HAL open science

Groupe d'automorphismes des codes de Reed-Muller P-aires

Thierry Pierre Berger

To cite this version:

Thierry Pierre Berger. Groupe d'automorphismes des codes de Reed-Muller P-aires. [Rapport de recherche] RR-1630, INRIA. 1992. inria-00074931

HAL Id: inria-00074931

https://inria.hal.science/inria-00074931

Submitted on 24 May 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNITE DE RECHERCHE
INRIA-ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P. 105
78153 Le Chesnay Cedex
France
Tél (1) 39 63 55 11

Rapports de Recherche
1992
25ème anniversaire
N° 1630

Programme 2
Calcul Symbolique, Programmation et Génie logiciel

GROUPE D'AUTOMORPHISMES DES CODES DE REED-MULLER *P*-AIRES

Thierry BERGER

Mars 1992

RR.1630

Groupe d'automorphismes des codes de Reed-Muller p-aires

Thierry Berger*

Résumé

Nous démontrons que le groupe d'automorphismes des codes de Reed-Muller p-aires est le groupe général affine. Les codes de Reed-Muller généralisés ont été définis par Kasami, Lin et Peterson, puis étudiés en détail par Delsarte, Goethals et MacWilliam. Les codes de Reed-Muller p-aires sont les puissances du radical d'une algèbre modulaire, et, sous cette forme, P.Charpin a donné une description de l'ensemble des mots de poids minimum de ces codes. Nous utilisons cette description pour caractériser géométriquement le groupe d'automorphismes de ces codes.

The automorphism group of p-ary Reed-Muller codes.

Abstract

We prove that the automorphism group of the p-ary Reed-Muller codes is the general linear nonhomogeneous group. The generalized Reed-Muller codes were introduced by Kasami, Lin and Peterson. Then an extensive study was made by Delsarte, Goethals and MacWilliam. The p-ary Reed-Muller codes are the radical powers of a modular algebra. Using this description, P.Charpin gave an explicit presentation of the minimum weight codewords. We characterize their automorphism group, by mean of geometric properties of these minimum weight codewords.

*UFR des Sciences de Limoges, 123 av. A.Thomas, 87060 Limoges Cedex, France.
Chercheur extérieur du Projet Codes

1 Introduction

Soit p un nombre premier. On désigne par G le groupe additif du corps fini F_{p^m}, $m \geq 1$, par K le corps fini F_{p^s}, et par A l'algèbre modulaire $K[G]$.

Un élément x de A est un polynôme formel

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

La multiplication dans A est le prolongement de l'addition dans F_{p^m}:

$$\sum_{g \in G} x_g X^g \ \times \sum_{g \in G} y_g X^g \ = \sum_{g,h \in G} x_g y_h X^{g+h} \ .$$

La structure du corps fini F_{p^m} restant sous-jacente, par abus de langage on identifiera G et F_{p^m}.

Le radical P de A est l'ensemble des éléments nilpotents de A :

$$P = \left\{ x = \sum_{g \in G} x_g X^g / \sum x_g = 0 \right\} \ .$$

L'idéal P^j, $1 \leq j \leq M$, $M = m(p-1)$, est le code de Reed-Muller p-aire de longueur p^m, et d'ordre $M - j$ (pour la démonstration des résultats, on pourra consulter [4]).

Soit $S(G)$ le groupe des permutations de G. Un élément $\sigma \in S(G)$ agit sur A de la manière suivante :

$$\sigma : \sum_{g \in G} x_g X^g \longrightarrow \sum_{g \in G} x_g X^{\sigma(g)} \ .$$

On note

T le groupe des translations de G:

$$T = \{\tau_b \in S(G) / b \in G \ , \forall g \in G \ , \tau_b(g) = g + b\} \ .$$

GL_m le groupe linéaire de F_{p^m} sur F_p.

GA_m le groupe affine de F_{p^m} sur F_p : il s'agit du groupe engendré par GL_m et T.

On désigne par $Per(P^j)$ le sous-groupe de $S(G)$ qui laisse P^j globalement invariant.

