Comparison of BCH-Codes over Galois Ring, Quasi-Galois Ring and their Residue Field.

By

MUHAMMAD SHOAIB ABID

Department of Mathematics

Quaid-i-Azam University Islamabad, Pakistan

Session: 2021-2023

Comparison of BCH-Codes over Galois Ring, Quasi-Galois Ring and their Residue Field.

By

Muhammad Shoaib Abid

Supervised By

Prof. Dr. Tariq Shah

Department of Mathematics

Quaid-i-Azam University Islamabad, Pakistan

Session: 2021-2023

Comparison of BCH-Codes over Galois Ring, Quasi-Galois Ring and their Residue Field.

By

Muhammad Shoaib Abid

Master of Philosophy
in
Mathematics

Supervised By

Prof. Dr. Tariq Shah

Department of Mathematics

Quaid-i-Azam University Islamabad, Pakistan

Session: 2021-2023

Comparison of BCH-Codes over Galois Ring, Quasi-Galois Ring and their Residue Field.

By

MUHAMMAD SHOAIB ABID

Certificate

A Dissertation Submitted in the Partial Fulfillment of the Requirements for the Degree of

Master of Philosophy in Mathematics

We Accept this Dissertation as Conforming to the Required Standard

Prof. Dr. Tariq Shah
(Supervisor)

Prof. Dr. Matloob Anwar
School of Natural Sciences
National University of Science and Technology, Islamabad
(External Examiner)

Prof. Dr. Tariq Shah
(Chairman)

Department of Mathematics

Quaid-i-Azam University Islamabad, Pakistan

Session: 2021-2023

Acknowledgment

All praises to Allah almighty, the most beneficent and most merciful. I am highly grateful to Allah Almighty who blessed me with more than what I deserve and enable me to compile this work today. He blessed me with the ***Holy Prophet Hazrat Muhammad (SAW)*** who always remained a source of inspiration for me.

Prof. Dr. Tariq Shah

It is a matter of great honor for me to express gratitude to my supervisor ***Prof. Dr. Tariq Shah***, Chairman, Department of Mathematics, Quaid-i-Azam University Islamabad, whose expertise was invaluable in formulating my research directions. I am grateful to him for his intellectual mentoring, consistent support, insightful recommendation and never ending inspiration throughout my research. With critical criticism and extensive conversation, he provided the backbone of this research work. His sympathetic attitude and encouragement broadened my knowledge and also increase my capabilities of hard work.

These acknowledgements will remain incomplete without mentioning my family. My special gratitude is for my father ***Abid Hussain*** and my mother, their love has been with me throughout my educational career. I must thankful to my brothers ***M. Waseem Abid(Late)*** and ***M. Naeem Abid*** and my sister for their moral support.

I especially thankful to my friends ***Malik Muhammad Suleman*** and ***Muhammad Dawood Hameed*** for their joyful and cheerful company making the time in MPhil memorable, these guys made me believe that I had so much strength and courage to persevere even when I felt lost.

At last but not least, my heartiest thanks to ***Dr. Muhammad Sajjad*** and ***Dr. Umair Safdar*** for great cooperation throughout the degree, and thanks to all my fellows, seniors, juniors and all those who directly or indirectly assisted me during my research work.

May Almighty Allah shower his choicest blessing and prosperity on all of us.

Muhammad Shoaib Abid

April 2023.

Preface:

The goal of coding theory is to successfully transmit data over a noisy channel and to fix errors in corrupted communications. For many applications in computer science and engineering, it is crucial. The main notion is that the sender should use redundant information to create an error-correcting code and encrypt the message. Development of data transferring codes were started with the first article (Interlando, 1995) of Claude Shannon in 1948. In 1950, for this purpose Hamming (Hamming, 1950) and Golay (Golay, 1949) introduced cyclic block code known as binary hamming and Golay codes respectively. These classes of codes have the capability to detect up to two errors and correct one error. In 1953, Muller (Muller, 1953) introduced a multiple error correcting codes techniques and Reed (Reed, 1953) developed technique of such type of codes. In 1957, (Prange, 1959) initiated an idea of cyclic codes in two symbols. In addition, (Prange, 1959) used the coset equivalence for decoding the Group codes in 1959. The cyclic codes initially developed over binary field $\mathbb{Z}_2$ and into its Galois field extension $GF\left(2^m\right)$. Though it was further extended over the prime filed $\mathbb{Z}_p$ and its Galois field extension $GF\left(p^m\right)$.

The remarkable development in coding theory began when in 1960, Hoequenghem, Bose and Chaudhuri explained the large class of codes which correct multiple errors known as BCH-Code. In 1960, Peterson gave error correction procedure for BCH-Code over finite field. Forney gave the decoding technique of BCH-Code by using Barlekamp Massey algorithm in 1965. In 1972, (Blake I. , 1972) proposed the concept of linear codes over $\mathbb{Z}_n$, the ring of integers modulo *n* where *n* is the product of primes. However, he did not explain the codes over the local ring $\mathbb{Z}_{p^m}$, $m>1$. In 1975, (Blake I. F.) went on to talk about linear codes across the ring $\mathbb{Z}_n$ when $n=p^m$, where *p* is a prime and *m* is a positive integer. (Spiegel, 1977) and (E. Spiegel, 1978) demonstrated in 1977 and 1978 that codes over $\mathbb{Z}_{p^m}$ can be defined in terms of codes over $\mathbb{Z}_p$. As a result, we can establish codes over $\mathbb{Z}_n$, for every positive integers *n*. (Shankar, 1979) created BCH-Code over $\mathbb{Z}_{p^m}$ in 1979 and she also devised BCH-Code for arbitrary integers. She created BCH-Code over the GR using the maximal cyclic Subgroup of the Group of units of GR and related these to BCH-Code over the Galois filed using the reduction map. In 1999, (de Andrade, 1999) built BCH-Code over finite unitary commutative rings. The cyclic Subgroup of the Group of units of a GR was specified in both (De Andrade, 1999) and (Shankar, 1979) building procedures. In 2012, (Shah t. a., 2012) devised a decoding approach that enhances code rate. In addition, (Shah T. M., 2013) explained how to decode a lengthy binary BCH-Codes using cyclic code in 2013. In 2017, (Shah T. N., 2017) devised an approach for constructing the maximal cyclic Subgroup of any arbitrary Group of units of GRs.

There are four chapters in this thesis. In chapter 1, some key concepts of abstract algebra and error correcting codes are introduced, which are crucial for understanding Subsequent chapters.

In Chapter 2, we will discuss a brief comparison between Galois and Q-GRs, we also discuss their properties and structures by an example.

We will design BCH-Code over GR, Q-GR and their Residue field and compare these codes in each of these three cases in chapter 3.

Chapter 4 consist of method of designing Substitution Box over Sylow p-Subgroup of Group of units of GR by using a new concept of affine map.

Contents

Chapter # 1

Introduction to Algebraic Coding Theory

The theory of algebraic coding focuses on the creation of error-correcting codes for consistent data transmission via noisy channels (a channel prone to transmission errors is called a noisy channel). It allows for the practice of both traditional and contemporary Algebraic methods, including Group theory, polynomial algebra, and finite fields. Therefore, we must first introduce some fundamental concepts in abstract algebra before deliberating coding theory in detail.

1.1 Basics of Abstract Algebra:

Binary operation or composition $*$ is a function from Cartesian product of a set to itself. i.e. $*: S \times S \rightarrow S$. An **Algebraic structure** is a non-void set combined with one or additional binary operations. i.e. $(G, *)$ is an Algebraic structure, where G is taken to be non-void set and $*$ is a binary operation. A set G that is non-void and has a binary operation defined on it, is known as **Groupoid.**

If a binary operation is specified on G and the associative law is true in G, then G becomes a **Semi-Group**. In other words, a Groupoid becomes a Semi- Group when associative law applies to it.

Examples of Semi-Groups where cancellation laws include is the set of natural numbers under addition.

- In a Semi-Group, cancellation laws might not be applicable.
- If a finite Semi-Group complies with the cancellation laws, it is a Group.

When a Semi-Group has identity element, it becomes **monoid**. If the laws of cancellation apply to a monoid, it is a Group.

Group:

If the following axioms are true, an Algebraic structure $(G, *)$ is referred to as a Group.

i. Associative law is true.
ii. The identity element is present.
iii. Existence of each element's inverse.

There is no requirement to demonstrate closure property when the term "Algebraic structure" is used.

- Group of Residue: $\mathbb{Z}_n = \{0,1,2,...,n\}$ is a Group under addition modulo $(n \geq 1)$.
- $(\mathbb{Q}-\{0\},\cdot),(\mathbb{R}-\{0\},\cdot),(\mathbb{C}-\{0\},\cdot)$ are Groups under multiplication.

Ring:

If the following axioms are true, a non-void set R, along with the binary operations + and $\cdot$ defined on R, is referred to as a ring:

i. $(R,+)$ is an abelian (commutative) Group.

ii. $(R,\cdot)$ is Semigroup.

iii. "$\cdot$" is distributive with respect to +. i.e. for all $r,s,t \in R$

- $r\cdot(s+t) = r\cdot s + r\cdot t$ (Left Distributive Law).
- $(r+s)\cdot t = r\cdot t + s\cdot t$ (Right Distributive Law).

A ring becomes commutative if it is commutative under multiplication. Ring is referred to as a commutative ring with unity after possessing multiplicative identity number 1.

$(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$, $(\mathbb{Z},+,\cdot)$ are some well-known examples of commutative rings with identity.

An example of a finite commutative ring with unity is the ring of integers modulo *n*. These rings play a vital character in the theory of Algebraic coding.

The lowest number of times that the ring's multiplicative identity must be used in a sum to obtain the additive identity is the **characteristic of a ring** R, that is, the smallest positive integer *n* such that $\underbrace{1+1+...+1}_{n-summand} = 0$. The components of a ring that reverse when multiplied (invertible elements). A ring element *u* is mathematically considered to be a **unit** if $u.v = v.u = 1$ such that *v* exists in R. If there is a positive number *n* (also known as an index or occasionally a degree) such that $\theta^n = 0$, then element θ of a ring R is referred to be **nilpotent**.

If there is a non-zero element *u* in R that exists in such a way that $u\cdot v = 0$ then the non-zero element *v* of a commutative ring R with unity is known as a **zero-divisor** in R.

Integral Domain (I-D):

A commutative ring D with unity is identified as an I-D if $d_1 d_2 = 0$, where $d_1, d_2 \in D$, then either $d_1 = 0$ or $d_1 = 0$. In other words, there is no zero-divisor in an I-D. Sometimes it is unnecessary to state the commutative condition for an I-D.

$\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}\left[\sqrt{2}\right], \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are few illustrations of an I-D. Additionally, every field is an I-D, but contradiction does not hold in general.

Every finite I-D is a Field.

- ### Euclidean Domain (ED):

Supposing R is an I-D. A function *f* from $R/\{0\}$ to the non-negative integers that fulfill the fundamental property of division with remainder is known as a **Euclidean function** on R.

Existing *q* and *r* in R such that $a_1 = a_2 q + r$ and either $r = 0$ or $f(r) < f(a_2)$, if a_1 and a_2 are in R and a_2 is non zero.

An I-D that is capable of receiving at least one Euclidean function is known as a Euclidean domain.

Any field is a Euclidean domain. Define $f(x) = 1$ for all non-zero *x*. $\mathbb{Z}$ is also Euclidean domain.

- ### Principal ideal Domain (PID):

An I-D in which each ideal is generated by a single element (principal ideal) is known as a principal ideal domain, or PID. PID is referred to as primary rings by certain writers. The ring of integers $\mathbb{Z}$ and the ring of Gaussian integers $\mathbb{Z}[i]$ are two examples of PID. Unlike a principle ideal domain, a principal ideal ring can have zero divisors.

Every ED is PID.

- ### Unique Factorization Domain (UFD):

According to formal definitions, a UFD is an I-D R in which any non-zero element *v* of R may be expressed as the product of irreducible components p_i of R and a unit *u*:

$$v = u p_1 p_2 \ldots p_n \quad , n \geq 0$$

But in a broader sense, we might say that a UFD is an I-D R in which each non-zero element can be expressed as the product of a unit and a prime element of R

If a non-zero, non-unit element in an I-D is not the outcome of the product of two other non-unit elements, it is said to be irreducible in abstract algebra. In other words, every component of such an element has at least one unit.

An element p in a commutative ring R that is non-zero and non-unit is referred to as a **prime element** if, whenever $p \mid r_1 r_2$ for some r_1 and r_2 in **R**, then $p \mid r_1$ or $p \mid r_2$. Every prime element in the I-D is irreducible.

All PID's (hence all ED) are UFD.

- ### Greatest Common Divisor (GCD) Domain:

An I-D **R** in which any two elements have a greatest common divisor is known as a GCD domain. i.e., there is a distinctive minimal principal ideal holding the ideal generated by two given elements. In other words, any two elements of **R** have a LCM

Every ED, PID, and UFD fall under the GCD.

Ideal of Ring:

A non-void set **I** of a commutative ring R is referred to be an ideal of **R** if

i. $m, n \in I \Rightarrow m - n \in I$.

ii. $m \in I,\ r \in R \Rightarrow rm \in I$.

Set of even integers is an ideal of ring of integers. Keep in mind that a Subring might not be ideal.

Let R be a commutative ring. An ideal $M \neq R$ is referred to as **maximal ideal** of R if there exist an ideal, $N \in R$, such that $M \subset N \subset R$ then either $M = N$ or $N = R$.

Supposing R is a commutative ring. An ideal $M \neq R$ is said to be maximal ideal of R if there exist an ideal, $N \in R$, such that $M \subset N \subset R$ then either $M = N$ or $N = R$.

A proper ideal **P** of a commutative ring **R** is **prime** if $r_1, r_2 \in R$ such that $r_1 r_2 \in P$ then either $r_1 \in P$ or $r_2 \in P$. In the ring $R = \mathbb{Z}$, the Subset of even number is a prime ideal, further $n\mathbb{Z}$ is prime ideal iff n is prime.

Nil radical of commutative ring R is the intersection of all prime ideals and the nil radical forms the smallest ideal of R, which is composed of all of its nilpotent constituents.

Local Ring:

A ring that contains unique maximal ideal is known as a local ring. All non-units of the ring R make up this particular maximum ideal.

For any prime *p* and *n* be any positive integer, $\left(\mathbb{Z}_{p^n},+,\cdot\right)$ is a local commutative ring with unity.

A commutative ring **R** with unity is said to be local if and only if the set of all its non-unit elements create an additive abelian Group. A commutative ring having unique prime ideal is known as a **primary ring.**

Residue Field:

If we take a local ring ***R*** with its unique maximal ideal ***M***. Then the quotient ring formed by its maximal ideal $\left(i.e.\ R/M=\{r+M:r\in R\}\right)$ is a field that is known as residue field.

Monic Polynomial:

A polynomial that contains only one variable with a leading coefficient of 1 (the highest degree variable's non-zero coefficient). $e.g.\quad x^4+3x^2+5x+1$

Irreducible Polynomial:

If a non-constant polynomial $f(x)\in\mathbb{F}[x]$ cannot be factored as the product of two non-constant polynomials over the field $\mathbb{F}$, then $f(x)$ becomes irreducible over $\mathbb{F}$.

