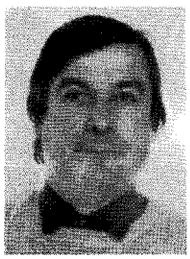
Différents aspects de la démultiplication des codes

Different aspects of q-ary images of codes



J. WOLFMANN

Groupe d'Étude du Codage de Toulon, (GECT), Université de Toulon, 83130 La GARDE

Professeur à l'Université de Toulon, Directeur du Groupe d'Étude du Codage de Toulon (GECT). Recherche dans le domaine de l'application de l'algèbre et la géométrie sur les corps de Galois et de la combinatoire à l'étude des codes correcteurs d'erreurs.

RÉSUMÉ

Cet article fait le point sur des résultats obtenus concernant la démultiplication des codes sur $\mathbb{F}_{q^m}$ (image q-aire) principalement à propos des codes cycliques, de codes autoduaux binaires à poids multiples de quatre et d'applications au décodage.

MOTS CLÉS

Codes correcteurs, images q-aires de codes, codes autoduaux, corps de Galois.

SUMMARY

This paper is a survey on results concerning q-ary images of codes over $\mathbb{F}_{q^m}$ mainly about cyclic codes, doubly even binary self dual codes and applications to decoding.

KEY WORDS

Error correcting codes, q-ary images of codes, self dual codes, Galois field.

TABLE DES MATIÈRES

Introduction

Cet article fait un bilan sur des travaux du GECT [Groupe d'Étude du Codage de Toulon] concernant la démultiplication sur $\mathbb{F}_q$ de codes sur $\mathbb{F}_{q^m}$ ($\mathbb{F}_{q^r}$ est le corps de Galois de q^r éléments). Rappelons que le démultiplié d'un code sur $\mathbb{F}_{q^m}$ (ou image q-aire) est le code obtenu en remplaçant dans chaque mot, chaque composante par son système de composantes par rapport à une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$.

On aborde tout d'abord les codes cycliques sur $\mathbb{F}_{q^m}$ en caractérisant ceux dont le démultiplié est cyclique. On construit une famille de codes sur $\mathbb{F}_4$ doublement circulants et formellement autoduaux à partir de démultipliés de codes cycliques sur $\mathbb{F}_{16}$.

On décrit une construction de codes autoduaux et, dans le cas binaire, on particularise l'étude au cas des codes à poids multiples de quatre.

Un résultat reliant les notions de démultiplié et de sous-code sur un sous-corps est indiqué et enfin les applications de la démultiplication au décodage sont abordées.

La partie 1 rappelle les définitions et motivations et la partie 2 indique les résultats obtenus.

Cet article ne contient aucune démonstration. A ce propos le lecteur est renvoyé aux textes signalés dans la bibliographie qui sont soit déjà publiés (pour la plupart d'entre eux), soit à paraître.

Le vocabulaire, les définitions usuelles, les résultats classiques sur le codage utilisés dans ce texte sont standard et peuvent se trouver dans [7].

1. Préliminaires

1.1. Démultiplication

1.1.1. *Définition*

Soit $\mathbb{F}_{q^r}$ le corps de Galois d'ordre q^r (q puissance d'un nombre premier) et $B=\{b_1, b_2, ..., b_r\}$ une base de $\mathbb{F}_{q^r}$ considéré comme espace vectoriel sur $\mathbb{F}_q$.

La démultiplication de $\mathbb{F}_{q^r}$ sur $\mathbb{F}_{q'}$ (par rapport à la base B) est l'application d définie par :

$$x=(x_1, ..., x_i, ..., x_n)\in(\mathbb{F}_{q^r})^n$$
$$\downarrow d$$
$$d(x)=(..., \underbrace{x_i^1, x_i^2, ..., x_i^r}, ...)\in(\mathbb{F}_q)^{rn}$$

avec $x_i=\sum_{j=1}^{r} x_i^j\, b_j$.

Le démultiplié d'un code C est son image d (C).

