Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 9, Number 5 (2013), pp. 475-482

http://www.ripublication.com/gjpam.htm

A New Approach of Free Cyclic Linear Codes over Commutative Finite Chain Rings

Fotue Tabue Alexandre and Mouaha Christophe

Department of mathematics
Faculty of Sciences, University of Yaoundé 1
alexfotue@gmail.com
Yaoundé-Cameroon, Box 700
Department of mathematics
Higher Teachers Training School of Yaoundé
cmouaha@yahoo.fr
Yaoundé-Cameroon, Box 47

Abstract

.

In this work, we generalize the approach of J. Bierbrauer [4] to the theory of cyclic codes over Galois field to commutative finite chain rings.This approach isbased on the action of Galois group over set of Teichmüller of a commutative finite chain ring.

Keywords: Galois extension of finite chain rings, cyclic codes, trace codes, cyclotomic coset.

AMS Subject Classification: 94B05

INTRODUCTION

The theory of cyclic codes over finite chain rings has been investigate in [5] and J. Bierbrauer gave in [4] a new approach of construction of cyclic codes over finite field using the functiontrace when the characteristic of the ring and the length of code are primer. This approach is elegant because that ituses the act of Galois group on the set of roots of the polynomial.

Let S and R be two finite chain rings such that $R \subseteq S$, so $S$is a Galois extension of R. It denotes by r the degree and $Aut_R(S)$the Galois group of the extension S. Let $\mathcal{C}$ be a S-linear code of length n, two new R-linear codes can be obtained from $\mathcal{C}$. The first construction is the subcode of code $\mathcal{C}$ over R and second construction is the image of $\mathcal{C}$ by the trace map of the extension $S$of$R$.Both constructions of linear codes

over Galois extensionsof$R$,give us the family of complexified linear codes. Additional information on Galois Theory on the finite chain ring can be found in [3] and linear codes over finite chain rings have been to investigateby T. Honold and I. Landjev in [6]. The purpose of this paper is to show that free linear cyclic codes are trace of a complexified code and we specify that this complexified codeis an idea of the ringequipped with Hadamard's product $(S^n; +, *)$whenthe characteristic of the ring and the length of code are primer.

This paper organizes as follow: Section.II is an investigation on the linear trace codes,Section.III gives and proves the main result.

LINEAR TRACE CODES

Let R be a commutative, finite chain ring, $J(R)$is its maximalideal, m the nilpotency index of$J(R)$,γa generator of $J(R)$ and$\pi : R \longrightarrow GF(q)$, the canonical epimorphism .

Lemma.2.1.*[[1], prop.2.1]* Let$R$ be a commutative finitechain ring. Then there exists an element b of $R^{\times}$ of order $q-1$ suchthat $\pi(b)$ is a primitive element of $GF(q)$and $\Gamma(R) := \langle b\rangle \cup \{0_R\}$ is acomplete system of representatives of R under congruence modulo$J(R)$in$R$.

We call $\Gamma(R) := \langle b\rangle \cup \{0_R\}$the set of Teichmüller's representatives of R under congruence modulom_R. Moreover the restriction of π at $\Gamma(R)$ is an one to one map.

The complexified of$R$-linear code$\mathcal{C}$ is the least S-linear code containing$\mathcal{C}$ and we denoteit$Ext^S(\mathcal{C}) := \langle \mathcal{C}\rangle_S$.The subring subcode of S-linear code$\mathcal{C}'$of length $n$and trace of$S$-linear code$\mathcal{C}'$are the R-linear codes defined by: $ResR(\mathcal{C}') := \mathcal{C} \cap R^n$ and$Tr_R^S(\mathcal{C}')$ respectively. We introduce the notion of algebraic dualityon $R^n$by:

$$< x; y >: = \sum_{i=0}^{n-1} x_i y_i$$

for any $x := (x_0; x_1; \cdots ; x_{n-1})$ and $y := (y_0; y_1; \cdots ; y_{n-1})$ in R^n.

The R-submodule of R^n defineby

$$\mathcal{C}^{\perp} := \{x \in R^n : \forall y \in \mathcal{C};\ < x; y >= 0\}$$

is called dual R-linear code of $\mathcal{C}$. For any R-linear code $\mathcal{C}_1$such that$\mathcal{C} \subseteq \mathcal{C}_1$. In [6],T. Honold and I. Landjev shown that $(\mathcal{C}^{\perp})^{\perp} = C$and ${\mathcal{C}_1}^{\perp} \subseteq \mathcal{C}^{\perp}$.

