Global Journal of Science Frontier Research: F
Mathematics and Decision Sciences
Volume 23 Issue 3 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4626 & Print ISSN: 0975-5896

Quasi-Cyclic Codes Over Finite Chain $m\Theta$ Pseudo Field $F(p^kZ, 1)$

By Pemha Binyam Gabriel Cedric

University of Douala

Abstract- The $m\Theta$ sets present an enrichment from the logical viewpoint compared with the classical sets. The subset of the $m\Theta$ invariants of a $m\Theta$ set is a classical set, which leads to the canonical construction of the structures of modal Θ-valent pseudo field. In this note the purpose is to define on a finite chain $m\Theta$ pseudo field, $\mathbb{F}(p^k\mathbb{Z}, 1)$, the structures of Quasi- Cyclic codes of length r.

Keywords: $m\Theta$ *set,* $m\Theta$ *pseudo field, chain* $m\Theta$ *pseudo field, quasi-cyclic* $m\Theta$ *codes, linear* $m\Theta$ *codes.*

GJSFR-F Classification: DDC Code: 663.1 LCC Code: TP505

Strictly as per the compliance and regulations of:

1. J. Jensen, *The concatened structure of cyclic and abelian codes*, IEE Trans. Inform. Theory, vol.31, no 6, pp. 788 - 793, 1985.

Quasi-Cyclic Codes Over Finite Chain $m\Theta$ Pseudo Field $\mathbb{F}(p^k\mathbb{Z}, 1)$

Pemha Binyam Gabriel Cedric

Abstract- The $m\Theta$ sets present an enrichment from the logical viewpoint compared with the classical sets. The subset of the $m\Theta$ invariants of a $m\Theta$ set is a classical set, which leads to the canonical construction of the structures of modal Θ-valent pseudo field. In this note the purpose is to define on a finite chain $m\Theta$ pseudo field, $\mathbb{F}(p^k\mathbb{Z}, 1)$, the structures of Quasi-Cyclic codes of length r.

Keywords: *m*Θ *set, m*Θ *pseudo field, chain m*Θ *pseudo field, quasi-cyclic m*Θ *codes, linear m*Θ *codes.*

I. Introduction

Cyclic codes are among the most useful and well-studied code families for various reasons, such as effective encoding and decoding. A cyclic code can be viewed as an ideal in a certain quotient ring obtained from a polynomial ring with coefficients from a finite field [1, 2]. Quasi-Cyclic codes are a generalization of cyclic codes [6, 8]. Algebraically, Quasi-Cyclic codes are modules rather than ideals [10, 13].

A $m\Theta$ approach of the notion of sets has allowed to bring out the new classes of sets: $m\Theta$ sets. The notion of modal Θ-valent set ($m\Theta$ set) noted ($\mathbb{F}_{p\mathbb{Z}}$, F_α), p prime, is defined by F. Ayissi Eteme in [12, 16, 7]. Research on modal algebra has evolved and led to the theory of $m\Theta$ codes [11, 15, 17].

The theory of error-correcting $m\Theta$ codes over finite fields has experienced tremendous growth since its inception [5]. Progress has been attained in the direction of determining the structural properties of $m\Theta$ codes over large families of $m\Theta$ fields. This paper is a contribution along those lines as we focus on codes over finite $m\Theta$ pseudo fields with a linear lattice of $m\Theta$ ideals (the so-called chain $m\Theta$ pseudo fields).

The purpose of this paper is to obtain structure theorems for Quasi-Cyclic codes in more general setting. The structures of Quasi-Cyclic codes of length r over finite chain $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, 1)$ are established when r is not divisible by the characteristic of the residue $m\Theta$ pseudo field $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}$. Some cases where r is divisible by the characteristic of the residue $m\Theta$ pseudo field $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}$ are also considered.

Author: *University of Douala, Faculty of Science, Department of Mathematics and computer sciences, Douala Cameroon. e-mail: gpemha@yahoo.fr*

After presenting preliminary concepts and results on $m\Theta$ set in Section 2. Section 3 presents a canonical construction of the structures of modal Θ-valent field and modal Θ-valent field. Section 4 is devoted to the notion of modal Θ-valent extension of a finite field. Section 5 define the intrinsic polynomial representation of the $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, r)$. Section 6 presents the $m\Theta$ Quasi-Cyclic codes. Lastly, section 7 presents the structure of Quasi-Cyclic code over finite chain $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, 1)$.

II. Preliminaries

a) The modal Θ-valent set structure and the algebra of $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha)$

$m\Theta$ sets are considered to be non-classical sets which are compatible with a non-classical logic called the chrysippian $m\Theta$ logic.

Definition 0.1. *[14] Let E be a non-empty set, I be a chain whose first and last elements are 0 and 1 respectively, $(F_\alpha)_{\alpha\in I_*}$ where $I_* = I\setminus\{0\}$ be a family of applications form E to E.*
A $m\Theta$ set is the pair $\left(E, (F_\alpha)_{\alpha\in I_*}\right)$ simply denoted by (E, F_α) satisfying the following four axioms :

- $\underset{\alpha}{\cap} F_\alpha(E) = \underset{\alpha\in I_*}{\cap}\{F_\alpha(x) : x\in E\} \neq \emptyset$;
- $\forall \alpha, \beta \in I_*$, *if* $\alpha \neq \beta$ *then* $F_\alpha \neq F_\beta$;
- $\forall \alpha, \beta \in I_*$, $F_\alpha \circ F_\beta = F_\beta$;
- $\forall x, y \in E$, *if* $\forall \alpha \in I_*, F_\alpha(x) = F_\alpha(y)$ *then* $x = y$.

Theorem 0.1. *[16] (The theorem of $m\Theta$ determination)*
Let (E, F_α) be a $m\Theta$ set.

$$\forall x,\, y \in E,\, x =_\Theta y \text{ if and only if } \forall \alpha \in I_*,\, F_\alpha(x) = F_\alpha(y).$$

Proof 0.1. *[16]*

Definition 0.2. *[5] Let $\mathrm{C}(E, F_\alpha) = \underset{\alpha\in I_*}{\cap} F_\alpha(E)$. We call $\mathrm{C}(E, F_\alpha)$ the set of $m\Theta$ invariant elements of the $m\Theta$ set (E, F_α).*

Proposition 0.1. *[16] Let (E, F_α) be a $m\Theta$ set. The following properties are equivalent:*

1. $x \in \underset{\alpha\in I_*}{\cap} F_\alpha(E)$;
2. $\forall \alpha \in I_*$, $F_\alpha(x) = x$;
3. $\forall \alpha, \beta \in I_*$, $F_\alpha(x) = F_\beta(x)$;
4. $\exists \mu \in I_*$, $x = F_\mu(x)$.

Ref
14. F. Ayissi Eteme, *Anneau chrysippien Θ-valent*, CRAS, Paris 298, série 1, 1984, pp.1 - 4.

16. F. Ayissi Eteme, *Logique et Algèbre de structure mathématiques modales Θ-valentes chrysippiennes*, Edition Hermann, Paris, 2009.

Proof 0.2. [16]

Definition 0.3. [12]

Let (E, F_α) and (E', F'_α) be two $m\Theta$ sets. Let X be a non-empty set. We shall call

1. *(E', F'_α) a modal Θ-valent subset of (E, F_α) if the structure of $m\Theta$ set (E', F'_α) is the restriction to E' of the structure of the $m\Theta$ set (E, F_α), this means:*
   - $E' \subseteq E$;
   - $\forall \alpha : \alpha \in I_*,\ F'_\alpha = F_{\alpha|_{E'}}$.
2. *X a modal Θ-valent subset of (E, F_α) if:*
   - $X \subseteq E$;
   - *$(X, F_{\alpha|_X})$ is a $m\Theta s$ which is a modal Θ-valent subset of (E, F_α).*

In all what follows we shall write $F_\alpha x$ for $F_\alpha(x)$, $F_\alpha E$ for $F_\alpha(E)$, etc $\cdots$

Let $p \in \mathbb{N}$, a prime number. Let us recall that if $a \in \mathbb{F}_{p\mathbb{Z}}$.

$$\mathbb{F}_{p\mathbb{Z}} = \mathbb{F}_p \cup \{x_{p\mathbb{Z}} : \neg(x \equiv 0\,(mod p))\}\,; \quad \mathbb{F}_p = \{0,\ 1,\ 2,\ \cdots, p-1\}.$$

We define the $m\Theta$ support of a denoted $s(a)$ as follows:

$$s(a) = \begin{cases} a & if\ a \in \mathbb{F}_p; \\ x & if\ a = x_{p\mathbb{Z}}\ with\ \urcorner(x \equiv 0\,(mod\, p)). \end{cases}$$

Thus $s(a) \in \mathbb{F}_p$.