Il est clair que $Per(P) = Per(P^M) = S(G)$. Lorsque $m = 1$, le code P^j est en fait un code de Reed-Solomon étendu. Son groupe d'automorphismes est connu (cf. [7, 2]), il s'agit du groupe des homothéthies-translations de G:

$$GA_1 = \{\sigma_{a,b} \in S(G)/a \in G^*, b \in G, \forall g \in G, \sigma_{a,b}(g) = ag + b\}$$

Lorsque $p = 2$, le groupe d'automorphismes des codes de Reed-Muller est aussi connu: il s'agit du groupe GA_m (cf. [10] ch.13).

Dans [6], P.Delsarte, J.M.Goethals et F.J.MacWilliams ont montré que, dans tous les cas, GA_m est inclus dans le groupe d'automorphismes des codes de Reed-Muller P^j.

Nous démontrons dans cet article la réciproque de la proposition précédente, à savoir que le groupe d'automorphismes des codes de Reed-Muller P^j, pour $1 < j < m(p-1)$, est exactement le groupe GA_m. Ce résultat a déjà été démontré par P.Knörr et W.Willem [9] d'une manière trés différente et assez sophistiquée, puisque leur démonstration utilise la classification des groupes simples finis deux fois transitifs. De plus, la démonstration donnée dans [9] utilise le fait que les codes considérés sont les puissances du radical, et de ce fait la démonstration ne peut pas s'étendre aux codes de Reed-Muller généralisés tels qu'ils sont définis par P.Delsarte, J.M.Goethals et F.J.MacWilliam dans [6].

Par contre, avec P.Charpin (cf. [3]) nous avons pû généraliser la démonstration présentée dans ce rapport. Celle-ci est malheureusement assez technique et délicate, et il nous a paru intéressant de présenter cette démonstration dans le cas particulier des puissances du radical, ce qui amène beaucoup de simplifications et évite d'introduire la définition de ces codes en tant que codes cycliques.

2 Notion d'automorphisme isométrique d'un code linéaire.

Un *code linéaire* C de longueur p^m sur $K = F_{p^s}$ est un sous-espace vectoriel de K^{p^m}.

On peut toujours considérer le code C comme un sous-espace vectoriel de A en utilisant l'isomorphisme suivant:

Si $\{e_1, ..., e_{p^m}\}$ est la base canonique de K^{p^m}, et si α est une racine primitive de $G = F_{p^m}$, à $e_i \in K^{p^m}, 1 \leq i < p^m$, on associe $X^{\alpha^i} \in A$, et à e_{p^m}, on associeX^0.

Nous considérerons donc les codes de longueur p^m comme des sous-espaces vectoriels de A.

A un élément $x = \sum_{g \in G} x_g X^g$ de A, appelé *mot* de A, on associe son *support*

$$Supp(x) = \{g \in G/x_g \neq 0\} \subset G$$

Le *poids* de x, noté $w(x)$, est le cardinal du support de x.
La *distance de Hamming* associée est définie par $d(x,y) = w(x-y)$.

Un automorphisme isométrique de A en tant que K−espace vectoriel est alors une bijection linéaire de A dans A qui conserve la distance de Hamming, donc le poids des mots de A.

Un tel automorphisme est entièrement défini par la donnée des images des éléments X^g, $g \in G$. La conservation des poids permet d'écrire

$$f(X^g) = a_g X^{g'}, a_g \in K^*, g' \in G.$$

Soit $\sigma \in S(G)$ la permutation définie par $\sigma(g) = g'$, alors

$$f(x) = \sum_{g \in G} a_g x_g X^{\sigma(g)}$$

Le groupe des automorphismes isométriques de A est alors le produit semi-direct $(K^*)^G \rtimes S(G)$, isomorphe au groupe des matrices monomiales $p^m \times p^m$ à coefficients dans K^* (il s'agit des matrices ayant un et un seul coefficient non nul par ligne et par colonne).