Definition.2.1. Let$\mathcal{C}$be aR-linear code of length$n$. We call a generator matrix of$R$-linear code $\mathcal{C}$over$R$, a matrixwhose rows forms an$R$-generator familyand minimal of R-linear code$\mathcal{C}$.

Let $\mathcal{B} := (b_0; b_1; \cdots ; b_{m-1})$be a$R$-basis of the Galois extension $S$of R. Then

$$\mathcal{B}^* := (b_0^*; b_1^*; \cdots ; b_{m-1}^*) = (b_0; b_1; \cdots ; b_{m-1})T^{-1}$$

is the R-trace-dual basis of $\mathcal{B}$. Where $T := \left(Tr_R^S(b_i b_j)\right)_{ij}$ is an $m \times m$ -singularmatrix over R.

In thesequel,$\mathcal{B} := (b_0; b_1; \cdots ; b_{m-1})$ be aR-basis of the Galois extension $S|_R$ and$\mathcal{B}^* := (b_0^* ; b_1^*; \cdots ; b_{m-1}^*)$ the R-trace-dual basis of $\mathcal{B}$.

Lemma.2.1. Let x be an element ofS^n: Then

$$x = \sum_{j=0}^{m-1} Tr_S^R(b_j^* x) b_j.$$

Proof. There exists an unique $(x_0; x_1; \cdots ; x_{m-1}) \in R^n$ suchthat

$$x = \sum_{j=0}^{m-1} x_j b_j \quad and \quad Tr_R^S(b_i^* x) = \sum_{j=0}^{m-1} Tr_R^S(b_i^* b_j) x_j = x_i;$$

since$\sum_{j=0}^{m-1} Tr_R^S(b_i^* b_j) = \delta_{ij}$.

Proposition.2.2. Let$\mathcal{C}$ be an$S$-linear code. Then$\mathcal{C} \subseteq \langle Tr_R^S(\mathcal{C})\rangle_S$.

Proof.Let $c \in \mathcal{C}$. Then for all$i \in \{0; 1; \cdots ; m-1\}$; via the equality of Lemma.2.1, we obtain$c = \sum_{j=0}^{m-1} Tr_S^R(u_j^* c) b_j$and $Tr_S^R(u_j^* c) \in Tr_R^S(\mathcal{C})$. Therefore $\mathcal{C} \subseteq \langle Tr_R^S(\mathcal{C})\rangle_S$.

Remark 2.1. Let $\mathcal{C}$ be an S-linear code. From Proposition.2.1, wealways have

$$rank_S(\mathcal{C}) \leq rank_R(Tr_R^S(\mathcal{C})).$$

Definition 2.2. Let $\mathcal{C}$ be an$S$-linear code. We say that $\mathcal{C}$ iscomplexified over Rif$\mathcal{C} = \langle Tr_R^S(\mathcal{C})\rangle_S$.

Theorem 2.1. (*Generalization of Delsarte'sTheorem[2]*) Let $\mathcal{C} \subseteq \langle Tr_R^S(\mathcal{C})\rangle_S$ bean S-linear code. Then $Tr_R^S(\mathcal{C}^\perp) = Res_R(\mathcal{C})^\perp$.

Proof Let us show that $Tr_R^S(\mathcal{C}^\perp) \subseteq Res_R(\mathcal{C}^\perp)$.Let $\$a \in \mathcal{C}^\perp$ and $\$c \in Res_R(\mathcal{C}^\perp)$ Then $< c, Tr_R^S(a) >= Tr_R^S(< a, c >) = 0$.From which the result.

Let us show $Res_R(\mathcal{C}^\perp) \subseteq Tr_R^S(\mathcal{C}^\perp)$. According to Proposition.2.2, we obtain $\mathcal{C}^\perp \subseteq Ext_S(Tr_R^S(\mathcal{C}^\perp))$, From which

$$Res_R(\mathcal{C}^\perp) \subseteq Res_R\left(Ext_S\left(Tr_R^S(\mathcal{C}^\perp)\right)\right),$$

since$Tr_R^S(\mathcal{C}^\perp)$ is an$R$-linear code, weobtain $Res_R(\mathcal{C}^\perp) \subseteq Tr_R^S(\mathcal{C}^\perp)$. We have done.