Definition 0.4. [14] Let $\perp$ be a binary operation on $\mathbb{F}_p$. So, $\forall a, b \in \mathbb{F}_p$, $a \perp b \in \mathbb{F}_p$. Let $x, y \in \mathbb{F}_{p\mathbb{Z}}$. We define a binary operation $\perp^*$ on $\mathbb{F}_{p\mathbb{Z}}$ as follows :

$$x \perp^* y = \begin{cases} s(x) \perp s(y) & if \begin{cases} x, y \in \mathbb{F}_p \\ (s(x) \perp s(y)) \equiv 0\,(mod\, p) \quad otherwise \end{cases} \\ (s(x) \perp s(y))_{p\mathbb{Z}} & otherwise. \end{cases}$$

$\perp^*$ as defined above on $\mathbb{F}_{p\mathbb{Z}}$ will be called a $m\Theta$ law on $\mathbb{F}_{p\mathbb{Z}}$ for $x, y \in \mathbb{F}_{p\mathbb{Z}}$.

Thus we can define $x + y \in \mathbb{F}_{p\mathbb{Z}}$ and $x \times y \in \mathbb{F}_{p\mathbb{Z}}$ for every $x, y \in \mathbb{F}_{p\mathbb{Z}}$, where $+$ and $\times$ are $m\Theta$ addition and $m\Theta$ multiplication respectively.

Theorem 0.2. [12] $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha, +, \times)$ is a $m\Theta$ ring of unity 1 and of $m\Theta$ unity $\frac{1}{p\mathbb{Z}}$.

Proof 0.3. [12]

Remark 0.1. Since p is prime, $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha)$ is a $m\Theta$ field.

Definition 0.5. [4] x is a divisor of zero in $(\mathbb{F}_{p\mathbb{Z}}, F_\alpha)$ if it exists $y \in \mathbb{F}_{p\mathbb{Z}}$ such that $x \times y = 0$

Example 0.1. [4]

$p = 2$, we have $\mathbb{F}_{2\mathbb{Z}} = \{0,\ 1,\ 1_{2\mathbb{Z}},\ 3_{2\mathbb{Z}}\}$

The table of $m\Theta$ determination and tables laws of $\mathbb{F}_{2\mathbb{Z}}$.

$\mathbb{F}_{2\mathbb{Z}}$	0	1	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
F_1	0	1	1	*0*
F_2	0	1	0	*1*

$+^{\Theta}$	*0*	*1*	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
0	*0*	*1*	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
1	*1*	*0*	*0*	*0*
$1_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$	*0*	*0*	*0*
$3_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$	*0*	*0*	*0*

$\times^{\Theta}$	*0*	*1*	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
0	*0*	*0*	*0*	*0*
1	*0*	*1*	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
$1_{2\mathbb{Z}}$	*0*	$1_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$
$3_{2\mathbb{Z}}$	*0*	$3_{2\mathbb{Z}}$	$3_{2\mathbb{Z}}$	$1_{2\mathbb{Z}}$

Observation:

$\mathbb{F}_{2\mathbb{Z}}$ has no divisor of zero, is a $m\Theta$ ring from four elements, that's a $m\Theta$ field of four elements.

III. Canonical Construction of Modal Θ-Valent Fields ($m\,\Theta f$) and Modal Θ-Valent Pseudo Fields($m\Theta pf$)

Let p be a prime number, $k \neq 0$ a positive integer, $q = p^k$ and $\mathbb{F}_q$ a finite field with q elements. Two $m\Theta f$ K_1 and K_2 of same characteristic p and of same cardinal p^{2k} are $m\Theta$ isomorphic.

a) Canonical construction of modal Θ-valent fields ($m\Theta f$)[9]

Consider that $k = 1$, so $q = p$. $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ is the prime field of characteristic p and of p elements. The modal Θ-valent quotient ring ($m\Theta qr$) $\mathbb{F}_{p\mathbb{Z}}$ as the modal Θ-valent quotient $\frac{\mathbb{Z}_{p\mathbb{Z}}}{p\mathbb{Z}_{p\mathbb{Z}}}$.

Let $\mathbb{F}^*_{p\mathbb{Z}} = \mathbb{F}_{p\mathbb{Z}} - \{0\}$. $\forall x \in \mathbb{F}^*_{p\mathbb{Z}},\ \exists x' \in \mathbb{F}^*_{p\mathbb{Z}}\ /\ x \cdot x' = \frac{1_{p\mathbb{Z}}}{p\mathbb{Z}_{p\mathbb{Z}}}$.

$\mathbb{F}_{p\mathbb{Z}}$ has p^2 elements but has no proper sub $m\Theta$ ring verifying the preceding property for $\mathbb{F}^*_{p\mathbb{Z}}$.

For which reason, $\mathbb{F}_{p\mathbb{Z}}$ is the prime $m\Theta f$ with p^2 elements. $\mathbb{F}_p$ is the prime sub field of the $m\Theta$ invariants of $\mathbb{F}_{p\mathbb{Z}}$. Let f be a polynomial with coefficients in $\mathbb{F}_p$. Clearly, it is all the same that:

1. $f_p(x)$ irreducible over $\mathbb{F}_p$.
2. $f_{p\mathbb{Z}}(x)$ irreducible over $\mathbb{F}_{p\mathbb{Z}}$.

Observations:

Let $\mathbb{F}(p\mathbb{Z}, r) = \frac{\mathbb{F}_{p\mathbb{Z}}[X]}{(f(X))}$ be the $m\Theta r$ modulo $f(x)$, $(m\Theta r(f))$. $f(x) \in \mathbb{F}_p[X]$. $deg(f) = r,\ r \in \mathbb{N}^*,\ f$ irreducible over $\mathbb{F}_p$.

$$\mathbb{F}_{p\mathbb{Z}}[X] \longrightarrow \mathbb{F}(p\mathbb{Z}, r) : g \longmapsto r_g;\ g = q_g \cdot \underset{r-1}{f(x)} + r_g,\ 0 \leq dg(r_g) < dg(f).$$

$(\mathbb{F}_{p\mathbb{Z}})^r \longrightarrow \mathbb{F}(p\mathbb{Z}, r) : (a_0, \cdots, a_{r-1}) \longmapsto \sum_{i=0} a_i x^i$ is a bijection and therefore becomes a $m\Theta r$ isomorphism for the $m\Theta$ laws modulo $f(x)$. Since f is irreducible over $\mathbb{F}_{p\mathbb{Z}}$, $\mathbb{F}(p\mathbb{Z}, r)$ is a $m\Theta f$.

Ref

9. F. Ayissi Eteme, *chrm Θ introducing pure and applied mathematics*, Lambert academic publishing saarbrüken, Germany, 2015.

Theorem 0.3. *1.* $\mathbb{F}(p\mathbb{Z}, r)$ *is a* $m\Theta f$ *of cardinal* p^{2r}*;*

2. $\mathbb{F}_{p\mathbb{Z}}$ *is its prime sub* $m\Theta f$ *of cardinal* p^2*;*

3. $\mathbb{F}_{p\mathbb{Z}}$ *and* $\mathbb{F}(p\mathbb{Z}, r)$ *are booth of characteristic* p *since* $\forall i$:

$$i = 0, \cdots, p-1; \quad \underbrace{1+1+\cdots+1}_{i\,times} + \underbrace{1_{p\mathbb{Z}}+\cdots+1_{p\mathbb{Z}}}_{(p-i)\,times} = 0$$

Proof 0.4. [9]

According to a previous notation,

$$\mathbb{F}(p\mathbb{Z}, 1) = \mathbb{F}_{p\mathbb{Z}}, \ \mathbb{F}(p, 1) = \frac{\mathbb{Z}}{p\mathbb{Z}}, \ \mathbb{F}(p, r) = \mathbb{GF}(p, r).$$

b) Canonical construction of modal Θ*-valent pseudo fields (*$m\Theta pf$*)*

Consider that $k \neq 1$, so $q = p^k$. Let then $\mathbb{F}(p^k\mathbb{Z}, 1)$ denote the quotient $m\Theta r$ $\mathbb{F}_{p^k\mathbb{Z}} = \frac{\mathbb{Z}_{p\mathbb{Z}}}{p^k\mathbb{Z}_{p\mathbb{Z}}}$ and let

$$O(p^k, 1) = O_{p^k} = \{\frac{a}{p^k\mathbb{Z}_{p\mathbb{Z}}} : a \in \mathbb{Z}_{p\mathbb{Z}}, s(a)/p^k\} = \{\frac{a}{p^k\mathbb{Z}} : a \in \mathbb{Z}, a/p^k\}.$$

Let $\mathbb{F}^*(p^k\mathbb{Z}, 1) = \mathbb{F}(p^k\mathbb{Z}, 1) - O(p^k, 1); k \in \mathbb{N}^*$. Then $\forall x : x \in \mathbb{F}^*(p^k\mathbb{Z}, 1), \exists x' : x' \in \mathbb{F}^*(p^k\mathbb{Z}, 1) : x \cdot x' = \frac{1_{p\mathbb{Z}}}{p^k\mathbb{Z}_{p\mathbb{Z}}}$.