Soit C un code de A. on désigne par $ML(C)$ (groupe monomial de C) le sous-groupe de $(K^*)^G \rtimes S(G)$ qui laisse le code C globalement invariant, par $Per(C)$ le sous-groupe de $ML(C)$ composé des permutations de G, et par $Aut(C)$ l'image de $ML(C)$ par la projection π

$$\begin{array}{rccc} \pi : & ML(C) & \longrightarrow & S(G) \\ & (a,\sigma) & \longrightarrow & \sigma \end{array}$$

L'inclusion $Per(C) \subset Aut(C)$ est évidente.

Soit i l'injection de K^* dans $(K^*)^G$ définie par $i(a) = (a_g)_{g \in G}$ avec $a_g = a$ pour tout g de G.

Lorsque $Per(C) = Aut(C)$, la suite

$$K^* \xrightarrow{i} ML(C) \xrightarrow{\pi} Aut(C)$$

est exacte et scindée, on a alors

$$ML(C) = K^* \times Per(C) \tag{1}$$

Dual d'un code. Si $x = \sum_{g \in G} x_g X^g$, et $y = \sum_{g \in G} y_g X^g$, on définit le produit scalaire de x et y par

$$< x, y >= \sum_{g \in G} x_g y_g$$

Le code dual $\widehat{C}$ du code C est alors l'ensemble des mots $y \in A$ tels que $< x, y >= 0$ pour tout $x \in C$.

Proposition 1 *Soit C un code linéaire et $\widehat{C}$ son dual, alors*

1. $Per(\widehat{C}) = Per(C)$
2. $Aut(\widehat{C}) = Aut(C)$
3. $ML(\widehat{C}) = \{(a^{-1}, \sigma) / \ (a, \sigma) \in ML(C)\}$
   avec $a = (a_g)_{g \in G}$, $a_g \in K^*$, *et* $a^{-1} = (a_g^{-1})_{g \in G}$

Preuve. Les égalités 1 et 2 sont les conséquences directes de l'égalité 3.

Soit $f = (a, \sigma)$ et $f' = (a^{-1}, \sigma)$, alors, quelque soient les éléments x et y de A,

$$< f(x), f'(y) >= \sum_{g \in G} a_{\sigma(g)} x_{\sigma(g)} a^{-1}_{\sigma(g)} y_{\sigma(g)}$$

$$< f(x), f'(y) >= \sum_{g \in G} x_{\sigma(g)} y_{\sigma(g)} = \sum_{g \in G} x_g y_g$$

$$< f(x), f'(y) >=< x, y >$$

Supposons maintenant que $f \in ML(C)$, pour tout élément x de C et y de $\widehat{C}$, $f^{-1}(x) \in C$, donc

$$< x, f'(y) >=< f(f^{-1}(x)), f'(y) >=< f^{-1}(x), y >= 0$$

ce qui démontre que $f'(y)$ est élément de $\widehat{C}$, c'est-à-dire $f' \in ML(\widehat{C})$, d'où le résultat.

3 Mots de plus petit poids des codes de Reed-Muller

La distance minimale des codes de Reed-Muller est bien connue (cf. [6]): si $j = r(p-1) + t$, $r \in [1, m(p-1)[$, $t \in [0, p-1[$, la distance minimale du code P^j est alors $(t+1)p^r$.

Dans [6], P.Delsarte, J.M.Goethals et F.J.MacWilliams ont dénombrés les mots de plus petit poids des codes de Reed-Muller. La démonstration de ce résultat est longue et compliquée, mais à ma connaissance, il n'existe pas actuellement de démonstration plus directe.

