


Algebraic Coding Theory and Related Algebraic Problems

Assoc.Prof.Dr.Chakkrid Klin-eam
Department of Mathematics, Faculty of Science,
Naresuan University, Phitsanulok,65000
Email : chakkridk@nu.ac.th

Conference on Recent Trends in Algebra and Related Topics
January 19-20, 2023

Algebraic coding theory studies the design of error-correcting codes for reliable transmission of information across noisy channels.

OUTLINE

1. **Basics of coding theory**
2. **Linear codes**
3. **Cyclic codes**
4. **Constacyclic codes**
5. **Research Topic in Algebraic Coding Theory**

Introduction

• Transmission of classical information in time and space is nowadays very easy (through noiseless channel).

It took centuries, and many ingenious developments and discoveries (writing, book printing, photography, movies, radio transmissions,TV, sounds recording) and the idea of the digitalization of all forms of information to discover fully this property of information.

Coding theory develops methods to protect information against a noise.

Cryptography develops methods how to protect information against an enemy (or an unauthorized user).

Basics of coding theory

Coding theory - theory of error correcting codes - is one of the most interesting and applied part of mathematics and informatics.

All real systems that work with digitally represented data, as CD players, TV, fax machines, internet, satelites, mobiles, require to use error correcting codes because all real channels are, to some extent, noisy.

- Coding theory problems are therefore among the very basic and most frequent problems of storage and transmission of information.

- Coding theory results allow to create reliable systems out of unreliable systems to store and/or to transmit information.

- Coding theory methods are often elegant applications of very basic concepts and methods of (abstract) algebra.

Channel

is the physical medium through which information is transmitted.

(Telephone lines and the atmosphere are examples of channels.)

NOISE

may be caused by sunpots, lighting, meteor showers, random radio disturbance, poor typing, poor hearing, ….

TRANSMISSION GOALS

1. Fast encoding of information.
2. Easy transmission of encoded messages.
3. Fast decoding of received messages.
4. Reliable correction of errors introduced in the channel.
5. Maximum transfer of information per unit time.

Basic Idea

METHOD OF FIGHTING ERRORS: REDUNDANCY!!!

0 is encoded as 00000 and 1 is encoded as 11111.

The details of techniques used to protect information against noise in practice are sometimes rather complicated, but basic principles are easily understood.

The key idea is that in order to protect a message against a noise, we should encode the message by adding some redundant information to the message.

In such a case, even if the message is corrupted by a noise, there will be enough redundancy in the encoded message to recover, or to decode the message completely.

EXAMPLE: Codings of a path avoiding an enemy territory

Story **Alice and Bob share an identical map (Fig.1) gridded as shown in Fig.1. Only Alice knows the route through which Bob can reach her avoiding the enemy territory. Alice wants to send Bob the following information about the safe route he should take.**

EXAMPLE: Codings of a path avoiding an enemy territory

NNWNNWWSSWWNNNNWWN

Three ways to encode the safe route from Bob to Alice are:

1. $C_1 = \{00, 01, 10, 11\}$

Any error in the code word

00000100000101111101010000000010100

would be a disaster.

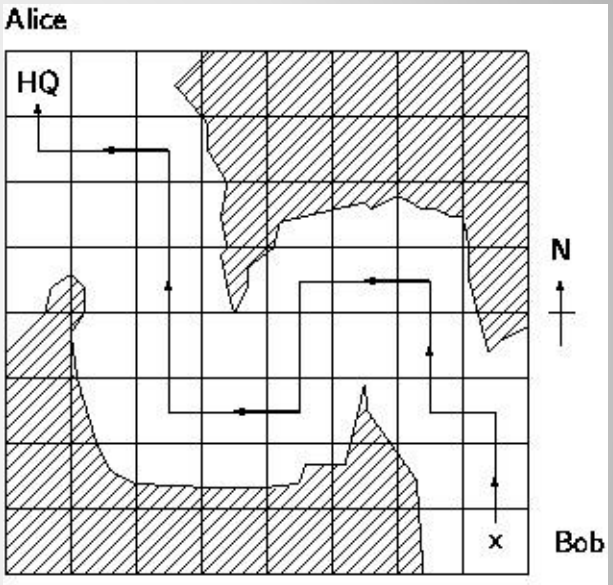


Fig. 1

EXAMPLE: Codings of a path avoiding an enemy territory

2. $C_2 = \{000, 011, 101, 110\}$

A single error in encoding each of symbols N, W, S, E could be detected.

3. $C_3 = \{00000, 01101, 10110, 11011\}$

A single error in decoding each of symbols N, W, S, E could be corrected.

Basic terminology

Block code - a code with all words of the same length.

Codewords - words of some code.

Basic assumptions about channels

1. Code length preservation Each output codeword of a channel has the same length as the input codeword.
2. Independence of errors The probability of any one symbol being affected in transmissions is the same.

Basic strategy for decoding

For decoding we use the so-called maximal likehood principle, or nearest neighbor decoding strategy, which says that the receiver should decode a word *w*' as that codeword *w* that is the closest one to *w*'.

Hamming distance

The intuitive concept of “closeness" of two words is well formalized through Hamming distance $d(x, y)$ of words x, y.

For two words x, y

$d(x, y)$ = the number of symbols x and y differ.

Example: $d(10101, 01100) = 3$, $d(\textit{fourth, eighth}) = 4$

Properties of Hamming distance

(1) $d(x, y) = 0$ iff $x = y$

(2) $d(x, y) = d(y, x)$

(3) $d(x, z) \leq d(x, y) + d(y, z)$ triangle inequality

An important parameter of codes C is their minimal distance.

$$d(C) = \min \{d(x, y) \mid x,y \in C, x \neq y\},$$

because it gives the smallest number of errors needed to change one codeword into anther.

Theorem Basic error correcting theorem

(1) A code C can detected up to t errors if $d(C) \geq t+ 1$.

(2) A code C can correct up to t errors if $d(C) \geq 2t + 1$.