So we call $\mathbb{F}_{p^k\mathbb{Z}}$ a $m\Theta$ pseudo field ($m\Theta pf$). $\mathbb{F}_{p^k\mathbb{Z}}$ has p^{k+1} elements and is of characteristic p^k. It has no proper sub $m\Theta pf$ with the same as the preceding properties for $\mathbb{F}^*(p^k\mathbb{Z}, 1)$. Finally, $\mathbb{F}(p^k\mathbb{Z}, 1)$ is the prime $m\Theta pf$ with p^{k+1} elements.

Let now $f \in \mathbb{Z}_{p^k}[X] : dg(f) = r$ and f irreducible over $\mathbb{Z}_{p^k} = \frac{\mathbb{Z}}{p^k\mathbb{Z}}$. Let $\mathbb{F}(p^k\mathbb{Z}, r) = \frac{\mathbb{F}(p^k\mathbb{Z}, 1)[X]}{(f(X))}$ $m\Theta r$ modulo $f(x)$. $\mathbb{F}(p^k\mathbb{Z}, r)$ is a $m\Theta pf$.

$(\mathbb{F}(p^k\mathbb{Z}, 1))^r \longrightarrow \mathbb{F}(p^k\mathbb{Z}, r) : (a_0, \cdots, a_{r-1}) \longmapsto \sum_{i=0}^{r-1} a_i x^i$ is a bijection and therefore a $m\Theta$ ring modulo $f(X)$ isomorphism. Since $card\mathbb{F}(p^k\mathbb{Z}, 1) = p^{k+1}$, $card\mathbb{F}(p^k\mathbb{Z}, r) = p^{(k+1)r}$.

Theorem 0.4. [9] $\forall k \in \mathbb{N} - \{0\}$,

1. $\mathbb{F}(p^k\mathbb{Z}, r)$ *is a* $m\Theta pf$ *of cardinal* $p^{(k+1)r}$*.*

2. $\mathbb{F}(p^k\mathbb{Z}, 1)$ *is its prime sub* $m\Theta pf$ *of* p^{k+1} *elements.*

3. $\mathbb{F}(p^k\mathbb{Z}, 1)$ *and* $\mathbb{F}(p^k\mathbb{Z}, r)$ *are booth of characteristic* p^k*.*

Proof 0.5. [9]

$\mathbb{F}(p^k, r) = G\mathbb{F}(p^k, r)$ is the sub pseudo field of the $m\Theta$ invariants of the $m\Theta pf$ $\mathbb{F}(p^k\mathbb{Z}, r)$. $\mathbb{F}_{p^k} = \frac{\mathbb{Z}}{p^k\mathbb{Z}}$ is the prime sub pseudo field of the $m\Theta$ invariants of $\mathbb{F}_{p^k\mathbb{Z}}$; the prime sub $m\Theta pf$ with p^{k+1} elements.

Ref

9. F. Ayissi Eteme, *chrm Θ introducing pure and applied mathematics*, Lambert academic publishing saarbrüken, Germany, 2015.

Theorem 0.5. [9]

1. *Any $m\Theta f$ K of characteristic p prime and then of cardinal p^{2r}, $r \in \mathbb{N}^*$ is $m\Theta$ isomorphic to the $m\Theta f$ $\mathbb{F}(p\mathbb{Z}, r)$;*
2. *Any $m\Theta f$ K' of characteristic p^k, p prime and then of cardinal $p^{(k+1)r}$, $r \in \mathbb{N}^*$ is $m\Theta$ isomorphic to the $m\Theta f$ $\mathbb{F}(p^k\mathbb{Z}, r)$.*

Proof 0.6. [9]

IV. Modal Θ-Valent Extension of a Finite Field

Note that K is a finite field of cardinal p^n, $p, n \in \mathbb{N}^*$ and then of characteristic p prime. $\beta \in K$, of minimal polynomial $m_\beta(x) \in \mathbb{F}_p[x]$, $r = deg_{\mathbb{F}_p}(m_\beta(x)) \in \mathbb{N}^*$, $m_\beta(x)$ is irreducible over $\mathbb{F}_p$.

Observations: Let $I_\beta = \langle m_\beta(x)\rangle_{\mathbb{F}_p[x]}$ the principal ideal of $\mathbb{F}_p[x]$ generated by $m_\beta(x)$. Since $\mathbb{F}_p \subset \mathbb{F}_{p\mathbb{Z}}$, $\mathbb{F}_p[x] \subset \mathbb{F}_{p\mathbb{Z}}[x]$.
Let $a \in {\mathbb{F}^*}_{p\mathbb{Z}}$: $\exists \mu$, $F_\mu a \neq 0$, then $F_\mu a \in {\mathbb{F}^*}_p$, thus $m_\beta(F_\mu a) \neq 0$ and since $F_\mu m_\beta(a) = m_\beta(F_\mu a)$, $F_\mu m_\beta(a) \neq 0$. Then $m_\beta(a) \neq 0$.

Therefore, $m_\beta(x)$ is also irreducible over $\mathbb{F}_{p\mathbb{Z}}$. It is known that $\frac{\mathbb{F}_{p\mathbb{Z}}[x]}{\langle m_\beta(x)\rangle}$ is a $m\Theta$ field with p^{2r} elements and then of characteristic p. $\frac{\mathbb{F}_p[x]}{m_\beta(x)}$ is its subfield of the Θ-invariants who has p^r elements and characteristic p.

Let $I_{\beta\ p\mathbb{Z}} = \langle m_\beta(x)\rangle_{\mathbb{F}_{p\mathbb{Z}}[x]}$ the principal $m\Theta$ ideal of $\mathbb{F}_{p\mathbb{Z}}[x]$ generated by $m_\beta(x)$. $\forall \alpha$, $F_\alpha I_{\beta\ p\mathbb{Z}} = I_\beta$ therefore $I_{\beta\ p\mathbb{Z}}$ is a $m\Theta$ maximal ideal of $\mathbb{F}_{p\mathbb{Z}}[x]$. Then define $\Phi_{\beta\ p\mathbb{Z}} : \mathbb{F}_{p\mathbb{Z}}[x] \longrightarrow \mathbb{F}(p\mathbb{Z}, n)$ as follows; if $f(x) = \sum_{i=0}^{q} a_i x^i \in \mathbb{F}_{p\mathbb{Z}}[x]$,

$$\Phi_{\beta\ p\mathbb{Z}}(f(x)) = f(\beta) = \sum_{i=0}^{q} a_i \beta^i \in \mathbb{F}(p\mathbb{Z}, n).$$

By definition $\Phi_{\beta\ p\mathbb{Z}}$ is a $m\Theta$ ring morphism since then $\Phi_{\beta\ p\mathbb{Z}}(\mathbb{F}_{p\mathbb{Z}}[x]) = \{f(\beta) \,|\, f(x) \in \mathbb{F}_{p\mathbb{Z}}[x]\}$ is a sub $m\Theta$ field of $\mathbb{F}(p\mathbb{Z}, n)$. Therefore the following diagram $m\Theta$ commutes

$$\begin{array}{ccccc} \mathbb{F}_{p\mathbb{Z}}[x] & \xrightarrow{\Phi_{\beta\ p\mathbb{Z}}} & \varphi_{\Phi_{\beta\ p\mathbb{Z}}}(\mathbb{F}_{p\mathbb{Z}}[x]) & \xrightarrow{i_{p\mathbb{Z}}} & \mathbb{F}(p\mathbb{Z}, n) \\ \downarrow{\scriptstyle \varphi_{\Phi_{\beta\ p\mathbb{Z}}}} & \nearrow{\scriptstyle \tilde{\Phi}_{\beta\ p\mathbb{Z}} = \frac{\Phi_{\beta\ p\mathbb{Z}}}{\langle m_\beta(x)\rangle}} & & & \\ \frac{\mathbb{F}_{p\mathbb{Z}}[x]}{I_\beta} & & & & \end{array}$$

- $\frac{\mathbb{F}_{p\mathbb{Z}}[x]}{I_\beta} = \frac{\mathbb{F}_{p\mathbb{Z}}[x]}{\langle m_\beta(x)\rangle}$ is a $m\Theta$ field of cardinal p^{2r} and then of characteristic p.

Ref
9. F. Ayissi Eteme, *chrm Θ introducing pure and applied mathematics*, Lambert academic publishing saarbrüken, Germany, 2015.

- Through the $m\Theta$ ring isomorphism $\widetilde{\Phi}_{\beta\ p\mathbb{Z}}$, $\widetilde{\Phi}_{\beta\ p\mathbb{Z}}(\mathbb{F}_{p\mathbb{Z}}[x])$ becomes a $m\Theta$ subfield of $\mathbb{F}(p\mathbb{Z}, n)$ with the $m\Theta$ field structure of p^{2r} elements exported from $\frac{\mathbb{F}_{p\mathbb{Z}}[x]}{\langle m_\beta(x)\rangle}$ by $\widetilde{\Phi}_{\beta\ p\mathbb{Z}}$.

