ON THE GENERATORS OF CODES OF IDEALS OF THE POLYNOMIAL RING $F_2^N[X]/\langle X^N - 1\rangle$ FOR ERROR CONTROL

Fanuel Olege

A thesis submitted in partial fulfillment of the requirements for the Degree of Doctor of Philosophy in Pure Mathematics of Masinde Muliro University of Science and Technology

OCTOBER, 2017

pagenumberingroman

DECLARATION

This thesis is my original work prepared with no other than the indicated sources and support and has not been presented elsewhere for a degree or any other award.

Signature... Date ....

Name: Fanuel Olege
SEP/H/05/10

APPROVAL

We the undersigned certify that we have read and hereby recommend for acceptance of Masinde Muliro University of Science and Technology a research thesis entitled, "On the generators of codes of ideals of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ for error control."

Signature.. Date..............................

Prof. Shem Aywa
Department of Mathematics
Kibabii University.

Signature.. Date....................................

Prof. Maurice Owino Oduor
Department of Mathematics and Computer Science
University of Kabianga.

Signature... Date....................................

Dr. Colleta Akinyi Okaka
Department of Mathematics
Masinde Muliro University of Science and Technology.

COPYRIGHT

DEDICATION

I dedicate this work exclusively to my beloved children: Keren, Esther and Barnabas.

ACKNOWLEDGEMENTS

I acknowledge the invaluable support I have received from my supervisors: Prof. Shem Aywa, Prof. Maurice Owino Oduor and Dr. Okaka Akinyi Colleta. They are able supervisors, who were always available whenever I needed them. Their constant guidance and encouragement through this research kept me moving. I acknowledge the input of Mr. Daniel Ochieng Achola of Maseno University for providing a tutorial on the use of GAP software. Thanks to the Programme leader Dr. Simiyu for his valuable pieces of advice concerning this research. I thank my classmate Mr. Wanambisi for his moral and academic assistance throughout the course. I thank Masinde Muliro University of Science and Technology for granting me opportunity to study and characterize generators of codes of ideals of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ for error control. I thank the National Commission for Science Technology and Innovation for funding this research. I would like to express my gratitude to my wife Ephelly for moral and emotional support she gave towards the success of this work. Finally, glory be to God who by His grace, favour and wisdom has enabled me go through this work.

ABSTRACT

Shannon introduced error detection and correction codes to address the growing need of efficiency and reliability of code vectors. Ideals in algebraic number system have mainly been used to preserve the notion of unique factorization in rings of algebraic integers and to prove Fermat's Last Theorem. Generators of codes of ideals of polynomial rings have not been fully characterized. Ideals in Noetherian rings are closed in polynomial addition and multiplication. This property has been used to characterize cyclic codes. This class of cyclic codes has a rich algebraic structure which is a valuable tool in coding design. The Golay Field which has been used to generate codes over the years provides codes of fixed length which do not reach Shannon's limit. This research has used Shannon's proposed model to determine generators of codes of ideals of the polynomial ring to be used for error control. It presents generators of codes of ideals of the polynomial ring associated with the codewords of a cyclic code C. If the set of generator polynomials corresponding to codewords is given by $I(C)$ (a set of principal ideals of the polynomial ring), it has been shown that $I(C)$ is a cyclic code. Additionally the suitability of codes of ideals of the polynomial ring for error control has been established. Application of Shannon's Theorem on optimal codes has been done to characterize generators of codes of ideals of the polynomial ring for error control. The generators of codes of the candidate polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ have been investigated and characterized using lattices, simplex Hamming codes and isometries. The results of this research contribute significantly towards characterization of generators of codes from ideals of polynomial rings.

TABLE OF CONTENTS

DECLARATION . . . ii

COPYRIGHT . . . iii

DEDICATION . . . iv

ACKNOWLEDGEMENTS . . . v

ABSTRACT . . . vi

INDEX OF NOTATIONS . . . xiii

CHAPTER ONE : INTRODUCTION 1

1.1 Background information . . . 1

1.1.1 Types of Computer Errors . . . 1

1.1.2 Error detection, correction and control . . . 1

1.1.3 Ideals in a commutative ring . . . 3

1.2 Statement of the Problem . . . 4

1.3 Objectives . . . 5

1.3.1 General Objective . . . 5

1.3.2 Specific Objectives . . . 5

1.4 Significance of the study . . . 5

1.5 Methodology . . . 5

CHAPTER TWO : LITERATURE REVIEW 7

2.1 Introduction to ideals in algebraic number fields . . . 7

2.2 Noetherian rings . . . 7

2.3 Principal ideals . . . 8

2.4 Cyclic codes . . . 8

2.5 Error Control coding . . . 10

2.5.1 Construction, development and application of error control codes . 10

2.5.2 Shortcomings in the present error control codes 15

CHAPTER THREE : APPLICATION OF ALGEBRAIC CODING THEORY TO IDEALS OF THE POLYNOMIAL RING $F_2^n[x]/\langle x^n - 1\rangle$ 16