L'application d est $\mathbb{F}_q$ linéaire et si C est un code linéaire (n, k, δ) sur $\mathbb{F}_{q^r}$ alors d (C) est un code linéaire (nr, kr, D) sur $\mathbb{F}_q$ avec $D\geqq\delta$.

1.2.2. *Problèmes et motivations*

Le problème général de la démultiplication consiste en la construction et l'étude de codes intéressants sur $\mathbb{F}_q$ comme démultiplié de codes sur $\mathbb{F}_{q^m}$. Par exemple les fameux codes de Justesen (*voir* [7]) sont obtenus par démultiplication. C'est aussi le cas des codes « en cascades » de Dumer et Zinoviev [3]; MacWilliams, Karlin, Bhargava Tavares ont étudié les démultipliés des codes résidus quadratiques sur $\mathbb{F}_4$ (*voir* [5] et [6]).

Une des motivations est la recherche de classes de « bons codes » au sens de Shannon (telle que celle des codes de Justesen) ou bien la recherche de codes qui sont individuellement intéressants comme, par exemple, les codes autoduaux binaires à poids multiples de quatre et extrémaux.

D'autre part, l'utilisation des codes démultipliés se prête naturellement au décodage des paquets d'erreurs.

Deux aspects viennent récemment de créer des liens avec la démultiplication : le contre-exemple de Patterson et Wiedeman [10] sur une conjecture concernant le rayon de recouvrement du code de Reed-Muller d'ordre 1 en dimension impaire peut s'interpréter en termes de démultiplication et enfin, la percée de la géométrie algébrique en codage (*voir* [4]) qui fournit des constructions intéressantes de codes sur $\mathbb{F}_{q^m}$.

1.2. CHOIX D'UNE BASE DE $\mathbb{F}_{q^m}$ SUR $\mathbb{F}_q$

La démultiplication dépend du choix d'une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$. On décrit maintenant les différents types de bases utilisées :

– L'opérateur « trace » de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ est défini, comme usuellement par si $Z \in \mathbb{F}_{q^m}$:

$$\text{tr}\, Z = Z + Z^q + \ldots + Z^{q^i} + \ldots + Z^{q^{m-1}}.$$

– Si $B = \{b_1, \ldots, b_m\}$ est une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ sa base duale $B' = \{b'_1, \ldots, b'_m\}$ est l'unique base telle que :

$$\text{tr}\, b_i\, b'_j = \delta_{ij} \quad (1 \text{ si } i=j \text{ et } 0 \text{ sinon}).$$

1.2.1. *Bases « naturelles »*

$B = \{1, \alpha, \ldots, \alpha^{m-1}\}$ ou α racine primitive de $\mathbb{F}_{q^m}$.

1.2.2. *Bases « traces orthogonales »* (TOB)

Si $B = B'$ (tr $b_i b_j = \delta_{ij}$).

Propriété : Si $C = C^\perp$ alors $d(C) = d(C)^\perp$.

1.2.3. *Bases normales*

$$B = \{u, u^q, u^{q^2}, \ldots, u^{q^i} \ldots u^{q^{m-1}}\}$$

existe toujours (*voir* [7]).

1.2.4. *Bases normales trace-orthogonale* (NTOB)

B est à la fois normale et trace-orthogonale.

1.2.5. *Base hermitienne*

Notations : Si $v \in \mathbb{F}_{g^m}$,

$$\bar{v} = v^{q^t} \qquad (t \in \mathbb{N});$$

si :

$$x = (x_1, \ldots, x_n), \qquad \bar{x} = (\bar{x}_1, \ldots, \bar{x}_n).$$

Définition :

$$B = \{u_1, u_2, \ldots, u_m\}$$

telle que :

$$\text{tr}\, u_i\, \bar{u}_j = \delta_{ij}.$$

Propriété : Si pour tout x, y de C, $x.\bar{y} = 0$ alors $d(C) = d(C)^\perp$.

(Le point « . » désigne le produit scalaire usuel.)

