0, 1, \ldots, r-1 \tag{20}$$

qui sont précisément les équations (3) de vérification de parité du code. Réciproquement, si les relations (20) sont satisfaites, $G(z) \,.\, B(z)=[G(z) \,.\, B(z)]_N$ est la transformée de Fourier du vecteur de composantes c_i pour $i=1, 2, \ldots, n$ qui est, d'après (17), un mot de code lorsque les relations de conjugaison sont vérifiées.

4. Cyclicité des codes de Goppa et de leur extension par parité

Nous abordons dans cette section le problème relatif à l'élaboration de conditions qui spécifient une classe de codes de Goppa qui sont soit cycliques soit extensibles à un code cyclique par adjonction d'un symbole de parité. L'intérêt essentiel de cette analyse ne réside pas tant dans l'originalité des résultats qui ont par ailleurs déjà été publiés dans les travaux de Berlekamp-Moreno [9] et Tzeng-Zimmermann-Yu [10, 11] mais plutôt dans l'élégance de l'approche proposée qui est basée uniquement sur l'utilisation de la transformation de Galois-Fourier.

Dans une première étape nous caractérisons les codes cycliques par leurs propriétés dans l'espace des transformées. A cette fin, nous supposons que n et q sont relativement premiers, m représente l'ordre multiplicatif de q modulo n et γ est une racine primitive n-ième de l'unité de F_{q^m}. Étant donnée U une réunion de q-orbites de Z_n (l'ensemble des entiers modulo n) comprenant $n-k$ éléments, le code cyclique (n, k) correspondant est formé de l'ensemble des n-uples $(c_0, \ldots, c_{n-1})$ sur F_q tels que les polynômes associés $\sum c_i x^j$ soient divisibles par le générateur

$$g(x)=\prod_{j \in U} (x-\gamma^j).$$

Si L_n représente l'ensemble des racines n-ièmes de l'unité, supposé ordonné suivant les puissances croissantes d'une racine primitive de l'unité, cette définition nous conduit à énoncer la proposition suivante :

Proposition 3 : *Le code* (n, k) *est cyclique si et seulement si les composantes de la transformée de Galois-Fourier des mots de code suivant* L_n *s'annulent pour les valeurs d'indice appartenant à une réunion de q-orbites de* Z_n.

Considérons la classe des codes de Goppa dont le polynôme est $G(z)=(z-\alpha)^r$, $r \geqq 1$ et l'ensemble de localisation de la forme $L=L_n \cup \{0\}-\{\alpha\}$ (α élément de $L_n \cup \{0\}$). Il apparaît que tout code dans cette classe peut se construire à partir de l'ensemble de localisation $L'=\{\beta_i=\alpha_i-\alpha/\alpha_i \in L\}$ et du polynôme de Goppa $G'(z)=z^r$. Considérons donc la transformée polynômiale de Galois-Fourier par rapport à L' de n'importe quel mot de code qui d'après (18) doit être un multiple de z^r. Il en découle que les composantes spectrales satisfont $C_i=0$ pour $i=n-1, n-2, \ldots, n-r$. Elles s'annulent d'ailleurs aussi pour les valeurs d'indices appartenant à la réunion des ensembles de q-orbites contenant $n-1, n-2, \ldots, n-r$. Il s'ensuit d'après la proposi-

tion 3 que le code est cyclique si et seulement si L′ est formé de l'ensemble des racines n-ièmes de l'unité; ce qui est le cas pour toute valeur de α appartenant à $L_n \cup \{0\}$. La classe de codes ainsi spécifiée s'identifie avec celle des codes BCH restreints dont le générateur est le plus petit commun multiple des polynômes minimaux de $\gamma^{-1}, \gamma^{-2}, \ldots, \gamma^{-r}$. Si $L_n \cup \{0\} = F_{q^m}$, les codes obtenus sont de plus primitifs.

De façon plus générale, considérons le polynôme de Goppa $G(z) = (z-\alpha)^r$ pour $\alpha \in F_{q^m}$ et le code correspondant sur le sous-ensemble de F_{q^m} à $n-1$ éléments $L = \{\alpha_1, \ldots, \alpha_{n-1}\}$ tel que $n \mid q^m - 1$ et α n'appartienne pas à L. En se référant au code équivalent d'ensemble de localisation $L' = \{\beta_i = \alpha_i - \alpha / \alpha_i \in L\}$ et de polynôme de Goppa $G'(z) = z^r$, on peut donc écrire, en utilisant la transformée de Galois-Fourier de longueur $N = q^m - 1$;

$$(21) \qquad \sum_{i=1}^{n-1} c_i . \beta_i^{-j} = 0, \qquad j = 1, 2, \ldots, r.$$

