# Construction d'une famille de codes autoduaux binaires

## A family of binary self dual codes

J. A. THIONG-LY

AAECC, Laboratoire LSI, Université Paul-Sabatier, 31000 TOULOUSE

**RÉSUMÉ**

On donne une caractérisation des codes de Reed-Solomon généralisés autoduaux sur $\mathbb{F}_{q^m}$, et une construction d'une famille de codes autoduaux binaires à poids multiple de quatre.

**MOTS CLÉS**

Codes Reed-Solomon, trace, image binaire, autoduaux.

***SUMMARY***

*First, we give a characterization of autodual generalized Reed-Solomon codes over $\mathbb{F}_{q^m}$, then we give a family of binary autodual codes with weight divisible by four.*

***KEY WORDS***

*Reed-Solomon, codes, trace, binary image, self dual.*

## TABLE DES MATIÈRES



## Introduction

Généralisant certains travaux de P. Camion sur les H-codes binaires [1], G. Pasquier dans [2] étudie les codes sur une extension de $\mathbb{F}_2$ et leurs images binaires par rapport à une base trace « orthogonale » [5], pour obtenir des codes autoduaux binaires.

J. Wolfmann dans [4], propose une nouvelle construction du (24, 12, 8) code de Golay binaire.

Dans le présent article, nous proposons un résultat nouveau (th. 1) pour caractériser les codes de Reed-Solomon généralisés (codes GRS) sur $\mathbb{F}_{q^m}$ qui sont autoduaux.

En particulier, lorsque $q=2$, pour tout sous-ensemble de $\mathbb{F}_{2^m}$ de cardinal pair N, nous construisons un code GRS autodual sur $\mathbb{F}_{2^m}$ de longueur N.

Ceci permet, en prenant l'image binaire par rapport à une base trace orthogonale de construire des codes autoduaux binaires de longueur $m$ N.

Nous mettons de cette manière en évidence une famille de codes autoduaux binaires à poids multiple de 4, qui contient le (24, 12, 8) code de Golay.

## 1. Codes généralisés de Reed-Solomon autoduaux

Soient deux N-uplets $a$ et $v$ à composantes dans $\mathbb{F}_{q^m}$ :

$$a=(a_1, \ldots, a_N),$$

où les $a_i$ sont tous distincts,

$$v=(v_1, \ldots, v_N),$$

où les $v_i$ sont tous non nuls mais non nécessairement distincts.

On pose :

$$F(x)=\prod_{i=1}^{N}(x-a_i),$$

et on note $F'(x)$ sa dérivée.

*Définition du code* [3], p. 303

Pour tout entier K ($K \leqq N$), désignons par $E_K$ le sous-espace des polynomes à coefficients dans $\mathbb{F}_{q^m}$, de degré inférieur ou égal à $K-1$.

L'ensemble des N-uplets de $\mathbb{F}_{q^m}^N$ de la forme

$$(v_1 u(a_1), \ldots, v_N u(a_N)),$$

lorsque $u(x)$ parcourt $E_K$, est appelé un code de Reed-Solomon généralisé.

On notera un tel code : $GRS_K(a, v)$.

C'est un (N, K) code linéaire de distance minimale :

$$D=N-K+1.$$

Un code GRS est donc un code « MDS », [3].

Il résulte de la définition que $GRS_K(a, v)$ admet une matrice génératrice de la forme :

$$(I)\begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_N \\ \vdots & \vdots & & \vdots \\ a_1^{K-1} & a_2^{K-1} & \ldots & a_N^{K-1} \end{pmatrix} \times \begin{pmatrix} v_1 & & & 0 \\ & v_2 & & \\ & & \ddots & \\ 0 & & & v_n \end{pmatrix}$$

Démontrons la proposition suivante :