2. Résultats

2.1. DÉMULTIPLIÉS DE CODES CYCLIQUES

2.1.1. *Démultipliés de codes cycliques qui sont cycliques*

Soit C un code cyclique sur $\mathbb{F}_{q^s}$ de longueur n et de générateur $g(x)$.

d (C) est son démultiplié par rapport à la base naturelle $\{1, \alpha, \ldots, \alpha^{s-1}\}$ ou α est une racine primitive *de* $\mathbb{F}_{q^s}$.

Lorsque $d(C)$ est cyclique son générateur est noté $\tilde{g}(x)$.

Théorème (Rabizzoni, *voir* [13]) : d (C) *est un code cyclique sur* $\mathbb{F}_q$ *si et seulement si :*

(*a*) $$g(x) \in \mathbb{F}_q[x]$$

et alors :

$$\tilde{g}(x) = g(x^s)$$

ou :

(*b*) $$g(x) = (x - \alpha^s)\, r(x),$$

avec $r(x) \in \mathbb{F}_q[x]$ *et alors :*

$$\tilde{g}(x) = m_\alpha(x)\, r(x^s),$$

avec $m_\alpha(x)$ *polynome minimal de* α *sur* $\mathbb{F}_q$.

Dans V on donnera un exemple d'application de ce théorème au décodage des paquets d'erreurs.

2.1.2. *Codes doublement circulants et formellement autoduaux sur* $\mathbb{F}_4$

Le problème de la découverte de codes autoduaux à poids pairs sur $\mathbb{F}_4$ et extrémaux est largement ouvert (*voir* [7]). Dans le but de contribuer à la résolution de cette question, Delclos et Rabizzoni construisent dans [2] une famille de codes sur $\mathbb{F}_4$ doublement circulants et formellement autoduaux à partir de démultipliés de codes cycliques sur $\mathbb{F}_{16}$. Ils généralisent ainsi des résultats de Beenker.

La présentation des résultats est trop technique pour être retranscrite ici et le lecteur est renvoyé à [2].

2.2. CONSTRUCTION DE CODES AUTODUAUX

2.2.1. *Introduction*

Les codes autoduaux ($C = C^\perp$) sont particulièrement intéressants. Ils possèdent des propriétés algébriques et combinatoires particulières et il a été démontré que (*voir* [7]) :

(*a*) il existe une classe de bons codes linéaires binaires autoduaux;

(*b*) il existe une classe de bons codes linéaires binaires autoduaux à poids multiples de quatre.

On connaît les bornes suivantes (*voir* [7]) :

Si C est un code autodual (ou formellement autodual) binaire de poids minimal $d_{\min}$ alors :

– Si les poids sont pairs :

$$d_{\min} \leqq 2\left[\frac{n}{8}\right] + 2.$$

– Si les poids sont multiples de quatre :

$$d_{\min} \leqq 4\left[\frac{n}{24}\right] + 4$$

([x] désigne la partie entière de x).

Lorsque la borne est atteinte le code est dit extrémal.

Un des objectifs de l'étude des codes autoduaux est de construire effectivement une classe de bons codes et aussi de construire des codes extrémaux.

La méthode utilisée ici pour construire des codes autoduaux sur $\mathbb{F}_q$ est la suivante : on recherche des codes autoduaux sur $\mathbb{F}_{q^m}$ et on les démultiplie sur $\mathbb{F}_q$ par rapport à une base trace orthogonale (TOB) (*voir* 1.2).

Pour trouver des codes autoduaux sur $\mathbb{F}_{q^m}$ on utilisera certains idéaux d'algèbres de groupes particulières.

2.2.2. *Utilisation d'une algèbre de groupe*

Soit G un groupe commutatif fini et K un corps fini $A = K[G]$. L'algèbre du groupe G sur K, est l'ensemble des combinaisons linéaires formelles :

$$x = \sum_{g \in G} x_g X^g \qquad \text{avec} \quad x_g \in K,$$

muni des opérations :

$$x + y = \sum (x_g + y_g) X^g,$$

$$xy = \sum_k \left(\sum_{g+h=k} x_g y_h \right) X^k$$

(la somme $g+h$ est calculée dans G),

$$\lambda x = \sum (\lambda x_g) X^g.$$

Si $G = \{g_0, g_1, ..., g_{n-1}\}$ alors $x = \sum x_g X^g$ est identifié avec $(x_{g_0}, x_{g_1}, ..., x_{g_{n-1}})$.