Basic Irreducible Polynomial:

Let ***R*** be a local commutative ring with unity having unique maximal ideal ***M***. An irreducible polynomial $a_o+a_1x+\ldots+a_nx^n$ becomes a basic irreducible polynomial over ***R*** if the polynomial $\overline{a_o}+\overline{a_1}x+\ldots+\overline{a_n}x^n$ is irreducible over the residue field R/M.

Regular Polynomial:

A polynomial $f(u)$ is referred to as regular if it is not zero divisor in $R[u]$, where $R[u]$ is a polynomial ring in variable *u* over ring **R**.

Minimal Polynomial:

A minimal polynomial of an element ω of a field is the lowest degree monic polynomial having coefficients in the field, such that ω is a root of the polynomial. It is unique if the minimal polynomial ω of exists.

Primitive Polynomial:

Primitive polynomials are defined as polynomials that produce all of the elements of an extension field produces a base field. Irreducible polynomials include primitive polynomials.

For every prime *p* or power of prime $q = p^k$ and any positive integer *m*, there exist a primitive polynomial of degree *m* over $GF(q)$. There are

$$a_q(n) = \frac{\phi(q^n - 1)}{m}$$

Primitive polynomials over $GF(q)$, where ϕ is the totient function. Any finite field $\mathbb{F}$ having cardinality p^n contains a primitive element α of order $p^n - 1$.

1.2 Fundamental Notions in Algebraic Coding Theory:

Information medium, such as communication systems and data storage devices, are not always totally trustworthy in practice due to noise or other sorts of additional interference. To find or even fix mistakes is one of the responsibilities involved in coding theory.

1.2.1 What is a Code?

A Code is a set of principles used to transform information such as letters, words, sounds, images, or gestures into a more concise or hidden form for transmission across a communication channel. Generally speaking, if we have a finite set **A** of **q (> 1)** symbols that can be communicated across the communication route. The alphabet of transmission is what we call **A**. We are going to provide **A** with some Algebraic structures so that one can participate in mathematical games. Let $V = A^n$ denote the collection of every *n*-tuple of items in the set **A**, where *n* is a certain positive integer bigger than 1. Thus V consists of q^n words or vectors as its constituent parts. The term "q-ary code of length" is used to refer to C that is a non-void Subset of V. In particular, C is referred to as a **binary code** if $q = 2$. It is referred to as **ternary code** if $q = 3$. Codewords are the components or constituents of a code C. **Trivial code** is described as C if it just has one codeword or if $C = q^n$. Additionally, if each codeword in C is a vector with the form $a\,a \ldots a$ for some $a \in A$, then C is known as a repetition code.

1.2.2 Error Correcting Codes (Nagpaul, 2005):

An error-correcting code is a type of encoding that sends messages as binary integers in a way that allows for message recovery even in the event of a bit error. The main goal of error-correcting code is to increase the message's redundancy so that the problem can often be found and fixed.

Let us deliberate a very simple example. Presume the only messages we desire to send are 'YES' and 'NO'. We have a digital communication channel through which the symbols 1 and 0 can be transmitted. Let us decide to represent the message YES by 1 and NO by 0. We assume this scheme of representation is known also to the recipient of the message. If the channel is not noisy then there is no problem. When we wish to send the message YES we transmit 1. If no error occurs during transmission, the recipient receives the message 1 and interprets it to mean YES. But if channel is noisy, it is possible that when we transmit 1, we may get 0, which interprets to mean NO.

An obvious method for dealing with the problem of transmission errors is to repeat the message. Let us represent YES as 11 and NO as 00. We refer to this representation as encoding and refer to 11 and 00 as codewords. The set $C=\{11,00\}$ is called a code. Suppose we wish to send the message YES, and therefore we transmit 11. If no error occurs, the received message is 11, which is correctly interpreted as YES. If an error takes place in one of the two symbols, the received message is 10 or 01. Because neither of these is a codeword, the receiver conclude that an error has occurred, but cannot determined whether the original message was 11 or 00. Further if an error occurs in the both digits the received message is 00 which interpreted as NO in this case we get a wrong message. We thus see that we have an encoding scheme in which one error in the message can be detect but if two errors then they remain un detected. Since the probability of two errors occurring is less than the probability of one error. Chances of a wrong message being accepted as correct are less now than in the previous scheme where we represented YES and NO by single symbol.

We observe that the ability to detect an error the received message is a result of the redundancy that we introduce in the codewords by using two symbol in place of one. Let us see what happens if we further increase redundancy. Let us represent YES as 111 and NO as 000. As before suppose we transmit 111 to send the message YES. Now, if one of the three digits is received in error, the received message is 110, 101 or 011. If two errors occur the received message is 100, 010 or 001. Because none of these is a codeword, the receiver concludes that an error has occurred. But if three errors occur, the received message is 000, which being a codeword, is wrongly accepted as the message NO. We thus see that with this code we can detect up to two errors in the received message. In fact with this code $C=\{111,000\}$, we can do more than just detect up to two errors. We can recover the correct message if only one error has occurred in the received message. If the received message is 110, 101 or 011 and we assume that only one error has occurred than the original message must have been 111. So we adopt the following rule: if the received message is 111, 110, 101 or 011, we decode it as 111. If on the other hand, the received message is 000, 100, 010 or 001, we decode it as 000. This is called **nearest neighbor decoding** or **maximum likelihood decoding**. Thus we see that this code can detect up to two errors and, with the nearest neighbor decoding procedure it can accurate one error. Of course if additional error has occurred in the received message then the nearest neighbor decoding rule will give a wrong result but the chances of two or three errors occurring are less than the chance of one error so on the whole we are in a better situation than before.

1.3 Linear Codes:

According to theory of algebraic coding, a linear code is a class of error-correcting codes for which every linear combination of code words is also a code word.

1.3.1 Hamming Distance:

Let $\delta, \lambda \in A^n$, $\delta = \delta_1\delta_2 \ldots \delta_n$, $\lambda = \lambda_1\lambda_2 \ldots \lambda_n$. The **Hamming distance** between the vectors δ and λ , denoted by $d(\delta, \lambda)$, is defined to be the number of Subscript i such that $\delta_i \neq \lambda_i$; that is

$$d(\delta, \lambda) = |\{i \mid \delta_i \neq \lambda_i\}|$$

For example, in $\{0,1\}^3, d(110, 011) = 2$.

1.3.2 Minimum Distance:

The smallest distance between any two unique code words in a code C denoted by $d(C)$ and defined as:

$$d(C) = \min\{d(\delta, \lambda) \mid \delta, \lambda \in C, \delta \neq \lambda\},$$

is known as the minimum distance of a code C

For instance, the binary repetition code $C = \{000, 111\}$ has minimum distance 3.

The number of nonzero components in δ is the definition of a **vector's weight**, represented as $w(\delta)$. The definition instantly implies that for every vector $\delta, \lambda \in \mathbb{F}^n$,

$$d(\delta, \lambda) = w(\delta - \lambda)$$

Theorem 1.3.3

Consider *C* be a code having minimum distance *d*. Let $s = \left\lfloor \frac{d-1}{2} \right\rfloor$. Then

1. C can find up to $d-1$ errors in any codeword that is communicated.
2. Any transmitted codeword may have up to *s* errors that C can fix.

1.3.4 Generator and Parity-Check Matrix:

Assume that C is a linear $[n,k]$-code. Let G be a $k \times n$ matrix whose rows generate a basis of C. G is thus referred to be a **generator matrix** of the code C. Given that there are other ways to choose the basis for C, the matrix G is not the only generator matrix for C.

A generator matrix totally determines a linear code. Let G represent a generator matrix for a C $[n,k]$-code over F. Then each element $u \in C$ is a linear combination of the rows of G that is, $u = a_1G_1 + ... + a_kG_k$, where $a_1,...,a_k \in F$ and $G_1,...,G_k$ are the rows of G. Thus, **C** is the row space of the matrix G.

Theorem 1.3.5

Suppose **C** be an $[n,k]$-code over **F** having generator matrix G. Then

$$C = \{vG : v \in F^k\}$$

This representation of C offers an encoding method. Let G represent a generating matrix for $[n,k]$ -code C over $F = \mathbb{F}_q$. A bijective mapping determined by the matrix G is provided by $e : F^k \to C$. This mapping is used to represent q^k distinct messages using codewords. We utilize the encoding mapping *e* after adopting a fixed strategy for associating the q^k vectors in F^k are identified with q^k messages. However, it is irrelevant for our purposes how the components of F^k are connected to the actual messages. Therefore, we may regard F^k as a collection of message words. The components of F^k are referred to as message words. Each k-tuple message word v is therefore encoded as an *n*-tuple codeword. The number $n-k$ is referred to as the code C's redundant number and k/n as its *transaction rate*.

1.3.6 Dual Code:

Let **C** be an $[n,k]$-code over **F**. Then the ***dual code*** over **C** is defined as

$$C^{\perp} = \{u \in F^n \mid u \cdot v = 0, \forall v \in C\}$$

If $u \cdot v = 0$, then two vectors $u, v \in F^n$ are referred to as orthogonal. As a result, each vector in $C^{\perp}$ and each vector in C are orthogonal. If every vector in a linear code C, is orthogonal to both itself and all other vector in C, then C is said to be self-orthogonal. To put it another way, C is self-orthogonal if $C^{\perp}$.

Theorem 1.3.7

Suppose C is $[n,k]$-code. Then $C^{\perp}$ is $[n,n-k]$-code and $(C^{\perp})^{\perp}=C$.

Let **C** be a linear $[n,k]$-code over **F**. Suppose H be a generator matrix of the dual code $C^{\perp}$. Then H is called a ***Parity-Check matrix*** of the code **C**. The parity-check matrix of the $[n,k]$-code is an $(n-k)\times n$ matrix H whose rows form the basis for $C^{\perp}$.

Further for any $y\in F$, the ***syndrome*** of *y*, denoted by $S(y)$, is defined to be:

$$S(y)=yH^{T}$$

Be aware that the syndrome is described in terms of a particular parity-check matrix H. An alternative parity-check matrix will result in an alternative syndrome.

1.4 Cyclic Codes:

According to coding theory, a cyclic code is an error-correcting code in which every cyclic shift of each codeword results in a new codeword. The mapping $\lambda:\mathbb{F}^{n}\to\mathbb{F}^{n}$ given by:

$$\lambda(v_1,v_2,\ldots,v_n)=(v_n,v_1,\ldots v_{n-1})$$

is known as **cyclic shift**.

Cyclic codes are a specific kind of linear code that, in comparison to conventional linear codes, contain ring-theoretic qualities and a richer Algebraic structure. These properties are useful for effective error detection and repair. Additionally, this Group includes numerous significant codes.

1.5 BCH-Codes:

Boss-Chaudhuri-Hoequenghem codes, often known as BCH-Codes in coding theory, are a kind of cyclic error-correcting codes that are designed by using polynomials over a finite field or Galois field. French mathematicians Alexis Hoequenghem and Raj Bose independently developed BCH-codes in 1959 and 1960, respectively.

The following describes a BCH-Code:

Consider c,d,q,n be positive integers such that $2\le d\le n$, *q* is a prime power, and *n* is relatively prime to *q*. Assume that *m* be the least positive integer such that $q^{m}\equiv 1(\bmod n)$. Thus *n* divides $q^{m}-1$. Let ζ be a primitive *nth* root of unity in $\mathbb{F}_{q^m}$. Let $m_i(x)\in\mathbb{F}_q[x]$ denote the minimal polynomial of ζ^{i}. Let $g(x)$ be the product of distinct polynomials among $m_i(x), i=c,c+1,\ldots,c+d-2$, that is,

$$g(x)=lcm\{m_i(x) \mid i=c,c+1,\ \ldots,c+d-2\}$$

Since $m_i(x)$ divides $x^n - 1$ for each i, it follows that $g(x)$ divides $x^n - 1$. Let C be the cyclic code with generator polynomial $g(x)$ in the ring $\mathbb{F}_q[x]_n$. Then C is referred to as BCH-Codes of length n over $\mathbb{F}_q$ with design distance d.

If $n = q^m - 1$, then BCH-Codes C is known as **primitive**. If $c = 1$, then C is referred to be a **Narrow Sense BCH-code**.

Theorem 1.5.1

Let $\alpha \in \mathbb{F}_{p^n}$. Then $\alpha, \alpha^p, \alpha^{p^2}, \ldots$ have same minimal polynomial over $\mathbb{F}_p$.

Theorem 1.5.2

Consider C a linear code. The smallest weight of the nonzero codewords in C is then equal to the minimal distance of C, which is

$$d(C) = \min\{w(\sigma) \mid \sigma \in C, \sigma \neq 0\}$$

1.5.3 Binary Hamming Code:

Binary Hamming Codes are an example of BCH-Code.

Construction:

If we take $q = 2$ and $n = 2^r - 1$, Then $m = r$, So $\mathbb{F}_{2^r}$. Suppose β be the primitive *nth* root of unity in $\mathbb{F}_{2^r}$, then β will be the primitive element in $\mathbb{F}_{2^r}$. Suppose $g(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of β. Then $g(x)$ is the primitive polynomial of degree r. Now β and β^2 will have the same minimal polynomial. Thus $m_1(x) = m_2(x) = g(x)$. So

$$g(x) = lcm\{m_i(x) \mid i = 1, 2\}$$

Hence this $Ham(r, 2)$ is narrow sense BCH-Codes with design distance 3 generated by $g(x)$.

Example 1.5.4

Design a binary narrow sense BCH-code of length 15 and designed distance 7. Show that its minimum distance is 7.

Sol:

Here $q=2,\ n=15,$ so $m=4$ and $2^4-1=15$. The polynomial

$$p(x)=x^4+x+1$$

is a primitive irreducible polynomial over $\mathbb{F}_2$. So we can represent the field $\mathbb{F}_{2^4}$ as

$$\mathbb{F}_{2^4}=\left\{c_o+c_1\alpha+c_2\alpha^2+c_3\alpha^3 \mid c_o,c_1,c_2,c_3\in\mathbb{F}_2\right\}$$

Where, α satisfy the relation, $\alpha^4+\alpha+1=0$. Using this relation, by taking exponents of α, we obtain the following table:

Exp.	Polynomial	Binary String
1	α	0010
2	α^2	0100
3	α^3	1000
4	$1+\alpha$	0011
5	$\alpha+\alpha^2$	0110
6	$\alpha^2+\alpha^3$	1100
7	$1+\alpha+\alpha^3$	1011
8	$1+\alpha^2$	0101
9	$\alpha+\alpha^3$	1010
10	$1+\alpha+\alpha^2$	0111
11	$\alpha+\alpha^2+\alpha^3$	1110
12	$1+\alpha+\alpha^2+\alpha^3$	1111
13	$1+\alpha^2+\alpha^3$	1101
14	$1+\alpha^3$	1001
15	1	0001

Table: 1.1

So, α is a primitive 15th root of unity in $\mathbb{F}_{2^4}$ and $p(x)$ is the minimal polynomial of α. To obtain a BCH-Codes of designed distance $d=7$, we need the minimal polynomials of α^i for $i=1,2,\ldots,6$. By theorem 1.5.1 α,α^2,α^4 have identical minimal polynomial $p(x)$. Let $q(x)$ be the minimal polynomial of α^3. Then $\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \ldots$ all have same minimal polynomial $q(x)$. Using the relation $\alpha^{15} = 1$, we see that the roots of $q(x)$ are $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$.