En adjoignant au code un symbole de parité c_∞ tel que :

$$(22) \qquad c_\infty + \sum_{i=1}^{n-1} c_i = 0;$$

il s'avère que, pour tout $b \in F_{q^m} - \{0\}$, (21) et (22) sont équivalentes aux relations :

$$(23) \qquad \begin{cases} c_\infty + \sum_{i=1}^{n-1} c_i . (1 + b . \beta_i^{-1})^j = 0, \\ \qquad j = 0, 1, \ldots, r. \end{cases}$$

En conséquence, si pour une valeur de b la transformation $(1 + b . (\alpha_i - \alpha)^{-1})$ applique L dans $L_n - \{1\}$; il apparaît, d'après la proposition 3, que ce code devient cyclique pour un certain réarrangement des éléments de L (c_∞ étant associé à l'élément 1 de L_n). D'autre part ses zéros incluent $\{1, \gamma, \gamma^2, \ldots, \gamma^r\}$ ainsi que leurs conjugués. On remarque de plus qu'aucun autre zéro n'est possible puisque la dimension du code doit rester identique à celle du code de Goppa original (c'est-à-dire $\geq n - 1 - r . m$). Le réarrangement de L qui donne l'extension cyclique est spécifié à partir de γ, une racine n-ième primitive de l'unité, par la relation :

$$(24) \qquad \alpha_i = \frac{\alpha . \gamma^i + b - \alpha}{(\gamma^i - 1)}, \qquad i = 1, 2, \ldots, n-1.$$

Les résultats provenant de la discussion précédente peuvent se résumer dans la proposition suivante :

Proposition 4 : *Étant donné un code de Goppa de polynôme* $(z-\alpha)^r$, $\alpha \in F_{q^m}$, *et d'ensemble de localisation* L, *un sous-ensemble de* $n-1$ *éléments de* F_{q^m} *tel que* $n \mid q^m - 1$; *ce code devient cyclique par adjonction d'un symbole de parité s'il existe un élément non nul* b *de* F_{q^m} *tel que la transformation* $(1 + b . (\alpha_i - \alpha)^{-1})$ *applique* L *dans l'ensemble* $L_n - \{1\} = \{\gamma, \gamma^2, \ldots, \gamma^{n-1}\}$.

Ce résultat général conduit aux corollaires suivants.

Soient α et b deux éléments de F_{q^m} et $L = F_{q^m} - \{\alpha, \alpha - b\}$. Si γ est un élément primitif de F_{q^m}, l'application (24) est évidemment une injection de $F_{q^m} - \{0, 1\} = \{\gamma^i / i = 1, 2, \ldots, q^m - 2\}$ dans F_{q^m}. Les deux éléments exclus sont précisément α et $\alpha - b$ de sorte que (24) est de ce fait une bijection sur L. Les résultats de la proposition 4 sont donc applicables à tout code de Goppa défini sur L et de polynôme $(z-\alpha)^r$ ou $(z - \alpha + b)^{r'}$ dont l'extension par adjonction d'un symbole de parité devient cyclique. Il en est de même du code intersection de polynôme $(z-\alpha)^r (z - \alpha + b)^{r'}$. Ces résultats nous conduisent au corollaire suivant :

Corollaire 5 : *Pour toute paire d'éléments distincts* α *et* β *de* F_{q^m} *et* $L = F_{q^m} - \{\alpha, \beta\}$; *les codes de Goppa définis sur* L *par les polynômes* $(z-\alpha)^r$, $(z-\beta)^{r'}$, $(z-\alpha)^r (z-\beta)^{r'}$ *sont cycliques par adjonction d'un symbole de parité.*

Ce dernier résultat sera illustré par l'exemple suivant :

Exemple 6 : Considérons F_{3^2} et γ l'élément primitif défini par l'équation $\gamma^2 = 2\gamma + 1$. Soit $L = F_{3^2} - \{\gamma, \gamma^3\}$ que l'on peut ordonner conformément à (24) suivant $\{\gamma^6, 0, \gamma^7, 1, \gamma^2, 2, \gamma^5\}$. Soient C_1, C_2 et $C_3 = C_1 \cap C_2$ les trois codes de Goppa sur F_3 construits sur L au moyen des polynômes de Goppa $(z-\gamma)$, $(z-\gamma^3)^2$ et $(z-\gamma)(z-\gamma^3)^2$.

(1) C_1 possède comme matrice de vérification de parité sur F_{3^2} :

$$H = \left| 2 \quad \gamma^3 \quad 1 \quad \gamma^6 \quad \gamma \quad \gamma^5 \quad \gamma^7 \right|.$$

La matrice génératrice systématique du code étendu est donc :

$$G = \left| \begin{array}{cccccccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 2 & 2 & 1 & 0 & 0 & 1 & 0 & 0 \\ 2 & 1 & 2 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array} \right| .$$

On vérifie *a posteriori* qu'il s'agit d'un code cyclique (8,5) de générateur $(x-1)(x-\gamma)(x-\gamma^3) = 1 + x + x^3$.