Les sous-espaces vectoriels de A sont donc identifiés à des codes linéaires sur K de longueur $n = |G|$ et c'est le cas, en particulier, des idéaux de A.

2.2.3. *H-codes*

Les H-codes ont été introduit, dans le cas binaire, par Camion [1].

(*a*) *Théorème et définition*

$$K = \mathbb{F}_{2^r}, \qquad G = (\mathbb{F}_2^k, +),$$

soit :

$$x = \sum_{g \in G} x_g X^g \in K[G].$$

Soit H un hyperplan de $\mathbb{F}_2^k$ (sous-espace de dimension $k-1$).

Soit $C = (x)$ l'idéal principal engendré par x dans K[G].

Si :

$$\sum_{g \in H} x_g = \sum_{g \notin H} x_g = 1,$$

alors :

(*a*) C est un code linéaire autodual sur K;

(*b*) une base de C est $(x X^g)_{g \in H}$.

C sera appellé un H-code.

(*b*) *la construction de Rabizzoni* (voir [12])

Elle permet de trouver simplement une matrice génératrice d'un H-code à partir des composantes d'un générateur x convenable.

On peut formaliser cette construction (*voir* [12]). On va simplement ici décrire le procédé et donner un exemple : soit :

$$x = (x_1, x_2, x_3, x_4, ..., x_{2^r-1}, x_{2^r}) \in \mathbb{F}_2^{2^r},$$

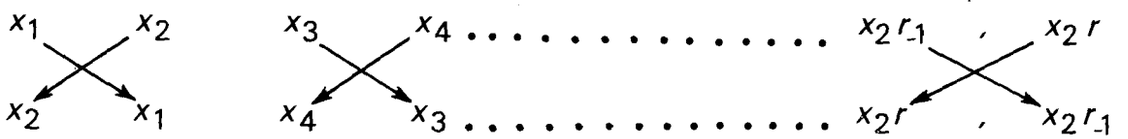
avec

$$\sum_{i=1}^{2^{r-1}} x_i = \sum_{i=2^{r-1}+1}^{2^r} x_i = 1$$

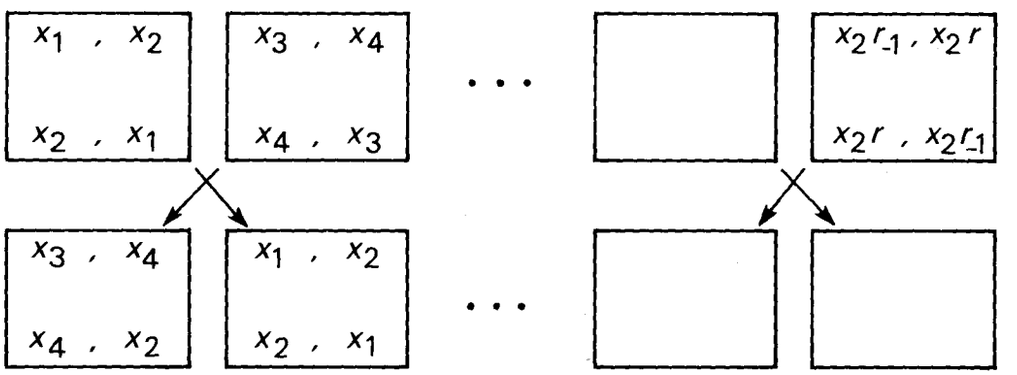
(condition du théorème).

La première ligne de la matrice est x.

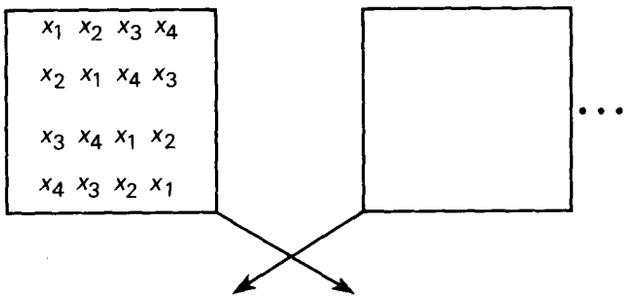
Première étape (construction de la ligne n° 2) :



Deuxième étape (construction des lignes 3 et 4) :



Troisième étape (construction des lignes 5, 6, 7, 8) :



etc.