Notation and Examples

Notation: An (n,M,d) - code C is a code such that

- n - is the length of codewords.
- M - is the number of codewords.
- d - is the minimum distance in C.

Example:

$C_1 = \{00, 01, 10, 11\}$ is a (2,4,1)-code.

$C_2 = \{000, 011, 101, 110\}$ is a (3,4,2)-code.

$C_3 = \{00000, 01101, 10110, 11011\}$ is a (5,4,3)-code.

Comment: A good (n,M,d) code has small n and large M and d.

The main coding theory problems

A good (n,M,d) -code has small n, large M and large d.

The main coding theory problem is to optimize one of the parameters n, M, d for given values of the other two.

Notation: $A_q(n,d)$ is the largest M such that there is an q -nary (n,M,d) -code.

Theorem (a) $A_q(n,1) = q^n$;

(b) $A_q(n,n) = q$.

Theorem Suppose d is odd. Then a binary (n,M,d) -code exists iff a binary $(n+1,M,d+1)$ -code exists.

A BIT OF HISTORY

The subject of error-correcting codes arose originally as a response to practical problems in the reliable communication of digitally encoded information.

The discipline was initiated in the paper

Claude Shannon: A mathematical theory of communication, Bell Syst.Tech. Journal V27, 1948, 379-423, 623-656

Shannon's paper started the scientific discipline **information theory** and **error-corecting codes** are its part.

Originally, information theory was a part of electrical engineering. Nowadays, it is an important part of mathematics and also of informatics.

Linear codes

Most of the important codes are special types of so-called linear codes.

Linear codes are of importance because they have

very concise description,

very nice properties,

very easy encoding

and

in principle quite easy decoding.

Linear codes

Linear codes are special sets of words of the length n over an alphabet $\{0,..,q-1\}$, where q is a power of prime.

Since now on sets of words F_q^n will be considered as vector spaces $V(n,q)$ of vectors of length n with elements from the set $\{0,..,q-1\}$ and arithmetical operations will be taken modulo q.

The set $\{0,..,q-1\}$ with operations + and $\bullet$ modulo q is called also the Galois field $GF(q)$.

Definition A subset $C \subseteq V(n,q)$ is a linear code if

(1) $u + v \in C$ for all $u, v \in C$

(2) $au \in C$ for all $u \in C$, $a \in GF(q)$

Example Codes C_1, C_2, C_3 are linear codes.

Lemma A subset $C \subseteq V(n,q)$ is a linear code if one of the following conditions is satisfied

(1) C is a subspace of $V(n,q)$

(2) sum of any two codewords from C is in C (for the case $q = 2$)

If C is a k -dimensional subspace of $V(n,q)$, then C is called [n,k] -code. It has q^k codewords.

Linear codes are also called "group codes".

Which of the following binary codes are linear?

C_1 = {00, 01, 10, 11}

C_2 = {000, 011, 101, 110}

C_3 = {00000, 01101, 10110, 11011}

C_5 = {101, 111, 011}

C_6 = {000, 001, 010, 011}

C_7 = {0000, 1001, 0110, 1110}

How to create a linear code

Notation If S is a set of vectors of a vector space, then let $\langle S \rangle$ be the set of all linear combinations of vectors from S.

Theorem For any subset S of a linear space, $\langle S \rangle$ is a linear space that consists of the following words:

- the zero word,
- all words in S,
- all sums of two or more words in S.

Example $S = \{0100, 0011, 1100\}$

$\langle S \rangle = \{0000, 0100, 0011, 1100, 0111, 1011, 1000, 1111\}$.

Basic properties of linear codes

Notation: $w(x)$ (weight of x) is the number of non-zero entries of x.

Lemma If $x, y \in V(n,q)$, then $d(x,y) = w(x - y)$.

Proof $x - y$ has non-zero entries in exactly those positions where x and y differ.

Theorem Let C be a linear code and let weight of C, notation $w(C)$, be the smallest of the weights of non-zero codewords of C. Then $d(C) = w(C)$.

Basic properties of linear codes

If C is a linear $[n,k]$ -code, then it has a basis consisting of k codewords.

Example

Code

$$C_4 = \{0000000, 1111111, 1000101, 1100010,$$
$$0110001, 1011000, 0101100, 0010110,$$
$$0001011, 0111010, 0011101, 1001110,$$
$$0100111, 1010011, 1101001, 1110100\}$$

has the basis

$$\{1111111, 1000101, 1100010, 0110001\}.$$

How many different bases has a linear code?

Advantages and disadvantages of linear codes

Advantages - big.

1. Minimal distance $d(C)$ is easy to compute if C is a linear code.
2. Linear codes have simple specifications.

- To specify a non-linear code usually all codewords have to be listed.
- To specify a linear $[n,k]$ -code it is enough to list k codewords.

Definition A $k \times n$ matrix whose rows form a basis of a linear $[n,k]$ -code (subspace) C is said to be the generator matrix of C.

Example The generator matrix of the code

$$C_4 \quad \text{is} \quad \begin{Bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{Bmatrix}$$

3. There are simple encoding/decoding procedures for linear codes.

Advantages and disadvantages of linear codes

Disadvantages of linear codes

are small:

1. Linear q -codes are not defined unless q is a prime power.
2. The restriction to linear codes might be a restriction to weaker codes than sometimes desired.

Encoding with a linear code

is a vector × matrix multiplication

Let C be a linear $[n,k]$ -code over $GF(q)$ with a generator matrix G.

Theorem C has q^k codewords.

Proof Theorem follows from the fact that each codeword of C can be expressed uniquely as a linear combination of the basis vectors.

Corollary The code C can be used to encode uniquely q^k messages.

Let us identify messages with elements $V(k,q)$.