(2) C_2 est caractérisé par la matrice de contrôle de parité sur F_{3^2} :

$$H = \left| \begin{array}{ccccccc} \gamma^6 & \gamma^2 & \gamma^2 & 2 & 1 & \gamma^6 & 1 \\ 2 & 0 & \gamma & 2 & \gamma^2 & \gamma^2 & \gamma^5 \end{array} \right|,$$

à laquelle correspond la matrice génératrice systématique du code étendu :

$$G = \left| \begin{array}{cccccccc} 1 & 0 & 2 & 1 & 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 1 & 1 & 0 & 0 & 1 \end{array} \right| ,$$

qui spécifie un code cyclique (8,3) de générateur

$$(x-1)(x-\gamma^5)(x-\gamma^7)(x-\gamma^2)(x-\gamma^6) = 1+2x^2+x^3+x^4+x^5.$$

(3) La matrice de vérification de parité de C_3 sur F_{3^2} s'écrit :

$$H=\begin{vmatrix} \gamma^2 & \gamma^5 & \gamma^2 & \gamma^2 & \gamma & \gamma^3 & \gamma^7 \\ 1 & 0 & \gamma & \gamma^2 & \gamma^3 & \gamma^7 & \gamma^4 \\ \gamma^6 & 0 & 1 & \gamma^2 & \gamma^5 & \gamma^3 & \gamma \end{vmatrix}.$$

Le code étendu possède la matrice génératrice systématique :

$$G=|2 \quad 1 \quad 2 \quad 1 \quad 2 \quad 1 \quad 2 \quad 1|.$$

Il s'agit du code cyclique (8,1) intersection des codes C_1 et C_2 et dont le polynôme générateur est le plus petit commun multiple des générateurs de C_1 et C_2 est donné par

$$(x-1)(x-\gamma)(x-\gamma^3)(x-\gamma^5)(x-\gamma^7)(x-\gamma^2)(x-\gamma^6) = 2+x+2x^2+x^3+2x^4+x^5+2x^6+x^7.$$

Nous considérons maintenant $n=q^m+1$ et α et β deux éléments de $F_{q^{2m}}$ n'appartenant pas à F_{q^m} et que l'on suppose de plus conjugués sur F_{q^m}. α et β sont donc les solutions du polynôme du second degré

$$G_2(z)=(z-\alpha)(z-\beta)=z^2-z.(\alpha+\beta)+\alpha.\beta$$

dont les coefficients appartiennent à F_{q^m}. Ils s'obtiennent l'un de l'autre par les relations $\alpha=\beta^{n-1}$ et $\beta=\alpha^{n-1}$. Considérons $L=F_{q^m}$ et δ un élément primitif de $F_{q^{2m}}$. Du fait de l'identité $(q^{2m}-1)=(q^m-1)(q^m+1)$, il s'avère que $\gamma=\delta^{n-2}$ est une racine n-ième de l'unité. Il s'ensuit que si $b=\alpha+\beta$, l'application (24) est une bijection de $\{\gamma, \gamma^2, \ldots, \gamma^{n-1}\}$ dans F_{q^m} car, dans ce cas, α_i défini par (24) satisfait pour $i=1, 2, \ldots, n-1=q^m$

$$\alpha_i^{q^m}=\frac{(\alpha.\gamma^i-\beta)^{n-1}}{(\gamma^i-1)^{n-1}} = \frac{(\alpha^{n-1}.\gamma^{-i}-\beta^{n-1})}{(\gamma^{-i}-1)}=\frac{(\beta.\gamma^{-i}-\alpha)}{(\gamma^{-i}-1)}=\alpha_i$$

et appartient donc à F_{q^m}. La proposition 4 stipule alors que les codes de Goppa définis sur $L=F_{q^m}$ par les polynômes $(z-\alpha)^r$, $(z-\beta)^{r'}$, $G_2(z)^r=[(z-\alpha)(z-\beta)]^r$ et $(z-\alpha)^r(z-\beta)^{r'}$ deviennent cycliques par adjonction d'un symbole de parité. A ce point il importe cependant de remarquer que, du fait que α et β n'appartiennent pas à F_{q^m}, les codes définis par les polynômes $(z-\alpha)^r$, $(z-\beta)^{r'}$, et $(z-\alpha)^r(z-\beta)^{r'}$ pour r différent de r' sont des codes de Goppa « impropres » puisque les coefficients des polynômes de Goppa correspondant n'appartiennent pas nécessairement à F_{q^m}. Le seul code authentique dans cette famille est celui dont le polynôme est $G_2(z)^r$. Ces remarques constituent la démonstration d'une généralisation par Tzeng et Zimmerman [8] d'un résultat antérieur de Berlekamp et Moreno que nous résumons dans le corollaire suivant.