STOP : lorsque le nombre de colonnes est égal à deux fois le nombre de lignes.

La matrice obtenue est une matrice génératrice du H-code engendré par x.

Exemple : sur $\mathbb{F}_8$,

$$\alpha^3=\alpha+1,$$
$$x=(1, 0, 0, 0, 1, \alpha\ \alpha^2\ \alpha^4)$$

on vérifie :

$$\sum_{i=1}^{4} x_i=\sum_{i=5}^{8} x_i=1$$

et on obtient la matrice :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & \alpha & \alpha^2 & \alpha^4 \\ 0 & 1 & 0 & 0 & \alpha & 1 & \alpha^4 & \alpha^2 \\ 0 & 0 & 1 & 0 & \alpha^2 & \alpha^4 & 1 & \alpha \\ 0 & 0 & 0 & 1 & \alpha^4 & \alpha^2 & \alpha & 1 \end{pmatrix}.$$

2.2.4. *Cas cycliques*

On utilise ici, pour $q=2$ et n entier impair l'algèbre de groupe $K[G]$ avec $K=\mathbb{F}_{2^m}$ corps des racines n-ièmes de l'unité sur $\mathbb{F}_2$, $G=(\mathbb{Z}_n, +)$ le groupe additif des entiers modulo n.

Cette algèbre est semi-simple et isomorphe à celle des polynômes sur K modulo x^n-1 (comme classiquement).

Les idéaux sont principaux et ce sont les codes cycliques (*voir* [7]).

Soit I une partie de $\{0, 1, ..., n-1\}$ et C_I le code cyclique engendré par :

$$g(x)=\prod_{i\in C_I}(x-\alpha^i),$$

où α est une racine n-ième de l'unité sur $\mathbb{F}_2$.

Théorème 1 (*voir* [18]) : *Si* I *et* $-$I *forment une partition de* $\{1, 2, ..., n-1\}$ *alors le code étendu de* C_I *est un code autodual sur* K.

Théorème 2 (*voir* [18]) : *Si* $n=2^m-1$ *et* $I=\{1, 2, ..., (n-1)/2\}$ *alors le code étendu de* C_I (*Reed-Solomon*) *est équivalent à un* H-*code.*

Théorème 3 (*voir* [11]) : *Le* H-*code du théorème* 2 *est engendré* (*dans l'algèbre de groupe correspondante*) *par :*

$$a=1+\sum_{\substack{v\in\mathbb{F}_{2^m}\\ \mathrm{tr}\,v=1}} v^{-1}X^v.$$

2.2.5. *Résultats obtenus*

On indique maintenant les codes autoduaux sur $\mathbb{F}_2$ et $\mathbb{F}_3$ obtenus comme démultipliés par rapport à des bases TOB ou hermitiennes.

(*a*) *Codes binaires autoduaux*

Cas général :

Pour chaque r et k on obtient un code autodual avec :

- longueur : $n=r\,2^k$;
- poids : $d_{\min}\leqq 2^k$.

Démultipliés des codes de Reed-Solomon étendus (th. 2) :

- longueur : $n=k\,2^k$;
- poids : $2^{k-1}+1\leqq d_{\min}\leqq 2^k$.

Exemples :

n	8	12	16		20	24			
$d_{\min}$	4	4	4	4	4	4	6	8	4
Poids multiples de 4	X			X		X	X	X	6 codes
Extrémal	X			X				X	
								↑code de Golay	

n	32	40	64	80	160
d_{min}	8	8	12	$d \in \{8, 12, 16\}$	$d \in \{20, 24, 28\}$
Poids multiples de 4	X	X	X	X	X
Extrémal	X	X	X	?	?