Encoding of a message $u = (u_1, \ldots, u_k)$ with the code C:

$$u \cdot G = \sum_{i=1}^{k} u_i r_i \quad \text{where} \quad r_1, \ldots, r_k \quad \text{are rows of} \quad G.$$

Uniqueness of encodings

with linear codes

Theorem If G is a generator matrix of a binary linear code C of length n and dimension k, then

$$v = uG$$

ranges over all 2^k codewords of C as u ranges over all 2^k words of length k.

Therefore

$$C = \{ uG \mid u \in \{0,1\}^k \}$$

Moreover

$$u_1G = u_2G$$

if and only if

$$u_1 = u_2.$$

Decoding of linear codes

Decoding problem: If a codeword: $x = x_1 \ldots x_n$ is sent and the word $y = y_1 \ldots y_n$ is received, then $e = y - x = e_1 \ldots e_n$ is said to be the error vector. The decoder must decide from y which x was sent, or, equivalently, which error e occurred.

To describe main Decoding method some technicalities have to be introduced

Definition Suppose C is an $[n,q]$ -code over $GF(q)$ and $a \in V(n,q)$. Then the set

$$a + C = \{ a + x \mid x \in C \}$$

is called a coset of C in V(n,q).

Decoding of linear codes

Example Let C = {0000, 1011, 0101, 1110}

Cosets:

$0000 + C = C$,

$1000 + C = \{1000, 0011, 1101, 0110\}$,

$0100 + C = \{0100, 1111, 0001, 1010\}$,

$0010 + C = \{0010, 1001, 0111, 1100\}$.

Are there some other cosets in this case?

Theorem Suppose C is a linear $[n,k]$ -code over $GF(q)$. Then

(a) every vector of $V(n,k)$ is in some coset of C,

(b) every coset contains exactly q^k elements,

(c) two cosets are either disjoint or identical.

Dual codes

Inner product of two vectors (words)

$$u = u_1 \ldots u_n, \quad v = v_1 \ldots v_n$$

in $V(n,q)$ is an element of $GF(q)$ defined by

$$u \cdot v = u_1 v_1 + \ldots + u_n v_n.$$

Example In $V(4,2)$: $1001 \cdot 1001 = 0$

In $V(4,3)$: $2001 \cdot 1210 = 2$

If $u \cdot v = 0$ then words (vectors) u and v are called orthogonal.

Properties

If $u, v, w \in V(n,q)$, $\lambda, \mu \in GF(q)$, then

$$u \cdot v = v \cdot u, \quad (\lambda u + \mu v) \cdot w = \lambda (u \cdot w) + \mu (v \cdot w).$$

Given a linear $[n,k]$ -code C, then dual code of C, denoted by $C^{\perp}$, is defined by

$$C^{\perp} = \{v \in V(n,q) \mid v \cdot u = 0 \text{ if } u \in C\}.$$

Lemma Suppose C is an $[n,k]$ -code having a generator matrix G. Then for $v \in V(n,q)$

$$v \in C^{\perp} <=> vG^{T} = 0,$$

where G^{T} denotes the transpose of the matrix G.

Proof Easy.

Parity check matrices

Theorem Suppose C is a linear $[n,k]$ -code over $GF(q)$, then the dual code $C^{\perp}$ is a linear $[n,n-k]$ -code.

Definition A parity-check matrix H for an $[n,k]$ -code C is a generator matrix of $C^{\perp}$.

Theorem If H is parity-check matrix of C, then

$$C = \{x \in V(n,q) \mid xH^{T} = 0\},$$

and therefore any linear code is completely specified by a parity-check matrix.

Theorem If $G = [I_k \mid A]$ is the standard form generator matrix of an $[n,k]$ -code C, then a parity check matrix for C is $H = [-A^{T} \mid I_{n-k}]$.

Cyclic codes

Cyclic codes are of interest and importance because

- They posses rich algebraic structure that can be utilized in a variety of ways.
- They have extremely concise specifications.
- They can be efficiently implemented using simple *shift registers*.
- Many practically important codes are cyclic.

BASIC DEFINITION AND EXAMPLES

Definition A code C is cyclic if

(i) C is a linear code;

(ii) any cyclic shift of a codeword is also a codeword, i.e. whenever $a_0, \ldots a_{n-1} \in C$, then also $a_{n-1}\, a_0 \ldots a_{n-2} \in C$.

Example

(i) Code C = {000, 101, 011, 110} is cyclic.

(ii) The binary linear code {0000, 1000, 0100, 0010, 0001} is not a cyclic

EXAMPLE of a CYCLIC CODE

The code with the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

has codewords

c_1 = 1011100 c_2 = 0101110 c_3 =0010111

$c_1 + c_2$ = 1110010 $c_1 + c_3$ = 1001011 $c_2 + c_3$ = 0111001

$c_1 + c_2 + c_3$ = 1100101

and it is cyclic because the right shifts have the following impacts

$c_1 \rightarrow c_2$, $c_2 \rightarrow c_3$, $c_3 \rightarrow c_1 + c_3$

$c_1 + c_2 \rightarrow c_2 + c_3$, $c_1 + c_3 \rightarrow c_1 + c_2 + c_3$, $c_2 + c_3 \rightarrow c_1$

$c_1 + c_2 + c_3 \rightarrow c_1 + c_2$

POLYNOMIALS over GF(q)

A codeword of a cyclic code is usually denoted

$$a_0\, a_1 \ldots a_{n-1}$$

and to each such a codeword the polynomial

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}$$

is associated.

$F_q[x]$ denotes the set of all polynomials over $GF(q)$.
deg (f(x)) = the largest m such that x^m has a non-zero coefficient in $f(x)$.

Multiplication of polynomials If f(x), g(x) $\in F_q[x]$, then

$$deg\ (f(x)\ g(x)) = deg\ (f(x)) + deg\ (g(x)).$$

POLYNOMIALS over GF(q)

Division of polynomials For every pair of polynomials a(x), b(x) $\neq$ 0 in $F_q[x]$ there exists a unique pair of polynomials q(x), r(x) in $F_q[x]$ such that

$$a(x) = q(x)b(x) + r(x), \deg(r(x)) < deg\ (b(x)).$$

Definition Let f(x) be a fixed polynomial in $F_q[x]$. Two polynomials g(x), h(x) are said to be congruent modulo f(x), notation

$$g(x) \equiv h(x) \pmod{f(x)},$$

if g(x) - h(x) is divisible by f(x).