Corollaire 7 : *Tous les codes de Goppa définis sur* $L=F_{q^m}$ *par le polynôme irréductible du second degré* $z^2+\gamma z+\delta$ *ainsi que ses puissances successives sont cycliques par adjonction d'un symbole de parité.*

Note : Lorsque r est la puissance à laquelle est élevé le polynôme irréductible et γ est une racine de l'unité d'ordre q^m+1, les codes cycliques obtenus sont réversibles et admettent pour zéros $\{1, \gamma^{\pm 1}, \ldots, \gamma^{\pm r}\}$ ainsi que leurs conjugués.

Exemple 8 : En se référant à l'exemple 6, les codes C_1, C_2 et C_3 peuvent être raccourcis à la longueur 3 en considérant l'application (24) où l'on a remplacé γ par ω une racine primitive d'ordre 4 de F_{3^2} (ω sera de la forme γ^2 si γ est un élément primitif de F_{3^2}). Ceci conduit à choisir l'ensemble L ordonné comme $L=\{0, 1, 2\}$ et les trois codes deviennent donc des codes de Goppa « impropres ». Néanmoins, conformément au corollaire 7, ils deviennent cycliques par adjonction d'un symbole de parité. Il s'avère que seul C_1 conduit à un code non trivial. Par rapport à L, C_1 est caractérisé par la matrice de vérification de parité :

$$H=|\gamma^3 \quad \gamma^6 \quad \gamma^5|.$$

la matrice génératrice systématique du code étendu correspondant s'écrit :

$$G=|2 \quad 1 \quad 2 \quad 1|,$$

qui est associée au code cyclique (4,1) généré par $2+x+2x^2+x^3$. De façon semblable, le code de Goppa d'ensemble de localisation $L=\{0, 1, 2\}$ et de polynôme $(z-\gamma)(z-\gamma^3)=z^2+z+2$ conduit à la matrice de contrôle de parité sur F_3 :

$$H=\begin{vmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \end{vmatrix}.$$

Le code étendu correspondant est précisément le même code cyclique (4,1) de polynôme générateur $2+x+2x^2+x^3$.

5. Décodage algébrique des codes de Goppa

Nous abordons ici le problème du décodage des mots d'un code de Goppa $\Gamma(L, G)$ sur F_q après leur transmission sur un canal q-aire sans mémoire. Formellement, le problème peut s'énoncer sous la forme suivante. Si $\mathbf{c}$ est le mot de code émis et $\mathbf{e}$ est la séquence d'erreur, le n-uple reçu $\mathbf{r}=(r_1, \ldots, r_n)$ peut s'écrire comme :

$$\mathbf{r}=\mathbf{c}+\mathbf{e}.$$

Il reste donc à trouver dans $\Gamma(L, G)$ un n-uple $\mathbf{c}^*$ tel que :

$$d_H(\mathbf{c}^*, \mathbf{r}) = \min_{\mathbf{c} \in \Gamma(L, G)} \{d_H(\mathbf{c}, \mathbf{r})\},$$

où $d_H(.,.)$ représente la distance de Hamming. Dans ce cas, le pouvoir de correction du code garantit l'existence d'une solution unique lorsque le poids de Hamming w de $\mathbf{e}$ satisfait $w \leqq [r/2]$ où r est le degré du polynôme de Goppa et la notation $[x]$ représente la partie entière de x.

De façon équivalente, la solution peut s'obtenir en estimant tout d'abord le vecteur d'erreur de poids de Hamming minimal compatible avec la séquence reçue et en le soustrayant du n-uple reçu. Cette approche s'avère de fait la plus fructueuse et nous la poursuivrons par la suite.

A ce point, nous introduisons la séquence étendue de syndrome $\mathbf{S} = (S_0, S_1, \ldots, S_{N-1})$:

$$(25) \quad S_j = \sum_{i=1}^{n} r_i / G(\alpha_i)\, \alpha_i^j, \qquad j = 0, 1, \ldots, N-1,$$

définie comme la transformée de Galois-Fourier sur F_{q^m} du n-uple dont les composantes sont $r_i/G(\alpha_i)$, $i = 1, \ldots, n$.