Remark 2.2.

i. In *[Prop.3.13[5]]*,G.H. Norton and A. Sălăgeanshown that an$R$-linear code is free if, and only if its dual is an$R$-linearfree code. By Theorem. 2.1, we obtain that an S-linear code is freeif, and only if its trace is free a R-linear free code.

ii. Let $\mathcal{C}$ be an$R$-linear code. by Theorem. 2.1, we obtain

$$\mathcal{C} = Tr_R^S(Ext_S(\mathcal{C}));$$

for any Galois extension $S|_R$.

Definition 2.4. We denote by σ the generator of Galois group $Aut_R(S)$ ofGalois extension $S|_R$.Let $\mathcal{C}$ be an S-linear is Galois invariant if $\sigma(\mathcal{C}) = \mathcal{C}$.

The following theorem gives the Characteristics proprieties of$S$-linear complexified codes over$R$.

Theorem.2.2. Let$\mathcal{C}$ be aS-linear code of the length n. Thefollowing conditions are equivalent.

$\mathcal{C}$ is complexified over R;

$\mathcal{C}$ possess a generator matrix over R;

$\mathcal{C} = Ext_R^S(Res_R(\mathcal{C}));$

The code $\mathcal{C}$is Galois invariant;

$Res_R(\mathcal{C}) = Tr_R^S(\mathcal{C});$

$Res_R(\mathcal{C})^{\perp} = ResR(\mathcal{C}^{\perp}).$

Proof. (i)⟹ (ii) If $\mathcal{C}$ is complexified over R, then $Tr_R^S(\mathcal{C})$is an S-generator family of $\mathcal{C}$: As $TrSR(\mathcal{C}) \subseteq R^n$; we obtain theresult.

(ii) ⟹ (iii) It's straightforward.

(iii) ⟹ (iv) Suppose that $\mathcal{C} = Ext_S(Res_R(\mathcal{C}))$.Let $\{u_0; u_1; \cdots u_{r-1}\}$be an$R$-generator family and minimal of $Res_R(\mathcal{C})$. Then

$Ext_S(Res_R(\mathcal{C})) = \langle\{u_0; u_1; \cdots; u_{r-1}\}\rangle_S.$

As, for all$i \in \{0; 1; \cdots r-1\}$; $\sigma(u_i) = u_i$; we obtain $\sigma(\mathcal{C}) = \mathcal{C}$.

(iv) ⟹ (v) Suppose that $\mathcal{C}$ is an S-linear code $\mathcal{G}$-invariant.Let $c \in \mathcal{C}$. Then

$$Tr_R^S(c) = \sum_{\kappa \in Aut\_R(S)} \kappa(c) \in \mathcal{C}$$

and $Tr_R^S(c) \in R^n$;therefore $Tr_R^S(c) \in Res_R(\mathcal{C})$ and $Tr_R^S(\mathcal{C}) \subseteq Res_R(\mathcal{C})$.Fromwhich Proposition 2.2, we obtain $Res_R(\mathcal{C}) \subseteq Tr_R^S(\mathcal{C})$: From which$Res_R(C) = Tr_R^S(\mathcal{C})$.

(v) ⟹ (vi) Using the Theorem. 2.1, we have $Tr_R^S(\mathcal{C}) = Res_R(\mathcal{C}^{\perp})^{\perp}$ and $Res_R(C) = Tr_R^S(\mathcal{C})$. We obtain $Res_R(\mathcal{C}^{\perp}) = Res_R(\mathcal{C})^{\perp}$.

(vi) ⟹ (i): By Theorem.2.1 and considering the hypothesis, wehave done.