Notation 0.1.

$$\mathbb{F}_{p\mathbb{Z}}(\beta) = \Phi_{p\mathbb{Z}}(\beta) = \widetilde{\Phi}_{\beta\ p\mathbb{Z}}(\mathbb{F}_{p\mathbb{Z}}[x]) = \{f(\beta) \,|\, f(x) \in \mathbb{F}_{p\mathbb{Z}[x]}\}$$

Theorem 0.6. *1. $\mathbb{F}_{p\mathbb{Z}}[\beta]$ has p^{2r} elements and characteristic p.*

2. $\mathbb{F}_{p\mathbb{Z}}$ is the prime $m\Theta$ subfield of $\mathbb{F}_{p\mathbb{Z}}[\beta]$.

3. Any sub $m\Theta$ field of $\mathbb{F}(p\mathbb{Z}, n)$ containing $\mathbb{F}_{p\mathbb{Z}}$ and β contains $\mathbb{F}_{p\mathbb{Z}}[\beta]$.

4. $\forall a\,;\, a \in \mathbb{F}_{p\mathbb{Z}}[\beta]$, $\exists a_i$, $i = 0, 1, \cdots, r-1 \,/\, a_i \in \mathbb{F}_{p\mathbb{Z}} : a = \sum_{i=0}^{r-1} a_i\beta^i$.

Definition 0.6. *Henceforth we call $\mathbb{F}_{p\mathbb{Z}}[\beta]$ the $m\Theta$ extension of $\mathbb{F}_p$ and $\mathbb{F}_{p\mathbb{Z}}$ to β.*

Definition 0.7. *We call a $m\Theta$ primitive element of $\mathbb{F}(p\mathbb{Z}, n)$ any generator if there exists one, noted α, of $\mathbb{F}(p\mathbb{Z}, n) - \mathbb{F}(p, n)$. This meaning that $\forall a : a \in \mathbb{F}(p\mathbb{Z}, n) - \mathbb{F}(p, n), \exists m \in \mathbb{N} : 0 \leq m \leq \omega(\mathbb{F}^*(p\mathbb{Z}, n); a = \alpha^m$.*

Example 0.2. *$2_{3\mathbb{Z}}$ and $5_{3\mathbb{Z}}$ are two $m3$ generators of $\mathbb{F}_{3\mathbb{Z}}$.*

Proposition 0.2. *If $\alpha \in \mathbb{F}(p\mathbb{Z}, n)$ is a $m\Theta$ primitive element then $\mathbb{F}(p\mathbb{Z}, n) = \mathbb{F}_{p\mathbb{Z}}(\alpha)$.*

Proof 0.7. *Suppose $u \in \mathbb{F}(p\mathbb{Z}, n) - \mathbb{F}(p, n)$ and α is a $m\Theta$ primitive element: $\exists m, m \in \mathbb{N} : 0 \leq m \leq \omega(\mathbb{F}^*(p\mathbb{Z}, r), u = \alpha^m$. Let $f(x) = x^m \in \mathbb{F}_{p\mathbb{Z}}[x]$, $\Phi_{\beta\, p\mathbb{Z}}(f(x)) = f(\alpha) = x^m$.*

Therefore $u = \alpha^m = f(\alpha) \in \mathbb{F}_{p\mathbb{Z}}(\alpha)$. Thus $\mathbb{F}(p\mathbb{Z}, n) = \mathbb{F}_{p\mathbb{Z}}(\alpha)$.

V. The Intrinsic Polynomial Representation of the $m\Theta$ Pseudo Field $\mathbb{F}(p^k\mathbb{Z}, r)$

Let $k \in \mathbb{N}$, r, $p \in \mathbb{N}^*$, p prime $2 \leq p$. It is plain in [7] that:

$$\prod_{a \in \mathbb{F}^*(p^k\mathbb{Z}, 1)} (x - a) = \prod_{x \in \tilde{\mathbb{F}}^*_{p^k}} (x - a) \times \prod_{a \in \mathbb{F}^*(p^k\mathbb{Z}, 1) - \mathbb{F}^*_{p^k}} (x - a)$$

$$= (x^{\varphi(p^k)} - 1)(x^{\varphi(p^{k+1})} - 1_{p\mathbb{Z}}).$$

$\mathbb{F}(p^k, 1) = \frac{\mathbb{Z}}{p^k\mathbb{Z}}$.

Proposition 0.3. *Let $< x^{\varphi(p^k)} - 1 >$ and $< x^{\varphi(p^{k+1})} - 1_{p\mathbb{Z}} >$ be the ideals of $\mathbb{F}(p^k, 1)[x]$ respectively generated by $x^{\varphi(p^k)} - 1$ and $x^{\varphi(p^{k+1})} - 1_{p\mathbb{Z}}$, then*

1. *$< x^{\varphi(p^k)} - 1 >$ is a maximal $m\Theta$ ideal of $\mathbb{F}(p^k, 1)[x]$;*
2. *$< x^{\varphi(p^{k+1})} - 1_{p\mathbb{Z}} > \subsetneqq < x^{\varphi(p^k)} - 1 >$.*

Proof 0.8. 1. *$< x^{\varphi(p^k)} - 1 >$ is a $m\Theta$ ideal since generated by the $m\Theta\Theta$ invariant polynomial $x^{\varphi(p^k)} - 1$; this Θ ideal is a maximal since $< x^{\varphi(p^k)} - 1 >_{\mathbb{F}_{p^k}[x]}$ is maximal in $\mathbb{F}_{p^k}[x]$ and $\forall \alpha \in I_*, F_\alpha < x^{\varphi(p^k)} - 1 > = < x^{\varphi(p^k)} - 1 >_{\mathbb{F}_{p^k}[x]}$. This is sufficient to claim that $\frac{\mathbb{F}(p^k,1)[x]}{<x^{\varphi(p^k)}-1>}$ is a $m\Theta$ pseudo field, and as such $m\Theta$ isomorphic to the $m\Theta$ pseudo field $\mathbb{F}(p^k, \varphi(p^k))$.*

2. *$x^{\varphi(p^{k+1})} - 1_{p\mathbb{Z}} \in < x^{\varphi(p^k)} - 1 >$. Since $\varphi(p^{k+1}) = p\varphi(p^k)$, $x^{\varphi(p^{k+1})} = x^{p\varphi(p^k)}$. Henceforth,*

$$\begin{aligned} x^{\varphi(p^{k+1})} - 1_{p\mathbb{Z}} &= x^{p\varphi(p^k)} - 1_{p\mathbb{Z}} \\ &= (x^{\varphi(p^k)})^p - 1^p_{p\mathbb{Z}} \\ &= (x^{\varphi(p^k)} - 1_{p\mathbb{Z}})^p \\ &= (x^{\varphi(p^k)} - 1)(x^{\varphi(p^k)} - 1_{p\mathbb{Z}})^{p-1} \end{aligned}$$

This last expression shows that $x^{\varphi(p^{k+1})} - 1_{p\mathbb{Z}} \in < x^{\varphi(p^k)} - 1 >$. Trivially, $x^{\varphi(p^k)} - 1 \notin < x^{\varphi(p^{k+1})} - 1_{p\mathbb{Z}} >$. Therefore $< x^{\varphi(p^{k+1})} - 1_{p\mathbb{Z}} > \subsetneqq < x^{\varphi(p^k)} - 1 >$, $\forall k \in \mathbb{N}^*$. Thus $< x^{p(p-1)} - 1_{p\mathbb{Z}} > \subsetneqq < x^{p-1} - 1 >$.

Definition 0.8. *The $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, \varphi(p^k)) = \frac{\mathbb{F}(p^k\mathbb{Z},1)[x]}{<x^{\varphi(p^k)}-1>}$ is what we call the intrinsic polynomial representation of the $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, r)$.*

Corollary 0.1. *$\mathbb{F}(p\mathbb{Z}, \varphi(p)) = \frac{\mathbb{F}(p\mathbb{Z},1)[x]}{<x^{(p-1)}-1>}$ is the intrinsic polynomial representation of $\mathbb{F}(p\mathbb{Z}, r)$ with $r = \varphi(p) = p - 1$, $k = 1$.*

Proposition 0.4. *For a finite commutative $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, 1)$ the following conditions are equivalent:*

1. *$\mathbb{F}(p^k\mathbb{Z}, 1)$ is a local $m\Theta$ pseudo field and the maximal $m\Theta$ ideal M of $\mathbb{F}(p^k\mathbb{Z}, 1)$ is principal;*
2. *$\mathbb{F}(p^k\mathbb{Z}, 1)$ is a local principal $m\Theta$ ideal pseudo field;*
3. *$\mathbb{F}(p^k\mathbb{Z}, 1)$ is a chain $m\Theta$ pseudo field.*