Après substitution de $r_i = c_i + e_i$ il vient :

$$(26) \quad S_j = \sum_{i=1}^{n} e_i / G(\alpha_i)\, \alpha_i^j, \qquad j = 0, 1, \ldots, r-1,$$

de sorte que les r premières composantes du syndrome sont caractéristiques de l'erreur indépendamment du mot code transmis. Notre problème se trouve donc résolu puisqu'il est possible d'identifier l'erreur à partir de cette fraction du syndrome lorsque son poids ne dépasse pas le pouvoir de correction du code. A cet effet nous considérons le développement en série de puissance de z^{-1} de la fraction rationnelle :

$$(27) \quad \sum_{i=1}^{n} \frac{e_i/G(\alpha_i)}{(z-\alpha_i)} = \sum_{j=0}^{\infty} \sum_{i=1}^{n} e_i/G(\alpha_i)\, \alpha_i^j\, z^{-j-1}.$$

Si w représente le poids de Hamming de $\mathbf{e}$, et i_k, $k = 1, 2, \ldots, w$, sont les valeurs d'indice correspondant aux termes non nuls de $\mathbf{e}$, nous définissons les variables de position des erreurs par rapport à l'ensemble de localisation L comme :

$$X_k = \alpha_{i_k}, \qquad k = 1, 2, \ldots, w.$$

Nous introduisons d'autre part les variables de l'amplitude des erreurs :

$$Y_k = e_{i_k}/G(\alpha_{i_k}), \qquad k = 1, 2, \ldots, w.$$

Compte tenu de cette notation, le terme de gauche de l'expression (27) s'écrit :

$$\sum_{k=1}^{w} \frac{Y_k}{(z-X_k)} = \frac{\omega(z)}{\sigma(z)},$$

si $\sigma(z) = \prod_{k=1}^{w} (z - X_k)$ est le polynôme de degré w de localisation des erreurs et $\omega(z)$ le polynôme de degré $w-1$ d'évaluation de l'amplitude des erreurs dont la définition est :

$$\omega(z) = \sum_{j=1}^{w} Y_j \cdot \prod_{\substack{k=1 \\ k \neq j}}^{w} (z - X_k);$$

nous venons de démontrer, compte tenu des identités (25), (26) et (27), la relation fondamentale suivante :

$$(28) \quad \frac{\omega(z)}{\sigma(z)} = \sum_{j=0}^{r-1} S_j \cdot z^{-j-1} + O(z^{-1}),$$

où $O(z^{-1})$ représente des termes d'ordre supérieur à r. Étant donné le développement en série (27), nous dirons que la paire de polynômes $\{\sigma_k(z), \omega_k(z)\}$ en constitue une réalisation d'ordre k si les premiers k termes de la série rationnelle $\omega_k(z)/\sigma_k(z)$ sont identiques à ceux de la série (27). D'autre part, l'approximation sera dite minimale lorsque le degré de $\sigma_k(z)$ est minimal sur l'ensemble des réalisations d'ordre k. L'algorithme de Réalisation Partielle Minimale (RPM) dont la description suit permet de trouver récursivement une solution minimale pour toute valeur de $k \geqq 1$:

ALGORITHME RPM

1. *Initialisation*

$$\sigma(z) = 1, \qquad \omega(z) = 0, \qquad b(z) = 0,$$
$$c(z) = -1, \qquad d_p = 1.$$

2. *Procédure itérative*

Répéter pour $k = 1, 2, \ldots, M$ (la valeur d'ordre d'approximation désirée)

$$d = \sum_{j=0}^{w} S_{k-1-j} \cdot \sigma_{w-j},$$

$$\left(w = \deg\{\sigma(z)\},\ \sigma(z) = \sum_{j=0}^{w} \sigma_j \cdot z^j,\ \sigma_w = 1 \right)$$

si $d \neq 0$,

$$u = d_p - w,$$

si $u \leqq 0$,

$$\sigma(z) = \sigma(z) - d \cdot z^{-u} \cdot b(z),$$
$$\omega(z) = \omega(z) - d \cdot z^{-u} \cdot c(z),$$
$$d_p = d_p + 1, \quad \text{continuer}$$

autrement

$$d_p = w, \qquad t_1(z) = \sigma(z), \qquad t_2(z) = \omega(z)$$
$$\sigma(z) = z^u \cdot \sigma(z) - d \cdot b(z),$$

$$\omega(z) = z^{u}.\omega(z) - d.c(z),$$
$$b(z) = d^{-1}.t_1(z), \qquad c(z) = d^{-1}.t_2(z),$$
$$d_p = d_p + 1, \quad \text{continuer}$$

autrement,

$$d_p = d_p + 1, \quad \text{continuer.}$$

Les propriétés fondamentales de cet algorithme peuvent se résumer comme il suit [12] :

(1) Si la série (27) est rationnelle et le dénominateur de degré D, l'algorithme aura déterminé l'unique solution après 2 D itérations.