MAIN RESULTS

Let R be a finite chain ring and $GF(q)$ its residual field, $n \geq 2$an integer such that $gcd(q; n) = 1$; m be a multiplicative orderof q modulo n. Denote by S a Galois extension of R such that$rank_R(S) = m$ and H a multiplicative subgroup of $\Gamma(S)^*$order n of generator ξ and; $\emptyset \neq A \subseteq Z/nZ := \{0; 1; \cdots; n\}$.The coordinate wise multiplication on S^n is defined by $\boldsymbol{a} * \boldsymbol{b} := (a_1 b_1; \cdots; a_n b_n)$for $\boldsymbol{a} := (a_1; \cdots; a_n) \in S^nand\boldsymbol{b} := (b_1; \cdots; b_n) \in S^n$.Themodule $S^n$with this multiplication becomes a commutative ring withthe unit $\mathbf{1} := (1; \cdots; 1)$.Consider the isomorphism of the rings and of the S-modules

$$ev_\xi : \begin{matrix} (S_n[X]; +, \times) & \longrightarrow & (S^n; +, *; \mathbf{0}, \mathbf{1}) \\ P & \longmapsto & (\widetilde{P}(\xi^0); \widetilde{P}(\xi^a); \cdots; \widetilde{P}(\xi^{(n-1)a})) \end{matrix}$$

where$S_n[X] := S[X]/(X^n - 1)$.

In the sequel, we regard the ideal$\mathcal{I}(A) := ev_\xi(\langle\{X^a | a \in A\}\rangle)$ of the ring $S^n$and we give some properties of the ideal $\mathcal{I}(A)$. The subgroup $H = \langle\xi\rangle$ is the set of the roots of$X^n - 1$. TheGalois group

$$\mathcal{G} := \left\{\sigma^j : x \longmapsto x^{q^j} : 0 \leq j \leq m - 1\right\}$$

of theextension $S|_R$ acts on H in the following natural way:

$$\sigma^j(\xi^i) = \xi^{iq^j \bmod n};$$

Therefore the orbits of this action are $b_q(\xi^{i_\ell}) := \{\sigma^j(\xi^{i_\ell}) \mid 0 \leq j \leq m - 1\}$; denoted t is the number of the orbits of this action and $0 \leq \ell \leq t - 1$.From G. Ganske and B. R. McDonald in [3];G.H. Norton and A. Sălăgean in [5], the polynomial $X^n - 1$ over Shas an unique factorizations into b-polynomials over R. Therefore

$$X^n - 1 = \prod_{\ell=0}^{t-1} f_\ell$$

where the f_ℓ are the b-polynomial over R, we obtain

$$f_\ell := \prod_{w \in Orb_q(\xi^{i_\ell})} (X - w)$$

With ξ^{i_ℓ} a root off_ℓ.

Consider the Zech's logarithm of basis ξ, defined by

$$\mathrm{Log}_\xi : \begin{matrix} H & \longrightarrow Z/nZ \\ \xi^i & \longmapsto i \bmod n \end{matrix}$$

The sets $\mathcal{Z}_q(i) := Log_\xi(Orb_q(\xi^i))$ are called cyclotomic cosetsof $q$modulo n. We denote $\widetilde{\mathcal{Z}_q(i)}$a coset of the representatives ofthe cyclotomic cosetof $\mathcal{Z}_q(i)$;

$$\tilde{A} := \bigcup_{\ell \in \widetilde{Z_q} \cap A} \mathcal{Z}_q(\ell) \text{ and } \widetilde{\mathcal{Z}_q} := \bigcup_{\substack{\ell \equiv i q^j \bmod n \\ 0 \le j \le m-1 \\ 0 \le i \le n-1}} \widetilde{\mathcal{Z}_q(\ell)}$$

Definition 3.1. The code $\mathcal{C}$ of length n is cyclic if
$(c_0; c_1; \cdots; c_{n-2}; c_{n-1}) \in \mathcal{C} \Rightarrow (c_{n-1}; c_0; c_1; \cdots; c_{n-3}; c_{n-2}) \in \mathcal{C}$.

Proposition.3.1. Let $\emptyset \neq A \subset Z/nZ$. Thenthe following assertions hold.
The S-linear code $\mathcal{I}(\tilde{A})$ is free, cyclic and complexified over$R$;
$Tr_R^S(\mathcal{I}(\tilde{A})) = Tr_R^S(\mathcal{I}(A))$;
$\mathcal{I}(A)^{\perp} = \mathcal{I}(-\bar{A})$.