Proposition 1 : *Pour tout entier* K ($1 \leqq K \leqq N-1$), *l'orthogonal de* $GRS_K(a, v)$ *est* $GRS_{N-K}(a, w)$ *où les composantes de* $w=(w_1, \ldots, w_N)$ *sont :*

$$w_i=\frac{1}{v_i F'(a_i)} \qquad (1 \leqq i \leqq N).$$

*Démonstration :* Considérons la matrice A suivante :

$$A=\begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_N \\ \vdots & \vdots & & \vdots \\ a_1^{N-2} & a_2^{N-2} & \ldots & a_N^{N-2} \end{pmatrix}.$$

Montrons que le noyau de A est engendré par

$$\left(\frac{1}{F'(a_1)}, \ldots, \frac{1}{F'(a_N)}\right).$$

En effet, dire que $(y_1, \ldots, y_N)$ est dans le noyau de A, équivaut à écrire :

$$\begin{pmatrix} 1 & \ldots & 1 \\ a_1 & \ldots & a_{N-1} \\ \vdots & & \vdots \\ a_1^{N-2} & \ldots & a_{N-1}^{N-2} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_{N-1} \end{pmatrix} = -y_N \begin{pmatrix} 1 \\ a_N \\ \vdots \\ a_N^{N-2} \end{pmatrix}.$$

La résolution de ce système conduit aux valeurs :

$$y_i=-y_N \frac{\Delta(a_1, \ldots, a_{i-1}, a_N, a_{i+1}, \ldots, a_{N-1})}{\Delta(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_{N-1})} \qquad (1 \leqq i \leqq N-1),$$

où $\Delta(x_1, \ldots, x_{N-1})$ désigne le déterminant de Van Der Monde des éléments $x_1, \ldots, x_{N-1}$.

Posons :

$$y_N=\frac{1}{F'(a_N)}.$$

On vérifie alors que :

$$y_i=\frac{1}{F'(a_i)} \qquad (1 \leqq i \leqq N-1).$$

Déterminons maintenant le vecteur $w$.

Pour cela, cherchons l'orthogonal du code $GRS_{N-1}(a, v)$.

Dire qu'un vecteur $(y_1, \ldots, y_N)$ appartient à l'orthogonal de $GRS_{N-1}(a, v)$ équivaut à dire que $(v_1, y_1, \ldots, v_N y_N)$ appartient au noyau de la matrice A précédente.

Posons :

$$w=(w_1, \ldots, w_N),$$

avec :

$$w_i=\frac{1}{v_i F'(a_i)} \qquad (1 \leqq i \leqq N).$$

Pour tout $i$ ($1 \leqq i \leqq N$), $w_i$ est non nul.

Il en résulte que l'orthogonal de $GRS_{N-1}(a, v)$ est $GRS_1(a, w)$.

Enfin, montrons que $GRS_K(a, w)$ et $GRS_{N-K}(a, w)$ sont orthogonaux.

Effectuons le produit scalaire d'une ligne $i\,(i \leqq K-1)$ de la matrice génératrice de $GRS_K(a, v)$ et d'une ligne $j$ $(j \leqq N-K-1)$ de la matrice génératrice de $GRS_{N-K}(a, w)$ :

$$\sum_{s=1}^{N} (a_s^i v_s)(a_s^j w_s) = \sum_{s=1}^{N} a_s^{i+j} v_s w_s = \sum_{s=1}^{N} a_s^{i+j} \frac{1}{F'(a_s)}.$$

Or nous avons vu que :

$$\left( \frac{1}{F'(a_1)}, \ldots, \frac{1}{F'(a_N)} \right),$$

appartient au noyau de la matrice A. ce produit est donc nul.

Autrement dit : l'orthogonal de $GRS_K(a, v)$ est $GRS_{N-K}(a, w)$.

C.Q.F.D.

*Remarques :* la proposition précédente est démontrée dans [3], th. 4, p. 304, mais sans préciser la valeur de $w$.