RING of POLYNOMIALS

The set of polynomials in $F_q[x]$ of degree less than *deg* (f(x)), with addition and multiplication modulo f(x) forms a **ring denoted** $\mathbf{F_q[x]/f(x)}$.

Example Calculate $(x + 1)^2$ in $F_2[x] / (x^2 + x + 1)$. It holds

$$(x + 1)^2 = x^2 + 2x + 1 \equiv x^2 + 1 \equiv x \pmod{x^2 + x + 1}.$$

How many elements has $F_q[x] / f(x)$?

Result $| F_q[x] / f(x) | = q^{\deg (f(x))}$.

Example Addition and multiplication in $F_2[x] / (x^2 + x + 1)$

+	0	1	x	1 + x
0	0	1	x	1 + x
1	1	0	1 + x	x
x	x	1 + x	0	1
1 + x	1 + x	x	1	0

•	0	1	x	1 + x
0	0	0	0	0
1	0	1	X	1 + x
x	0	x	1 + x	1
1 + x	0	1 + x	1	x

RING of POLYNOMIALS

Definition A polynomial f(x) in $F_q[x]$ is said to be reducible if f(x) = a(x)b(x), where a(x), b(x) $\in F_q[x]$ and

$$deg\ (a(x)) < deg\ (f(x)), \qquad deg\ (b(x)) < deg\ (f(x)).$$

If f(x) is not reducible, it is irreducible in $F_q[x]$.

Theorem The ring $F_q[x]$ / f(x) is a field if f(x) is irreducible in $F_q[x]$.

$R_n = F_q[x] / (x^n - 1)$

Computation modulo $x^n - 1$

Since $x^n \equiv 1 \pmod{x^n - 1}$ we can compute $f(x) \bmod x^n - 1$ as follow:
In $f(x)$ replace x^n by 1, x^{n+1} by x, x^{n+2} by x^2, x^{n+3} by x^3, …

Identification of words with polynomials

$$a_0 a_1 \ldots a_{n-1} \leftrightarrow a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}$$

Multiplication by x in R_n corresponds to a single cyclic shift

$$x (a_0 + a_1 x + \ldots a_{n-1} x^{n-1}) = a_{n-1} + a_0 x + a_1 x^2 + \ldots + a_{n-2} x^{n-1}$$

Algebraic characterization of cyclic codes

Theorem A code C is cyclic if C satisfies two conditions

(i) $a(x), b(x) \in C \Rightarrow a(x) + b(x) \in C$

(ii) $a(x) \in C, r(x) \in R_n \Rightarrow r(x)a(x) \in C$

Proof

(1) Let C be a cyclic code. C is linear $\Rightarrow$ (i) holds.

(ii) Let $a(x) \in C$, $r(x) = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1}$

$$r(x)a(x) = r_0 a(x) + r_1 x a(x) + \ldots + r_{n-1} x^{n-1} a(x)$$

is in C by (i) because summands are cyclic shifts of $a(x)$.

(2) Let (i) and (ii) hold

- Taking $r(x)$ to be a scalar the conditions imply linearity of C.
- Taking $r(x) = x$ the conditions imply cyclicity of C.

CONSTRUCTION of CYCLIC CODES

Notation If $f(x) \in R_n$, then

$$\langle f(x) \rangle = \{r(x)f(x) \mid r(x) \in R_n\}$$

(multiplication is modulo $x^n - 1$).

Theorem For any $f(x) \in R_n$, the set $\langle f(x) \rangle$ is a cyclic code (generated by f).

Proof We check conditions (i) and (ii) of the previous theorem.

(i) If $a(x)f(x) \in \langle f(x) \rangle$ and $b(x)f(x) \in \langle f(x) \rangle$, then

$$a(x)f(x) + b(x)f(x) = (a(x) + b(x))\, f(x) \in \langle f(x) \rangle$$

(ii) If $a(x)f(x) \in \langle f(x) \rangle$, $r(x) \in R_n$, then

$$r(x)\,(a(x)f(x)) = (r(x)a(x))\, f(x) \in \langle f(x) \rangle .$$

CONSTRUCTION of CYCLIC CODES

Example $C = \langle 1 + x^2 \rangle$, $n = 3$, $q = 2$.

We have to compute $r(x)(1 + x^2)$ for all $r(x) \in R_3$.

$$R_3 = \{0, 1, x, 1 + x, x^2, 1 + x^2, x + x^2, 1 + x + x^2\}.$$

Result

$$C = \{0, 1 + x, 1 + x^2, x + x^2\}$$

$$C = \{000, 011, 101, 110\}$$

Characterization theorem for cyclic codes

We show that all cyclic codes C have the form $C = \langle f(x) \rangle$ for some $f(x) \in R_n$.

Theorem Let C be a non-zero cyclic code in R_n. Then

- there exists unique monic polynomial $g(x)$ of the smallest degree such that
- $C = \langle g(x) \rangle$
- $g(x)$ is a factor of $x^n - 1$.

Characterization theorem for cyclic codes

Proof

(i) Suppose g(x) and h(x) are two monic polynomials in C of the smallest degree. Then the polynomial g(x) - h(x) $\in C$ and it has a smaller degree and a multiplication by a scalar makes out of it a monic polynomial. If g(x) $\neq$ h(x) we get a contradiction.

(ii) Suppose a(x) $\in C$. Then a(x) = q(x)g(x) + r(x) (*deg* r(x) < *deg* g(x))
and r(x) = a(x) - q(x)g(x) $\in C$. By minimality r(x) = 0
and therefore a(x) $\in \langle$ g(x)$\rangle$.