Proof.Let'us prove (i). The set $\{X^a | a \in \tilde{A}\}$ is an$S$-independent familyof $S_n[X]$. As ev_ξ is an S-isomorphism, the set $\{ev_\xi(X^a) | a \in \tilde{A}\}$is a$S$-basis of $\mathcal{I}(\tilde{A})$.Since the order of $\xi$is n; it's straightforward to prove that$\mathcal{I}(\tilde{A})$is cyclic.

We have $\sigma(\mathcal{I}(\tilde{A})) = \langle\{\sigma\left(ev_\xi(X^a)\right) | a \in \tilde{A}\}\rangle_Sand\sigma(ev_\xi(X^a)) = ev_\xi(X^{qa})$.As $a \in \tilde{A} \Leftrightarrow qa \in \tilde{A}$; we obtain$\sigma(\mathcal{I}(\tilde{A})) = \mathcal{I}(\tilde{A})$. From Theorem.2.2, $\mathcal{I}(\tilde{A})$is complexified overR.

Let'us prove (ii). Let a be an element of$\tilde{A}$. Then there exists $b \in A$ such that $a = q^i b$ for some $i \in \mathbb{N}$: Thus

$$\begin{aligned} Tr_R^S(ev_\xi(X^a)) &= Tr_R^S\left(ev_\xi(X^{q^i b})\right); \\ &= Tr_R^S(\sigma(ev_\xi(X^b))); \\ &= Tr_R^S\left(\left(ev_\xi(X^b)\right)\right); \end{aligned}$$

because $Tr_R^S \, o\sigma = \sigma o \, Tr_R^S = Tr_R^S$.

The previous equality prove that $r_S^R(\mathcal{I}(\tilde{A})) = Tr_S^R(\mathcal{I}(A))$.

Let'us prove (iii). Let a be an element of $-\bar{A}$and $b \in A$. Then $0 < a - b < n$ and

$$\sum_{i=0}^{n-1} \xi^{(b-a)i} = 0$$

Therefore $\mathcal{I}(A)^{\perp} \supseteq \mathcal{I}(-\bar{A})$.As$\mathcal{I}(A)$ and$\mathcal{I}(-\bar{A})$ are S-free, we have
$rank_S(\mathcal{I}(A)^{\perp}) = rank_S(\mathcal{I}(-\bar{A})) = n - |A|$; we obtain $\mathcal{I}(A)^{\perp} = \mathcal{I}(-\bar{A})$.

Remark 3.1.*[[5].Chap.4]* An R-linear code $\mathcal{C}$ over R of length$n$ is cyclic if $\mathcal{C}$ is identified to an ideal of the quotient ring $R_n[X] = R[X]/(X^n - 1)$ and if$gcd(q; n) = 1$ then$R_n[X]$ is a principal ring.Let g be a divisor of$X^n - 1$, we denote

$$Spec(g) = \{\xi^i \in H | g(\xi^i) = 0\}.$$

Proposition 3.2. The R-linear code $Tr_R^S(\mathcal{I}(A))$ of length n isfree and

$$rank_R(Tr_R^S(\mathcal{I}(A))) = |\tilde{A}|.$$

Proof.*Proposition.[3.1,(i) and (ii)]*gives $Tr_R^S(\mathcal{I}(\tilde{A})) = Tr_R^S(\mathcal{I}(A))$ and $\mathcal{I}(\tilde{A})$ is complexified over R, from *Theorem. 2.2*,we obtain the result

$$rank_R(Tr_R^S(\mathcal{I}(A))) = rank_S(\mathcal{I}(\tilde{A})) = |\tilde{A}|.$$

Proposition.3.3. Let$\mathcal{C}$ be an$R$-linear cyclic free code of generator polynomial$g$. The complexified of $\mathcal{C}$is $\mathcal{I}(-\bar{A})$; where$A = Log_\xi(Spec(g))$.

Proof. We have $\mathcal{I}(-\bar{A}) = \langle\{P_b(X) := \sum_{i=0}^{n-1}\xi^{ib}X^i \mid b \in -\bar{A}\}\rangle_S$. For all $a \in A$; $-b \in \bar{A}$; we obtain $P_b(\xi^a) = 0$; because$0 < a - b < n$. Thus g divides all $P_b(X)$. Therefore $\mathcal{I}(-\bar{A}) \subseteq Ext_S(\mathcal{C})$. As

$$rank_S(\mathcal{I}(-\bar{A})) = rank_S(Ext_S(\mathcal{C})) = n - |A|;$$

it has the equality.