Notes

Proof 0.9. *i) $\Longrightarrow$ ii). Let I be an $m\Theta$ ideal of $\mathbb{F}(p^k\mathbb{Z}, 1)$. If $I = \mathbb{F}(p^k\mathbb{Z}, 1)$ then I is generated by the identity 1. If $I \subsetneq \mathbb{F}(p^k\mathbb{Z}, 1)$, then $I \subseteq M$. By i), M is generated by an element, say $M = \langle a\rangle$. Therefore, $I = \langle a^i\rangle$, for some integer k. Hence, $\mathbb{F}(p^k\mathbb{Z}, 1)$ is a local principal $m\Theta$ ideal pseudo field.*

ii) $\Longrightarrow$ iii). Let $\mathbb{F}(p^k\mathbb{Z}, 1)$ be a local principal $m\Theta$ ideal pseudo field with the maximal ideal $M = \langle a\rangle$, and A, B be proper ideals of $\mathbb{F}(p^k\mathbb{Z}, 1)$. Then $A, B \subseteq M$, whence there exist integers l, m such that $A = \langle a^l\rangle$, $B = \langle a^m\rangle$ ($l, m \leq$ the nilpotency of a). Hence, either $A \subseteq B$, or $B \subseteq A$. Thus, $\mathbb{F}(p^k\mathbb{Z}, 1)$ is a chain $m\Theta$ pseudo field.

iii) $\Longrightarrow$ i). Assume $\mathbb{F}(p^k\mathbb{Z}, 1)$ is a finite commutative chain $m\Theta$ pseudo field, then clearly $\mathbb{F}(p^k\mathbb{Z}, 1)$ is local. To show the maximal $m\Theta$ ideal M of $\mathbb{F}(p^k\mathbb{Z}, 1)$ is principal, suppose to the contrary that M is generated by more than one element, say b, c are in the generator set of M and $b \notin c\mathbb{F}(p^k\mathbb{Z}, 1)$, $c \notin b\mathbb{F}(p^k\mathbb{Z}, 1)$. Then $\langle b\rangle \nsubseteq \langle c\rangle$ and $\langle c\rangle \nsubseteq \langle b\rangle$, a contradiction with the assumption that $\mathbb{F}(p^k\mathbb{Z}, 1)$ is a chain $m\Theta$ pseudo field. Thus, M is principal, proving i).

Let a be a fixed generator of the maximal ideal M. Then a is nilpotent and we denote its nilpotency index by t. The ideals of $\mathbb{F}(p^k\mathbb{Z}, 1)$ for a chain

$$\mathbb{F}(p^k\mathbb{Z}, 1) = \langle a^0\rangle \supsetneq \langle a^1\rangle \supsetneq \cdots \supsetneq \langle a^{t-1}\rangle \supsetneq \langle a^t\rangle = \langle 0\rangle.$$

Let $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)} = \frac{\mathbb{F}(p^k\mathbb{Z}, 1)}{M}$. By $^- : \mathbb{F}(p^k\mathbb{Z}, 1)[x] \longrightarrow \overline{\mathbb{F}(p^k\mathbb{Z}, 1)}[x]$, we denote the natural $m\Theta$ pseudo field homomorphism that maps $\rho \longmapsto \rho + M$ and the variable x to x.

Proposition 0.5. *Let $\mathbb{F}(p^k\mathbb{Z}, 1)$ be a finite commutative chain $m\Theta$ pseudo field, with maximal ideal $M = \langle a\rangle$, and let t be a nilpotency a. Then we get the following statements.*

1. *For some prime p and positive integers k, l ($k \geq l$), $|\mathbb{F}(p^k\mathbb{Z}, 1)| = p^{k+1}$, $|\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}| = p^{l+1}$, and the characteristic of $\mathbb{F}(p^k\mathbb{Z}, 1)$ and $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}$ are powers of p.*
2. *For $i = 0, \cdots, t$, $|\langle a^i\rangle| = |\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}|^{t-i}$. In particular, $|\mathbb{F}(p^k\mathbb{Z}, 1)| = |\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}|^t$, so, $k = lt$.*

Two $m\Theta$ polynomials $f_1, f_2 \in \mathbb{F}(p^k\mathbb{Z}, 1)[x]$ are called $m\Theta$ coprime if $\langle f_1\rangle + \langle f_2\rangle = \mathbb{F}(p^k\mathbb{Z}, 1)[x]$. A $m\Theta$ polynomial $f \in \mathbb{F}(p^k\mathbb{Z}, 1)[x]$ is called basic $m\Theta$ irreducible if $\overline{f}$ is $m\Theta$ irreducible in $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}[x]$. A $m\Theta$ polynomial $f \in \mathbb{F}(p^k\mathbb{Z}, 1)[x]$ is called regular if it is not a zero divisor.

VI. $m\Theta$ Quasi-Cyclic Codes

For a finite $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, 1)$, consider the set $\mathbb{F}^r(p^k\mathbb{Z}, 1)$ of n-tuples of elements from $\mathbb{F}(p^k\mathbb{Z}, 1)$ as a module over $\mathbb{F}(p^k\mathbb{Z}, 1)$ in the usual way. A subset $C \subseteq \mathbb{F}^r(p^k\mathbb{Z}, 1)$ is called a linear $m\Theta$ code of length r over $\mathbb{F}(p^k\mathbb{Z}, 1)$ if C is an $\mathbb{F}(p^k\mathbb{Z}, 1)$-submodule of $\mathbb{F}^r(p^k\mathbb{Z}, 1)$. C is called $m\Theta$ cyclic if, for every $m\Theta$ codeword $x = (x_0, x_1, \cdots, x_{r-1}) \in C$, its cyclic shift $(x_{n-1}, x_0, x_1, \cdots, x_{n-2})$ is also in C. An n-tuple $c = (c_0, c_1, \cdots, c_{r-1}) \in \mathbb{F}^r(p^k\mathbb{Z}, 1)$ is identified with the $m\Theta$ polynomial $c_0 + c_1x + \cdots + c_{r-1}x^{r-1}$ in $\frac{\mathbb{F}(p^k\mathbb{Z}, 1)[x]}{<x^r-1>}$, which is called the $m\Theta$ polynomial representation of $c = (c_0, c_1, \cdots, c_{r-1})$.

It is well known that a code C of length r over $\mathbb{F}(p^k\mathbb{Z}, 1)$ is $m\Theta$ cyclic if and only if the $m\Theta$ set of polynomial representations of its $m\Theta$ codewords is an $m\Theta$ ideal of $\frac{\mathbb{F}(p^k\mathbb{Z}, 1)[x]}{<x^r-1>}$.

Given $x = (x_0, x_1, \cdots, x_{r-1})$, $y = (y_0, y_1, \cdots, y_{r-1}) \in \mathbb{F}^r(p^k\mathbb{Z}, 1)$, their scalar product is

$$x \cdot y = x_0y_0 + x_1y_1 + \cdots + x_{r-1}y_{r-1}.$$

(evaluated in $\mathbb{F}(p^k\mathbb{Z}, 1)$). Two $m\Theta$ words x, y are called orthogonal if $\forall \alpha \in I_*$, $F_\alpha(x) \cdot F_\alpha(y) = 0$. For a linear $m\Theta$ code C over $\mathbb{F}(p^k\mathbb{Z}, 1)$, its dual code $C^\perp$ is the set of $m\Theta$ words over $\mathbb{F}(p^k\mathbb{Z}, 1)$ that are orthogonal to all $m\Theta$ codewords of C;

$$C^\perp = \{x \in \mathbb{F}(p^k\mathbb{Z}, 1) | \forall \alpha \in I_*,\ F_\alpha(x) \cdot F_\alpha(y) = 0,\ \forall y \in C\}.$$

A $m\Theta$ code C is called self-dual if $C = C^\perp$. For a finite $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, 1)$ with maximal ideal $\langle a \rangle$ and the nilpotency t of a is even, the code $\langle a^{\frac{t}{2}} \rangle$ is self-dual and is called the trivial self-dual code.

Proposition 0.6. *Let $\mathbb{F}(p^k\mathbb{Z}, 1)$ be a finite commutative $m\Theta$ pseudo field and*

$$a(x) = a_0 + a_1x + \cdots + a_{r-1}x^{r-1};$$

$$b(x) = b_0 + b_1x + \cdots + b_{r-1}x^{r-1} \in \mathbb{F}(p^k\mathbb{Z}, 1)[x].$$

Then $a(x)b(x) = 0$ in $\frac{\mathbb{F}(p^k\mathbb{Z}, 1)[x]}{<x^r-1>}$ if and only if $(a_0, a_1, \cdots, a_{r-1})$ is $m\Theta$ orthogonal to $(b_{r-1}, b_{r-2}, \cdots, b_0)$ and all its cyclic shifts.

