IMHOTEP

AFRICAN JOURNAL OF PURE AND APPLIED MATHEMATICS

Imhotep Mathematical Proceedings
Volume 4, Numéro 1, (2017),
pp. 19 - 22.

Codes affines-invariants linéaires de longueur impaire sur Z_4

C. T. Gueye
Département de Mathématiques. Faculté des Sciences et Techniques, Université Cheikh Anta Diop de Dakar (Sénégal). B.P. 5005, Dakar-Fann.
cheikht.gueye@ucad.edu.sn

R. F. Babindamana
Département de Mathématiques, Faculté des Sciences et Techniques de Brazzaville, Universit Marien Ngouabi (Congo). B.P. 69 Brazaville, Congo.
regis.babindamana@yahoo.fr

Abstract

Nous caractérisons les codes affines invariants de longueur impaire sur Z_4. Nous utilisons le relèvement de Hensel pour construire des codes sur Z_4.
(English summary.) We characterize the invariant affine codes of odd length on Z_4. We use the Hensel bearing to build linear codes on Z_4.

Proceedings of the 6^{th} annual workshop on CRyptography, Algebra and Geometry (CRAG-6), 15 - 17 June 2016, University of Bamenda, Bamenda, Cameroon.

IMHOTEP - Math. Proc. **4** (2017), 19–22
1608-9324/010019–18, DOI 13.1007/s00009-003-0000

IMHOTEP Mathematical Proceedings

Codes affines-invariants linéaires de longueur impaire sur Z_4

C. T. Gueye and R. F. Babindamana

Abstract. Nous caractérisons les codes affines invariants de longueur impaire sur Z_4. Nous utilisons le relèvement de Hensel pour construire des codes sur Z_4.
English summary. We characterize the invariant affine codes of odd length on Z_4. We use the Hensel bearing to build linear codes on Z_4.

I. Introduction

L'étude des codes linéaires sur $\mathbb{Z}_4$ a donné des résultats sur des codes non-linéaires sur $\mathbb{F}_2$. Notamment, un code cyclique est un code invariant par l'action d'un groupe de permutations circulaires. Il est naturel de chercher ce qui se produit en regardant les codes qui sont invariants par l'action d'autres groupes (par exemple les groupes affines). Un code affine-invariant C de longueur n sur l'anneau $\mathbb{Z}_4$ est un sous-ensemble de $\mathbb{Z}_4^n$ qui est globalement invariant sous l'action d'un groupe affine G.

Nous décrivons les codes affines invariants linéaires de longueur impaire sur $\mathbb{Z}_4$.

II. Codes affines-invariants sur un anneau

Définition II.1. *Soit R un anneau commutatif et n un entier positif.*
Un code C de longueur n sur l'anneau R est un sous-ensemble de R^n.

La représentation polynômiale d'un mot $x = (x_0, x_1, ..., x_{n-1})$ de C est le polynôme $x_0+x_1X+x_2X^2+...+x_{n-1}X^{n-1}$ de l'anneau $R[X]/(X^n-1)$. On note : $x = (x_0, x_1, ..., x_{n-1}) = \sum_{i=0}^{n-1} x_iX^i$.

La représentation polynômiale du code C notée I est l'ensemble des représentations polynômiales des mots de C. C'est-à-dire, $I = \{\sum_{i=0}^{n-1} x_iX^i, (x_0, ..., x_{n-1}) \in C\}$, c'est un sous-ensemble de $R[X]/(x^n - 1)$.

Considérons l'anneau $\mathbb{Z}_n$ et $Sym(\mathbb{Z}_n)$ le groupe des permutations de $\mathbb{Z}_n$ appelé groupe symétrique sur $\mathbb{Z}_n$. Ce groupe opère sur le code C de la manière suivante: Si $\sigma \in Sym(\mathbb{Z}_n)$ et $x = (x_0, ..., x_{n-1}) \in C$ alors,

$$\sigma(x) = (x_{\sigma^{-1}(0)}, ..., x_{\sigma^{-1}(n-1)})$$

Communication presentée au $6^{ème}$ atelier annuel sur la CRyptographie, Algèbre et Géométrie (CRAG-6), 15 - 17 Juin 2016, Université de Bamenda, Bamenda, Cameroun / Paper presented at the 6^{th} annual workshop on CRyptography, Algebra and Geometry (CRAG-6), 15 - 17 June 2016, University of Bamenda, Bamenda, Cameroon.