3.1 Properties of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ 16

3.2 Application of Maximum Likelihood Decoding to Codes of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ 19

3.3 Application of Minimum Distance Decoding to Codes of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ 20

3.4 Application of Incomplete Minimum Distance Decoding to Codes of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ 22

3.5 Application of Features of an optimal code to codewords of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ 22

3.6 Measurement of Efficiency and Reliability of codewords of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ 24

CHAPTER FOUR : GENERATORS OF CODES OF IDEALS OF THE POLYNOMIAL RING $F_2^n[x]/\langle x^n - 1\rangle$ FOR ERROR CONTROL 26

4.1 Generators of codes of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ obtained by multiplication mod $(x^n - 1)$ 26

4.2 Generators of codes of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ using cyclic shifts 27

4.3 Generators of codes of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ obtained by irreducible polynomials 28

4.4 Generators of codes of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ obtained using an online tool 29

4.5 Characterization of the set $I(C)$ of polynomials 30

4.6 Error Control with the proposed code 31

4.7 Construction of the proposed code of the candidate ring 33

4.8 Residue classes 49

4.9 Characterization of codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$. 50

4.9.1 Syndromes of the simplex codes in the candidate ring 76

CHAPTER FIVE : CONCLUSION AND RECOMMENDATIONS 79

5.1 Conclusion 79

5.2 Recommendations 79

REFERENCES 81

List of Tables

Table 1: Comparison of Efficiency and reliability of code vectors for the polynomial ring $F_2^6\,[x]/\langle x^6-1\rangle$ 24

Table 2: Comparison of Efficiency and reliability of code vectors for the polynomial ring $F_2^7\,[x]/\langle x^7-1\rangle$ 25

Table 3: Factorization of x^n-1 over $\mathbb{F}_2^n$ for selected n....34

Table 4: Generator Polynomials of $F_2^{11}\,[x]/\langle x^{11}-1\rangle$ 35

Table 5: Generator Polynomials of $F_2^{15}\,[x]/\langle x^{15}-1\rangle$ 36

Table 6: Generator Polynomials of $F_2^{17}\,[x]/\langle x^{17}-1\rangle$ 39

Table 7: Generator Polynomials of $F_2^{21}\,[x]/\langle x^{21}-1\rangle$ 39

Table 8: Generator Polynomials of $F_2^{30}\,[x]/\langle x^{30}-1\rangle$ 42

Table 9: Generator Polynomials of $F_2^{31}\,[x]/\langle x^{31}-1\rangle$ 43

Table 10: Analysis of (n, m, d_{max}) over $F_2^n\,[x]/\langle x^n-1\rangle$ 47

Table 11: Relationship between κ and δ for $F_2^{31}\,[x]/\langle x^{31}-1\rangle$ 48

List of Figures

Figure 1: Graph of the Code Region of $F_2^{31}[x]/\langle x^{31}-1\rangle$ 48

Figure 2: Lattice diagram of the generators of $x^{11}-1$..54

Figure 3: Lattice diagram of the generators of $x^{15}-1$..57

Figure 4: Lattice diagram of the generators of $x^{17}-1$..60

Figure 5: Lattice diagram of the generators of $x^{31}-1$..72

Abbreviations and Acronyms

GAP : Groups, Algorithms and Programming

mSC: m-ary Symmetric Channel

BSC: Binary Symmetric Channel

MLD: Maximum Likelihood Decoding

HD: Hamming Distance

CRC: Cyclic Redundancy Code

BCH: Bose, Ray-Chaudhuri and Hocquenghem Code

RS: Reed- Solomon Code

RM: Reed- Muller Code

CD: Compact Disk

DVD: Digital Video Decoder

CDPD: Cellular Digital Packet Data

TCM: Trellis Coded Modulation

IETF: Internet Engineering Task Force

ACC: Ascending Chain Condition

DCC: Descending Chain Condition

MATLAB: Matrix Laboratory

INDEX OF NOTATIONS

R: A commutative ring

W_c: Minimum weight of codeword C

1_R: Multiplicative identity element in R

δ: Normalised minimum distance

κ: Normalised rate

$C^{\perp}$: Dual of code C

$\mathbb{F}[x]$: A set of polynomials in indeterminate x over a field $\mathbb{F}$