↑
voir
[9]

Codes autoduaux à poids multiples de 4 et extrémaux.
Le tableau ci-dessous indique parmi les longueurs de code extrémaux connus celles correspondantes à des codes obtenus comme démultipliés.

n	8	16	24	32	40	48	56	64	80	88	104
Démultipliés	X	X	X	X	X	?	?	X	?	X	?

(on sait que $n=0 \pmod 8$), *voir* [7]).

(*b*) *Code autodual sur* $\mathbb{F}_3$

Soit C le code cyclique sur $\mathbb{F}_9$ de longueur 5 engendré par $g(x)=x^2+\alpha x+1$ avec $\alpha^2=\alpha+1$ et $\hat{C}$ le code étendu.

Le démultiplié de $\hat{C}$ par rapport à la base (hermitienne) $\{\alpha, \alpha^3\}$ est le code de Golay sur $\mathbb{F}_3$ (12, 6, 6).

2.3. Construction de codes autoduaux binaires a poids multiples de quatre

2.3.1. *La construction*

Soit :

$$K=\mathbb{F}_{2^r}, \qquad G=(\mathbb{F}_{2^m}, +),$$
$$x=\sum_{g\in G} x_g X^g \in K[G],$$

$C=(x)$ idéal principal engendré par x dans $K[G]$.
$B=\{u, u^2, ..., u^{2^j}, ..., u^{2^{r-1}}\}$ une base NTOB de $\mathbb{F}_{2^r}$.

Théorème (Wolfmann, *voir* [16]) : *Si :*

– C *est un* H*-code;*

– $(x_g)_{g\in G}$ *est une réunion de classes pour la conjugaison dans* $\mathbb{F}_{2^r}$;

– $d(ux)$ *a un poids multiple de* 4.

Alors :

Le démultiplié de C *par rapport à* B *est un code linéaire autodual à poids multiple de* 4.

2.3.2. *Exemple* 1 : *utilisation d'un code cyclique* (voir [16])

Soit $B=u, u^2, ..., u^{2^{n-1}}$ une base NTOB de $\mathbb{F}_{2^m}$ sur $\mathbb{F}_2$ et C un code cyclique (n, k) sur $\mathbb{F}_2$, $k>3$.

A chaque mot non nul de C, soit $m(X)=\sum_{i=0}^{n-1} a_i X^i$ on associe par l'application désignée par F, l'élément $\theta=\sum_{i=0}^{n-1} a_i u^{2^i}$ de $\mathbb{F}_2^n$.

Soit $\theta_1, \theta_2, ..., \theta_{2^k-1}$ les images des mots non nul de C par F.

Soit $\varepsilon=(\varepsilon_1, ..., \varepsilon_{2^k}) C \mathbb{F}_2^{2^k}$ tel que le poids $W(\varepsilon)$ de ε vérifie :

$$W(\varepsilon)=-1 \pmod 4.$$

Soit :

$$x=(\varepsilon_1, \varepsilon_2, ..., \varepsilon_{2^k}, 1, \theta_1, \theta_2, ..., \theta_{2^k-1}).$$

Alors x satisfait aux conditions du théorème précédent.

La construction de Rabizzoni appliquée au mot x donne la matrice génératrice d'un code sur $\mathbb{F}_{2^n}$ dont le démultiplié par rapport à B est un code autodual à poids multiple de quatre.

2.3.3. *Exemple* 2 (voir [15])

Soit m entier :

$$r=2^{m-1}-1, \qquad G=(\mathbb{F}_{2^m}, +)$$

et

$$B=u, u^2, ..., u^{2^{r-1}}$$

une base NTOB de $\mathbb{F}_{2^r}$.

Soit H un hyperplan de $\mathbb{F}_{2^m}$ tel que :

$$\mathbb{F}_{2^m} H=\{g_0, g_1, ..., g_{2^{m-1}-1}\},$$

alors :

$$x=1+X^{g_0}+\sum_{i=1}^{2^{m-1}-1} (u^{2^{i-1}}+u^{2^i}) X^{g_i},$$

satisfait aux conditions du théorème (même remarque que pour l'exemple 1 concernant la construction du code correspondant).