(iii) Clearly,

$$x^n - 1 = q(x)g(x) + r(x) \quad \text{with} \quad deg\ r(x) < deg\ g(x)$$

and therefore r(x) $\equiv$ -q(x)g(x) (mod x^n -1) and

r(x) $\in C \Rightarrow$ r(x) = 0 $\Rightarrow$ g(x) is a factor of x^n -1.

GENERATOR POLYNOMIALS

Definition If for a cyclic code C it holds

$$C = \langle g(x) \rangle ,$$

then g is called the **generator polynomial** for the code C.

HOW TO DESIGN CYCLIC CODES?

The last claim of the previous theorem gives a recipe to get all cyclic codes of given length n.

Indeed, all we need to do is to find all factors of

$$x^n - 1.$$

Problem: Find all binary cyclic codes of length 3.

Solution: Since

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

both factors are irreducible in $GF(2)$

we have the following generator polynomials and codes.

Generator polynomials	Code in R_3	Code in $V(3,2)$
1	R_3	$V(3,2)$
$x + 1$	$\{0, 1 + x, x + x^2, 1 + x^2\}$	{000, 110, 011, 101}
$x^2 + x + 1$	$\{0, 1 + x + x^2\}$	{000, 111}
$x^3 - 1\ (= 0)$	$\{0\}$	{000}

Design of generator matrices for cyclic codes

Theorem Suppose *C* is a cyclic code of codewords of length *n* with the generator polynomial

$$g(x) = g_0 + g_1 x + \ldots + g_r x^r.$$

Then *dim* (*C*) = n - r and a generator matrix G_1 for *C* is

$$G_1 = \begin{pmatrix} g_0 & g_1 & g_2 & \ldots & g_r & 0 & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & g_2 & \ldots & g_r & 0 & 0 & \ldots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \ldots & g_r & 0 & \ldots & 0 \\ .. & .. & & & & & & & & .. \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & g_0 & \ldots & g_r \end{pmatrix}$$

Example

The task is to determine all ternary codes of length 4 and generators for them.

Factorization of $x^4 - 1$ over $GF(3)$ has the form

$$x^4 - 1 = (x - 1)(x^3 + x^2 + x + 1) = (x - 1)(x + 1)(x^2 + 1)$$

Therefore there are $2^3 = 8$ divisors of $x^4 - 1$ and each generates a cyclic code.

Generator polynomial	Generator matrix
1	I_4
$x - 1$	$\begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}$
$x + 1$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
$x^2 + 1$	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
$(x - 1)(x + 1) = x^2 - 1$	$\begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$
$(x - 1)(x^2 + 1) = x^3 - x^2 + x - 1$	[-1 1 -1 1]
$(x + 1)(x^2 + 1)$	[1 1 1 1]
$x^4 - 1 = 0$	[0 0 0 0]

Check polynomials and parity check matrices for cyclic codes

Let C be a cyclic $[n,k]$-code with the generator polynomial $g(x)$ (of degree $n - k$). By the last theorem $g(x)$ is a factor of $x^n - 1$. Hence

$$x^n - 1 = g(x)h(x)$$

for some $h(x)$ of degree k (where $h(x)$ is called the check polynomial of C).

Theorem Let C be a cyclic code in R_n with a generator polynomial $g(x)$ and a check polynomial $h(x)$. Then an $c(x) \in R_n$ is a codeword of C if $c(x)h(x) \equiv 0$ - this and next congruences are modulo $x^n - 1$.

POLYNOMIAL REPRESENTATION of DUAL CODES

Since *dim* (⟨ h(x)⟩) = *n* - *k* = *dim* ($C^{\perp}$) we might easily be fooled to think that the check polynomial h(*x*) of the code *C* generates the dual code $C^{\perp}$.

Reality is “slightly different":

Theorem Suppose *C* is a cyclic [*n*,*k*]-code with the check polynomial

$$h(x) = h_0 + h_1 x + \ldots + h_k x^k,$$

then

(i) a parity-check matrix for *C* is

$$H = \begin{pmatrix} h_k & h_{k-1} & \ldots & h_0 & 0 & \ldots & 0 \\ 0 & h_k & \ldots & h_1 & h_0 & \ldots & 0 \\ .. & .. & & & & & \\ 0 & 0 & \ldots & 0 & h_k & \ldots & h_0 \end{pmatrix}$$

(ii) $C^{\perp}$ is the cyclic code generated by the polynomial $\overline{h}(x) = h_k + h_{k-1}x + \ldots + h_0 x^k$

i.e. the reciprocal polynomial of h(*x*).

Constacyclic Codes

Definition Let R be a finite commutative ring with identity. A code C of length n over R is linear if it is R-submodule of R^n.

Example A code $C = \{0000, 1111, 2222, 3333, 0202, 1313, 2020, 3131, 0022, 1133, 2200, 3311, 0220, 1331, 2002, 3113\}$ is a linear code of length 4 over $\mathbb{Z}_4$.

Note If $R = \mathbb{F}_{p^m}$, a linear code over R is a subspace of R^n

Definition Let λ be a unit of a finite ring R. A code C of length n over R is λ-constacyclic if $(\lambda c_{n-1}, c_0, \dots, c_{n-2}) \in C$, for any $(c_0, c_1, \dots, c_{n-1}) \in C$.

Constacyclic Codes

- If $\lambda = 1$, it is said to be cyclic.
- If $\lambda = -1$, it is said to be negacyclic.