(2) Lorsque l'algorithme atteint la fin de la k-ième itération, l'ensemble de toutes les solutions du problème RPM d'ordre k est un espace affine de dimension $w - d_p + 1$.

(3) Étant donnée l'approximation d'ordre $k(\sigma_k(z), \omega_k(z))$, les termes d'ordre r supérieur à k correspondant au développement de la fraction rationnelle $\omega_k(z)/\sigma_k(z)$ peuvent se calculer suivant la récurrence :

$$(29) \qquad \begin{cases} Y'_r = -\sum_{j=1}^{w} Y'_{r-j}.\sigma_{w-j}, & r > j, \\ Y'_1 = S_0, \ \ldots, \ Y'_k = S_{k-1}. \end{cases}$$

Une conséquence immédiate de la propriété (1) nous conduit à observer que, lorsque le poids de l'erreur de transmission est $\leq r/2$ (c'est-à-dire dans les limites prédéfinies de correction du code), l'algorithme MPR aura trouvé le polynôme de localisation d'erreurs après r itérations. Une fois le polynôme de localisation $\sigma(z)$ déterminé, l'évaluation de ses racines, suivant, par exemple, la méthode de Chien [13] permet de spécifier la position des erreurs. Finalement, l'amplitude de la k-ième erreur peut s'évaluer conformément aux relations :

$$Y_k = \sum_{j=1}^{w} \frac{Y_j.(z - X_k)}{(z - X_j)}\bigg|_{z = X_k} = \frac{\omega(z).(z - X_k)}{\sigma(z)}\bigg|_{z = X_k} = \frac{\omega(X_k)}{\sigma'(X_k)}.$$

On en déduit :

$$(30) \qquad e_{i_k} = \frac{\omega(X_k).G(X_k)}{\sigma'(X_k)}, \qquad k = 1, 2, \ldots, w.$$

Cette méthode, suggérée initialement par Retter [14], peut aussi utiliser l'algorithme de Berlekamp-Massey [13] qui est équivalent à l'algorithme de RPM dans ce cas particulier.

Il importe cependant de remarquer que la recherche des racines du polynôme de localisation des erreurs ainsi que de leur amplitude n'est pas nécessaire lorsque l'on opère dans le domaine des transformées. A cette fin, nous rappelons que si l'ensemble L exclut la valeur 0, la transformée de Galois-Fourier $S'(z)$ de la séquence d'erreur modifiée $(e_i/G(\alpha_i)/i = 1, \ldots, n)$ satisfait :

$$(31) \qquad \frac{S'(z)}{(z^N - 1)} = \sum_{i=1}^{w} \frac{Y_i}{(z - X_i)} = \frac{\omega(z)}{\sigma(z)},$$

de sorte que $S'(z)$ s'obtient simplement à partir de la série rationnelle associée à $\omega(z)/\sigma(z)$ tronquée à ses N premiers termes et multiplication par z^{N-1}. De façon équivalente, les coefficients de $S'(z)$ peuvent être évalués suivant la récurrence (29).

D'autre part, si $S(z)$ est le polynôme transformé associé à la séquence étendue de syndrome, le polynôme défini par :

$$(32) \qquad C(z) = [S(z) - S'(z)].G(z)$$

est de degré $N-1$ d'après (26) et (28). Comme il est multiple de $G(z)$, il représente, d'après (18), le polynôme transformé d'un mot de code si les relations de conjugaison sont satisfaites. Dans ces conditions, nous obtenons par inversion de (32) :

$$c_i = N^{-1}.\alpha_i[S(\alpha_i) - S'(\alpha_i)].G(\alpha_i) = r_i - e_i, \quad i = 1, \ldots, n$$

et $\mathbf{c} = (c_1, \ldots, c_n)$ représente bien le mot code recherché.

La procédure de décodage par transformée suggérée peut se résumer comme il suit :

(1) Calcul de la séquence étendue de syndrome

$$S_j = \sum_{i=1}^{n} r_i/G(\alpha_i)\alpha_i^j, \qquad j = 0, 1, \ldots, N-1$$

et du polynôme transformé associé $S(z)$.

(2) Calcul des polynômes de localisation et d'évaluation des erreurs $\sigma(z)$ et $\omega(z)$ par l'algorithme RPM.

(3) Évaluation de la transformée de Galois-Fourier $S'(z)$ de la séquence d'erreur modifiée estimée $(e_i/G(\alpha_i)/i = 1, 2, \ldots, n)$ par application de la récursion (29).

(4) Inversion du vecteur transformé

$$C(z) = G(z).[S(z) - S'(z)].$$

Remarque 1 : Une erreur non corrigible est détectée chaque fois que les composantes de $C(z)$ ne satisfont pas aux relations de conjugaison.