Dans le cadre des codes de Goppa, la valeur de $w$ est indiquée dans [3], th. 4, p. 340 et problème 2, p. 341.

Nous pouvons maintenant énoncer notre caractérisation des GRS codes autoduaux :

Théorème 1 : *on suppose* N *pair.*

*Il existe un code* $GRS_{N/2}(a, v)$ *autodual sur* $\mathbb{F}_{q^m}$ *si et seulement si il existe un polynome* $G(x)$ *à coefficients dans* $\mathbb{F}_{q^m}$ *tel que :*

$$F'(x) \equiv \lambda [G(x)]^2 \text{ modulo } F(x) \quad (\lambda \in \mathbb{F}_{q^m}^*).$$

*Démonstration :* D'après la proposition 1, $GRS_{N/2}(a, v)$ autodual équivaut à :

$$GRS_{N/2}(a, v) = GRS_{N/2}(a, w).$$

D'après [3], p. 305, ceci équivaut à :

$$v = \mu w \qquad \text{avec} \quad \mu \in \mathbb{F}_{q^m}^*.$$

C'est-à-dire :

$$v_i = \mu w_i = \mu \frac{1}{v_i F'(a_i)}.$$

De manière équivalente :

$$F'(x) \equiv \lambda [G(x)]^2 \text{ modulo } F(x) \quad (\lambda \in \mathbb{F}_{q^m}^*),$$

où $G(x)$ est défini par :

$$G(a_i) = v_i^{-1} \qquad (1 \leqq i \leqq N).$$

Q.E.D.

Une matrice génératrice du code s'écrit alors :

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_N \\ \vdots & \vdots & & \vdots \\ a_1^{(N/2)-1} & a_2^{(N/2)-1} & \ldots & a_N^{(N/2)-1} \end{pmatrix} \times \begin{pmatrix} G(a_1)^{-1} & & & 0 \\ & G(a_2)^{-1} & & \\ & & \ddots & \\ 0 & & & G(a_N)^{-1} \end{pmatrix}$$

Dans le cas où le corps $\mathbb{F}_q$ est de caractéristique 2, quel que soit $f(x)$ appartenant à $\mathbb{F}_q[x]$, la dérivée $f'(x)$ est un carré.

On peut donc énoncer le :

Corollaire 1 : *On suppose* N *pair et* $\mathbb{F}_q$ *de caractéristique* 2.

*Pour tout sous-ensemble* $\{a_1, \ldots, a_N\}$ *de* $\mathbb{F}_{q^m}$, *on pose :*

$$F(x) = \prod_{i=1}^{N} (x - a_i).$$

*Notons :*

$$F'(x) = [G(x)]^2.$$

*Alors le code* $GRS_{N/2}(a, v)$ *où :*

$$a = (a_1, \ldots, a_N)$$

*et*

$$v = (G(a_1)^{-1}, \ldots, G(a_N)^{-1})$$

*est un code autodual sur* $\mathbb{F}_{q^m}$.

Illustrons le corollaire 1 sur un exemple.

*Exemple :*

$$m = 2, \qquad q = 2^2, \qquad \mathbb{F}_{2_2} = F_2(\alpha),$$

$$F_{4^2} = \mathbb{F}_4(\beta) = \frac{F_4[x]}{(x^2 + x + \alpha)}$$

($\alpha$ racine primitive de $\mathbb{F}_{2^2}$, $\beta$ racine primitive de $F_{4^2}$).