Théorème 1 *Si $j = r(p-1) + t$, $r \in [1, m(p-1)[$, $t \in [0, p-1[$, le nombre de mots de plus petit poids du code P^j est*

$$L_j = |K^*| \, E_r \, N_{r,t}$$

où E_r est le nombre de variétés affines de dimension $r+1$ dans G considéré comme espace affine sur F_p, et $N_{r,t}$ est le nombre d'ensembles distincts de $t+1$ variétés affines parallèles de dimension r contenues dans une même variété affine de dimension $r+1$

Dans [5], P.Charpin donne une nouvelle caractérisation des mots de plus petit poids des codes de Reed-Muller lorsque l'on considère ces mots dans l'algèbre A:

Théorème 2 *Si $j = r(p-1)+t$, $r \in [1, m(p-1)[$, $t \in [0, p-1[$, les mots de plus petit poids du code P^j sont de la forme*

$$x = kaX^h \sum_{g \in V} X^g$$

avec $k \in K^*, h \in G$, et V un sous-espace vectoriel de dimension r sur F_p et

si $t = 0, a = 1$

si $t \neq 0, a$ est un mot de A de poids $t+1$ de la forme

$$a = \sum_{i=t}^{p-1} a_i (X^f - 1)^i, \ a_i \in F_p, \ f \notin V$$

Pour la démonstration, on pourra consulter [5], nous en donnons cependant les grandes lignes.

En utilisant la propriété $\binom{i}{p-1} = (-1)^i \bmod p$, on démontre que, si $\{e_1, ..., e_r\}$ est une base de V, alors

$$y = \sum_{g \in V} X^g = \prod_{i=1}^{r} (X^{e_i} - 1)^{p-1}$$

Le mot y est alors un élément du code $P^{r(p-1)}$.

Le mot a est en fait un mot de plus petit poids du code de Reed-Solomon étendu de longueur p et de distance minimale $t+1$ sur F_p.

On démontre alors que le mot ay est un mot du code P^j. Le code P^j étant un idéal, $kX^h ay$ est encore un élément du code P^j.

Pour terminer, il suffit alors de dénombrer les mots ainsi construits, et de vérifier, en utilisant le théorème 1, qu'ils sont tous de cette forme.

Remarque

- Si $t = 0$, les supports des mots de plus petit poids sont les variétés affines de dimension r.
- Si $t \neq 0$, les supports des mots de plus petit poids sont les réunions de $t+1$ translatés d'une même variété affine de dimension r, réunion contenue elle même dans une variété affine de dimension $r+1$.

4 Groupes d'automorphismes des codes de Reed-Muller.

Nous allons maintenant utiliser les propriétés géométriques des supports des mots de plus petit poids des codes de Reed-Muller. Pour cela, nous avons besoin d'un théorème connu sous le nom de théorème fondamental de la géométrie affine. Le lecteur pourra en trouver une démonstration dans [1, 8].

Théorème 3 *Soit E un espace affine sur un corps K, dim $E \geq 2$ et $K \neq F_2$. Soit f une bijection de E dans E qui transforme toute droite affine en droite affine, alors f est semi-affine.*

Remarques

- Lorsque $K = F_p$ est un corps fini premier, le seul automorphisme du corps étant l'identité, f est alors affine.
- Le cas F_2 ne pose pas de problème de par la caractéristique 2, mais de par le fait qu'il n'y a alors que deux points par droite, et que tout couple de points définit une droite. On peut cependant établir le théorème suivant dans ce cas:

Théorème 4 *Soit E un espace affine sur F_2, dim $E \geq 3$. Soit f une bijection de E dans E qui transforme tout plan affine en un plan affine, alors f est affine.*

preuve. On peut remarquer que, si $\{0, a, b, c\}$ est un plan vectoriel de E, alors $a + b = c$, $a + c = b$, et $b + c = a$.

Soit f une bijection de E dans E qui conserve les plans affines. On peut supposer sans restreindre le problème que $f(0) = 0$, il suffit de composer éventuellement f avec une translation.

Soient a, b deux points distincts non nuls de E. L'ensemble $\{0, a, b, a + b\}$ est un plan vectoriel de E, son image $\{0, f(a), f(b), f(a + b)\}$ est également un plan vectoriel. De par la remarque préliminaire, on a alors $f(a + b) = f(a) + f(b)$.