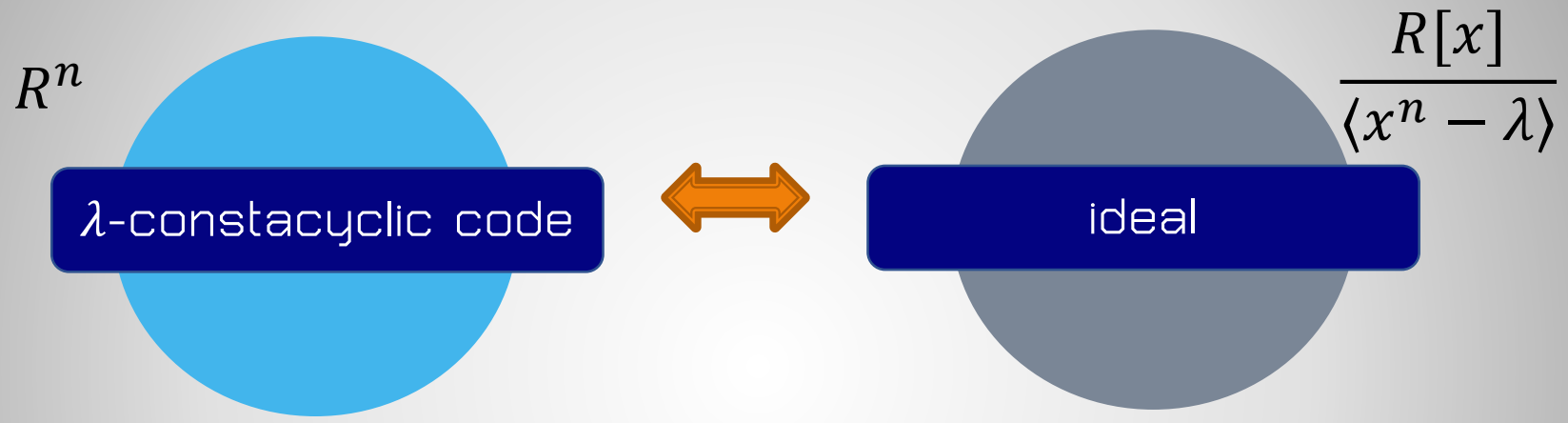
The map $\pi: R^n \to \frac{R[x]}{\langle x^n - \lambda \rangle}$ defined by

$$\pi(c_0, c_1, \dots, c_{n-1}) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}, \forall (c_0, c_1, \dots, c_{n-1}) \in R^n.$$

Proposition A linear code C of length n over R is λ-constacyclic if and only if $\pi(C)$ is an ideal of $\frac{R[x]}{\langle x^n - \lambda \rangle}$.

Thus, we usually view $(c_0, c_1, \dots, c_{n-1})$ as $c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ and a linear λ-constacyclic code as an ideal of $\frac{R[x]}{\langle x^n - \lambda \rangle}$.

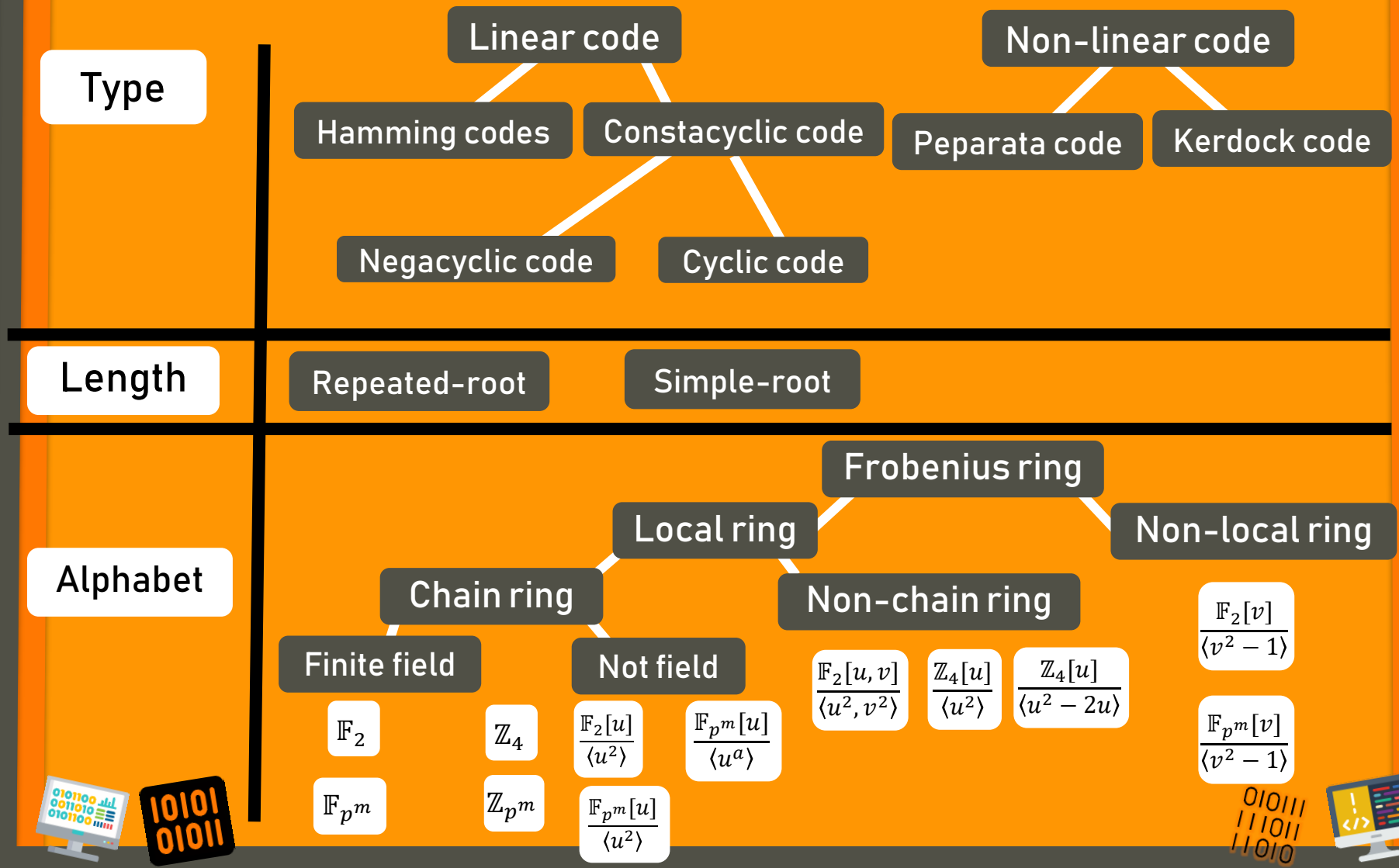
Constacyclic Codes



A dual code $C^{\perp}$ is a set of n-tuple over R that codewords in $C^{\perp}$ are orthogonal to all codeword in C.