Hence,

$$\begin{aligned} q(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12}) \\ &= x^4 - (\alpha^3+\alpha^6+\alpha^9+\alpha^{12})x^3 + (\alpha^3+\alpha^6+\alpha^9+\alpha^{12})x^2 - (\alpha^3+\alpha^6+\alpha^9+\alpha^{12})x + 1 \\ &= x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

Similarly, minimal polynomial $h(x)$ of α^5 has roots α^5, α^{10}, so

$$\begin{aligned} h(x) &= (x-\alpha^5)(x-\alpha^{10}) \\ &= x^2 + x + 1 \end{aligned}$$

Hence, the generator polynomial of the desired BCH-Codes is

$$\begin{aligned} g(x) &= lcm\{m_i(x) \mid i = 1,2,3,4,5,6\} \\ &= p(x)q(x)h(x) \\ &= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1 \end{aligned}$$

Cyclic code C generated by $g(x)$ in $\mathbb{F}_2[x]_{15}$ has dimension 5, so C is a $[15,5]$ primitive narrow sense BCH-Codes of design distance 7. Hence $d(c) \geq 7$. Now $g(x)$ is itself a code polynomial and has 7 non zero terms, so it is a codeword of weight 7. Hence, by theorem 1.5.3, $d(C) \leq 7$. This proves that the minimum distance of C is 7, So C is a $[15,5,7]$-code.

Chapter # 2

Galois and Quasi-Galois Rings

In this chapter, we'll study the structure of Galois Rings and Quasi-Galois Rings with the aid of a simple example. Both finite commutative ring classes create a chain of ideals and are local. One might imagine the "bricks" of finite commutative algebra as belonging to the Galois Ring. Every finite commutative ring may undoubtedly be measured as an algebra over a given Galois Ring. However, while the features of Quasi-Galois Rings differ from those of Galois Rings, but their element expressions are very similar to those of Galois Rings.

When the context is clear, we write GR for Galois Ring and Q-GR for Quasi-Galois Ring.

2.1 Galois Ring:

GR is a finite, commutative, local ring of order p^{ns} and characteristic p^n. This ring is called Galois extensions of local rings of the form $\mathbb{Z}_{p^n}$, where *p* is a prime and *n* a positive integer. It is denoted by $GR(p^n, s)$ and defined as:

$$GR(p^n, s) = \mathbb{Z}_{p^n}[\omega] = \frac{\mathbb{Z}_{p^n}[x]}{< H_{(p,s)}(x) >}$$

It contains all residue classes of polynomials in x over $\mathbb{Z}_{p^n}$, modulo the polynomial $H_{(p,s)}(x)$.

Here, ω is a formal root of the monic, basic irreducible polynomial $H_{(p,s)}(x) \in \mathbb{Z}_{p^n}[x]$, calculated by **Hensel's Lemma** from primitive polynomial $h_{(p,s)}(x) \in \mathbb{Z}_p[x]$ of order *s*, such that

$$\mathbb{F}_{p^s} = GF\left(p^s\right) = \frac{\mathbb{F}_p[x]}{\left(h_{(p,s)}(x)\right)}$$

Thus, the polynomial $H_{(p,s)}(x)$ is linked to $h_{(p,s)}(x)$ by epi-morphism

$$\mu : \mathbb{Z}_{p^n}[x] \to \mathbb{Z}_p[x], \quad i.e.\ \mu\left(H_{(p,s)}(x)\right) = h_{(p,s)}(x) \in \mathbb{Z}_p[x].$$

2.1.1 Hensel's Lemma (Bini, pp. 90-91):

Hensel's Lemma reduces to simple calculations if $h_{(p,s)}(x) \in \mathbb{Z}_p[x]$ is monic, irreducible polynomial of the form:

$$h_{(p,s)}(x) = x^s + c_{s-1}x^{s-1} + \ldots + c_o$$

In this case, we have

$$H_{(p,s)}(x) = x^s + \left(p^n - p + c_{c-1}\right)x^{s-1} + \ldots + \left(p^n - p + c_o\right) \in \mathbb{Z}_{p^n}[x]$$

Note that, since each $c_j \in \mathbb{Z}_p$, $j \in \{0,1,\ldots,s-1\}$, $p^n - p + c_j < p^n$ as a positive integer, so it make sense that $H_{(p,s)}(x) \in \mathbb{Z}_{p^n}[x]$. Such a polynomial generates a proper ideal in $\mathbb{Z}_{p^n}[x]$.

Explicitly, we have

$$GR(p^n,s) = \{\sum_{j=0}^{s-1} c_j\alpha^j \,\Big|\, c_j \in \mathbb{Z}_{p^n}, 0 \le j \le s-1\}$$

Where, α is root of $H_{(p,s)}(x)$. i.e. $H_{(p,s)}(\alpha) = 0$.

- $GR(p^n,1)$ is the ring of integers modulo P^n.
- $GR(p,s)$ is a finite field of order p^s.

2.1.2 Units in GR:

For a given $GR(p^n,s)$, *p* a prime and *n* ,*s* are positive integers. Units in GR form a Group. Further

$$U\left(GR\left(p^n,s\right)\right) \cong G_1 \times G_2$$

Where, G_1 is a cyclic Group of order $p^s - 1$, G_2 is a Group of order $p^{s(n-1)}$.

$GR(p^n,s)$ contains $p^{ns} - p^{s(n-1)}$ units.

2.1.3 ideal Structure of $GR(p^n,s)$:

Since every $GR(p^n,s)$ is local, so it contains unique maximal ideal that is:

$$\langle p \rangle = p\,GR\left(p^n,s\right)$$

Elements in maximal ideal can be individually stated as:

$$pGR\left(p^n, s\right) = \left\{ p \sum_{j=0}^{s-1} c_j \alpha^j \,\middle|\, c_j \in \mathbb{Z}_{p^n},\ 0 \le j \le s-1 \right\}$$

Or more precisely,

$$pGR\left(p^n, s\right) = \left\{ \sum_{j=0}^{s-1} c_j \alpha^j \,\middle|\, c_j \in p\mathbb{Z}_{p^n},\ 0 \le j \le s-1 \right\}$$

Remaining possible ideals are

$$I_k = p^k GR\left(p^n, s\right),\ 1 \le k \le n-1$$

Clearly, each ideal in a GR is generated by single element, so these ideals are principle ideals.

Example 2.1.4

Discuss structure of GR having cardinality 64.

Sol:

If we take $p = 2,\ n = 2,\ s = 3$ in the above mention definition of GR, we get

$$GR\left(2^2, 3\right) = \frac{\mathbb{Z}_{2^2}[x]}{< H_{(2,3)}(x) >} = \left\{ \sum_{j=0}^{2} c_j \alpha^j \,\middle|\, c_j \in \mathbb{Z}_4 \right\}$$
$$= \left\{ c_o + c_1\alpha + c_2\alpha^2 \,\middle|\, c_o, c_1, c_2 \in \mathbb{Z}_4 \right\}$$

Where, $H_{(2,3)}(x)$, is monic, basic irreducible polynomial over $\mathbb{Z}_{2^2}[x]$.

Also, $$\left|GR\left(2^2, 3\right)\right| = 2^{(2)(3)} = 2^6 = 64$$

S. No.	Polynomial	String mod4	S. No.	Polynomial	String mod4
1.	0	000	33.	$2\alpha+2\alpha^2$	220
2.	1	001	34.	$2\alpha+3\alpha^2$	320
3.	2	002	35.	$3\alpha+\alpha^2$	130
4.	3	003	36.	$3\alpha+2\alpha^2$	230
5.	α	010	37.	$3\alpha+3\alpha^2$	330
6.	2α	020	38.	$1+\alpha+\alpha^2$	111
7.	3α	030	39.	$1+\alpha+2\alpha^2$	211
8.	α^2	100	40.	$1+\alpha+3\alpha^2$	311
9.	$2\alpha^2$	200	41.	$1+2\alpha+\alpha^2$	121
10.	$3\alpha^2$	300	42.	$1+2\alpha+2\alpha^2$	221
11.	$1+\alpha$	011	43.	$1+2\alpha+3\alpha^2$	321
12.	$1+2\alpha$	021	44.	$1+3\alpha+\alpha^2$	131
13.	$1+3\alpha$	031	45.	$1+3\alpha+2\alpha^2$	231
14.	$1+\alpha^2$	101	46.	$1+3\alpha+3\alpha^2$	331
15.	$1+2\alpha^2$	201	47.	$2+\alpha+\alpha^2$	112
16.	$1+3\alpha^2$	301	48.	$2+\alpha+2\alpha^2$	212
17.	$2+\alpha$	012	49.	$2+\alpha+3\alpha^2$	312
18.	$2+2\alpha$	022	50.	$2+2\alpha+\alpha^2$	122
19.	$2+3\alpha$	032	51.	$2+2\alpha+2\alpha^2$	222
20.	$2+\alpha^2$	102	52.	$2+2\alpha+3\alpha^2$	322
21.	$2+2\alpha^2$	202	53.	$2+3\alpha+\alpha^2$	132
22.	$2+3\alpha^2$	302	54.	$2+3\alpha+2\alpha^2$	232
23.	$3+\alpha$	013	55.	$2+3\alpha+3\alpha^2$	332
24.	$3+2\alpha$	023	56.	$3+\alpha+\alpha^2$	113
25.	$3+3\alpha$	033	57.	$3+\alpha+2\alpha^2$	213
26.	$3+\alpha^2$	103	58.	$3+\alpha+3\alpha^2$	313
27.	$3+2\alpha^2$	203	59.	$3+2\alpha+\alpha^2$	123
28.	$3+3\alpha^2$	303	60.	$3+2\alpha+2\alpha^2$	223
29.	$\alpha+\alpha^2$	110	61.	$3+2\alpha+3\alpha^2$	323
30.	$\alpha+2\alpha^2$	210	62.	$3+3\alpha+\alpha^2$	133
31.	$\alpha+3\alpha^2$	310	63.	$3+3\alpha+2\alpha^2$	233
32.	$2\alpha+\alpha^2$	120	64.	$3+3\alpha+3\alpha^2$	333

Table 2.1: Elements of $GR(2^2,3)$:

Nilpotent elements in $GR(2^2,3)$:

All shaded elements in above table indicates nilpotent elements because 0 (obviously nilpotent) and 2 are nilpotent elements in $\mathbb{Z}_4$. Polynomials (elements) in $GR(2^2,3)$ are nilpotent elements if they have coefficients only from nilpotent elements of $\mathbb{Z}_4$.

Units in $GR(2^2,3)$:

All remaining unshaded elements are units in $GR(2^2,3)$. Polynomials (elements) in $GR(2^2,3)$ are unit elements if they have at least one coefficient from units of $\mathbb{Z}_4$. Number of units in $GR(2^2,3)$ are $p^{ns}-p^{s(n-1)}=2^{2\times 3}-2^{3(2-1)}=56$. As we know that these units form a Group under multiplication, further

$$U\left(GR\left(2^2,3\right)\right)\cong G_1\times G_2$$

Where, G_1 is cyclic Group of cardinality $p^s-1=2^3-1=7$ and G_2 is Group of cardinality $p^{s(n-1)}=2^{3(2-1)}=8$.

Maximal ideal of $GR(2^2,3)$:

Elements in maximal ideal of $GR(2^2,3)$ can be uniquely expressed as:

$$\begin{aligned}\langle 2\rangle = 2GR\left(2^2,3\right) &= \left\{\sum_{j=0}^{3-1} c_j\alpha^j \,\middle|\, c_j\in 2\mathbb{Z}_4,\ 0\le j\le 3-1\right\}\\ &= \left\{c_0+c_1\alpha+c_2\alpha^2 \,\middle|\, c_j\in 2\mathbb{Z}_4\right\}\end{aligned}$$

Maximal ideal consist of only nilpotent elements of $GR(2^2,3)$.

2.2 Quasi-Galois Ring:

Q-GR is a local ring that is finite, commutative, and has cardinality p^{ns} and characteristic p (p is a prime and *n,s* are any positive integers). Particularly from the perspective of applications in coding theory and finite geometry, Q-GRs are highly intriguing because they have the desirable attribute of consisting a prime characteristic. It is indicated by $A\left(p^s,n\right)$ and defined as:

$$A\left(p^s,n\right)=\frac{F_{p^s}[x]}{<x^n>}=\left\{\sum_{i=0}^{n-1}a_i\theta^i \,\middle|\, a_i\in F_{p^s}\right\}$$

Where, θ is a formal, non-trivial root of polynomial $x^n\in\mathbb{F}_{p^s}[x]$, i.e. $\theta^n=0$.

2.2.1 Nilpotent Elements in Q-GR:

In the expression $A\left(p^s,n\right)=\frac{F_{p^s}[x]}{<x^n>}=\left\{\sum_{i=0}^{n-1}a_i\theta^i \,\middle|\, a_i\in F_{p^s}\right\}$, if we take $a_o=0$ then we get all possible nilpotent elements of $A\left(p^s,n\right)$.

2.2.2 Units in Q-GR:

In the expression $A\left(p^s,n\right)=\frac{F_{p^s}[x]}{<x^n>}=\left\{\sum_{i=0}^{n-1}a_i\theta^i \,\middle|\, a_i\in F_{p^s}\right\}$, if we take $a_o\neq 0$ then we get all possible unit elements of $A\left(p^s,n\right)$. For $a_o=1$ we get **principle unit elements.**

Proposition 2.2.3

Consider a Q-GR $A\left(p^s,n\right)$, *p* a prime and *n ,s* are positive integers. Units in Q-GR form a Group which is isomorphic to a direct product of Groups,

$$U\left(A\left(p^s,n\right)\right)\cong G_1\times G_2$$

Where, G_1 is a cyclic Group of order p^s-1, G_2 is an abelian p-Group of order $p^{s(n-1)}$ such that If $s=1$ and $n=2$, then G_2 is cyclic Group of order *p*. If $p=2, s=1$ and $n=3$, then $G_2\cong C_4$.

2.2.4 Ideal Structure of Q-GR $A\left(p^s,n\right)$:

Since Q-GR is a local ring, so its contains a unique maximal ideal that is:

$$m\left(p^s,n\right)=\left\{\sum_{i=1}^{n-1} a_i\theta^i \,\middle|\, a_i \in F_{p^s}\right\},\quad \theta^n=0.$$

Every proper ideal in Q-GR is of the form $A\left(p^s,n\right)$:

$$J_k=\theta^k A\left(p^s,n\right),\ 1\le k\le n-1$$

Example 2.2.5

Discuss Structure of Q-GR of cardinality 64.