L'égalité $f(a + b) = f(a) + f(b)$ étant encore vraie lorsque $a = b$ ou lorsque un des deux points est nul, la bijection f est F_2-linéaire à une translation près, donc f est affine.

Le corollaire suivant est en fait une généralisation des deux théorèmes précédents lorsque E est un espace affine sur un corps fini premier F_p.

corollaire 1 *Soit E un espace affine de dimension m sur F_p, soit $r \in [1, m[$, $rp \geq 3$. si f est une bijection de E dans E qui transforme toute variété affine de dimension r en une variété affine de dimension r, alors f est affine.*

Preuve.

- Si $p \neq 2$

  Lorsque $r = 1$, il s'agit du théorème 3.

  Lorsque $r > 1$, comme $r < m$, toute droite affine possède p éléments, et peut être considérée comme l'intersection de plusieurs variétés affines de dimension r. Son image par f est donc l'intersection des images de ces variétés affines, c'est donc l'intersection de plusieurs variétés affines; c'est une variété affine à p éléments, il s'agit d'une droite, ce qui permet de se ramener au cas précédent.

- Si $p = 2$

  Lorsque $r = 2$, il s'agit du théorème 4.

  Lorsque $r > 1$, on peut refaire le raisonnement précédent en remplaçant droite affine par plan affine, et p éléments par 4 éléments.

Nous pouvons alors énoncer le principal résultat de notre rapport.

Théorème 5 *Pour $2 \leq j \leq m(p-1)-1$, le groupe monomial du code P^j est*

$$ML(P^j) = K^* \times GA_m$$

son groupe de permutations est

$$Per(P^j) = GA_m$$

de plus, nous avons l'égalité

$$Per(P^j) = Aut(P^j).$$

Preuve. On sait que $GA_m \subset Per(P^j) \subset Aut(P^j)$, il suffit de montrer l'inclusion $Aut(P^j) \subset GA_m$, l'égalité $ML(P^j) = K^* \times GA_m$ étant alors une conséquence directe de l'égalité $Per(P^j) = Aut(P^j)$ (cf. p.4 relation (1)).

Pour $m = 1$, le code P^j est en fait un code de Reed-Solomon (cf. [4]). Dans [7], A.Dür a démontré l'égalité $Aut(P^j) = GA_m$, d'où le résultat dans ce cas.

Nous supposons donc maintenant $m > 1$, et nous allons montrer l'inclusion $Aut(P^j) \subset GA_m$.

Tout élément de $ML(P^j)$ transforme un mot de plus petit poids de P^j en mot de plus petit poids.

Soit $\sigma \in Aut(P^j)$; la permutation σ transforme alors le support de tout mot de plus petit poids en un support d'un autre mot de plus petit poids.
Posons $j = r(p-1) + t$, $rs \in [0, m[$, $t \in [0, p-1[$.

1. Si $t = 0$, en utilisant la caractérisation des mots de plus petit poids obtenue au théorème 2, les mots de plus petit poids ont pour support les variétés affines de dimension r ($r \neq 0$ car $j \geq 2$).

   La permutation σ transforme donc toute variété affine de dimension r en une variété affine de dimension r; d'après le corollaire 1, σ est alors affine et $Aut(P^j) \subset GA_m$.

2. Si $2 \leq t < p-1$, $0 \leq r < m-1$.

   Soit V' une variété affine de dimension $r+1$, V le sous-espace vectoriel associé, $V' = V + h$, $h \in G$.

   Soit U un sous-espace vectoriel de V de dimension r, et f un élément de $V - U$.
   Soit $\qquad a = (X^f - 1)^t = \sum_{i=0}^{t} \binom{t}{i} X^{if}$.

   D'après le théorème 2, le mot $x_0 = aX^h \sum_{g \in U} X^g$ est un mot de plus petit poids du code P^j, qui a pour support la réunion des $t+1$ translatés de $V + h$ par $0, f, 2f, \ldots, tf$:

$$V_0' = Supp(x_0) = (V + h) \cup (V + h + f) \cup \ldots \cup (V + h + tf)$$

   On construit alors les mots $x_i = X^{if} x_0$, $0 \leq i \leq p - 1 - t$.