Proposition The dual of a λ–constacyclic code of length n over R is a λ^{-1}-constacyclic code.

Research Topic in Algebraic Coding Theory



Introduction and preliminaries

During the first 40 years, the alphabet was usually a finite field. However, there were a few papers written where the alphabet was a ring.

The finite rings

$\mathbb{Z}_4$ $\quad \frac{\mathbb{F}_2[u]}{\langle u^2 \rangle}(\mathbb{F}_2 + u\mathbb{F}_2)$ $\quad \mathbb{F}_4$ $\quad \frac{\mathbb{F}_2[v]}{\langle v^2+v \rangle}(\mathbb{F}_2 + v\mathbb{F}_2)$

The central result of this work was that certain non-linear codes over $\mathbb{Z}_2$ could be viewed as linear codes over $\mathbb{Z}_4$ via a Gray map in [3,4].

Introduction and preliminaries

The length of codes

Repeated-root codes

The length of codes is not relatively prime with characteristic of a finite ring. In addition, some repeated-root codes have a good parameter for coding theory.

Simple-root codes

The length of codes is relatively prime with characteristic.

To study ideals of $\frac{R[x]}{\langle x^n-\lambda \rangle}$, the factorization of $x^n - \lambda$ depends on n and unit λ. Thus, the repeated-root codes are easy to determine, i.e., $x^{np^s} + 1 = (x^n + 1)^{p^s}$ over $\mathbb{F}_{p^m}$.

The scope of this research

Type

Negacyclic codes

- Gray image of negacyclic codes over $\mathbb{Z}_4$ is a binary cyclic code .
- There exist quantum codes constructed from negacyclic codes

Length

Repeated-root $3p^s$ and $8p^s$

Alphabet

Finite commutative chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

- It has the unique maximal ideal $\langle u \rangle$.
- $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} := \frac{\mathbb{F}_{p^m}[u]}{\langle u^2 \rangle} = \{a + ub : a, b \in \mathbb{F}_{p^m}\}$
- $a + ub$ is invertible if and only if a is a unit.

Literature Review

Outline of repeated-root constacyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

- 2009 — Constacyclic codes of length 2^s over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ [10]
- 2010 — Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ [11]
- 2015 — Negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ [12]
- 2016 — Constacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ [13]

Length $3p^s$??

- 2017 — Constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}, p^m \equiv 1 \ (mod\ 4)$ [14]
- 2018 2019 — Constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}, \ p^m \equiv 3 \ (mod\ 4)$ [15,16]

Length $8p^s$??

Main results (Negacyclic codes of length $3p^s$)

Let $p \neq 3$ be a prime. Each negacyclic code is viewed as an ideal of $\frac{\left(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}\right)[x]}{\langle x^{3p^s}+1\rangle}$.

$\boldsymbol{p^m \equiv 1 \ (mod\ 3)}$

$$\delta_i = -\xi^{\frac{i(p^m-1)p^s}{3}}$$

$$\boldsymbol{x^{3p^s}+1 = (x^{p^s}+1)(x^{p^s}-\delta_1)(x^{p^s}-\delta_2)}$$

$\boldsymbol{p^m \equiv 2 \ (mod\ 3)}$

$$\boldsymbol{x^{3p^s}+1 = \left(x^{p^s}+1\right)\left(x^2-x+1\right)^{p^s}}$$

Discrete Mathematics, Algorithms and Applications
Vol. 12, No. 5 (2020) 2050063 (35 pages)

DOI: 10.1142/S1793830920500639

World Scientific
www.worldscientific.com

Explicit constructions of cyclic and negacyclic codes of length $3p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

Jirayu Phuto*,‡ and Chakkrid Klin-Eam*,†,§

*Department of Mathematics, Faculty of Science
Naresuan University, Phitsanulok 65000, Thailand

†Research Center for Academic Excellence in Mathematics
Naresuan University, Phitsanulok 65000, Thailand
‡jirayup60@email.nu.ac.th
§chakkridk@nu.ac.th

Received 1 November 2019
Accepted 19 April 2020
Published 4 June 2020

Let p be a prime such that $p \neq 3$. The algebraic structures of all cyclic and negacyclic codes of length $3p^s$ over the finite commutative chain ring $R := \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}(u^2 = 0)$ are obtained that the conditions depend on the factorization of polynomial $x^2 + x + 1$ over R. Therefore, we classify the structures of cyclic and negacyclic codes of length $3p^s$ over R into 2 cases, i.e., $p^m \equiv 1 \pmod 3$ and $p^m \equiv 2 \pmod 3$. From that we obtain the number of all cyclic and negacyclic codes of length $3p^s$ over R. After that, we give some situations for such cyclic and negacyclic codes are self-dual codes.