Sol:

If we take $p=2, s=3, n=2$ in the above mention definition of Q-GR, we get

$$A\left(2^3,2\right)=\frac{F_{2^3}[x]}{<x^2>}=\left\{\sum_{i=0}^{1} a_i\theta^i \,\middle|\, a_i \in F_{2^3}\right\},\ \theta^2=0$$

$$=\left\{a_o+a_1\theta \,\middle|\, a_o,a_1\in F_{2^3}\right\}$$

Where, $F_{2^3}=\dfrac{\mathbb{Z}_2[x]}{<x^3+x+1>}=\left\{0,\,1,\,\alpha,\,\alpha^2,\,1+\alpha,\,1+\alpha^2,\,\alpha+\alpha^2,\,1+\alpha+\alpha^2\right\}$

α is the root of monic, irreducible polynomial of x^3+x+1. i.e. $\alpha^3+\alpha+1=0$.

Also, $$\left|A\left(2^3,2\right)\right|=2^{(3)(2)}=2^6=64.$$

	S. No.	Elements	Order	S. No.	Elements	Order
Nilpotent Elements (Nilradical)	1.	0		33.	$1+\alpha$	7
	2.	θ		34.	$1+\alpha+\theta$	14
	3.	$\alpha\theta$		35.	$1+\alpha+\alpha\theta$	14
	4.	$\alpha^2\theta$		36.	$1+\alpha+\alpha^2\theta$	14
	5.	$(1+\alpha)\theta$		37.	$1+\alpha+(1+\alpha)\theta$	14
	6.	$(1+\alpha^2)\theta$		38.	$1+\alpha+(1+\alpha^2)\theta$	14
	7.	$(\alpha+\alpha^2)\theta$		39.	$1+\alpha+(\alpha+\alpha^2)\theta$	14
	8.	$(1+\alpha+\alpha^2)\theta$		40.	$1+\alpha+(1+\alpha+\alpha^2)\theta$	14
Principal Unit Elements (Abelian 2-Group)	9.	1	1	41.	$1+\alpha^2$	7
	10.	$1+\theta$	2	42.	$1+\alpha^2+\theta$	14
	11.	$1+\alpha\theta$	2	43.	$1+\alpha^2+\alpha\theta$	14
	12.	$1+\alpha^2\theta$	2	44.	$1+\alpha^2+\alpha^2\theta$	14
	13.	$1+(1+\alpha)\theta$	2	45.	$1+\alpha^2+(1+\alpha)\theta$	14
	14.	$1+(1+\alpha^2)\theta$	2	46.	$1+\alpha^2+(1+\alpha^2)\theta$	14
	15.	$1+(\alpha+\alpha^2)\theta$	2	47.	$1+\alpha^2+(\alpha+\alpha^2)\theta$	14
	16.	$1+(1+\alpha+\alpha^2)\theta$	2	48.	$1+\alpha^2+(1+\alpha+\alpha^2)\theta$	14
	17.	α	7	49.	$\alpha+\alpha^2$	7
	18.	$\alpha+\theta$	14	50.	$\alpha+\alpha^2+\theta$	14
	19.	$\alpha+\alpha\theta$	14	51.	$\alpha+\alpha^2+\alpha\theta$	14
	20.	$\alpha+\alpha^2\theta$	14	52.	$\alpha+\alpha^2+\alpha^2\theta$	14
	21.	$\alpha+(1+\alpha)\theta$	14	53.	$\alpha+\alpha^2+(1+\alpha)\theta$	14
	22.	$\alpha+(1+\alpha^2)\theta$	14	54.	$\alpha+\alpha^2+(1+\alpha^2)\theta$	14
	23.	$\alpha+(\alpha+\alpha^2)\theta$	14	55.	$\alpha+\alpha^2+(\alpha+\alpha^2)\theta$	14
	24.	$\alpha+(1+\alpha+\alpha^2)\theta$	14	56.	$\alpha+\alpha^2+(1+\alpha+\alpha^2)\theta$	14
	25.	α^2	7	57.	$1+\alpha+\alpha^2$	7
	26.	$\alpha^2+\theta$	14	58.	$1+\alpha+\alpha^2+\theta$	14
	27.	$\alpha^2+\alpha\theta$	14	59.	$1+\alpha+\alpha^2+\alpha\theta$	14
	28.	$\alpha^2+\alpha^2\theta$	14	60.	$1+\alpha+\alpha^2+\alpha^2\theta$	14
	29.	$\alpha^2+(1+\alpha)\theta$	14	61.	$1+\alpha+\alpha^2+(1+\alpha)\theta$	14
	30.	$\alpha^2+(1+\alpha^2)\theta$	14	62.	$1+\alpha+\alpha^2+(1+\alpha^2)\theta$	14
	31.	$\alpha^2+(\alpha+\alpha^2)\theta$	14	63.	$1+\alpha+\alpha^2+(\alpha+\alpha^2)\theta$	14
	32.	$\alpha^2+(1+\alpha+\alpha^2)\theta$	14	64.	$1+\alpha+\alpha^2+(1+\alpha+\alpha^2)\theta$	14

Table 2.2: Elements of Q-GR $A(2^3,2)$

Nilpotent Elements in $A\left(2^3,2\right)$:

All shaded elements in above table indicates nilpotent elements in $A\left(2^3,2\right)$. In the expression, $A\left(2^3,2\right)=\dfrac{F_{2^3}[x]}{<x^2>}=\left\{a_o+a_1\theta \,\middle|\, a_o,a_1\in F_{2^3}\right\}$ whenever we take $a_o=0$ then we get all nilpotent elements.

Units in $A\left(2^3,2\right)$:

All unshaded elements in above table indicates units in $A\left(2^3,2\right)$. In the expression, $A\left(2^3,2\right)=\dfrac{F_{2^3}[x]}{<x^2>}=\left\{a_o+a_1\theta \,\middle|\, a_o,a_1\in F_{2^3}\right\}$ whenever we take $a_o\neq 0$ then we get all unit elements.

Maximal ideal of $A\left(2^3,2\right)$:

Elements in maximal ideal of $A\left(2^3,2\right)$ can be uniquely expressed as:

$$\begin{aligned} m\left(2^3,2\right) &= \left\{\sum_{i=1}^{2-1} a_i\theta^i \,\middle|\, a_i\in F_{2^3}\right\} \\ &= \left\{a_1\theta \,\middle|\, a_1\in F_{2^3}\right\} \end{aligned}$$

Clearly, maximal ideal consist of only nilpotent elements of $A\left(2^3,2\right)$.

2.2.7 Cyclic Subgroups of Group of Units of $A(2^3,2)$:

Since, calculated elements of Q-GR in table 2.2, there are 56 unit elements and elements from 9 to 16 forms an abelian 2 Group that is obviously not cyclic. Now if we look at elements of the serial number 17, 25, 33, 41, 49, 57 in table 2.2, these are the elements of $\mathbb{F}_{2^3}{}^*$ (non-zero elements of residue field) which is clearly cyclic Group under multiplication. Now we have remaining 42 elements, let us check their order structure, so that we can draw some conclusion about any cyclic Subgroup other than $\mathbb{F}_{2^3}{}^*$.

Exp.	$\alpha+\theta$	
1	$\alpha+\theta$	Generator
2	α^2	
3	$1+\alpha+\alpha^2\theta$	Generator
4	$\alpha+\alpha^2$	
5	$1+\alpha+\alpha^2+(\alpha+\alpha^2)\theta$	Generator
6	$1+\alpha^2$	
7	$1+(1+\alpha^2)\theta$	Principal Unit element
8	α	
9	$\alpha^2+\alpha\theta$	Generator
10	$1+\alpha$	
11	$\alpha+\alpha^2+(1+\alpha)\theta$	Generator
12	$1+\alpha+\alpha^2$	
13	$1+\alpha^2+(1+\alpha+\alpha^2)\theta$	Generator
14	1	

Exp.	$\alpha^2+\theta$	Exp.	$\alpha+\alpha\theta$
1	$\alpha^2+\theta$	1	$\alpha+\alpha\theta$
2	$\alpha+\alpha^2$	2	α^2
3	$1+\alpha+\alpha^2+(\alpha+\alpha^2)\theta$	3	$1+\alpha+(1+\alpha)\theta$
4	α	4	$\alpha+\alpha^2$
5	$1+\alpha+\alpha\theta$	5	$1+\alpha+\alpha^2+(1+\alpha+\alpha^2)\theta$
6	$1+\alpha+\alpha^2$	6	$1+\alpha^2$
7	$1+(1+\alpha+\alpha^2)\theta$	7	$1+\theta$
8	α^2	8	α
9	$\alpha+\alpha^2+\alpha^2\theta$	9	$\alpha^2+\alpha^2\theta$
10	$1+\alpha^2$	10	$1+\alpha$
11	$\alpha+(1+\alpha^2)\theta$	11	$\alpha+\alpha^2+(\alpha+\alpha^2)\theta$

12	$1+\alpha$	12	$1+\alpha+\alpha^2$
13	$1+\alpha+\alpha^2+(1+\alpha)\theta$	13	$1+\alpha^2+(1+\alpha^2)\theta$
14	1	14	1
Exp.	$\alpha+\alpha^2\theta$	Exp.	$\alpha+(1+\alpha)\theta$
1	$\alpha+\alpha^2\theta$	1	$\alpha+(1+\alpha)\theta$
2	α^2	2	α^2
3	$1+\alpha+(\alpha+\alpha^2)\theta$	3	$1+\alpha+(1+\alpha+\alpha^2)\theta$
4	$\alpha+\alpha^2$	4	$\alpha+\alpha^2$
5	$1+\alpha+\alpha^2+(1+\alpha^2)\theta$	5	$1+\alpha+\alpha^2+\theta$
6	$1+\alpha^2$	6	$1+\alpha^2$
7	$1+\alpha\theta$	7	$1+\alpha^2\theta$
8	α	8	α
9	$\alpha^2+(1+\alpha)\theta$	9	$\alpha^2+(\alpha+\alpha^2)\theta$
10	$1+\alpha$	10	$1+\alpha$
11	$\alpha+\alpha^2+(1+\alpha+\alpha^2)\theta$	11	$\alpha+\alpha^2+(1+\alpha^2)\theta$
12	$1+\alpha+\alpha^2$	12	$1+\alpha+\alpha^2$
13	$1+\alpha^2+\theta$	13	$1+\alpha^2+\alpha\theta$
14	1	14	1
Exp.	$\alpha^2+(1+\alpha^2)\theta$	Exp.	$\alpha+(\alpha+\alpha^2)\theta$
1	$\alpha^2+(1+\alpha^2)\theta$	1	$\alpha+(\alpha+\alpha^2)\theta$
2	$\alpha+\alpha^2$	2	α^2
3	$1+\alpha^2+(1+\alpha)\theta$	3	$1+\alpha+(1+\alpha^2)\theta$
4	α	4	$\alpha+\alpha^2$
5	$1+\alpha+\theta$	5	$1+\alpha+\alpha^2+\theta$
6	$1+\alpha+\alpha^2$	6	$1+\alpha^2$
7	$1+(\alpha+\alpha^2)\theta$	7	$1+(1+\alpha)\theta$
8	α^2	8	α
9	$\alpha+\alpha^2+\alpha\theta$	9	$\alpha^2+(1+\alpha+\alpha^2)\theta$
10	$1+\alpha^2$	10	$1+\alpha$
11	$\alpha+(1+\alpha+\alpha^2)\theta$	11	$\alpha+\alpha^2+\theta$
12	$1+\alpha$	12	$1+\alpha+\alpha^2$
13	$1+\alpha+\alpha^2+\alpha^2\theta$	13	$1+\alpha^2+\alpha^2\theta$
14	1	14	1

Table 2.3: Cyclic Subgroup other than $\mathbb{F}_{2^3}^{\ *}$ of Group of Units in $A\left(2^3,2\right)$

Consequently, each of remaining 42 elements have order 14 and generates a cyclic Group of order 14. But these cyclic Groups are not distinct because each cyclic Group has 6 generators (each finite cyclic Group with three or more elements have even number of generators). Therefore, there exist 7 unique cyclic Groups of order 14. We can also observe that each of these cyclic Group has a generator at the same exponents of a generator and at 7th power of each generator of a unique cyclic Group gives same principal unit element.

Now at the end of this chapter we will compare Subgroup of Group of units of both Galois and Q-GR and after that we will give a general comparison between Galois and Q-GR with the help of flow chart diagram.

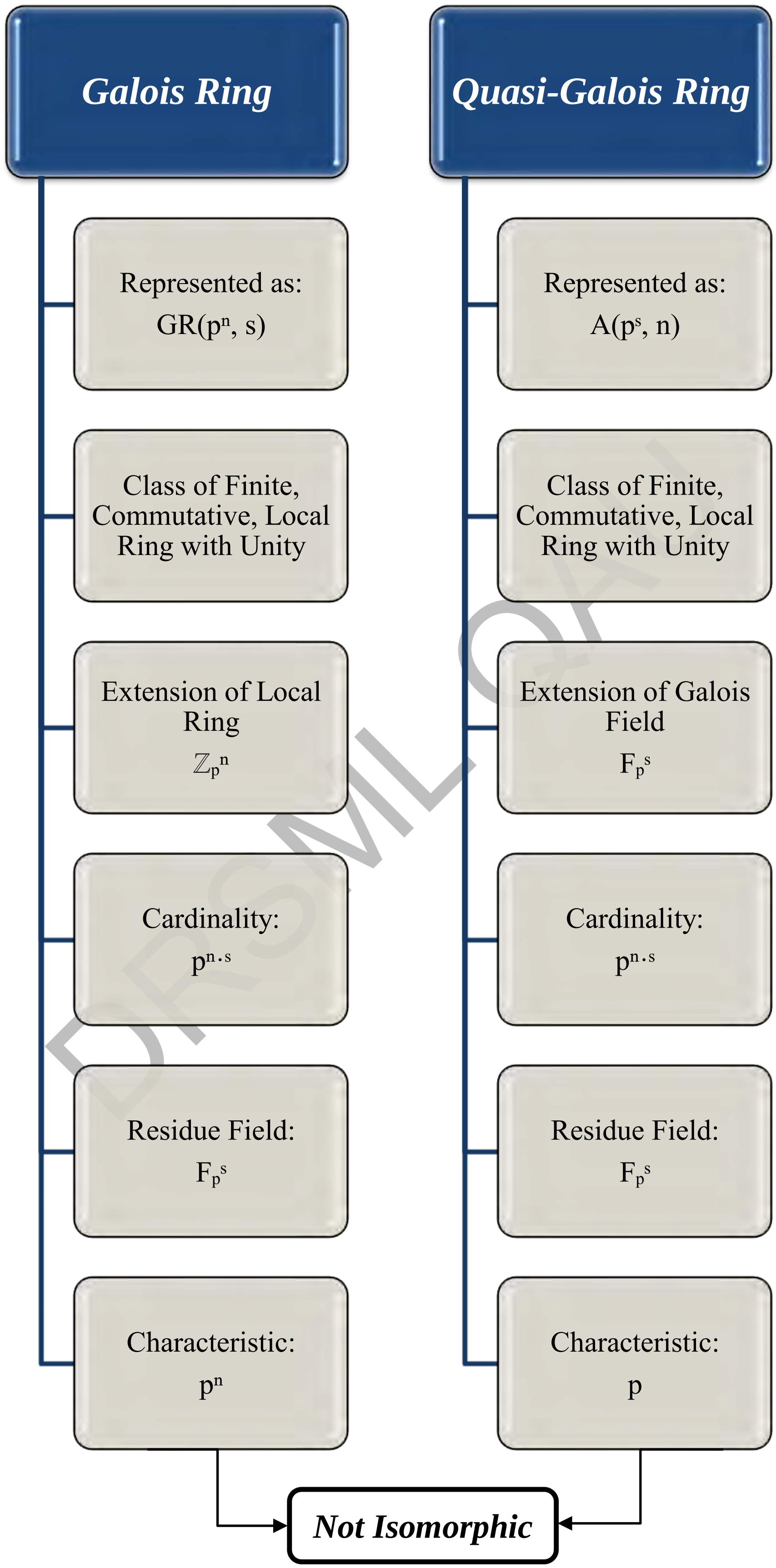
	$U(GR(2^2,3)) \cong G_1 \times G_2$		$U(A(2^3,2)) \cong G_1' \times G_2'$	
	G_1	G_2	G_1'	G_2'
Calculation Method	$f(x) \in \mathbb{Z}_{2^2}[x]$, Such that, $f(\alpha)=0$ $G_1 = <\alpha^p>$, Since, $\lvert\alpha^p\rvert = p^r - 1$.	$1+2GR(2^2,3)$ Where, $2GR(2^2,3)$ is maximal ideal of $GR(2^2,3)$	$F_{2^3}^{\ *} = F_{2^3} - \{0\}$	$1+m(8,2)$ Where, $m(8,2)$ is maximal ideal of $A(2^3,2)$
Calculated Elements	1 $\alpha+2\alpha^2$ α^2 $1+3\alpha$ $1+2\alpha+\alpha^2$ $2+3\alpha+\alpha^2$ $1+3\alpha+3\alpha^2$	1 3 $1+2\alpha$ $1+2\alpha^2$ $3+2\alpha$ $3+2\alpha^2$ $1+2\alpha+2\alpha^2$ $3+2\alpha+2\alpha^2$	1 α α^2 $1+\alpha$ $1+\alpha^2$ $\alpha+\alpha^2$ $1+\alpha+\alpha^2$	1 $1+\theta$ $1+\alpha\theta$ $1+\alpha^2\theta$ $1+(1+\alpha)\theta$ $1+(1+\alpha^2)\theta$ $1+(\alpha+\alpha^2)\theta$ $1+(1+\alpha+\alpha^2)\theta$