Remarque 2 : La restriction de cette procédure aux codes BCH est équivalente à la technique de décodage par transformée de Blahut [7].

L'algorithme tel que décrit ci-dessus n'est pas directement applicable lorsque l'ensemble de localisation L contient l'élément 0 puisque, dans ce cas, la relation (31) n'est pas satisfaite. On doit alors opérer comme il suit :

La séquence de syndrome est calculée d'après (25) en utilisant la convention $0^0 = 1$ et comme valeur de N

le plus petit commun multiple de l'ordre des éléments de $L^* = L - \{0\}$. L'algorithme RPM fournit alors les polynômes de localisation et d'évaluation des erreurs $\sigma(z)$ et $\omega(z)$ comme dans la procédure normale. Si $\sigma(z)$ ne possède pas la racine 0, il n'y a pas d'erreur à la position indexée par 0, le symbole décodé correspondant est donc $c_0 = r_0$. Par contre si $\sigma(z)$ possède la racine 0, l'amplitude e_0 de l'erreur indexée par 0 peut être évaluée d'après (30) comme :

$$e_0 = \frac{\omega(0).G(0)}{\sigma'(0)},$$

et le symbole décodé qui lui correspond est $c_0 = r_0 - e_0$. Le reste de la procédure normale s'applique ensuite en utilisant la formule d'inversion modifiée :

$$c_i = N^{-1}.\left\{\alpha_i.[S(\alpha_i) - S'(\alpha_i)] - \frac{c_0}{G(0)}\right\}.G(\alpha_i) \qquad \text{pour} \quad i>0.$$

Nous illustrons la procédure par les exemples suivants.

Exemple 9 : Considérons le code de Goppa sur F_3 de polynôme z^4 et d'ensemble de localisation $L = \{1, \alpha, \alpha^2, \ldots, \alpha^7\}$ (α élément primitif de F_{3^2} satisfaisant $\alpha^2 + \alpha + 2 = 0$). Si le 8-uple reçu est (10021000), on peut calculer la séquence de syndrome suivant les relations $S_j = 1 + 2\alpha^{3j+4} + \alpha^{4j}$, $j = 0, 1, \ldots, 7$ ce qui donne $\mathbf{S} = (0, \alpha^3, \alpha^7, \alpha, 1, \alpha^7, \alpha^5, \alpha^5)$.

L'algorithme RPM appliqué aux quatre premières composantes du syndrome fournit :

m	S_{m-1}	$\sigma(z)$	$\omega(z)$	d	$b(z)$	$c(z)$	d_p
		1	0		0	-1	1
1	0	1	0	0	0	-1	2
2	α^3	z^2	α^3	α^3	α^5	0	1
3	α^7	$z^2 - \alpha^4 z$	α^3	α^7	α^5	0	2
4	α	$z^2 - \alpha^4 z - \alpha^7$	α^3	α^2	α^5	0	3

Le polynôme de localisation des erreurs est donc $\sigma(z) = z^2 + z + \alpha^3$ dont les racines sont $X_1 = \alpha^5$ et $X_2 = \alpha^6$. Les amplitudes des erreurs correspondantes sont d'après (30) :

$$e_{i_1} = \frac{\alpha^3.\alpha^{20}}{2\alpha^5 + 1} = 1, \qquad e_{i_2} = \frac{\alpha^3.1}{2\alpha^6 + 1} = 1,$$

de sorte que le mot de code décodé est (10021220).

En utilisant la technique de décodage par transformée on obtient tout d'abord :

$$\mathbf{S}' = (0, \alpha^3, \alpha^7, \alpha, \alpha^4, \alpha^5, \alpha^4),$$

d'où $\mathbf{C} = (2, \alpha^6, 0, \alpha^2, 0, 0, 0, 0)$. Comme les relations de conjugaison sont satisfaites, l'inversion conduit au mot de code :

$$\mathbf{c} = (1, 0, 0, 2, 1, 2, 2, 0).$$

Exemple 10 : Soit le code de Goppa sur F_3 de polynôme $(z - \alpha^7)^4$ et d'ensemble de localisation $L = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$ (α défini comme à l'exemple 9). Pour le 8-uple (11220001), nous calculons la séquence de syndrome modifiée suivant les relations

$$S_0 = 2, \qquad S_j = \alpha^4 + 2\alpha^j + 2\alpha^{4+2j} + \alpha^{6j}, \quad j>0$$

et obtenons $S = (2, \alpha^3, \alpha^6, \alpha, 2, \alpha^6, \alpha^2, \alpha^2)$.