   Le mot x_i est un mot de plus petit poids du code P^j, et a pour support

$$V_i' = Supp(x_i) = (V + h + if) \cup \ldots \cup (V + h + (t+i)f)$$

   Par construction,

$$V' = \bigcup_{i=0}^{p-1-t} V_i' \text{ et, pour } i < p-1-t,\ |V_i' \cap V_{i+1}'| = p^r t.$$

   L'image par $\sigma \in Aut(P^j)$ de chaque support V_i' est un support d'un mot de plus petit poids du code P^j. en utilisant la caractérisation des mots de plus petit poids du théorème 2, on sait que $\sigma(V_i')$ est une réunion de $t+1$ translatés d'une variété affine de dimension r, réunion contenue dans une variété affine W_i' de dimension $r+1$.

   Pour $0 \leq i < p-1-t$, $W_i' \cap W_{i+1}'$ est alors une variété affine contenant $\sigma(V_i' \cap V_{i+1}')$, donc de cardinal supérieur ou égal à $p^r t > p^r$, car $t \geq 2$ par hypothèse. C'est donc une variété affine de dimension $r+1$, donc $W_i' = W_{i+1}'$ pour tout i. Par conséquence, $\sigma(V') = W_0'$, l'image de toute variété affine de dimension $r+1$, $r+1 < m$, est une variété affine de dimension $r+1$, en utilisant le corollaire 1, σ est affine, $Aut(p^j) = GA_m$.

Le code dual du code de Reed-Muller P^j est le code de Reed-Muller $P^{j'}$, avec $j' = m(p-1) - j + 1$ (cf. [10, 4]). On en déduit alors $Aut(P^j) = Aut(P^{j'})$.

En utilisant cette propriété, nous pouvons terminer la démonstration.

3. Si $t = 1$, $j = r(p-1) + I$, alors $j' = (m-r)(p-1)$, nous sommes ramené au cas 1, $Aut(P^j) = Aut(P^{j'}) = GA_m$.

4. Si $r = m-1$ et $2 \leq t < p-1$, $j = (m-1)(p-1) + t$, alors $j' = t' = (p-1) - t + 1$ avec $2 \leq t' < p-1$, nous sommes ramené au cas 2, $Aut(P^j) = Aut(P^{j'}) = GA_m$.

Dans tous les cas, pour $2 \leq j \leq m(p-1) - 1$, nous avons bien $Aut(P^j) = GA_m$, ce qui termine la démonstration.

Bibliographie

[1] M.Berger *Géométrie T1* Cedic, Fernand-Nathan, Paris (1977).

[2] T.Berger *A direct proof for the automorphism group of Reed-Solomon codes* Eurocode'90 Lecture Notes in Computer Science 514 (1991).

[3] T.Berger, P.Charpin *The automorphism group of the Generalized Reed-Muller codes* Discrete Mathematics (à paraître).

[4] P.Charpin *Codes cycliques étendus invariants sous le groupe affine* Thèse de Doctorat d'Etat, Université Paris VII, LITP (1987).

[5] P.Charpin *Codes idéaux de certaines algèbres modulaires* Thèse de 3ième cycle, Université de Paris VII (1982).

[6] P.Delsarte, J.M.Goethals, F.J.MacWilliams *On generalized Reed-Muller codes and their relatives* Info. and Control, 16 (1974).

[7] A.Dür *The automorphism groups of Reed-Solomon codes* Journal of Combinatorial Theory vol. 44, Janvier 1987.

[8] J.Frenkel *Géométrie pour l'élève professeur* Hermann, Paris (1973).

[9] R.Knörr W.Willems *The automorphism groups of Generalized Reed-Muller codes* S.M.F. Astérisque 181-182 (1990).

[10] F.J.MacWilliams N.J.A.Sloane *The theory of error correcting codes* North Holland, Amsterdam (1977).

ISSN 0249-6399