Table 2.4: Comparison between Subgroups of Group of Units of Galois and Q-GR

After focus on this comparison, we conclude that if we calculate G_1 first and apply mod 2 on G_1 then we attain G_1' without calculation.

Remarks:

An extensive class of finite, commutative local rings with identity includes the GR and Quasi-GRs as particular examples. These rings are known as finite chain rings because they are finite and their ideals under inclusion form a chain.



Galois Ring
Represented as: $GR(p^n, s)$
Class of Finite, Commutative, Local Ring with Unity
Extension of Local Ring $\mathbb{Z}_{p^n}$
Cardinality: $p^{n.s}$
Residue Field: F_{p^s}
Characteristic: p^n
Quasi-Galois Ring
Represented as: $A(p^s, n)$
Class of Finite, Commutative, Local Ring with Unity
Extension of Galois Field F_{p^s}
Cardinality: $p^{n.s}$
Residue Field: F_{p^s}
Characteristic: p
Not Isomorphic

Chapter # 3

Designing of BCH-Codes over Galois Ring, Quasi-Galois Ring and their Residue Field

In this chapter, we give a transitory overview on designing of BCH-Code over well known finite Commutative local rings that are known as GRs and Q-GRs and their residue field. Further we also associate our outcomes by using a simple example that we debated in the prvious chapter.

Because of its remarkable applications, particularly in the creation of BCH-Codes, Algebraic coding theory has recently become deeply concerned with the configuration of the multiplicative group of units of some finite local commutative rings. Using a multiplicative roup of units of an Galois extension of $\mathbb{Z}_{p^m}$, (Shankar, 1979) has constructed BCH-Code over $\mathbb{Z}_{p^m}$. On the other hand, (De Andrade, 1999) have further protracted this construction of BCH-Code over finite commutative rings with identity. The methodology of specifying a cyclic Subgroup of the Group of Units of an Extension Ring of Finite Commutative Rings has been applied to both construction skills of (Shankar, 1979) and (De Andrade, 1999). The tricky part of this strategy is to first generate the generator polynomial for the BCH-Code by factorizing over the group of units of the applicable extension ring of the provided local ring.

In preceding chapter, we briefly argued Galois and Q-GRs and after discussion we conclude that both Galois and Q-GRs have same residue Field as shown in figure 3.

Our objective is to construct BCH-Code over Galois and Q-GRs. We also construct BCH-Code over residue field of these two rings and after that we will compare our results.

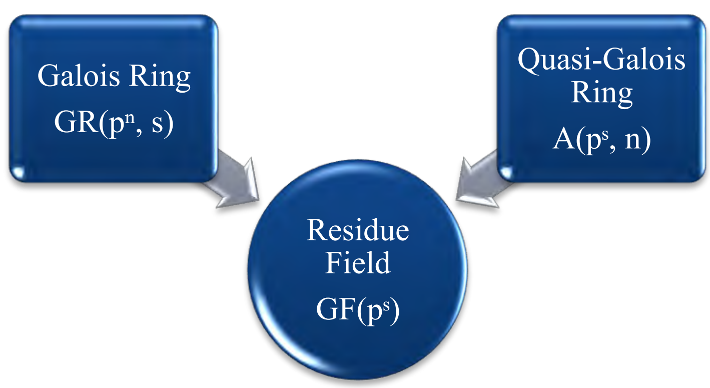


Figure: 3

For this purpose, we will make use of Galois and its comparative Quasi- GR having cardinality 64 that already discussed in the previous chapter. After construction of BCH-Code over this example, we will give a general debate about the comparison between these three cases.

3.1 BCH-Codes over GR:

In the field of theory of algebraic coding, the maximal cyclic subgroup of the group of units of a GR has presumed a remarkable position. At first, (Shankar, 1979) proposed a construction method for the BCH-Code over a local commutative ring $\mathbb{Z}_{p^n}$ based on the maximal cyclic Subgroup G_s of the Group of units of a Galois extension ring $GR(p^n, s)$ of $\mathbb{Z}_{p^n}$. We can acquire G_s by mod-*p* reduction map from the ring $\mathbb{Z}_{p^n}$ to its residue field $\mathbb{Z}_p$.

3.1.1 Generator Polynomial of BCH-Codes using Maximal Cyclic Subgroup:

In case of GR, the generator polynomial of BCH-Codes of length *n* is defined as:

$$g(x) = lcm\{m_i(x) | i = c, c+1, ..., c+d-2\},$$

Where, $m_i(x)$ are minimal polynomials corresponding to each ω^i, for $i = 1, 2, 3, ..., d-1$ by taking $c = 1$. The parity-check matrix of the BCH-Code having the generator polynomial $g(x)$ is of the form:

$$H = \begin{bmatrix} 1 & \omega^c & \omega^{2c} & \cdots & \omega^{(n-1)c} \\ 1 & \omega^{c+1} & \omega^{2(c+1)} & \cdots & \omega^{(n-1)(c+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{c+d-2} & \omega^{2(c+d-2)} & \cdots & \omega^{(n-1)(c+d-2)} \end{bmatrix}$$

Evenly, code C is null space of this matrix.

The following steps are used to construct generator polynomial of n-length BCH-Code over GR.

- Create the maximal cyclic Subgroup of order *n*.
- Compute the minimal polynomials for each design distance.
- Calculate the LCM of all the minimum polynomials.

$GR(2^2, 3)$ that is defined as:

$$GR(2^2, 3) = \frac{\mathbb{Z}_{2^2}[x]}{< f(x) >}$$

Where, $f(x) \in \mathbb{Z}_4[x]$ is a monic, irreducible polynomial of degree 3.

Here, $\mathbb{Z}_2$ is a base field and $x^3 + x + 1$ is a monic irreducible polynomial over $\mathbb{Z}_2[x]$. Now by using Hensel's Lemma we get a monic irreducible polynomial of degree 3 over $\mathbb{Z}_4[x]$.

Since, $$p = 2,\ n = 2,\ s = 3$$

$$x^3+\left(2^2-2+0\right)x^2+\left(2^2-2+1\right)x+\left(2^2-2+1\right)=x^3+2x^2+3x+3\in\mathbb{Z}_4[x]$$

$f\left(x\right)=x^3+2x^2+3x+3\in\mathbb{Z}_4[x]$ is required monic, irreducible polynomial.

More precisely,

$$GR\left(2^2,3\right)=\left\{\sum_{j=0}^{2}c_j\alpha^j\,\middle|\,c_j\in\mathbb{Z}_4\right\}$$
$$=\left\{c_o+c_1\alpha+c_2\alpha^2\,\middle|\,c_o,c_1,c_2\in\mathbb{Z}_4\right\}$$

Where, α satisfy the relation $f\left(\alpha\right)=\alpha^3+2\alpha^2+3\alpha+3=0$. Using this relation, by taking exponents of α , we get the following table.

Exp.	Polynomial	String mod4
1	α	010
2	α^2	100
3	$1+\alpha+2\alpha^2$	211
4	$2+3\alpha+\alpha^2$	132
5	$1+3\alpha+\alpha^2$	131
6	$1+2\alpha+\alpha^2$	121
7	$1+2\alpha$	021
8	$\alpha+2\alpha^2$	210
9	$2+2\alpha+\alpha^2$	122
10	$1+3\alpha$	031
11	$\alpha+3\alpha^2$	310
12	$3+3\alpha+3\alpha^2$	333
13	$3+2\alpha+\alpha^2$	123
14	1	001

Table: 3.1

Here, order of α is 14. Thus the resultant maximal cyclic Subgroup G_7 is generated by $\beta=\alpha^2$.

$$G_7=\left\{\beta,\beta^2,\beta^3,\beta^4,\beta^5,\beta^6,\beta^7=1\right\}$$

So, β is a primitive 7th root of unity in G_7 . If we take design distance $d=5$, we need the minimal polynomials of β^i for $i=1,2,3,4$.

Consider $m_1(x)$ is the minimal polynomial of β, then from theorem 1.2, β, β^2, β^4 have same minimal polynomial $m_1(x)$ which is given as:

$$\begin{aligned} m_1(x) &= (x-\beta)(x-\beta^2)(x-\beta^4) \\ &= x^3 - (\beta^4+\beta^2+\beta)x^2 + (\beta^6+\beta^5+\beta^3)x - \beta^7 \\ &= x^3 - 2x^2 + x - 1 \\ &= x^3 + 2x^2 + x + 3, \qquad \bmod 4 \end{aligned}$$

Let $m_2(x)$ be the minimal polynomial of β^3. Then $\beta^3, \beta^6, \beta^{12}, \ldots$ all have same minimal polynomial $m_2(x)$. Using the relation $\beta^7 = 1$, we see that the roots of $m_2(x)$ are $\beta^3, \beta^5, \beta^6$.

Hence,

$$\begin{aligned} m_2(x) &= (x-\beta^3)(x-\beta^5)(x-\beta^6) \\ &= x^3 - (\beta^3+\beta^5+\beta^6)x^2 + (\beta+\beta^2+\beta^4)x - \beta^7 \\ &= x^3 - x^2 + 2x - 1 \\ &= x^3 + 3x^2 + 2x + 3, \qquad \bmod 4 \end{aligned}$$

Hence generator polynomial $g(x)$ of desired BCH-Codes is given as:

$$\begin{aligned} g(x) &= lcm\{m_i(x) \mid i = 1,2,3,4\} \\ &= m_1(x) \cdot m_2(x) \\ &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \qquad, r = 6 \end{aligned}$$

Dimension of code C is $k = n - r = 7 - 6 = 1$. Hence the cyclic code C generated by $g(x)$ over G_7 in $GR(2^2,3)$ has dimension 1.

C is [7,1] primitive narrow sense BCH-Codes of design distance 5 over the maximal cyclic Subgroup of Group of units in $GR(2^2,3)$.

Furthermore, parity-check matrix of this code is given as

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^8 & \beta^{10} & \beta^{12} \end{bmatrix}$$

3.2 BCH-Codes over Residue Field:

Consider a $GR(2^2,3)$ and Q-GR $A(2^3,2)$, their residue field is given as:

$$GF(2^3) = \frac{\mathbb{Z}_2[x]}{< p(x) >} = \mathbb{F}_{2^3}$$

Where, $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ is a primitive, irreducible polynomial of degree 3 over $\mathbb{Z}_2[x]$. First we construct BCH-Codes over this residue field.

BCH-Code constructed on this residue field are binary. So, according to the definition of BCH-Code, we have:

$q = 2$ (binary code) and $m = 3$, Take $c = 1$ (Narrow sense BCH-Codes)

$$\Rightarrow\ n = q^m - 1 = 2^3 - 1 = 7$$

So, length of required BCH-Code over $\mathbb{F}_{2^3}$ will be 7.

We can represent $\mathbb{F}_{2^3}$ as:

$$\mathbb{F}_{2^3} = \{c_o + c_1\alpha + c_2\alpha^2 \mid c_o, c_1, c_2 \in \mathbb{F}_2\}$$

Where, α satisfy the relation, $\alpha^2 + \alpha + 1 = 0$. Using this relation, by taking exponents of α, we obtain the following table:

Exp.	Polynomial	String mod2
1	α	010
2	α^2	100
3	$1+\alpha$	011
4	$\alpha+\alpha^2$	110
5	$1+\alpha+\alpha^2$	111
6	$1+\alpha^2$	101
7	1	001

Table: 3.2

So, α is 7th root of unity in $\mathbb{F}_{2^3}$ and $p(x)$ is the minimal polynomial of α. If we take design distance $d = 5$, we prerequisite the minimal polynomials of α^i for $i = 1,2,3,4$.

From theorem 1.2, $\alpha, \alpha^2, \alpha^4$ have identical minimal polynomial $m_1(x)$.

$$\begin{aligned} m_1(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^4) \\ &= x^3 + x + 1 \end{aligned}$$

Let $m_2(x)$ be the minimal polynomial of α^3. Then $\alpha^3, \alpha^6, \alpha^{12}, \ldots$ all have same minimal polynomial $m_2(x)$. Using the relation $\alpha^7 = 1$, we see that the roots of $m_2(x)$ are $\alpha^3, \alpha^5, \alpha^6$.

Hence,

$$\begin{aligned} m_2(x) &= (x-\alpha^3)(x-\alpha^5)(x-\alpha^6) \\ &= x^3 - (\alpha^3 + \alpha^5 + \alpha^6)x^2 + (\alpha + \alpha^2 + \alpha^4)x - 1 \\ &= x^3 + x^2 + 1, \qquad \bmod 2 \end{aligned}$$

Hence generator polynomial $g(x)$ of desired BCH-Codes is given as:

$$\begin{aligned} g(x) &= lcm\{m_i(x) \mid i = 1,2,3,4\} \\ &= m_1(x) \cdot m_2(x) \\ &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \qquad , r = 6 \end{aligned}$$

Dimension of code C is $k = n - r = 7 - 6 = 1$. Hence the cyclic code C generated by $g(x)$ in $\mathbb{F}_2[x]_7$ has dimension 1.