L'algorithme RPM conduit à la séquence de calculs :

m	S_{m-1}	$\sigma(z)$	$\omega(z)$	d	$b(z)$	$c(z)$	d_p
		1	0		0	-1	1
1	2	z	2	2	2	0	1
2	α^3	$z + \alpha^3$	2	α^3	2	0	2
3	α^6	$z^2 + \alpha^3 z + \alpha^2$	$2z$	α^2	$\alpha^6 z + \alpha$	$2\alpha^6$	2
4	α	$z^2 + \alpha^7$	$2z + \alpha^7$	α	»	»	3

Le polynôme $\sigma(z)$ indique la présence d'erreurs aux positions indexées par 0 et α^3. la valeur de l'amplitude de e_0 s'obtient comme $\alpha^7.\alpha^4/\alpha^7 = 2$ d'où $c_0 = 1 - 2 = 2$. Appliquant la procédure par transformée conduit au mot de code :

$$\mathbf{c} = (21221001).$$

Pour conclure cette section, nous remarquerons que différentes généralisations de la technique de décodage par transformée sont possibles. En particulier la méthode est directement applicable aux codes alternants de Helgert [15] ainsi qu'aux codes algébriques récemment introduits par Chien et Choy [16] et dont une généralisation, basée sur la transformation de Galois-Fourier introduite dans cet article est présentée en [6].

6. Conclusions

Dans cet article nous avons présenté une transformation du type Galois-Fourier particulièrement adaptée à l'étude des codes de Goppa. Cette transformation possède la particularité de ne pas nécessiter l'utilisation d'une racine primitive de l'unité et s'applique donc à n'importe quel sous-ensemble du corps de Galois sous-jacent. Comme exemples d'application de cette technique, nous démontrons de façon simple et unifiée les résultats classiques relatifs à la cyclicité des codes de Goppa ou de leur extension par symbole de parité. Finalement, une méthode de décodage algébrique par transformée est présentée qui généralise aux codes de Goppa la procédure de Blahut. Nous mentionnons aussi que cette méthode est, de façon plus

générale, applicable à la classe des codes alternants de Helgert ainsi qu'à celle des codes BCH généralisés de Chien-Choy.

Manuscrit reçu le 27 *mars* 1986.

BIBLIOGRAPHIE

[1] V. D. Goppa, A New Class of Linear Error Correcting Codes, *Probl. Peredach. Inform.*, 6, sept. 1970, p. 24-30.

[2] V. D. Goppa, Rational Representation of Codes and (L, g) Codes, *Probl. Peredach. Inform.*, 7, sept. 1971, p. 41-49.

[3] E. R. Berlekamp, Goppa Codes, *IEEE Trans. Inform. Theory*, IT-19, sept. 1973, p. 590-592.

[4] V. D. Goppa, Binary Symmetric Channel Capacity is attained with Irreducible Codes, *Probl. Peredach. Unform.*, 10, mars 1974, p. 111-112.

[5] M. Loeloeian, Application des Transformées de Fourier en champs finis aux codes de Goppa généralisés, *Thèse de Ph. D.*, École Polytechnique de Montréal, octobre 1984.

[6] M. Loeloeian et J. Conan, A Transform Approach to Goppa Codes, *IEEE Trans. Inform. Theory*, IT-33, janvier 1987, p. 105-115.

[7] R. E. Blahut, *Theory and Pratice of Error Control Codes*, Addison-Wesley, Reading, MA, 1983,

[8] F. J. MacIlliams et N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, Amsterdam-New York-Oxford, 1977.

[9] E. R. Berlekamp et O. Moreno, Extended Double-error Correcting Binary Goppa Codes are Cyclic, *IEEE Trans. Inform. Theory*, IT-19, nov. 1973, p. 817-818.

[10] K. K. Tzeng et K. Zimmermann, On Extending Goppa Codes to Cyclic Codes, *IEEE Trans. Inform. Theory*, IT-21, nov. 1975, p. 712-716.

[11] K. K. Tzeng et C. Y. Yu, Characterization Theorems for extending Goppa Codes to Cyclic Codes, *IEEE Trans. Inform. Theory*, IT-25, mars 1979, p. 246-250.

[12] J. Conan, A Recursive Procedure for the Solution of the Minimal Partial Realization Problem for Scalar Rational Sequences, *Revue Roumaine de Mathématiques Pures et Appliquées*, XXX, août 1985, p. 625-645.

[13] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

[14] C. T. Retter, Decoding Goppa Codes with a BCH Decoder, *IEEE Trans. Inform. Theory*, IT-21, mars 1975, p. 112.

[15] H. J. Helgert, Alternant Codes, *Inform. and Control*, 26, 1975, p. 369-380.

[16] R. T. Chien et D. M. Choy, Algebraic Generalization of BCH-Goppa-Helgert Codes, *IEEE Trans. Inform. Theory*, IT-21, 1975, p. 70-75.