$\sum$: sum of

$\mathbb{Z}$: Ring of integers

d_c: Minimum distance of codeword C

d_{max}: Maximum distance of codeword C

w_{max}: Maximum weight of codeword C

$\mathbb{Z}_n$: Ring of integers modulo n

R/N: R mod N (quotient ring)

A^n: Code space of length n over a set A

η: Error detected symbol

H^T: Transpose of H

$d_c(u, v)$: minimum Hamming distance between the code vectors u and v

$|C|$: Number of distinct codewords contained in a code C or size of C

$\mathbb{GF}(q)$: Galois field with q distinct elements

$\mathbb{V}(n, q)$: Vector space of n elements from a field of alphabet q

$Res_{q,n}$: Residue class alphabet q length n.

Definition of terms

Algorithm is a set of defined procedures for solving a problem.

Elements $a, b \in R$ are **associates** if there exists a unit $u \in R$ with $b = ua$.

A **basis** of a vector space $\mathbb{V}$ is a linearly independent list that spans $\mathbb{V}$.

BCH codes are a class of error- correcting codes that are constructed using polynomials over a Galois field.

Binary repetition code exists for any length n and alphabet $q = 2$. A message consists of a letter of alphabet and it is encoded by being repeated n- times e.g. 000...0 or 111...1.

Binary parity check code has an even weight. Let r be a positive integer and let H be an $r \times (2^r - 1)$ matrix whose columns are the distinct vectors of $\mathbb{V}(r, 2)$. Then the code having H as its parity check matrix is called a **binary Hamming** code and is denoted Ham $(r, 2)$.

Capacity of the channel is the maximum number of bits that can be transmitted in a given time.

Let C be a cyclic $[n, \kappa]$ code with generator polynomial $g(x)$, a factor of $x^n - 1$. Then $x^n - 1 = g(x)h(x)$ for some polynomial $h(x)$. Since $g(x)$ is monic, so also is $h(x)$. The degree of $g(x)$ is $n - \kappa$ and so $h(x)$ has degree κ. The polynomial $h(x)$ is called the **check polynomial of** C.

A **commutative ring** R is a set with two binary operations, addition and multiplication such that:

(i)R is an abelian group under addition

(ii) $ab = ba$ for all $a, b \in R$

(iii) $a(bc) = (ab)c$ for all $a, b, c \in R$

(iv)there exists $I \in R$ with $Ia = a$ for all $a \in R$

(v) $a(b + c) = ab + ac$ for all $a, b, c \in R$

Coding is the short form description of data to ease the data handling during input and processing.

Suppose that C is an $[n, \kappa]$ - code over $\mathbb{GF}(q)$ and that $\mathbf{a}$ is any vector in $\mathbb{V}(n, q)$. Then the set $\{\mathbf{a} + C\}$ is called a **coset** of C. Coset leader is a vector with minimum weight in a coset.

Given a non-zero element e of a finite field $\mathbb{F}$, a linear code C of length n over $\mathbb{F}_q$ is called e-**constacyclic** if $(ec_{n-1}, c_0, ..., c_{n-2}) \in C$ for every $(c_0, c_1, ..., c_{n-1}) \in C$.

A linear Code C of length n is a **Cyclic Code** if it is invariant under any cyclic shifts.

Cyclic $[n, k]$ code is a cyclic code of length n and dimension k.

Cyclic Redundancy Code (CRC) is an even Cyclic Hamming sub-code used for detecting errors in computer applications.

Decoding is a process of retrieving processed data using output device with the aim of establishing the meaning.

Dimension of a code is the number of symbols in a code which carry information.

Let C be any code (not necessarily linear) in $\mathbb{F}_2^n$, for a field $\mathbb{F}$. The **dual code** of C, denoted as $C^{\perp}$ is the code $C^{\perp} = \{x \in \mathbb{F}^n \mid x \cdot c = 0 \text{ since } c \in C\}$.

Efficiency of a code$= \frac{\kappa(c)}{n} \times 100\%$.

Fermat's Last Theorem states that if an integer n is greater than 2 then the equation $a^n + b^n = c^n$ has no solutions in non-zero integers a, b and c.

A **field** $\mathbb{F}$ is a commutative ring with identity in which every non-zero element is invertible.