C is $[7,1]$ primitive narrow sense BCH-Codes of design distance 3 over the residue field $\mathbb{F}_{2^3}$.

Furthermore, parity-check matrix of this code is specified as

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \end{bmatrix}$$

3.3 BCH-Codes over Q-GR

Before designing BCH-Codes over Q-GRs, it is necessary to specify the Galois extension of Q-GRs in order to factorize $x^n - 1$ over the group of units of the applicable extension ring of the known local ring (Q-GR) and after that build the generator polynomial for BCH-Code.

3.3.1 Galois extension of Q-GR ($A(p^s, n)$)

As Q-GRs ($A(p^s, n)$, where *p* be a prime and *n* and *s* be any positive integers) are class of finite local rings with distinctive maximal ideal $m(p^s, n)$ and having residue field $K = A(p^s, n)/m(p^s, n) = GF(p^s)$.

Consider, $\pi : A(p^s, n)[x] \to K[x]$ be a natural projection map where $A(p^s, n)[x]$ indicates ring of polynomials in single variable x and coefficients from $A(p^s, n)$, defined as $\pi(a(x)) = \bar{a}(x)$. If we take $f(x)$ as a monic polynomial of degree *m* such that $\pi(f(x))$ is irreducible over *K* (residue field) then $f(x)$ is irreducible over $A(p^s, n)$.

The ring $R = A(p^s, n)[x]/\langle f(x) \rangle$ is Galois extension of Q-GR $A(p^s, n)$ and consist of the collection of polynomial of residue classes in variable x over $A(p^s, n)$ modulo a polynomial $f(x)$.

Elements of $R = A(p^s, n)[x]/\langle f(x) \rangle$ are of the form:

$$R = \frac{A(p^s, n)[x]}{\langle f(x) \rangle} = \left\{ \sum_{i=0}^{m-1} c_i \alpha^i \mid c_i \in A(p^s, n) \right\}$$

Where, α is the root of $f(x)$ (i.e. $f(\alpha) = 0$).

Let R^* be the multiplicative abelian Group of units of $R = A(p^s, n)[x]/\langle f(x) \rangle$ and consequently can be stated as direct product of Subgroups and cyclic Subgroup of R^* is denoted by G_s. Unit elements of *R* can be calculated as fallows

$$R^* = \left\{ x = c_o + c_1\alpha + .. + c_{m-1}\alpha^{m-1} \in R \mid at\,least\,one\,of\; c_i \in U\left(A(p^s, m)\right)\; for\; i \in \{0,1,...,m-1\} \right\}$$

Where, $U\left(A\left(p^s,n\right)\right)$ indicates unit elements of Q-GR $A\left(p^s,n\right)$. On the other side Nil-radical (set of all nilpotent elements of *R*) of *R* symbolized by $Nil\left(R\right)$ and defined as

$$Nil\left(R\right)=\left\{c_o+c_1\alpha+\ldots+c_{m-1}\alpha^{m-1} \mid \forall\ c_o,c_1,\ldots,c_{m-1}\in Nil\left(A\left(p^s,n\right)\right)\right\}$$

Where, $Nil\left(A\left(p^s,n\right)\right)$ denotes nil-radical of Q-GR $A\left(p^s,n\right)$.

Similarly,

$$K'=\frac{\left(A\left(p^s,n\right)/m\left(p^s,n\right)\right)[x]}{\left\langle \pi\left(f\left(x\right)\right)\right\rangle}=\frac{K[x]}{\left\langle \pi\left(f\left(x\right)\right)\right\rangle}$$

is extension of residue field of $A\left(p^s,n\right)$ having cardinality p^{ms} and K'^* be the multiplicative Group of units in K'.

Example 1:

BCH-Codes over $A(2,2)$

- **Finding elements of $A(2,2)$:**

We have

$$\begin{aligned} A\left(2,2\right) &= \frac{F_2\left[y\right]}{<y^2>} \\ &= \left\{\sum_{i=0}^{1} a_i\theta^i \mid a_i\in F_2\right\}, \quad where,\ \theta^2=0 \bmod 2 \\ &= \left\{a_o+a_1\theta \mid a_o,a_1\in F_2=\left\{0,1\right\}\right\} \\ &= \left\{0,\ 1,\ \theta,\ 1+\theta\right\} \end{aligned}$$

Here,

$$U\left(A\left(2,2\right)\right)=\left\{1,\ 1+\theta\right\}$$

- **Calculate Basic irreducible polynomial in $A(2,2)[x]$:**

Since, residue field of $A\left(2,2\right)$ is $\mathbb{F}_2$.

$$\pi : A(2,2)[x] \to \mathbb{F}_2[x]$$

Let $f(x) \in A(2,2)[x]$ be a monic polynomial of degree 3.

$$f(x) = x^3 + a_1 x + a_o \quad where,\ a_o, a_1 \in A(2,2)$$

If we take, $a_o = 1,\ a_1 = 1+\theta$

$$\Rightarrow \quad f(x) = x^3 + (1+\theta)x + 1$$

But $\pi(f) = x^3 + x + 1$ is monic irreducible polynomial over $\mathbb{F}_2$. Now we check irreducibility of $f(x)$ over $A(2,2)$.

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 1 + (1+\theta) + 1 = 1 + \theta \neq 0\ , && \text{mod}\,2 \\ f(\theta) &= (1+\theta)\theta + 1 = 1 + \theta \neq 0\ , && \text{mod}\,2 \\ f(1+\theta) &= (1+\theta)^3 + (1+\theta)^2 + 1 = 1 + \theta \neq 0\ , && \text{mod}\,2 \end{aligned}$$

This shows that $f(x)$ is basic irreducible polynomial in $A(2,2)[x]$.

- **Define extension of $A(2,2)$ w.r.t calculated irreducible polynomial:**

Extension of Q-GR $A(2,2)$ of degree 3 is defined as the ring

$$R = \frac{A(2,2)[x]}{\langle f(x) \rangle} = \left\{ \sum_{i=0}^{2} c_i \alpha^i \mid c_i \in A(2,2) \right\}$$

Where, $f(x) = x^3 + (1+\theta)x + 1$ is basic irreducible polynomial over $A(2,2)$ and $f(\alpha) = \alpha^3 + (1+\theta)\alpha + 1 = 0$.

- **Maximal Cyclic Subgroup of R^*:**

Since, $f(x) = x^3 + (1+\theta)x + 1$ is basic irreducible polynomial over $A(2,2)$ and α be the root of $f(x)$.

$$\begin{aligned} &\Rightarrow \quad \alpha^3 + (1+\theta)\alpha + 1 = 0 \\ &\Rightarrow \quad \alpha^3 = 1 + (1+\theta)\alpha\ , \qquad \text{mod}\,2 \end{aligned}$$

Thus by taking successive powers of α we get the following result:

Exp.	Polynomial	Exp.	Polynomial
1	α	8	$\alpha+\theta\alpha^2$
2	α^2	9	$\theta+\theta\alpha+\alpha^2$
3	$1+(1+\theta)\alpha$	10	$1+\alpha+\theta\alpha^2$
4	$\alpha+(1+\theta)\alpha^2$	11	$\theta+(1+\theta)\alpha+\alpha^2$
5	$(1+\theta)+\alpha+\alpha^2$	12	$1+\alpha+(1+\theta)\alpha^2$
6	$1+\alpha^2$	13	$(1+\theta)+\alpha^2$
7	$1+\theta\alpha$	14	1

Table: 1

Here, order of α is 14. As a result the corresponding maximal cyclic Subgroup G_7 isomorphic to residue field $K=\mathbb{F}_2[x]/\langle\pi(f(x))\rangle=\mathbb{F}_2[x]/\langle x^3+x+1\rangle$ is generated by $\gamma=\alpha^2$.

$$G_7=\{\gamma,\,\gamma^2,\,\gamma^3,\,\gamma^4,\,\gamma^5,\,\gamma^6,\,\gamma^7=1\}$$

$$\Rightarrow\quad G_7=\{\alpha^2,\,\alpha+(1+\theta)\alpha^2,\,1+\alpha^2,\,\alpha+\theta\alpha^2,\,1+\alpha+\theta\alpha^2,\,1+\alpha+(1+\theta)\alpha^2,\,1\}$$

- **Generator polynomial of BCH-Codes over** $R=A(2,2)[x]/\langle f(x)\rangle$

As, γ is a primitive 7^{th} root of unity in G_7. If we take design distance $d=5$, we need the minimal polynomials of γ^i for $i=1,2,3,4$.

Consider $m_1(x)$ is the minimal polynomial of γ, then from theorem 1.2, γ,γ^2,γ^4 have same minimal polynomial $m_1(x)$ which is given as:

$$\begin{aligned}m_1(x)&=(x-\gamma)(x-\gamma^2)(x-\gamma^4)\\&=x^3-(\gamma^4+\gamma^2+\gamma)x^2+(\gamma^6+\gamma^5+\gamma^3)x-\gamma^7\\&=x^3-(0)x^2+x-1\\&=x^3+x+1, \qquad \bmod 2\end{aligned}$$

Let $m_2(x)$ be the minimal polynomial of γ^3. Then $\gamma^3,\gamma^6,\gamma^{12},\ldots$ all have same minimal polynomial $m_2(x)$. Using the relation $\gamma^7=1$, we see that the roots of $m_2(x)$ are $\gamma^3,\gamma^5,\gamma^6$.

Hence,

$$\begin{aligned} m_2(x) &= (x-\gamma^3)(x-\gamma^5)(x-\gamma^6) \\ &= x^3-(\gamma^3+\gamma^5+\gamma^6)x^2+(\gamma+\gamma^2+\gamma^4)x-\gamma^7 \\ &= x^3-x^2+(0)x-1 \\ &= x^3+x^2+1\,, \qquad \bmod 2 \end{aligned}$$

Hence generator polynomial $g(x)$ of desired BCH-Codes is given as:

$$\begin{aligned} g(x) &= lcm\{m_i(x) \mid i=1,2,3,4\} \\ &= m_1(x)\cdot m_2(x) \\ &= x^6+x^5+x^4+x^3+x^2+x+1 \qquad ,r=6 \end{aligned}$$

Here, $q=2$ (binary code) and $m=3$, Take $c=1$ (Narrow sense BCH-Codes)

$$\Rightarrow\; n=q^m-1=2^3-1=7$$

So, length of required BCH-Code over $R=A(2,2)[x]/\langle f(x)\rangle$ will be 3.

Dimension of code C is $k=n-r=7-6=1$. Hence the cyclic code C generated by $g(x)$ over G_7 in $R=A(2,2)[x]/\langle f(x)\rangle$ has dimension 1.

C is [7,1] primitive narrow sense BCH-Codes of design distance 5 over the maximal cyclic Subgroup of Group of units in $R=A(2,2)[x]/\langle f(x)\rangle$.

Example 2:

BCH-Codes over $A(2,3)$

- **Finding elements of $A(2,3)$:**

We have

$$\begin{aligned} A(2,3) &= \frac{F_2[y]}{<y^3>} \\ &= \left\{ \sum_{i=0}^{2} a_i\theta^i \mid a_i \in F_2 \right\} \quad where,\ \theta^3 = 0 \bmod 2 \\ &= \left\{ a_o + a_1\theta + a_2\theta^2 \mid a_i \in F_2 = \{0,1\} \right\} \\ &= \left\{ 0,\ 1,\ \theta,\ 1+\theta,\ \theta^2,\ 1+\theta^2,\ \theta+\theta^2,\ 1+\theta+\theta^2 \right\} \end{aligned}$$

Here,

$$U\left(A(2,3)\right) = \left\{ 1,\ 1+\theta,\ 1+\theta^2,\ 1+\theta+\theta^2 \right\}$$

- **Calculate Basic irreducible polynomial in $A(2,3)[x]$:**

Since residue field of $A(2,3)$ is $\mathbb{F}_2$.

$$\pi : A(2,3)[x] \to \mathbb{F}_2[x]$$

Let $f(x) \in A(2,3)[x]$ be a monic polynomial of degree 2.

$$f(x) = x^2 + a_1x + a_o \quad where,\ a_o, a_1 \in A(2,3)$$

If we take, $a_o = 1,\ a_1 = 1+\varphi$

$$\Rightarrow \quad f(x) = x^2 + (1+\theta)x + 1$$

But $\pi(f) = x^2 + x + 1$ is monic irreducible polynomial over $\mathbb{F}_2$. Now we check irreducibility of $f(x)$ over $A(2,3)$.

$$f(0)=1$$
$$f(1)=1+(1+\theta)+1=1+\theta\neq 0\ , \qquad \bmod 2$$
$$f(\theta)=\theta^2+(1+\theta)\theta+1=1+\theta\neq 0\ , \qquad \bmod 2$$
$$f(\theta^2)=\theta^4+(1+\theta)^2+1=1+\theta^2\neq 0\ , \qquad \theta^3=0,\bmod 2$$
$$f(1+\theta)=(1+\theta)^2+(1+\theta)^2+1=1\neq 0\ , \qquad \bmod 2$$
$$f(1+\theta^2)=(1+\theta^2)^2+(1+\theta)(1+\theta^2)+1=1+\theta+\theta^2\neq 0\ , \qquad \theta^3=0,\bmod 2$$
$$f(\theta+\theta^2)=(\theta+\theta^2)^2+(1+\theta)(\theta+\theta^2)+1=1+\theta+\theta^2\neq 0\ , \qquad \theta^3=0,\bmod 2$$
$$f(1+\theta+\theta^2)=(1+\theta+\theta^2)^2+(1+\theta)(1+\theta+\theta^2)+1=1+\theta^2\neq 0\ , \qquad \theta^3=0,\bmod 2$$

This verify that $f(x)$ is basic irreducible polynomial in $A(2,3)[x]$.

- **Define extension of $A(2,3)$ w.r.t calculated irreducible polynomial:**

Extension of Q-GR $A(2,3)$ of degree 2 is defined as the ring

$$R=\frac{A(2,3)[x]}{\langle f(x)\rangle}=\left\{\sum_{i=0}^{1}c_i\alpha^i \mid c_i\in A(2,3)\right\}$$

Where, $f(x)=x^2+(1+\theta)x+1$ is basic irreducible polynomial over $A(2,3)$ and $f(\alpha)=\alpha^2+(1+\theta)\alpha+1=0$.