Proof 0.10. *Let ζ denote the cyclic shift for $m\Theta$ codewords of length r, i.e., for each $(x_0, x_1, \cdots, x_{r-1}) \in \mathbb{F}^r(p^k\mathbb{Z}, 1)$.*

$$\zeta(x_0, x_1, \cdots, x_{r-1}) = (x_{r-1}, x_0, \cdots, x_{r-2}).$$

Thus, $\zeta^i(b_{r-1}, b_{r-2}, \cdots, b_0),\ i = 1, 2, \cdots, r$ *are all cyclic shifts of* $(b_{r-1}, b_{r-2}, \cdots, b_0)$. *Let* $c(x) = c_0 + c_1x + \cdots + c_{r-1}x^{r-1} = a(x)b(x) \in \frac{\mathbb{F}(p^k\mathbb{Z}, 1)[x]}{<x^r-1>}$. *Then for* $k = 0, 1, \cdots, r-1$,

$$\begin{aligned} c_k &= \sum_{i+j=k \text{ or } i+j=r-k} a_i b_j \\ &= (a_0, a_1, \cdots, a_{r-1}) \cdot (b_k, b_{k-1}, \cdots, b_{k+1}) \\ &= (a_0, a_1, \cdots, a_{r-1}) \cdot \zeta^{k+1}(b_{r-1}, b_{r-2}, \cdots, b_0). \end{aligned}$$

Therefore, $c(x) = 0$ *if and only if* $c_k = 0$ *for* $k = 0, 1, \cdots, r-1$ *if and only if*

$$(a_0, a_1, \cdots, a_{r-1}) \cdot \zeta^{k+1}(b_{r-1}, b_{r-2}, \cdots, b_0) = 0,$$

for $k = 0, 1, \cdots, r-1$ *if and only if* $(a_0, a_1, \cdots, a_{r-1})$ *is orthogonal to* $(b_{r-1}, b_{r-2}, \cdots, b_0)$ *and all its cyclic shifts, as desired.*

Definition 0.9. *(quasi-cyclic* $m\Theta$ *code)*
A linear $m\Theta$ *code* C *of length* $r = lk$ *over a finite* $m\Theta$ *pseudo field* $\mathbb{F}(p^k\mathbb{Z}, 1)$ *is called a quasi-cyclic* $m\Theta$ *code of index* k *if for every* $m\Theta$ *codeword* $c \in C$ *there exists a number* k *such that the* $m\Theta$ *codeword obtained by* k *cyclic shifts is also a* $m\Theta$ *codeword in* C. *That is,*

$$c = (c_0, c_1, \cdots, c_{r-1}) \in C \Longrightarrow c' = \zeta^k(c) = (c_{r-k}, \cdots, c_0, \cdots, c_{r-k-1}) \in C.$$

In the definition k is defined as the smallest number of cyclic shifts where the $m\Theta$ code is invariant. Quasi-cyclic $m\Theta$ codes are a generalization of cyclic $m\Theta$ codes.

VII. Structure of Quasi-Cyclic Code Over Finite Chain $m\Theta$ Pseudo Field $\mathbb{F}(p^k\ \mathbb{Z}, 1)$

Let $\mathbb{F}(p^k\mathbb{Z}, 1)$ be a finite chain $m\Theta$ pseudo field with the maximal $m\Theta$ ideal $\langle a \rangle$, and t be the nilpotency of a. There exist a prime p and an integer l such that $|\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}| = p^l$, $|\mathbb{F}(p^k\mathbb{Z}, 1)| = p^{lt}$, the characteristic of $\mathbb{F}(p^k\mathbb{Z}, 1)$ and $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}$ are powers of p. In this section, we assume r to be a positive integer which is not divisible by p; that implies r is not divisible by the characteristic of the residue $m\Theta$ pseudo field $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}$, so that $x^r - 1$ is square free in $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}[x]$. Therefore, $x^r - 1$ has a unique decomposition as a product of basic irreducible pairwise coprime $m\Theta$ polynomials in $\mathbb{F}(p^k\mathbb{Z}, 1)[x]$.

Lemma 0.1. *Let $\mathbb{F}(p^k\mathbb{Z}, 1)$ be a finite chain $m\Theta$ pseudo field with the maximal $m\Theta$ ideal $\langle a\rangle$, and t be the nilpotency of a. If f is a regular basic irreducible $m\Theta$ polynomial of the $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, 1)[x]$, then $\frac{\mathbb{F}(p^k\mathbb{Z}, 1)[x]}{\langle f\rangle}$ is also a chain $m\Theta$ pseudo field with precisely the following ideals:*

$$\langle 0\rangle, \langle 1\rangle, \langle 1 + \langle f\rangle\rangle, \langle a + \langle f\rangle\rangle, \cdots, \langle a^{t-1} + \langle f\rangle\rangle.$$

Proof 0.11. *First we show that for distinct values of i, $j \in \{0, 1, \cdots, t-1\}$, $\langle a^i + \langle f\rangle\rangle \neq \langle a^j + \langle f\rangle\rangle$. Suppose $\langle a^i + \langle f\rangle\rangle = \langle a^j + \langle f\rangle\rangle$, for $0 \leq i < j \leq t-1$. Then, there exists $g(x) \in \mathbb{F}(p^k\mathbb{Z}, 1)[x]$ with $deg(g) < deg(f)$ such that $a^i + \langle f\rangle = a^j + \langle f\rangle$. That means $a^j g(x) - a^i \in \langle f\rangle$. As*

$$deg(a^j g(x) - a^i) \leq deg(g) < deg(f)$$

it follows that $a^j g(x) - a^i = 0$. Multiplying by a^{t-j} gives $a^{t+i-j} = 0$, which is a contradiction to our hypothesis that a has nilpotency t and $0 < t+i-j < t$. Let I be a nonzero ideal of $\frac{\mathbb{F}(p^k\mathbb{Z}, 1)[x]}{\langle f\rangle}$ and $h + \langle f\rangle$ a nonzero element of I. By assumption, f is a basic irreducible $m\Theta$ polynomial in $\mathbb{F}(p^k\mathbb{Z}, 1)[x]$, hence, $\bar{f}$ is irreducible in $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}[x]$. Therefore, $gcd(\bar{h}, \bar{f}) = 1$, or $\bar{f}$. If $gcd(\bar{h}, \bar{f}) = 1$, that is, $\bar{h}$, $\bar{f}$ are coprime in $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}[x]$, then h, f are coprime in $\mathbb{F}(p^k\mathbb{Z}, 1)[x]$. So there exist u, $v \in \mathbb{F}(p^k\mathbb{Z}, 1)[x]$ such that $uh + vf = 1$. That implies

$$(u + \langle f\rangle)(h + \langle f\rangle) = 1 + \langle f\rangle$$

whence $h + \langle f\rangle$ is invertible in $\frac{\mathbb{F}(p^k\mathbb{Z}, 1)[x]}{\langle f\rangle}$. Therefore,

$$I = \frac{\mathbb{F}(p^k\mathbb{Z}, 1)[x]}{\langle f\rangle} = \langle 1 + \langle f\rangle\rangle.$$

For the case $gcd(\bar{h}, \bar{f}) = \bar{f}$, for all $h + \langle f\rangle \in I$, which means $\bar{f}$ divides $\bar{h}$, hence, there exist w, $z \in \mathbb{F}(p^k\mathbb{Z}, 1)[x]$ such that $h = wf + az$. Whence

$$h + \langle f\rangle \in \langle a + \langle f\rangle\rangle, \quad for\ all\ h + \langle f\rangle \in I$$

implying $I \subseteq \langle a + \langle f\rangle\rangle$. Let k be the greatest integer $< t$ such that $I \subseteq \langle a^k + \langle f\rangle\rangle$. Then, as $I \nsubseteq \langle a^{k+1}\langle f\rangle\rangle$, there is a (nonzero) element $h' + \langle f\rangle \in I$ such that $h' + \langle f\rangle \notin \langle a^{k+1} + \langle f\rangle\rangle$. Since $h' + \langle f\rangle \in I \subseteq \langle a^k + \langle f\rangle\rangle$, there exist w', $z' \in \mathbb{F}(p^k\mathbb{Z}, 1)[x]$ such that $h' = w'f + a^k z'$. Now $gcd(\bar{z'}, \bar{f}) = 1$, or $\bar{f}$. Suppose $gcd(\bar{z'}, \bar{f}) = \bar{f}$, then $\bar{f}$ divides $\bar{z'}$ and so there exist w'', $z'' \in \mathbb{F}(p^k\mathbb{Z}, 1)[x]$ such that $z' = w''f + az''$. Hence,

$$\begin{aligned} h' &= w'f + a^k z' = w'f + a^k(w''f + az'') \\ &= (w' + a^k w'')f + a^{k+1} z''. \end{aligned}$$

It follows that $h' + \langle f\rangle \in \langle a^{k+1} + \langle f\rangle\rangle$, *a contradiction. Thus,* $gcd(\bar{z'},\,\bar{f}) = 1$. *The same argument as above yields that* $z' + \langle f\rangle$ *invertible in* $\frac{\mathbb{F}(p^k\mathbb{Z},\,1)[x]}{\langle f\rangle}$, *which means that there exists* $z_0 \in \mathbb{F}(p^k\mathbb{Z},\,1)[x]$ *such that*

$$(z' + \langle f\rangle)(z_0 + \langle f\rangle) = 1 + \langle f\rangle.$$

Therefore

$$\begin{aligned} a^k + \langle f\rangle &= (z_0 + \langle f\rangle)(a^k z' + \langle f\rangle) \\ &= (z_0 + \langle f\rangle)(h' + \langle f\rangle) \in I. \end{aligned}$$

Consequently, $I = \langle a^k + \langle f\rangle\rangle$.