Choisissons :

$$a = (\beta^3, \beta^5, \beta^7, \beta^8, \beta^{10}, \beta^{12}),$$

on trouve alors :

$$F'(x) = (\beta^9 x^2 + \beta^3 x - \beta^9)^2.$$

D'où :

$$v_i = G(a_i)^{-1} \qquad (1 \leqq i \leqq 6);$$

soit :

$$v = (\beta^5, \beta^9, \beta^{12}, \beta^{11}, \beta^4, \beta^{11}).$$

Avec ces valeurs de $a$ et de $v$, le code $GRS_3(a, v)$ est un (6, 3, 4) code autodual sur $\mathbb{F}_{4^2}$ admettant la matrice génératrice suivante :

$$\begin{pmatrix} \beta^5 & \beta^9 & \beta^{12} & \beta^{11} & \beta^4 & \beta^{11} \\ \beta^8 & \beta^{14} & \beta^4 & \beta^4 & \beta^{14} & \beta^8 \\ \beta^{11} & \beta^4 & \beta^{11} & \beta^{12} & \beta^9 & \beta^5 \end{pmatrix}.$$

Corollaire 2 : *Soit $c$ une racine $e$-ième de l'unité dans $\mathbb{F}_{2^m}$.*
*Alors* $GRS_{(e+1)/2}(a, v)$ *avec :*

$$a=(0, 1, c, \ldots, c^{e-1})$$

et

$$v=(1, 1, 1, \ldots, 1)$$

*est un code autodual sur $\mathbb{F}_{2^m}$.*

*Démonstration :* En effet :

$$F(x)=x^{e+1}-x.$$

Comme $e+1\equiv 0 \bmod 2$, on a $F'(x)=1$.
Soit $\alpha$ une racine primitive de $\mathbb{F}_{2^m}$. Posons $N=2^m$.

Corollaire 3 : *L'étendu* RS *du code de Reed-Solomon engendré par :*

$$g(x)=\prod_{i=1}^{2^{m-1}-1}(x-\alpha^i)$$

*dans $\mathbb{F}_{2^m}[x]/(x^{2^{m-1}}-1)$ est un code autodual sur $\mathbb{F}_{2^m}$.*

*Démonstration :* En effet :

$$RS=GRS_{N/2}(a, v),$$

avec :

$$a=(0, 1, \alpha, \ldots, \alpha^{N-2})$$

et

$$v=(1, 1, \ldots, 1).$$

*Remarque :* Les deux résultats précédents ne sont pas nouveaux : ils ont été démontrés par P. Camion (en utilisant les caractères de groupe) et sont décrits dans [2], p. 96 et 105.

## 2. Construction de codes autoduaux binaires

2.1. Rappels de quelques définitions et propriétés (*cf.* [2, 3] pour les démonstrations)

Soit $\{e_1, \ldots, e_m\}$ une $F_q$-base de $\mathbb{F}_{q^m}$. Tout élément $x$ de $\mathbb{F}_{q^m}$ s'écrit :

$$x=\sum_{i=1}^{m} x_i e_i \qquad (x_i \in \mathbb{F}_q).$$

L'image $q$-aire (ou image démultipliée) d'une partie P de $\mathbb{F}_{q^m}^N$ par rapport à la base $\{e_1, \ldots, e_m\}$ est la partie notée $d(P)$ de $\mathbb{F}_q^{mN}$ obtenue en remplaçant chaque composante $x^x$ d'un N-uplet de P par le $m$-uplet $(x_1, \ldots, x_m)$.

Propriété 1 : Si $c$ est un (N, K) code linéaire sur $\mathbb{F}_{q^m}$, sur image $q$-aire $d(c)$ est un $(mN, mK)$ code sur $\mathbb{F}_q$ de distance supérieure ou égale à la distance de $c$.

Propriété 2 : Si G est une matrice génératrice d'un code $c$ sur $\mathbb{F}_{q^m}$, et $\{e_1, \ldots, e_m\}$ une $\mathbb{F}_q$ base de $\mathbb{F}_{q^m}$, alors la matrice :

$$\begin{pmatrix} d(e_1 G) \\ d(e_2 G) \\ \vdots \\ d(e_m G) \end{pmatrix}$$

est une matrice génératrice de $d(c)$.

Une base $\{e_1, \ldots, e_m\}$ de $\mathbb{F}_{q^m}$ est dite trace orthogonale lorsque $\text{Trace}_{F_q}(e_i e_j)=\delta_{ij}$.