- **Multiplicative Group of Units in** $R = A(2,3)[x]/\langle f(x)\rangle$**:**

Let R^* be the multiplicative Group of units of *R*. Elements of R^* are given as:

S. No.	Unit element	Order	S. No.	Unit element	Order
1.	1	1	25.	$\theta+\alpha$	12
2.	$1+\theta$	4	26.	$\theta+(1+\theta)\alpha$	12
3.	$1+\theta^2$	2	27.	$\theta+(1+\theta^2)\alpha$	12
4.	$1+\varphi+\varphi^2$	4	28.	$\theta+(1+\theta+\theta^2)\alpha$	12
5.	α	12	29.	$\theta^2+\alpha$	12
6.	$(1+\theta)\alpha$	6	30.	$\theta^2+(1+\theta)\alpha$	6
7.	$(1+\theta^2)\alpha$	12	31.	$\theta^2+(1+\theta^2)\alpha$	12
8.	$(1+\varphi+\varphi^2)\alpha$	6	32.	$\theta^2+(1+\theta+\theta^2)\alpha$	3
9.	$1+\alpha$	8	33.	$(\theta+\theta^2)+\alpha$	12
10.	$1+(1+\theta)\alpha$	6	34.	$(\theta+\theta^2)+(1+\theta)\alpha$	6
11.	$1+(1+\theta^2)\alpha$	12	35.	$(\theta+\theta^2)+(1+\theta^2)\alpha$	12
12.	$1+(1+\theta+\theta^2)\alpha$	6	36.	$(\theta+\theta^2)+(1+\theta+\theta^2)\alpha$	12
13.	$(1+\theta)+\alpha$	12	37.	$1+\theta\alpha$	4
14.	$(1+\theta)+(1+\theta)\alpha$	12	38.	$(1+\theta)+\theta\alpha$	4
15.	$(1+\theta)+(1+\theta^2)\alpha$	12	39.	$(1+\theta^2)+\theta\alpha$	4
16.	$(1+\theta)+(1+\theta+\theta^2)\alpha$	6	40.	$(1+\theta+\theta^2)+\theta\alpha$	4
17.	$(1+\theta^2)+\alpha$	12	41.	$1+\theta^2\alpha$	2
18.	$(1+\theta^2)+(1+\theta)\alpha$	6	42.	$(1+\theta)+\theta^2\alpha$	4
19.	$(1+\theta^2)+(1+\theta^2)\alpha$	12	43.	$(1+\theta^2)+\theta^2\alpha$	2
20.	$(1+\theta^2)+(1+\theta+\theta^2)\alpha$	3	44.	$(1+\theta+\theta^2)+\theta^2\alpha$	4
21.	$(1+\theta+\theta^2)+\alpha$	12	45.	$1+(\theta+\theta^2)\alpha$	4
22.	$(1+\theta+\theta^2)+(1+\theta)\alpha$	12	46.	$(1+\theta)+(\theta+\theta^2)\alpha$	4
23.	$(1+\theta+\theta^2)+(1+\theta^2)\alpha$	12	47.	$(1+\theta^2)+(\theta+\theta^2)\alpha$	4
24.	$(1+\theta+\theta^2)+(1+\theta+\theta^2)\alpha$	12	48.	$(1+\theta+\theta^2)+(\theta+\theta^2)\alpha$	4

Table 2: Multiplicative Group of units of $R = A(2,3)[x]/\langle f(x)\rangle$

- **Maximal Cyclic Subgroup of** R^***:**

Since, $f(x)=x^2+(1+\theta)x+1$ is basic irreducible polynomial over $A(2,3)$ and α be the root of $f(x)$.

$$\Rightarrow \quad \alpha^2+(1+\theta)\alpha+1=0$$
$$\Rightarrow \quad \alpha^2=1+(1+\theta)\alpha\ , \qquad \bmod 2$$

Thus by taking successive powers of α we get the following result:

Exp.	Polynomial	Exp.	Polynomial
1	α	7	$(1+\theta^2)\alpha$
2	$1+(1+\theta)\alpha$	8	$(1+\theta^2)+(1+\theta+\theta^2)\alpha$
3	$(1+\theta)+\theta^2\alpha$	9	$(1+\theta+\theta^2)+\theta^2\alpha$
4	$\theta^2+(1+\theta+\theta^2)\alpha$	10	$\theta^2+(1+\theta)\alpha$
5	$(1+\theta+\theta^2)+(1+\theta^2)\alpha$	11	$(1+\theta)+\alpha$
6	$1+\theta^2$	12	1

Table: 3

Here, order of α is 12. Consequently the resultant maximal cyclic Subgroup G_3 isomorphic to residue field $K=\mathbb{F}_2[x]/\langle\phi(f(x))\rangle=\mathbb{F}_2[x]/\langle x^2+x+1\rangle$ is generated by $\gamma=\alpha^4$.

$$G_3=\{\gamma,\gamma^2,\gamma^3=1\}$$
$$\Rightarrow \quad G_3=\{\theta^2+(1+\theta+\theta^2)\alpha,\ (1+\theta^2)+(1+\theta+\theta^2)\alpha,\ 1\}$$

- **Generator polynomial of BCH-Codes over** $R=A(2,3)[x]/\langle f(x)\rangle$:

As, γ is a primitive cube root of unity in G_3. If we take design distance $d=3$, we need the minimal polynomials of γ^i for $i=1,2$.

Consider $m_1(x)$ is the minimal polynomial of γ, then from theorem 1.2, γ,γ^2 have same minimal polynomial $m_1(x)$ which is given as:

$$m_1(x)=(x-\gamma)(x-\gamma^2)$$
$$=x^2+x+1$$

Hence generator polynomial $g(x)$ of desired BCH-Codes is given as:

$$\begin{aligned} g(x) &= lcm\{m_i(x) \mid i = 1,2\} \\ &= m_1(x) \\ &= x^2 + x + 1 \qquad , r = 2 \end{aligned}$$

Here, $q = 2$ (binary code) and $m = 2$, Take $c = 1$ (Narrow sense BCH-Codes)

$$\Rightarrow \; n = q^m - 1 = 2^2 - 1 = 3$$

So, length of required BCH-Code over $R = A(2,3)[x]/\langle f(x)\rangle$ will be 3.

Dimension of code C is $k = n - r = 3 - 2 = 1$. Hence the cyclic code C generated by $g(x)$ over G_3 in $A(2,3)$ has dimension 1.

C is [3,1] primitive narrow sense BCH-Codes of design distance 3 over the maximal cyclic Subgroup of Group of units in *R*.

Conclusion:

In this section we will give a comparison of BCH-Codes over Galois rings and Q-GRs. For this we will give a comparative Galois ring $GR(2^2,3)$ to the above mentioned Example 1 and compare the BCH-codes of similar design distance as constructed above.

we have attained BCH-codes of same length and dimension (therefore similar Code rate) in both cases but in case of $R = A(2,2)[x]/\langle f(x)\rangle$ codewords of calculated BCH-codes are elements of Q-GR $A(2,2)$ and in case of $GR(2^2,3)$, codewords of calculated BCH-Codes are from $\mathbb{Z}_4$.

Chapter # 4

Construction of S-Box

After designing of BCH-Codes over GR, Q-GR and their residue field, we are going to discuss a crucial topic in Algebraic cryptography that is designing of Substitution Box (S-Box). In this chapter, we will design S-box over Sylow p Subgroup of Group of units of GR by using a new concept of Affine map. Before construction of S-box we will mention some basic information about S-Box.

4.1 Substitution Boxes (S-Box):

Substitution box are one amongst the crucial parts within a block cipher and play an important role in their security for being the only non-linear part of the system. The block ciphers are designed on the basis of Shanon's theory of confusion and diffusion which is also implemented in Substitution-permutation network (SPN). Such networks are basically consisting of a number of mathematical operations which are linked together. It takes as input a block of plaintext, a key and apply many rounds of Substitution-box or permutation box to get desired cipher text. The inverse of S-box or P-box is implemented in inverse way with the same key for decryption. The Data Encryption Standard (DES) and Advanced Encryption Standard (DES) cryptosystems are versions of SPN. S-boxes are essentially look up tables for vectorial Boolean functions. An S-box accepts a small block of bits and replaces it with another small block of bits. To ensure proper decryption, the Substitution should be one-by-one. In general, an S-box converts m-bits input to n-bits outputs. Thus, a $[m\times n]$ S-box can be regarded of as a lookup table having 2^m words each containing n-bits. The output length can be just like the input length, as in AES, but it can also be different, as in DES. To ensure the strength of a cryptosystem, a Substitution box should be developed in a way that every output bit is dependent on each input bit.

Why We Study S-Box?

The only nonlinear part of a SPN as a cryptosystem is the S-Box because S-Box is composed of highly nonlinear Boolean functions. Without them, adversaries would compromise the system with ease. The desirable properties of an S-Box are its design simplicity, fast encryption and decryption speed and resistance against known crypt-analysis attacks. The criteria of a good S-Box will encounter most of the standards set by the national institute of standards and technology.

4.2 Galois Ring $GR(2^2,8)$:

As in chapter 2 we already discuss GRs. Now in this chapter, for the construction of S-Box., we will make use of a specific GR that have Sylow p-Subgroup containing exactly 256 elements.

In case of $p=2,\ n=2,\ s=8$, $\quad R=GR(2^2,8)$

In this case, $\left|GR\left(2^2,8\right)\right|=65,536$

And $\left|U\left(GR\left(2^2,8\right)\right)\right|=65,280$

$$\left|GR\left(p^n,s\right)\right|=p^{ns}$$

$$\left|U\left(GR\left(p^n,s\right)\right)\right|=p^{ns}-p^{s(n-1)}$$

$$U(R)=U(GR(2^2,8))\cong G_1\times G_2$$

Where, $|G_1|=2^8-1=255$ and $|G_2|=2^{(2\times 8)-8}=256$

$$|G_1|=p^s-1$$

$$|G_2|=p^{s(n-1)}$$

Remaining 256 elements are nilpotent elements.

Elements of $GR\left(2^2,8\right)$:

$$GR\left(2^2,8\right)=\frac{\mathbb{Z}_{2^2}[x]}{<f(x)>}=\left\{\sum_{i=0}^{7}c_i\alpha^i \mid c_i\in\mathbb{Z}_4\right\}$$

$$=\left\{c_o+c_1\alpha+c_2\alpha^2+c_3\alpha^3+c_4\alpha^4+c_5\alpha^5+c_6\alpha^6+c_7\alpha^7 \mid c_o,c_1,\ldots,c_7\in\mathbb{Z}_4\right\}$$

Where, $f(x)\in\mathbb{Z}_4[x]$ is monic irreducible polynomial of degree 8 such that $f(\alpha)=0$.

Maximal ideal of GR $GR\left(2^2,8\right)$:

Maximal ideal of $GR\left(2^2,8\right)$ is $2GR\left(2^2,8\right)$. Elements in maximal ideal can be uniquely expressed as:

$$2GR\left(2^2,8\right)=\left\{\sum_{i=0}^{7}c_i\alpha^i \mid c_i\in 2\mathbb{Z}_4\right\}$$

$$=\left\{c_o+c_1\alpha+c_2\alpha^2+c_3\alpha^3+c_4\alpha^4+c_5\alpha^5+c_6\alpha^6+c_7\alpha^7 \mid c_o,c_1,\ldots,c_7\in 2\mathbb{Z}_4\right\}$$

From Table 2.3 we can calculate Subgroups of Group of units of GR $GR\left(2^2,8\right)$ as follows:

$U(GR(2^2,8)) \cong G_1 \times G_2$	
G_1	G_2 *or* S_p
$f\left(x\right) \in \mathbb{Z}_{2^2}[x]$, Such that, $f\left(\alpha\right)=0$ $G_1 = <\alpha^2>$, Since, $\left\|\alpha^2\right\| = 2^8 - 1$.	$1+2GR\left(2^2,8\right)$ Where, $2GR\left(2^2,8\right)$ is maximal ideal of $GR\left(2^2,8\right)$

Table: 4.1

Here, G_2 is our required Sylow p-Subgroup of Group of units of GR $GR\left(2^2,8\right)$ that can also be expressed as S_p. All elements of S_p are mentioned in following table and also conversion of each element to its 16-bit binary form, decimal form and hexadecimal form.

Sr. No.	$x \in S_p$	**16-bit Binary form**	**Decimal Form**	**Hexadecimal Form**
1.	00000001	0000000000000001	1	1
2.	20000001	1000000000000001	32769	8001
3.	02000001	0010000000000001	8193	2001
4.	22000001	1010000000000001	40961	A001
5.	00200001	0000100000000001	2049	801
6.	20200001	1000100000000001	34817	8801
7.	02200001	0010100000000001	10241	2801
8.	22200001	1010100000000001	43009	A801
9.	00020001	0000001000000001	513	201
10.	20020001	1000001000000001	33281	8201
11.	02020001	0010001000000001	8705	2201
12.	22020001	1010001000000001	41473	A201
13.	00220001	0000101000000001	2561	A01
14.	20220001	1000101000000001	35329	8A01
15.	02220001	0010101000000001	10753	2A01
16.	22220001	1010101000000001	43521	AA01
17.	00002001	0000000010000001	129	81
18.	20002001	1000000010000001	32897	8081
19.	02002001	0010000010000001	8321	2081
20.	22002001	1010000010000001	41089	A081
21.	00202001	0000100010000001	2177	881
22.	20202001	1000100010000001	34945	8881
23.	02202001	0010100010000001	10369	2881
24.	22202001	1010100010000001	43137	A881

25.	00022001	0000001010000001	641	281
26.	20022001	1000001010000001	33409	8281
27.	02022001	0010001010000001	8833	2281
28.	22022001	1010001010000001	41601	A281
29.	00222001	0000101010000001	2689	A81
30.	20222001	1000101010000001	35457	8A81
31.	02222001	0010101010000001	10881	2A81
32.	22222001	1010101010000001	43649	AA81
33.	00000201	0000000000100001	33	21
34.	20000201	1000000000100001	32801	8021
35.	02000201	0010000000100001	8225	2021
36.	22000201	1010000000100001	40993	A021
37.	00200201	0000100000100001	2081	821
38.	20200201	1000100000100001	34849	8821
39.	02200201	0010100000100001	10273	2821
40.	22200201	1010100000100001	43041	A821
41.	00020201	0000001000100001	545	221
42.	20020201	1000001000100001	33313	8221
43.	02020201	0010001000100001	8737	2221
44.	22020201	1010001000100001	41505	A221
45.	00220201	0000101000100001	2593	A21
46.	20220201	1000101000100001	35361	8A21
47.	02220201	0010101000100001	10785	2A21
48.	22220201	1010101000100001	43553	AA21
49.	00002201	0000000010100001	161	A1
50.	20002201	1000000010100001	32929	80A1
51.	02002201	0010000010100001	8353	20A1
52.	22002201	1010000010100001	41121	A0A1
53.	00202201	0000100010100001	2209	8A1
54.	20202201	1000100010100001	34977	88A1
55.	02202201	0010100010100001	10401	28A1
56.	22202201	1010100010100001	43169	A8A1
57.	00022201	0000001010100001	673	2A1
58.	20022201	1000001010100001	33441	82A1
59.	02022201	0010001010100001	8865	22A1
60.	22022201	1010001010100001	41633	A2A1
61.	00222201	0000101010100001	2721	AA1
62.	20222201	1000101010100001	35489	8AA1
63.	02222201	0010101010100001	10913	2AA1
64.	22222201	1010101010100001	43681	AAA1
65.	00000021	0000000000001001	9	9
66.	20000021	1000000000001001	32777	8009
67.	02000021	0010000000001001	8201	2009
68.	22000021	1010000000001001	40969	A009