En utilisant la représentation polynômiale, on obtient

$$\sigma(x) = \sum_{i=0}^{n-1} x_i X^{\sigma(i)} = \sum_{i=0}^{n-1} x_{\sigma^{-1}(i)} X^i$$

Proposition II.2. *Soit $U(\mathbb{Z}_n)$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}_n$. L'ensemble*

$$AGL(\mathbb{Z}_n) = \{\sigma_{u,b} \in Sym(\mathbb{Z}_n)/\sigma_{u,b}(i) = ui + b, u \in U(\mathbb{Z}_n), b \in \mathbb{Z}_n\}$$

est un groupe affine, appelé **groupe des permutations affines de** $\mathbb{Z}_n$.

Dans la suite nous considérons le groupe affine $G := AGL(\mathbb{Z}_n)$.

Définition II.3. *Un* **code affine-invariant** *C de longueur n sur l'anneau R est un sous-ensemble non vide de R^n tel que $G(C) \subseteq C$, c'est à dire, C est globalement invariant par l'action du groupe affine G.*

En particulier, un **code affine-invariant** *C de longueur n sur l'anneau $\mathbb{Z}_4$ est un sous-ensemble de $\mathbb{Z}_4^n$ qui est globalement invariant sous l'action du groupe affine G.*

Posons maintenant

$$R_n = R[X]/(X^n - 1)$$

Pour tout $f \in R_n$, $f(X) = \sum_{i=0}^{n-1} f_i X^i$, $f_i \in R$, et pour tout $\sigma_{u,b} \in G$, $\sigma_{u,b}(f)(X) = \sum_{i=0}^{n-1} f_i X^{ui+b}$

Proposition II.4. *Soit I la représentation polynômiale d'un code C. Si I est un idéal de R_n, alors I est cyclique si et seulement si $\sigma_{1,1}(I) = I$.*

Proposition II.5. *Soit $U(\mathbb{Z}_n) = \langle u_1, ..., u_t \rangle$, alors $G = \langle \sigma_{u_{1,0}}, ..., \sigma_{u_{t,0}}, \sigma_{1,1} \rangle$.*

En outre, on a $G(I) = I \Leftrightarrow \sigma_{u_{i,0}}(I) = I$, pour $(i = 1, ..., t)$ et $\sigma_{1,1}(I) = I$.

III. Codes affines invariants linéaires sur $\mathbb{Z}_4$

Définition III.1. *Un code C de longueur n sur $\mathbb{Z}_4$ est dit* **affine-invariant linéaire**, *s'il est à la fois linéaire et affine-invariant.*

Dans la suite, on confondra le code C à sa représentation polynômiale I et $A_4[n]$ désignera $\mathbb{Z}_4[X]/(x^n - 1)$, l'anneau des polynômes à coefficients dans $\mathbb{Z}_4$ modulo $x^n - 1$.

Proposition III.2. *Un sous-ensemble de $\mathbb{Z}_4^n$ est un code affine invariant linéaire de longueur n sur $\mathbb{Z}_4$ si et seulement si sa représentation polynômiale I est un idéal de $A_4[n]$ telle que $\sigma_{u_i,0}(I) = I$ pour $i \in \{1, ..., t\}$.*

Pour un Code affine invariant linéaire de longueur impaire sur $\mathbb{Z}_4$ on a le résultat ci-après.

Théorème III.3 (C. T. Gueye). *Soit I un code affine-invariant linéaire de longueur impaire n sur $\mathbb{Z}_4$.*

Alors,

a) *I est un idéal principal de $A_4[n]$;*
b) *I est engendré par un polynôme de la forme :*

$$g(x) = a(x)[b(x) + 2]$$

tel que g divise $\sigma_{u_i,0}(g)$ pour $i \in \{1, ...t\}$, $\sigma_{u_i,0} \in G$ et les u_i sont les générateurs de $U(\mathbb{Z}_n)$. Avec $x^n - 1 = a(x)b(x)c(x)$ dans $\mathbb{Z}_4[X]$ et les polynômes $a(x)$, $b(x)$ et $c(x)$ sont deux à deux premiers;
c) *Le cardinal de I est $4^{degc(x)}2^{degb(x)}$.*

Remarque III.4. *La connaissance des générateurs de $U(\mathbb{Z}_n)$ suffit pour dire si un code cyclique linéaire de longueur impaire est affine-invariant ou pas.*

Proposition III.5. *Si n est impair et si le groupe des unités de l'anneau $\mathbb{Z}_4$ est cyclique et engendré par θ $(U(\mathbb{Z}_n) = \langle\theta\rangle)$, alors le code C de longueur n sur $\mathbb{Z}_4$ est* **affine-invariant linéaire***, si et seulement si son polynôme générateur $g(x)$ divise $g(x^\theta)$.*

Algorithme de la décomposition de $x^n - 1$ sur $\mathbb{Z}_4$ (Méthode de Graeffe)

Soit $h(x)$ un facteur irréductible de $x^n - 1$ dans $\mathbb{F}_2[X]$.
On pose : $h(x) = e(x) + o(x)$

où $e(x)$ est la somme des monômes de degré paire et $o(x)$ est la somme des monômes de degré impaire.