Propriété 3 : L'image $q$-aire d'un code autodual sur $\mathbb{F}_{q^m}$ par rapport à une base trace orthogonale est un code autodual sur $\mathbb{F}_q$.

Propriété 4 : Pour tout entier $m$, $\mathbb{F}_{2^m}$ admet une $F_2$ base trace orthogonale [5].

Propriété 5 : Si un code binaire est inclus dans son orthogonal et admet une matrice génératrice dont les lignes sont à poids multiple de 4, alors tout mot de ce code est à poids multiple de 4.

Propriété 6 : La distance $d$ d'un code autodual binaire de longueur N à poids multiple de 4 vérifie :

$$d \leqq 4\left[\frac{N}{24}\right]+4.$$

2.2. Construction de codes autoduaux binaires de longueurs $mN$ $(N<2^m)$

On choisit dans $\mathbb{F}_{2^m}$, N (N pair) éléments distincts quelconques $a_1, \ldots, a_N$.
On construit un (N, N/2, (N+2)/2) code autodual

$$c=GRS_{N/2}(a, v)$$

en utilisant le corollaire 1.
Le code $d(c)$ image binaire du code $c$ par rapport à une base trace orthogonale de $\mathbb{F}_{2^m}$ est un $(mN, mN/2)$ code binaire autodual dont la distance $d$ vérifié :

$$\frac{N+2}{2} \leqq d \leqq 4\left[\frac{mN}{24}\right]+4.$$

2.3. Une famille de codes autoduaux binaires a poids multiple de 4

D'après le corollaire 2, les codes $GRS_{2^{m-1}}(a, v)$ avec :

(1) $$a=(0, 1, \alpha, \ldots, \alpha^{2^{m-2}}),$$

(2) $$v=(1, 1, \ldots, 1),$$

sont des codes autoduaux sur $\mathbb{F}_{2^m}$.

Proposition 2 : *Pour m tel que* $2^m-1$ *soit premier, l'image binaire par rapport à toute base trace orthogonale du* $GRS_{2^{m-1}}(a, v)$ *où a et v sont définis par* (1) *et* (2), *est un code autodual à poids multiple de* 4.

*Pour* $m=3$, *l'image binaire est le* (24, 12, 8) *code de Golay.*

*Démonstration :* Une matrice génératrice de $GRS_{2^{m-1}}(a, v)$ s'écrit :

$$G=\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \alpha & \dots & \alpha^{2^m-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & \alpha^{2^{m-1}-1} & \dots & \alpha^{(2^{m-1}-1)(2^m-2)} \end{pmatrix}.$$

Comme $2^m-1$ est premier, toutes les lignes de G sauf la première, sont des permutations de $\mathbb{F}_{2^m}$.

Soit $\{e_1, \dots, e_m\}$ une base de $\mathbb{F}_{2^m}$.

Une matrice génératrice $\bar{G}$ de l'image binaire s'écrit, d'après la propriété 2 :

$$\bar{G}=\begin{pmatrix} d(e_1 G) \\ \vdots \\ d(e_m G) \end{pmatrix}.$$

Montrons que les lignes de $\bar{G}$ sont à poids divisible par 4.

Pour tout $i$ $(1 \leqq i \leqq m)$, $e_i G$ admet pour première ligne $L_i=(e_i, e_i, \dots, e_i)$.

Le poids de $d(L_i)$ est donc un mutiple de $2^m$.

Toutes les autres lignes de $e_i G$ étant des permutations de $\mathbb{F}_{2^m}$, le poids de l'image binaire de chacune de ces lignes est $2^{m-1} \times m$.

Toutes les lignes de $\bar{G}$ sont donc à poids multiple de 4.

Si on choisit une base trace orthogonale pour démultiplier, le code engendré par $\bar{G}$ est autodual.