69.	00200021	0000100000001001	2057	809
70.	20200021	1000100000001001	34825	8809
71.	02200021	0010100000001001	10249	2809
72.	22200021	1010100000001001	43017	A809
73.	00020021	0000001000001001	521	209
74.	20020021	1000001000001001	33289	8209
75.	02020021	0010001000001001	8713	2209
76.	22020021	1010001000001001	41481	A209
77.	00220021	0000101000001001	2569	A09
78.	20220021	1000101000001001	35337	8A09
79.	02220021	0010101000001001	10761	2A09
80.	22220021	1010101000001001	43529	AA09
81.	00002021	0000000010001001	137	89
82.	20002021	1000000010001001	32905	8089
83.	02002021	0010000010001001	8329	2089
84.	22002021	1010000010001001	41097	A089
85.	00202021	0000100010001001	2185	889
86.	20202021	1000100010001001	34953	8889
87.	02202021	0010100010001001	10377	2889
88.	22202021	1010100010001001	43145	A889
89.	00022021	0000001010001001	649	289
90.	20022021	1000001010001001	33417	8289
91.	02022021	0010001010001001	8841	2289
92.	22022021	1010001010001001	41609	A289
93.	00222021	0000101010001001	2697	A89
94.	20222021	1000101010001001	35465	8A89
95.	02222021	0010101010001001	10889	2A89
96.	22222021	1010101010001001	43657	AA89
97.	00000221	0000000000101001	41	29
98.	20000221	1000000000101001	32809	8029
99.	02000221	0010000000101001	8233	2029
100.	22000221	1010000000101001	41001	A029
101.	00200221	0000100000101001	2089	829
102.	20200221	1000100000101001	34857	8829
103.	02200221	0010100000101001	10281	2829
104.	22200221	1010100000101001	43049	A829
105.	00020221	0000001000101001	553	229
106.	20020221	1000001000101001	33321	8229
107.	02020221	0010001000101001	8745	2229
108.	22020221	1010001000101001	41513	A229
109.	00220221	0000101000101001	2601	A29
110.	20220221	1000101000101001	35369	8A29
111.	02220221	0010101000101001	10793	2A29
112.	22220221	1010101000101001	43561	AA29

113.	00002221	0000000010101001	169	A9
114.	20002221	1000000010101001	32939	80A9
115.	02002221	0010000010101001	8361	20A9
116.	22002221	1010000010101001	41129	A0A9
117.	00202221	0000100010101001	2217	8A9
118.	20202221	1000100010101001	34985	88A9
119.	02202221	0010100010101001	10409	28A9
120.	22202221	1010100010101001	43177	A8A9
121.	00022221	0000001010101001	681	2A9
122.	20022221	1000001010101001	33449	82A9
123.	02022221	0010001010101001	8873	22A9
124.	22022221	1010001010101001	41641	A2A9
125.	00222221	0000101010101001	2729	AA9
126.	20222221	1000101010101001	35497	8AA9
127.	02222221	0010101010101001	10921	2AA9
128.	22222221	1010101010101001	43689	AAA9
129.	00000003	0000000000000011	3	3
130.	20000003	1000000000000011	32771	8003
131.	02000003	0010000000000011	8195	2003
132.	22000003	1010000000000011	40963	A003
133.	00200003	0000100000000011	2051	803
134.	20200003	1000100000000011	34819	8803
135.	02200003	0010100000000011	10243	2803
136.	22200003	1010100000000011	43011	A803
137.	00020003	0000001000000011	515	203
138.	20020003	1000001000000011	33283	8203
139.	02020003	0010001000000011	8707	2203
140.	22020003	1010001000000011	41475	A203
141.	00220003	0000101000000011	2563	A03
142.	20220003	1000101000000011	35331	8A03
143.	02220003	0010101000000011	10755	2A03
144.	22220003	1010101000000011	43523	AA03
145.	00002003	0000000010000011	131	83
146.	20002003	1000000010000011	32899	8083
147.	02002003	0010000010000011	8323	2083
148.	22002003	1010000010000011	41091	A083
149.	00202003	0000100010000011	2179	883
150.	20202003	1000100010000011	34947	8883
151.	02202003	0010100010000011	10371	2883
152.	22202003	1010100010000011	43139	A883
153.	00022003	0000001010000011	643	283
154.	20022003	1000001010000011	33411	8283
155.	02022003	0010001010000011	8835	2283
156.	22022003	1010001010000011	41603	A283

157.	00222003	0000101010000011	2691	A83
158.	20222003	1000101010000011	35459	8A83
159.	02222003	0010101010000011	10883	2A83
160.	22222003	1010101010000011	43651	AA83
161.	00000203	0000000000100011	35	23
162.	20000203	1000000000100011	32803	8023
163.	02000203	0010000000100011	8227	2023
164.	22000203	1010000000100011	40995	A023
165.	00200203	0000100000100011	2083	823
166.	20200203	1000100000100011	34851	8823
167.	02200203	0010100000100011	10275	2823
168.	22200203	1010100000100011	43043	A823
169.	00020203	0000001000100011	547	223
170.	20020203	1000001000100011	33315	8223
171.	02020203	0010001000100011	8739	2223
172.	22020203	1010001000100011	41507	A223
173.	00220203	0000101000100011	2595	A23
174.	20220203	1000101000100011	35363	8A23
175.	02220203	0010101000100011	10787	2A23
176.	22220203	1010101000100011	43555	AA23
177.	00002203	0000000010100011	163	A3
178.	20002203	1000000010100011	32931	80A3
179.	02002203	0010000010100011	8355	20A3
180.	22002203	1010000010100011	41123	A0A3
181.	00202203	0000100010100011	2211	8A3
182.	20202203	1000100010100011	34979	88A3
183.	02202203	0010100010100011	10403	28A3
184.	22202203	1010100010100011	43171	A8A3
185.	00022203	0000001010100011	676	2A3
186.	20022203	1000001010100011	33443	82A3
187.	02022203	0010001010100011	8867	22A3
188.	22022203	1010001010100011	41635	A2A3
189.	00222203	0000101010100011	2723	AA3
190.	20222203	1000101010100011	35491	8AA3
191.	02222203	0010101010100011	10915	2AA3
192.	22222203	1010101010100011	43683	AAA3
193.	00000023	0000000000001011	11	B
194.	20000023	1000000000001011	32779	800B
195.	02000023	0010000000001011	8203	200B
196.	22000023	1010000000001011	40971	A00B
197.	00200023	0000100000001011	2059	80B
198.	20200023	1000100000001011	34827	880B
199.	02200023	0010100000001011	10251	280B
200.	22200023	1010100000001011	43019	A80B

201.	00020023	0000001000001011	523	20B
202.	20020023	1000001000001011	33291	820B
203.	02020023	0010001000001011	8715	220B
204.	22020023	1010001000001011	41483	A20B
205.	00220023	0000101000001011	2571	A0B
206.	20220023	1000101000001011	35339	8A0B
207.	02220023	0010101000001011	10763	2A0B
208.	22220023	1010101000001011	43531	AA0B
209.	00002023	0000000010001011	139	8B
210.	20002023	1000000010001011	32907	808B
211.	02002023	0010000010001011	8331	208B
212.	22002023	1010000010001011	41099	A08B
213.	00202023	0000100010001011	2187	88B
214.	20202023	1000100010001011	34955	888B
215.	02202023	0010100010001011	10379	288B
216.	22202023	1010100010001011	43147	A88B
217.	00022023	0000001010001011	651	28B
218.	20022023	1000001010001011	33419	828B
219.	02022023	0010001010001011	8843	228B
220.	22022023	1010001010001011	41611	A28B
221.	00222023	0000101010001011	2699	A8B
222.	20222023	1000101010001011	35467	8A8B
223.	02222023	0010101010001011	10891	2A8B
224.	22222023	1010101010001011	43659	AA8B
225.	00000223	0000000000101011	43	2B
226.	20000223	1000000000101011	32811	802B
227.	02000223	0010000000101011	8235	202B
228.	22000223	1010000000101011	41003	A02B
229.	00200223	0000100000101011	2091	82B
230.	20200223	1000100000101011	34859	882B
231.	02200223	0010100000101011	10283	282B
232.	22200223	1010100000101011	43051	A82B
233.	00020223	0000001000101011	555	22B
234.	20020223	1000001000101011	33323	822B
235.	02020223	0010001000101011	8747	222B
236.	22020223	1010001000101011	41515	A22B
237.	00220223	0000101000101011	2603	A2B
238.	20220223	1000101000101011	35371	8A2B
239.	02220223	0010101000101011	10765	2A2B
240.	22220223	1010101000101011	43563	AA2B
241.	00002223	0000000010101011	171	AB
242.	20002223	1000000010101011	32939	80AB
243.	02002223	0010000010101011	8363	20AB
244.	22002223	1010000010101011	41131	A0AB

245.	00202223	0000100010101011	2219	8AB
246.	20202223	1000100010101011	34987	88AB
247.	02202223	0010100010101011	10411	28AB
248.	22202223	1010100010101011	43179	A8AB
249.	00022223	0000001010101011	683	2AB
250.	20022223	1000001010101011	33451	82AB
251.	02022223	0010001010101011	8875	22AB
252.	22022223	1010001010101011	41643	A2AB
253.	00222223	0000101010101011	2731	AAB
254.	20222223	1000101010101011	35499	8AAB
255.	02222223	0010101010101011	10923	2AAB
256.	22222223	1010101010101011	43691	AAAB

Table 4.2: Elements of Sylow p-Subgroup of Group of units of GR $GR\left(2^2,8\right)$.

4.3 Construction of S-Box on Sylow p-Subgroup:

In this section we utilize elements of S_p to construct Substitution box of order 16×16. For this purpose we define affine map $f:S_p\rightarrow S_p$ in such a way that

$$f\left(a\right)=ua+v \quad \text{such that} \quad \forall\ a\in S_p\text{, and for some fixed } \begin{cases} u\in S_p \\ v\in M \end{cases}$$

Where, M denotes maximal ideal of $GR\left(2^2,8\right)$ and we take $u=22220001,\ \ v=22002000$.

From table 4.1 elements of S_p are in the form $1+m$ where $m\in M$. So,

$$\begin{aligned} & f\left(a\right)=\alpha+v, \qquad where,\ \alpha=ua\in S_p \\ \Rightarrow\ & f\left(a\right)=\left(1+m\right)+v \\ \Rightarrow\ & \qquad =1+\left(m+v\right)=1+m'\in S_p, \qquad m'\in M \end{aligned}$$

Whereas, $g:S_p\rightarrow S_p$ is an inverse map such that

$$g\left(\mu\right)=\mu^{-1},\ \forall\ \mu\in S_p$$

So, S-Box is obtained by

$$fog:S_p\rightarrow S_p\text{, A random sequence of 256 elements over } S_p.$$

$$fog\left(\mu\right)=f\left(\mu^{-1}\right)=u\mu^{-1}+v$$

As every element of S_p is self-inverse.

Thus S-Box corresponding to $fog : S_p \to S_p$ is:

2689	35457	10881	43649	641	33409	8833	41601	2177	34945	10369	43137	129	32897	8321	41089
2561	35329	10753	43521	513	33281	8705	41473	2049	34817	10241	43009	1	32769	8193	40961
2721	35489	10913	43681	673	33441	8865	41633	2209	34977	10401	43169	161	32929	8353	41121
2593	35361	10785	43553	545	33313	8737	41505	2081	34849	10273	43041	33	32801	8225	40993
2697	35465	10889	43657	649	33417	8841	41609	2185	34953	10377	43145	137	32905	8329	41097
2569	35337	10761	43529	521	33289	8713	41481	2057	34825	10249	43017	9	32777	8201	40969
2729	35497	10921	43689	681	33449	8873	41641	2217	34985	10409	43177	169	32939	8361	41129
2601	35369	10793	43561	553	33321	8745	41513	2089	34857	10281	43049	41	32809	8233	41001
2691	35459	10883	43651	643	33411	8835	41603	2179	34947	10371	43139	131	32899	8323	41091
2563	35331	10755	43523	515	33283	8707	41475	2051	34819	10243	43011	3	32771	8195	40963
2723	35491	10915	43683	675	33443	8867	41635	2211	34979	10403	43171	163	32931	8355	41123
2595	35363	10787	43555	547	33315	8739	41507	2083	34851	10275	43043	35	32803	8227	40995
2699	35467	10891	43659	651	33419	8843	41611	2187	34955	10379	43147	139	32907	8331	41099
2571	35339	10763	43531	523	33291	8715	41483	2059	34827	10251	43019	11	32779	8203	40971
2731	35499	10923	43691	683	33451	8875	41643	2219	34987	10411	43179	171	32941	8363	41131
2603	35371	10795	43563	555	33323	8747	41515	2091	34859	10283	43051	43	32811	8235	41003

References

Bini, G. a. (2002). *Finite Commutatve Rings and Their Appliccations.* Springer Science and Business Media.

Blake, I. (1972). Codes over certain Rings. *Inform. and Control 20*, 396-404.

Blake, I. F. (1975). Codes over integer residue rings. *Inform. and Control 20*, 295-300.

De Andrade, A. A. (1999). "Construction and decoding of BCH codes over finite commutative rings.". *Linear Algebra Applications*, 69-85.

de Andrade, A. a. (1999). Construction and decoding of BCH codes over finite commutative rings. *Liinear Algebra and its Applications 286*, 69-85.

E. Spiegel. (1978). Codes over Zm,. *Inform. Control, 37*, 100-104.

Golay, M. J. (1949). Notes on digital coding. *Proc IEEE 37*.

Hamming, R. w. (1950). Error detecting and error correcting codes. *The Bell system technical journal*, 147-160.

Interlando, I. P. (1995). A note on cyclic codes over., . *Latin Amer. Appl. 25/S*, 83-85.

Muller, D. E. (1953). *Metric properties of Boolean Algebra and their application to switching circuits.* University of research board, University of Illiois.

Nagpaul, S. R. (2005). *Topics in applied Abstract Algebra, Vol 15.* American Mathimatical Soc.

Prange, E. (1959). *The use of coset Equivalence in the analysis and decoding of Group Codes.* Air Force Cambrige Research Lab Hanscom.

Reed, I. S. (1953). *A class of multiple error correecting codes and decoding scheme.* Massachusetts Inst. of Tech. Lexington Lincoln Lab.

Shah, t. a. (2012). a decoding procedure which improves code rate and error corrections. *Journal of advanced research in applied mathematics*, 37-50.

Shah, T. M. (2013). A Decoding method of an n length binary BCH code through (n+1)n length binary cyclic code. *Anais da academia brasileira de ciencias 85*, 863-872.

Shah, T. N. (2017). maximal cyclic Subgroups of the Groups of units of GRs, A computational approach. *Computational and applied mathematics*, 1273-1297.

Shankar. (1979). On BCH Codes over Arbitrary integer rings. *IEEE Transaction on Information Theory*, 480-483.

Spiegel, E. (1977). Codes over Zm. *Inf. Control, 37*, 48-51.