Customarily, for a $m\Theta$ polynomial f of degree k, its reciprocal $m\Theta$ polynomial $x^k f(x^{-1})$ will be denoted by f^*. Thus, for example, if $f(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1} + a_kx^k$, then

$$\begin{aligned} f^*(x) &= x^k(a_0 + a_1x^{-1} + \cdots + a_{k-1}x^{-(k-1)} + a_kx^{-k}) \\ &= a_k + a_{k-1}x + \cdots + a_1x^{k-1} + a_0x^k. \end{aligned}$$

Moreover, if $f(x)$ is a factor of $x^r - 1$, we denote $\hat{f}(x) = \frac{x^r-1}{f(x)}$.

Theorem 0.7. *Assume* $\mathbb{F}(p^k\mathbb{Z},\,1)$ *is a finite chain* $m\Theta$ *pseudo field with maximal* $m\Theta$ *ideal* $\langle a\rangle$, *and that* t *is the nilpotency of* a. *Let* $x^r - 1 = f_1f_2\cdots f_l$ *be a representation of* $x^r - 1$ *as a product of basic irreducible pairwise-coprime polynomials in* $\mathbb{F}(p^k\mathbb{Z},\,1)[x]$. *Then any ideal in* $\frac{\mathbb{F}(p^k\mathbb{Z},\,1)[x]}{\langle f\rangle}$ *is a sum of* $m\Theta$ *ideals of the form* $\langle a^j\hat{f}_i + \langle x^r - 1\rangle\rangle$, *where* $0 \le j \le t$, $1 \le i \le r$.

Proof 0.12. *By the Chinese Reminder theorem, we have*

$$\frac{\mathbb{F}(p^k\mathbb{Z},\,1)[x]}{\langle x^r - 1\rangle} = \frac{\mathbb{F}(p^k\mathbb{Z},\,1)[x]}{\cap_{i=1}^{l}\langle f_i\rangle} \cong \bigoplus\sum_{i=1}^{l}\frac{\mathbb{F}(p^k\mathbb{Z},\,1)[x]}{\langle f_i\rangle}.$$

Thus, any $m\Theta$ *ideal* I *of* $\frac{\mathbb{F}(p^k\mathbb{Z},\,1)[x]}{\langle x^r-1\rangle}$ *is of the form* $\bigoplus\sum_{i=1}^{l} I_i$, *where* I_i *is an* $m\Theta$ *ideal of* $\frac{\mathbb{F}(p^k\mathbb{Z},\,1)[x]}{\langle f_i\rangle}$. *According to the previous lemma, for* $1 \le i \le r$, $I_i = 0$ *or* $I_i = \langle a_k + \langle f_i\rangle\rangle$, *for some* $k \in \{0, \cdots, t-1\}$. *Then* I_i *correspond to* $\langle a^k\hat{f}_i + \langle x^r - 1\rangle\rangle$ *in* $\frac{\mathbb{F}(p^k\mathbb{Z},\,1)[x]}{\langle x^r-1\rangle}$. *Consequently,* I *is a sum of ideals of the form* $\langle a^j\hat{f}_i + \langle x^r - 1\rangle\rangle$.

Corollary 0.2. *Let $\mathbb{F}(p^k\mathbb{Z},\,1)$ be a finite $m\Theta$ pseudo field with maximal $m\Theta$ ideal $\langle a\rangle$, and t be the nilpotency of a. The numbers of quasi-cyclic $m\Theta$ codes over $\mathbb{F}(p^k\mathbb{Z},\,1)$ of length r is $(t+1)^l$, where l is the number of factors in the unique factorization of x^r-1 into a product of monic basic irreducible pairwise coprime $m\Theta$ polynomials.*

From now on, in order to simplify notation, we will just write $l_0+l_1x+\cdots+l_{r-1}x^{r-1}$ for the corresponding coset $l_0+l_1x+\cdots+l_{r-1}x^{r-1}+\langle x^r-1\rangle$ in $\frac{\mathbb{F}(p^k\mathbb{Z},\,1)[x]}{\langle x^r-1\rangle}$

Theorem 0.8. *Let C be a quasi-cyclic $m\Theta$ codes of length r over a finite $m\Theta$ pseudo field with maximal $m\Theta$ ideal $\langle a\rangle$, and t be the nilpotency of a. Then there exists a unique family of pairwise coprime monic $m\Theta$ polynomials $F_0,\,F_1,\,\cdots,\,F_t$ in $\mathbb{F}(p^k\mathbb{Z},\,1)[x]$ such that $F_0F_1\cdots F_t=x^r-1$ and $C=\langle\widehat{F_1},\,a\widehat{F_2},\,\cdots,\,a^{t-1}\widehat{F_t}\rangle$. Moreover*

$$|C|=(|\overline{\mathbb{F}(p^k\mathbb{Z},\,1)}|)^{\sum_{i=0}^{t-1}(t-i)deg(F_{i+1})}.$$

Proof 0.13. *Let $x^r-1=f_1\cdots f_l$ be the unique factorization of x^r-1 into a product of monic basic irreducible pairwise coprime $m\Theta$ polynomials. C is a direct sum of ideals of the form $\langle a^j\widehat{f_i}\rangle$, where $0\leq j\leq t$, $1\leq i\leq l$. After reordering if necessary, we can assume that*

$$\begin{aligned}C \;=\; &\langle\hat{f}_{k_1+1}\rangle\oplus\cdots\oplus\langle\hat{f}_{k_1+k_2}\rangle\oplus\langle a\hat{f}_{k_1+k_2+1}\rangle\oplus\cdots a\hat{f}_{k_1+k_2+k_3}\rangle\oplus\\ &\cdots\oplus\langle a^{t-1}\hat{f}_{k_1+\cdots+k_t+1}\rangle\oplus\cdots\oplus\langle a^{t-1}\hat{f}_r\rangle\end{aligned}$$

where $k_1,\,\cdots,\,k_t\geq 0$ and $k_1+\cdots+k_t+1\leq r$. Let $k_0=0$, and k_{t+1} be a nonnegative integer such that $k_1+\cdots+k_t+1\leq r$. For $i=0,\,\cdots,\,t$, define

$$F_i=f_{k_0+\cdots+k_i+1}\cdots f_{k_0+\cdots+k_i+1}.$$

Then by our construction, it is clear that $F_0,\,\cdots,\,F_t$ are pairwise coprime, $F_0\cdots F_t=f_1\cdots f_r=x^r-1$, and

$$C=\langle\widehat{F_1}\rangle\oplus\langle a\widehat{F_2}\rangle\oplus\cdots\oplus\langle a^{t-1}\widehat{F_t}\rangle.$$

To prove the uniqueness, assume $G_0G_1\cdots G_t=x^r-1$ and $C=\langle\widehat{G_1},\,a\widehat{G_2},\,\cdots,\,a^{t-1}\widehat{G_t}\rangle$. Then

$$\frac{\mathbb{F}(p^k\mathbb{Z},\,1)[x]}{\langle x^r-1\rangle}=\langle\widehat{G_0}\rangle\oplus\langle\widehat{G_1}\rangle\oplus\cdots\oplus\langle\widehat{G_s}\rangle$$

thus, $C = \langle\widehat{G_1}\rangle \oplus \langle a\widehat{G_2}\rangle \oplus \cdots \oplus \langle a^{t-1}\widehat{G_s}\rangle$. *Now there exist nonnegative integers* $l_0 = 0, l_1, \cdots, l_{t+1}$ *with* $l_0+l_1+\cdots+l_{t+1} = l$, *and a permutation* $\{f'_1, \cdots, f'_r\}$ *of* $\{f_1, \cdots, f_r\}$ *such that, for* $i = 0, 1, \cdots, t$

$$G_i = f'_{l_0+\cdots+l_i+1} \cdots f'_{l_0+\cdots+l_i+1}.$$

Hence,

$$\begin{aligned} C &= \langle \hat{f'}_{l_1+1}\rangle \oplus \cdots \oplus \langle \hat{f'}_{l_1+l_2}\rangle \oplus \langle a\hat{f'}_{l_1+l_2+1}\rangle \oplus \cdots a\hat{f'}_{l_1+l_2+l_3}\rangle \oplus \\ &\cdots \oplus \langle a^{t-1}\hat{f'}_{l_1+\cdots+l_t+1}\rangle \oplus \cdots \oplus \langle a^{t-1}\hat{f'}_r\rangle \end{aligned}$$

Now for $i = 0, \cdots, t$, *it follows that* $l_i = k_i$, *and, furthermore,*$\{f'_{l_0+\cdots+l_{i+1}}, \cdots, f'_{l_0+\cdots+l_{t+1}}\}$ *is a permutation of* $\{f_{k_0+\cdots+k_{i+1}}, \cdots, f_{k_0+\cdots+k_{t+1}}\}$. *Therefore,* $G_i = F_i$, *for* $i = 0, \cdots, t$.