On conclut en utilisant la propriété 5 que tous les mots du code engendré par $\bar{G}$ sont à poids multiple de 4.

*Pour* $m=3$ : $GRS_4(a, v)$ est un (8, 4, 5) code sur $\mathbb{F}_{2^3}$.

Son image binaire par rapport à toute base trace orthogonale est un (24, 12) code autodual dont la distance $d$ vérifie :

$$5 \leqq d \leqq 4\left[\frac{24}{4}\right]+4=8.$$

on conclut que $d=8$.

Corollaire 4 : *Lorsque* $2^m-1$ *est premier, l'image binaire* $d(RS)$ *par rapport à une base trace orthogonale d'un code de Reed-Solomon* RS *étendu d'un* RS *engendré par :*

$$g(x)=\prod_{i=1}^{2^{m-1}-1}(x-\alpha^i),$$

*est un code autodual binaire à poids multiple de* 4.

*Remarque :* Pour $m=5$, $GRS_{16}(a, v)$ est un (32, 16, 17) code sur $\mathbb{F}_{2^5}$.

Son image binaire par rapport à toute base trace orthogonale est un (160, 80) code autodual binaire dont la distance $d$ vérifie $28 \geqq d \geqq 20$.

*Cas où* $2^m-1$ *n'est pas premier*

Pour $i$ tel que $i/2^m-1$ et $i<2^{m-1}-1$, la ligne $(i+1)$ de la matrice G est constituée des éléments du sous-groupe $G_i$ engendré par $\alpha^i$.

Les lignes de la matrice $\bar{G}$ sont à poids multiple de 4 lorsque les images binaires des translatés $e_i G_i$ $(1 \leqq i \leqq m)$ de ces sous-groupes sont à poids multiple de 4.

*Exemple :* Un (64, 32, 12) code autodual binaire à poids multiple de 4.

On choisit :

$$m=4, \qquad \mathbb{F}_{2^4}=\mathbb{F}_2(\alpha)=\frac{\mathbb{F}_2[x]}{(x^4+x+1)}.$$

On a deux sous-groupes :

$$G_1=\{1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}\},$$
$$G_2=\{1, \alpha^5, \alpha^{10}\},$$

on vérifie que par rapport à la base trace orthogonale $\{\alpha^3, \alpha^7, \alpha^{12}, \alpha^{13}\}$, les images binaires $d(e_i G_j)$ $(1 \leqq i \leqq 4, 1 \leqq j \leqq 2)$ sont à poids multiple de 4.

On conclut suivant les mêmes arguments que précédemment.

Nous retrouvons ainsi le code décrit par G. Pasquier dans [2].

## Conclusion

Les deux résultats principaux que nous avons mis en évidence (théorème 1 et corollaire 1) nous ont permis d'une part de retrouver les propriétés des codes intéressants décrits par G. Pasquier dans [2], d'autre part, nous permet d'envisager la recherche (par ordinateurs) de bons codes autoduaux sur $\mathbb{F}_q$ démultipliées de codes autoduaux sur $\mathbb{F}_{q^m}$.

### BIBLIOGRAPHIE


[1] P. Camion, Étude de codes binaires abéliens modulaires autoduaux de petites longueurs, *Revue du CETHEDEC*, n° 5, NS79-2, p. 3-24.

[2] G. Pasquier, Étude des codes sur une extension de $F_2$ et de leurs images binaires, *Thèse de 3e cycle*, Université de Provence, 1980.

[3] F. J. Mac Williams et N. J. A. Sloane, *The Theory of Error correcting codes*, North Holland, 1978.

[4] J. Wolfmann, A New construction of the binary Golay Code (24, 12, 8) using a group algebra over a finite field, *Discrete Math.*, 31, 1980, p. 337-338.

[5] D. Lenpel, Matrix factorisation over GF(2) and trace orthogonal basis of F($2^m$), *SIAM J. COMP.*, 4, n° 2, 1971.