Alors $g(x)$ est le facteur irréductible de $x^n - 1$ dans $\mathbb{Z}_4[X]$, avec
$\mu(g(x)) = h(x)$ où $g(x^2) = \pm(e^2(x) - o^2(x))$ est μ est le relèvement de Hensel.

IV. Code affine-invariant linéaire de longueur 7 sur $\mathbb{Z}_4$

Exemple: Code affine-invariant linéaire de longueur 7 sur $\mathbb{Z}_4$
La décomposition de $x^7 - 1$ sur $\mathbb{F}_2$ est :

$$x^7 - 1 = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

Par le relèvement de Hensel, on trouve sa décomposition sur $\mathbb{Z}_4$:

$$\begin{aligned} x^7 - 1 &= (x-1)(x^3 + 2x^2 + x - 1)(x^3 - x^2 + 2x - 1) \\ &= 3(x^7 + x^6 - 3x^5 - 3x^4 - 3x^3 + x^2 + x) \\ &= (x-1)(x^6 + x^5 - 3x^4 - 3x^3 - 3x^2 + x + 1) \end{aligned}$$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, le groupe des éléments inversibles de $\mathbb{Z}_7$ est :

$$U(\mathbb{Z}_7) = \{1, 2, 3, 4, 5, 6\} = \langle 3\rangle.$$

Le groupe affine invariant est $G = \langle\sigma_{3,0}, \sigma_{1,1}\rangle$.
Prenons : $a(x) = x^6 + x^5 - 3x^4 - 3x^3 - 3x^2 + x + 1$ *et* $b(x) = 1$.

On a alors,

$$\begin{aligned} g(x) &= a(x)\,[b(x) + 2] \\ &= 3(x^6 + x^5 - 3x^4 - 3x^3 - 3x^2 + x + 1) \end{aligned}$$

et

$$\begin{aligned} \sigma_{1,1}(g(x)) &= xg(x) \\ &= 3(x^7 + x^6 - 3x^5 - 3x^4 - 3x^3 + x^2 + x) \\ &= 3(1 + x - 3x^2 - 3x^3 - 3x^4 + x^5 + x^6) \\ &= g(x) \end{aligned}$$

Donc C est cyclique.

Considérons le code cyclique linéaire engendré par $g(x)$, On a:

$$\begin{aligned} \sigma_{3,0}(g(x)) &= g(x^3) \\ &= 3(x^{18} + x^{15} - 3x^{12} - 3x^9 - 3x^6 + x^3 + 1) \\ &= 3(x^6 + x^5 - 3x^4 - 3x^3 - 3x^2 + x + 1) \\ &= g(x) \end{aligned}$$

Il est clair que $g(x)$ divise $g(x^3)$.
Donc le code cyclique linéaire sur $\mathbb{Z}_4$ engendré par $g(x)$ est **affine-invariant linéaire** de longueur 7 sur $\mathbb{Z}_4$.

Conclusion

Dans cet exposé nous avons établi une construction des codes affines invariants linéaires de longueur impaire sur $\mathbb{Z}_4$. L'étude se poursuivra sur les codes affines invariants linéaires de longueur paire sur $\mathbb{Z}_4$.

References

[1] T. P. Berger , *On automorphism group and the permutation group of an affine-invariant*, Proc. of 3^{rd} conf. on Finite Field and Applications, Glasgow, England, London Math.Soc., Lectures Series 233, Cambridge Univ. Press (1996).

[2] C. T. Gueye, *Binary images of affine-invariant codes over* $\mathbb{Z}_4$, J. Sci. **6** , $n^0$2, (2006) 75-84.

[3] M. Mignotte, *Mathematic for Computer Algebra*, Springer-Verlag, (1992).

[4] J. Wolfman, *Negacyclic and cyclic Codes over* $\mathbb{Z}_4$, IEE Trans. Inform. Theory, **45**, $n^0$7 November (1999) 2527-2532.

[5] J. Wolfman, *Binary Image of cyclic codes over* $\mathbb{Z}_4$, IEE Trans. Inform. Theory, **47**, $n^0$5, July (2001) 1773-1779.

C. T. Gueye
e-mail: `cheikht.gueye@ucad.edu.sn`
Département de Mathématiques. Faculté des Sciences et Techniques, Université Cheikh Anta Diop de Dakar (Sénégal). B.P. 5005, Dakar-Fann.

R. F. Babindamana
e-mail: `regis.babindamana@yahoo.fr`
Département de Mathématiques, Faculté des Sciences et Techniques de Brazzaville, Université Marien Ngouabi (Congo). B.P. 69 Brazaville, Congo.