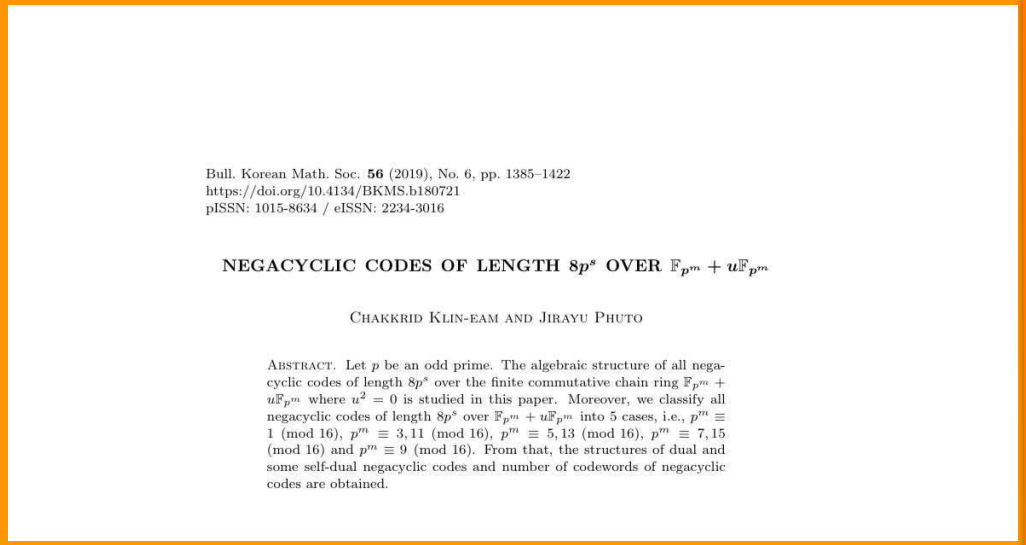
Keywords: Cyclic codes; chain rings; dual codes; negacyclic codes; repeated-root codes.

Mathematics Subject Classification 2020: 94B05, 13A99

Main results (Negacyclic codes of length $8p^s$)

Let p be an odd prime. Each negacyclic code is viewed as an ideal of $\frac{\left(\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}\right)[x]}{\langle x^{8p^s}+1\rangle}$. In this subsection, we divide it into 5 cases, i.e.,

1. $p^m \equiv 1\ (mod\ 16)$,
2. $p^m \equiv 3{,}11\ (mod\ 16)$,
3. $p^m \equiv 5{,}13\ (mod\ 16)$,
4. $p^m \equiv 7{,}15\ (mod\ 16)$,
5. $p^m \equiv 9\ (mod\ 16)$.



Bull. Korean Math. Soc. **56** (2019), No. 6, pp. 1385–1422
https://doi.org/10.4134/BKMS.b180721
pISSN: 1015-8634 / eISSN: 2234-3016

NEGACYCLIC CODES OF LENGTH $8p^s$ OVER $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

CHAKKRID KLIN-EAM AND JIRAYU PHUTO

ABSTRACT. Let p be an odd prime. The algebraic structure of all negacyclic codes of length $8p^s$ over the finite commutative chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ where $u^2 = 0$ is studied in this paper. Moreover, we classify all negacyclic codes of length $8p^s$ over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ into 5 cases, i.e., $p^m \equiv 1 \pmod{16}$, $p^m \equiv 3, 11 \pmod{16}$, $p^m \equiv 5, 13 \pmod{16}$, $p^m \equiv 7, 15 \pmod{16}$ and $p^m \equiv 9 \pmod{16}$. From that, the structures of dual and some self-dual negacyclic codes and number of codewords of negacyclic codes are obtained.

Discrete Mathematics 345 (2022) 112856

Contents lists available at ScienceDirect

Discrete Mathematics

www.elsevier.com/locate/disc

Duality of constacyclic codes of prime power length over the finite non-commutative chain ring $\frac{\mathbb{F}_{p^m}[u,\theta]}{\langle u^2\rangle}$

Jirayu Phuto, Chakkrid Klin-eam *

Department of Mathematics, Faculty of Science, Naresuan University, Phitsanulok 65000, Thailand

ARTICLE INFO

Article history:
Received 15 June 2021
Received in revised form 7 December 2021
Accepted 11 February 2022
Available online xxxx

Keywords:
Left constacyclic codes
Linear complementary dual codes
Non-commutative rings
Repeated-root codes
Self-dual codes

ABSTRACT

Let $R = \frac{\mathbb{F}_{p^m}[u,\theta]}{\langle u^2\rangle}$ where θ is an automorphism of $\mathbb{F}_{p^m}$ but it is not the identity. The list of (left and right) α-constacyclic codes of length p^s over R is provided where $\theta(\alpha) = \alpha$. The self-dual α-constacyclic codes are given. In addition, we derive the condition of LCD codes for those codes. For the remaining result, the condition of self-orthogonal left α-constacyclic codes is also obtained.

COMMUNICATIONS IN ALGEBRA®
https://doi.org/10.1080/00927872.2022.2072854

Taylor & Francis
Taylor & Francis Group

Check for updates

Explicit factorization of $x^{l_1^{m_1} l_2^{m_2} l_3^{m_3}} - a$ and a-constacyclic codes over a finite field

Supakarn Rakphon[a], Wutichai Chongchitmate[a], Jirayu Phuto[b], and Chakkrid Klin-eam[b]

[a]Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, Thailand; [b]Department of Mathematics, Faculty of Science, Naresuan University, Phitsanulok, Thailand

ABSTRACT

Let $\mathbb{F}_q$ be a finite field of order q, t be a prime and m_1, m_2, m_3 be positive integers. In this article, we find all irreducible divisors of $x^{l_1^{m_1} l_2^{m_2} l_3^{m_3}} - a$ over $\mathbb{F}_q$ where $a \in \mathbb{F}_q^*$ and $q^t - 1 = l_1^{v_1} l_2^{v_2} l_3^{v_3} c$ such that l_1, l_2, l_3 are distinct odd primes and c is a positive integer with $\gcd(l_1 l_2 l_3, c) = 1$ and $\gcd(l_1 l_2 l_3, q(q-1)) = 1$. Moreover, we construct an a-constacyclic code by using these irreducible divisors.

ARTICLE HISTORY
Received 20 September 2021
Revised 26 December 2021
Communicated by Ángel del Río Mateos

KEYWORDS
Constacyclic codes; cyclotomic coset; generator polynomials; irreducible factor polynomials

2020 MATHEMATICS SUBJECT CLASSIFICATION
94B05; 94B15

THANK YOU!