Longueur du code $n=2^{2m-1}-2^m$.
Pour $m=3$: (24, 12, 8) code de Golay.
Pour $m=4$: (112, 56, δ) avec $\delta \in 8, 12, 16$.

2.4. Démultiplié et sous-code sur un sous-corps

Si C est un code sur $\mathbb{F}_{q^m}$ le sous-code de C sur $\mathbb{F}_q$, soit C_0, est l'ensemble des mots de C à composantes dans $\mathbb{F}_q$, c'est-à-dire :
$C_0 = C \cap (\mathbb{F}_q)^n$ si n est la longueur du code C.
On dira que C_0 est un sous-code trivial si C est le sous-espace de $(\mathbb{F}_{q^m})^n$ engendré par C_0 sur $\mathbb{F}_{q^m}$. Ceci est équivalent au fait que C possède une matrice génératrice à coefficients dans $\mathbb{F}_q$.
On obtient le théorème suivant :

Théorème (Wolfmann, *voir* [17]) : *Le démultiplié d'un code est un sous-code sur un sous-corps non trivial.*

En conséquence, le code de Golay (24, 12, 8), les codes extrémaux indiqués dans le paragraphe précédent et les codes de Justesen sont des sous-codes sur des sous-corps non triviaux.

2.5. Applications au décodage

Lorsque un code C est un démultiplié il est naturel de l'utiliser pour le décodage de paquets d'erreurs.
En effet, un paquet d'erreur sur $\mathbb{F}_2$ de longueur nm peut être considéré comme le démultiplié d'un mot de longueur n sur $\mathbb{F}_{q^m}$ qui sera traité comme une erreur pour le code dont C est le démultiplié. Le fait que les erreurs sur $\mathbb{F}_q$ se présentent en « paquets » entraîne que plusieurs erreurs sur $\mathbb{F}_q$ correspondent à une seule erreur sur $\mathbb{F}_{q^m}$.

2.5.1. *Exemple* 1 (voir [13])

Cet exemple est une application du résultat de Rabizzoni indiqué en 2.1.1.
Le code BCH binaire (21, 9, 6) de polynôme générateur :

$$g(x)=1+x+x^4+x^6+x^9+x^{10}+x^{12}$$

corrige tous les paquets d'erreurs de longueur au plus 6.($b=6$)

Remarques :
– Ce code est le démultiplié d'un code de Reed-Solomon (7, 3, 5) sur $\mathbb{F}_8$.
– $b=6$ correspond à une valeur optimale ($b \leqq (n-k/2)$.
– Il existe un algorithme de décodage basé sur la démultiplication.

2.5.2. *Exemple* 2 : *décodage du code de Golay* (24, 12, 8) *par permutation* (voir [14])

Pour le principe du décodage par permutation le lecteur est renvoyé à [7] ou [14].
Le résultat suivant détermine un ensemble de permutation pour le code de Golay (24, 12, 8) avec le plus petit nombre possible de permutations nécessaire en résolvant ainsi un problème ouvert posé dans [7].

Théorème (Wolfmann) : I_r *désigne la matrice identité d'ordre r, soit :*

$$A=\begin{pmatrix}1&1&1\\1&0&0\\1&0&1\end{pmatrix} \quad et \quad G=(I_{12}, M).$$

Avec :

$$M=\begin{pmatrix}I_3&A&A^2&A^4\\A&I_3&A^4&A\\2A^2&A^4&I_3&A\\A^4&A^2&A&I_3\end{pmatrix}.$$

(*a*) Le code engendré par la matrice G est le code de Golay (24, 12, 8) [à une équivalence près].