Theorem 3.1. Let $\mathcal{C}$ be an R-linear cyclic free code of generatorpolynomial g.

Then

$$\mathcal{C} = Tr_R^S(\mathcal{I}(A))^\perp, where\ A = Log_\xi(Spec(g)).$$

Proof.Suppose that $\mathcal{C}$ is a free cyclic linear code over R. ThenG.H. Norton and A. Sălăgean shown in [5], $\mathcal{C} := id(g)$ where$g \in R[X]$ is a divisor of $X^n - 1$

Let $p(X) = \sum_{i=0}^{n-1} p_i X_i$ bea wordcode of $\mathcal{C}$. We have

$$< p(X); ev_\xi(X^a) >= p(\xi^a)$$

for all$a \in A := Log_\xi(Spec(g))$. As gdivides p, we obtain $p(\xi^a) = 0$. Therefore $p(X) \in Res_R(\mathcal{I}(A)^\perp)$. By *Theorem.2.1*, we obtain

$$Tr_R^S(\mathcal{I}(A))^\perp = Res_R(\mathcal{I}(A)^\perp)$$

and as$A = \tilde{A}$, we deduce from *Proposition.3.1* and *Theorem.2.2* that $Res_R(\mathcal{I}(A)^\perp) = Res_R(\mathcal{I}(A))^\perp$.We obtain $\mathcal{C} \subseteq Tr_R^S(\mathcal{I}(A))^\perp$.Therefore$\mathcal{C} = Tr_S^R(\mathcal{I}(A))^\perp$;because

$$rank_R(\mathcal{C}) = rank_R(Tr_R^S(\mathcal{I}(A)^\perp) = n - |\tilde{A}|$$

Corollary 3.1. Let $\mathcal{C}$ be an$R$-linear cyclic free code with generatorpolynomial g. Then $\mathcal{C} = Tr_R^S(\mathcal{I}(-\bar{A}))$, where $A = Log_\xi(Spec(g))$.

Proof. By *Theorem.3.1*, we have $\mathcal{C} = Tr_R^S(\mathcal{I}(A))^\perp$, where$A = Log_\xi(Spec(g))$.Therefore by*Proposition.3.1* and*Theorems.2.1* and*Theorems.*2.2, we have:

$$\begin{aligned} \mathcal{C} &= Tr_R^S\left(\mathcal{I}\left(\tilde{A}\right)\right)^{\perp}; \\ &= Res_R(\mathcal{I}\left(-\bar{\tilde{A}}\right)^{\perp}); \\ &= Res_R(\mathcal{I}(-\bar{\tilde{A}})); \end{aligned}$$

Finally $\mathcal{C} = Tr_R^S(\mathcal{I}(-\bar{\tilde{A}}))$, since$\tilde{A} = A$.

CONCLUSION AND PERSPECTIVES

After this work, we characterize cyclic codes over finite chain ringsusing the trace function. A problem arises for the characterization anyof a cyclic codewith this method and this problem will be the subject of the next work.

References

[1] E. Martinez-Moro, A.P. Nicolas and I.F. Rua, ***On trace codes and Galois invariance over finite commutative chain rings***, Finite Fields Appl. 2013; (22): 114-121

[2] P. Delsarte, ***On subfield subcodes of modified Reed-Solomon codes***; IEEE Trans. Inform. Theory IT-21 (5) (1975) 575-576.

[3] G. Ganske and B. R. McDonald, ***Finite Local rings****; Amer. J. Mathematics.* Vol 3. Number 4.(1973). p.521-540.

[4] Jurgen Bierbrauer, ***The Theory of Cyclic Codes and a Generalization to Additive Codes***, Designs, Codes and Cryptography 25 (2002), 189-206

[5] G.H. Norton and A. Sãlãgean, ***On the structure of linear and cyclic codes over a finite chain ring***; Appl. Algebra Engrg. Comm. Comput., Vol. 10, No.6(2000)pp. 489-506.

[6] T. Honold and I. Landjev, ***Linear Codes over Finite Chain rings***; Electron. J. Combin., 7 (2000), pp. research Paper 11, 22pp. (electronic)