To calculate the order $|C|$, *note that*

$$C = \langle\widehat{F_1}\rangle \oplus \langle a\widehat{F_2}\rangle \oplus \cdots \oplus \langle a^{t-1}\widehat{F_t}\rangle$$

and for $i = 0, 1, \cdots, t-1$

$$\begin{aligned} |\langle a^i\widehat{F_{i+1}}\rangle| &= \left(\frac{|\mathbb{F}(p^k\mathbb{Z}, 1)|}{|\langle a^{t-i}\rangle|}\right)^{(n-deg\widehat{F_{i+1}})} = \left(\frac{|\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}|^t}{|\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}|^i}\right)^{degF_{t+1}} \\ &= (|\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}|)^{(t-i)degF_{t+1}}. \end{aligned}$$

Hence,

$$\begin{aligned} |C| &= |\langle\widehat{F_1}\rangle| \cdot |\langle a\widehat{F_2}\rangle| \cdot \cdots \cdot |\langle a^{t-1}\widehat{F_t}\rangle| \\ &= (|\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}|)^{tdegF_1} \cdot (|\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}|)^{(t-1)degF_2} \cdots (|\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}|)^{degF_t} \\ &= (|\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}|)^{\sum_{i=0}^{t-1}(t-i)deg(F_{i+1})}. \end{aligned}$$

Theorem 0.9. *Let* C *be a quasi-cyclic code of length* r *over a finite chain* $m\Theta$ *pseudo field* $\mathbb{F}(p^k\mathbb{Z}, 1)$, *which has maximal* $m\Theta$ *ideal* $\langle a\rangle$ *and* t *is the nilpotency of* a. *Then there exist polynomials* $g_0, g_1, \cdots, g_{t-1}$ *in* $\mathbb{F}(p^k\mathbb{Z}, 1)[x]$ *such that* $C = \langle g_0, ag_1, \cdots, a^{t-1}g_{t-1}\rangle$ *and* $g_{t-1}|g_{t-2}|\cdots|g_1|g_0|(x^r-1)$.

Proof 0.14. *According to previous theorem, there exists a family of pairwise coprime monic* $m\Theta$ *polynomials* $F_0, F_1, \cdots, F_t$ *in* $\mathbb{F}(p^k\mathbb{Z}, 1)[x]$ *such that* $F_0F_1\cdots F_t = x^r - 1$ *and* $C = \langle\widehat{F_1}, a\widehat{F_2}, \cdots, a^{t-1}\widehat{F_t}\rangle$. *Define*

$$g_i = \begin{cases} F_0F_1\cdots F_t, & \text{if } 0 \le i \le t-2 \\ F_0, & \text{if } i = t-1. \end{cases}$$

Then clearly $g_{t-1}|g_{t-2}|\cdots|g_1|g_0|(x^r-1)$. *Moreover, for* $0 \leq i \leq t-1$, *we have*

$$a^i\hat{F}_{i+1} = a^iF_0\cdots F_iF_{i+2}\cdots F_t = a^ig_iF_1\cdots F_i.$$

Therefore, $C \subseteq \langle g_0, ag_1, \cdots, a^{t-1}g_{t-1}\rangle$. *On the other hand,* $g_0 = F_0F_1\cdots F_t \in C$. *Since* F_1, F_2 *are coprime* $m\Theta$ *polynomials in* $\mathbb{F}(p^k\mathbb{Z}, 1)[x]$, *there exist polynomials* $u, v \in \mathbb{F}(p^k\mathbb{Z}, 1)[x]$ *such that* $uF_1 + vF_2 = 1$. *It follows that*

$$\begin{aligned} g_1 &= F_0F_3\cdots F_t = (uF_1 + vF_2)F_0F_3\cdots F_t \\ &= uF_0F_1F_3\cdots F_t + cF_0F_2F_3\cdots F_t = u\widehat{F_2} + vg_0 \end{aligned}$$

whence $ag_1 = au\widehat{F_2} + avg_0 \in C$. *Continuing this process, we obtain* $a^ig_i \in C$ *for* $0 \leq i \leq t-1$, *which implies*

$$\langle g_0, ag_1, \cdots, a^{t-1}g_{t-1}\rangle \subseteq C.$$

Consequently, $C = \langle g_0, ag_1, \cdots, a^{t-1}g_{t-1}\rangle$.

VIII. Conclusion

This note studies the Quasi-Cyclic codes over a finite chain $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, 1)$, which leads to the modal structure of the notion Quasi-Cyclic codes over a finite chain pseudo field [3]. It appears that the Structures of Quasi-Cyclic codes of length r over a finite chain $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, 1)$ are established when r is not divisible by the characteristic of the residue $m\Theta$ pseudo field $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}$. Some cases where r divisible by the characteristic of the residue $m\Theta$ field $\overline{\mathbb{F}(p^k\mathbb{Z}, 1)}$ are also considered.
At the end of this study, some interesting problems remain to be solved:

1. We would like to construct the $m\Theta$ structure of cyclic dual codes and negacyclic codes over finite chain $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, 1)$.
2. We would like to define a necessary and sufficient condition for the existence of self-dual cyclic $m\Theta$ codes over a $m\Theta$ pseudo field $\mathbb{F}(p^k\mathbb{Z}, 1)$.

References Références Referencias

1. J. Jensen, *The concatened structure of cyclic and abelian codes*, IEE Trans. Inform. Theory, vol.31, no 6, pp. 788 - 793, 1985.
2. V. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over* $\mathbb{Z}_4$, IEE Trans. Inform. Theory, vol.42, pp. 1594 - 1600, Sept. 1996.
3. Norton and A. Slgean-Mandache, *On the structure of linear cyclic codes over finite chain rings,* Appl. Algebra Eng. Commun. Comput., vol. 10, no. 6, pp. 489 - 506, 2000.

Ref
3. Norton and A. Slgean-Mandache, *On the structure of linear cyclic codes over finite chain rings*, Appl. Algebra Eng. Commun. Comput., vol. 10, no. 6, pp. 489 -506, 2000.

4. F.A. Eteme and J.A. Tsimi, A $m\Theta$ *approach of the algebraic theory of linear codes,* Journal of Discrete Mathematical Sciences and Cryptography, vol.14 (2011), N˙. 6, pp. 559-581
5. F.A. Eteme and J.A. Tsimi, *A modal* Θ*-valent approach of the notion of code,* Journal of Discrete Mathematical Sciences and Cryptography, vol. 14, October 2011, pp. 445-473.
6. C. Gneri, B. zkaya, and P. Solé, *Quasi-cyclic complementary dual codes,* Finite Fields Appl. 42, pp. 67 - 80, 2016.
7. F. Ayissi Eteme, *Logique et algèbre de structures mathematiques modales* Θ*-valentes chrysipiennes,* Hermann, Paris, 2009.
8. K. Lally. *Quasicyclic codes of index l over* $\mathbb{F}_q$ *viewed as* $\mathbb{F}_q[x]$ *- submodules of* $\frac{\mathbb{F}_{q^l}[x]}{\langle x^m-1\rangle}$, in Proc. Conference on Applied Algebra and Error-correcting Codes, 2003, pp. 244 - 253.
9. F. Ayissi Eteme, *chrm* Θ *introducing pure and applied mathematics*, Lambert academic publishing saarbrüken, Germany, 2015.
10. K. Lally and P. Fitzpatrick, *Algebraic structure of quasi-cyclic codes,* Discrete Appl. Math, vol. 111, no 1 - 2, pp. 157 - 175, 2001.
11. Gabriel Cedric Pemha Binyam, Laurence Um Emilie, Yves Jonathan Ndje. *The* $m\Theta$ *Quadratic Character in the* $m\Theta$ *Set* $\mathbb{Z}_{n\mathbb{Z}}$*. Mathematics and Computer Science*. Vol. 8, No. 1, 2023, pp. 11 - 18.
12. J.A. Tsimi and G. Pemha, *On the Generalized modal* Θ*-valent Reed-Muller codes,* Journal of Information and Optimization Sciences (JIOS), 2021.
13. S. Ling and P. Solé, *On the algebraic structure of quasi-cyclic codes I: finite fields,* IEE Trans. Inform. Theory, vol 47, no. 7, pp. 2751 - 2760, 2001.
14. F. Ayissi Eteme, *Anneau chrysippien* Θ*-valent,* CRAS, Paris 298, série 1, 1984, pp.1 - 4.
15. J.A. Tsimi and G. Pemha, *An algorithm of Decoding of* $m\Theta$ *Reed-Muller codes,* Journal of Discrete Mathematical Sciences and Cryptography (JDMSC), 2021.
16. F. Ayissi Eteme, *Logique et Algèbre de structure mathé matiques modales* Θ*-valentes chrysippiennes,* Edition Hermann, Paris, 2009.
17. J.A. Tsimi and G. Pemha, A $m\Theta$ *spectrum of Reed-Muller codes,* Journal of Discrete Mathematical Sciences and Cryptography (JDMSC), Vol. 25 no. 6 pp. 1791 - 1807, 2022.

Notes