(*b*) L'ensemble D suivant est un ensemble minimal de permutations de décodage pour ce code.

$$D=\{t^i \circ s^j,\ i \in \{0, 1\},$$

$$j \in \{0, 1, 2, 3, 4, 5, 6\}\},$$

avec :

$$s=(4, 7, 16, 10, 22, 19, 13)$$
$$(5, 8, 17, 11, 23, 20, 14)$$
$$(6, 9, 18, 12, 24, 21, 15),$$
$$t=(1, 13)\ (2, 14)\ (3, 15)\ (4, 16)$$
$$(5, 17)\ (6, 18)\ (7, 19)\ (8, 20)$$
$$(9, 21)\ (10, 22)\ (11, 23)\ (12, 24).$$

Remarque : Ce résultat est obtenu à partir de la démultiplication indiquée en 2.2.5.

2.5.3. *Décodage de démultipliés de codes de Reed-Solomon*

Les codes de Reed-Solomon étendus de longueur 2^m sont invariants par le groupe affine de $\mathbb{F}_{2^m}$ (*voir* [7]). Cette propriété peut être utilisée pour le décodage. L'article de Papini [8] figurant dans le même numéro de cette revue traité de cette question.

Conclusion

L'étude systématique de la démultiplication a fourni des résultats intéressants et offre des perspectives notamment en ce qui concerne les techniques de décodage pour lesquelles des questions sont largement ouvertes.

BIBLIOGRAPHIE

[1] P. CAMION, Étude de codes binaires abéliens modulaires autoduaux de petites longueurs, *Revue du CETHEDEC*, NS79-2, 1979, p. 3-24.

[2] G. DELCLOS et P. RABIZZONI, exposé au *Colloque international Algèbre et codes correcteurs*, Toulouse, juin 1983, *Ann. Discrete Math.* (à paraître).

[3] I. I. DUMER et V. A. ZINOV'EV, *Some new maximal codes over* GF (4), *Problems of Information Transmission*, 1979.

[4] V. D. GOPPA, Codes on algebric curves, *Soviet Math. Dokl.*, 24, 1981, p. 170-172.

[5] M. KARLIN, V. K. BHARGAVA et S. E. TAVARES, A note on extended quaternary quadratic residue codes and their binary images, *Information and Control*, 38, 1978, p. 148-153.

[6] M. KARLIN et F. J. MACWILLIAMS, Quadratic residue codes over GF (4) and their binary images, *IEEE International Symposium on Information Theory*, Asilomar, Calif., 1972.

[7] F. J. MACWILLIAMS et N. J. A. SLOANE, *The theory of error correcting codes*, North-Holland, 1977.

[8] O. PAPINI, Permutations et décodage (*voir* le présent numéro).

[9] G. PASQUIER, A binary extremal doubly even self dual code (64, 32, 12) obtained from an extended Reed-Solomon code over $\mathbb{F}_{16}$, *IEEE Trans. Inf. Theory*, novembre 1981.

[10] N. J. PATERSON et D. H. WIEDEMAN, The covering radius of the (2^{15}, 16) Reed-Muller code is at least 16276, *IEEE Trans. Inf. Theory*, IT 29, 1983, p. 354-356.

[11] R. PONS, Expression de certains codes de Reed-Solomon étendus en tant que H-codes, *Revue du CETHEDEC*, 75, 1983, p. 35-48.

[12] P. RABIZZONI, Images binaires d'idéaux principaux d'une algèbre de groupe, *Revue du CETHEDEC*, NS81-2, 1981.

[13] P. RABIZZONI, exposé au *Colloque international Algèbre et codes correcteurs*, Toulouse, juin 1983, A paraître dans *Ann. Discrete Math.* (à paraître).

[14] J. WOLFMANN, A permutation decoding of the (24, 12, 8) Golay code, *IEEE Trans. Inf. Theory*, septembre 1983.

[15] J. WOLFMANN, Une classe de codes binaires autoduaux à poids multiples de quatre, exposé au *Colloque international Algèbre et codes correcteurs*, Toulouse, juin 1983, *Ann. Discrete Math.* (à paraître).

[16] J. WOLFMANN, Une construction de codes autoduaux binaires à poids multiples de quatre (soumis à publication).

[17] J. WOLFMANN, Démultipliés et sous-codes sur les sous-corps (en préparation).

[18] J. WOLFMANN et G. PASQUIER, A class of binary self dual codes, Rapport interne GECT.