In a non - zero cyclic code C, the monic polynomial of least degree is called the **generator polynomial of** C.

If H is a parity check matrix then $GH^T = 0$, where G is the generator matrix. A $k \times n$ matrix whose rows form the basis of an [n,k] linear - code is called a **generator matrix** of the code.

Hamming code is a set of error correcting codes that can be used to detect and correct bit errors that can occur when computer data is moved or stored.

The Hamming distance, $d_H(x, y)$ is the number of positions in which x and y differ.

Integral domain is a commutative ring R which satisfies two more axioms:

(i) Identity $I \neq 0$s.

(ii) If $ca = cb$ and $c \neq 0$ then $a = b$.

A polynomial $p(x)$ of positive degree in $\mathbb{F}[x]$ is said to be **irreducible over** $\mathbb{F}$ if it cannot be expressed as a product of two polynomials of positive degree in $\mathbb{F}[x]$.

An **isometry** of $\mathbb{R}^n$ is a function $f : \mathbb{R}^n \mapsto \mathbb{R}^n$ that preserves the distance between vectors: $\mid f(u) - f(v) \mid = \mid u - v \mid$.

The **length** n of a codeword is the total number of $0s$ and 1s in a word.

Maximal Ideal in a ring R is a proper ideal that is not contained in any strictly larger ideal.

A polynomial is **monic** if the leading coefficient is 1.

Normalized distance, δ of the length n code C is defined as $\delta_c = \frac{d_c}{n}$

Normalized rate is the ratio $\frac{\kappa(c)}{n}$ where $\kappa(c)$ is the total number of symbols in a code carrying information.

Parity check matrix is a generator matrix of $C^{\perp}$.

A code C of length n is called a **polynomial code** if there exists a polynomial $g(x)$ such that C, considered as the set of code polynomials, consists of multiples of $g(x)$ with degree less than n. The polynomial $g(x)$ is called the generator polynomial.

Let R be a commutative ring. Then $R[x] = a_0x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 : a_i \in R, n \in \mathbb{Z}$ is a **polynomial ring over** R in indeterminate x.

Principal Ideal in a ring R is an ideal generated by a single element.

A **Principal Ideal Domain** is an integral domain in which every ideal is generated by a single element.

If $p(x)$ is an irreducible polynomial of degree r such that x is a primitive element of the field $\mathbb{F}[x]/p(x)$ then $p(x)$ is called a **primitive polynomial**.

The set of cosets of a two sided ideal I, is given by $R/I = \{r + I, r \in R\}$, is a ring with an identity $I_R + I$ and zero element $0_R + I$ called a **quotient ring**.

Integers a and b are **relatively prime** if $gcd(a, b) = 1$.

Redundancy positions are positions in a codeword in excess of information position which, besides being used to protect a code against noise (disturbance), they are also used in error detection.

Reliability of a code $=\frac{d_c}{n} \times 100\%$

An element u in a commutative ring R is called a **unit** if there exists $v \in R$ with $uv = 1$.

Unique Factorization: If $\mathbb{F}$ is a field, then every polynomial $f(x) \in \mathbb{F}(x)$ of degree ≥ 1 is a product of non zero constant and monic irreducibles. If $f(x)$ has two such factorizations $f(x) = ap_1(x)...p_m(x)$ and $f(x) = bq_1(x)...q_n(x)$, that is a and b are nonzero constants and the p's and q's are monic irreducibles then $a = b$, $m = n$ and the q's may be re-indexed so that $q_i = p_i$ for all i.

R is a **Unique Factorization Domain** if:

(i) every $r \in R$, neither 0 nor a unit, is a product of irreducibles

(ii) $up_1...p_m = vq_1...q_n$ where u and v are units and p_i and q_j are irreducibles, then $m = n$ and there is a permutation $\sigma \in s_n$ with p_i and $q_{\sigma(i)}$ associates of all i.

A non-empty subset $S \subseteq F^n$ is called a **vector space** if it is closed under vector addition and multiplication by scalars. A vector space U contained in a vector space V is called a subspace of V.

Weight is the number of non-zero entries in a codeword.

An element a in a ring R is called a **zero divisor** if $a \neq 0$ and there exists a non zero $b \in R$ with $ab = 0$.

CHAPTER ONE

INTRODUCTION

This chapter consists of five sections. Section 1.1 presents background information, Section 1.2 deals with statement of the problem, Section 1.3 presents objectives of the study, Section 1.4 presents significance of the study and Section 1.5 deals with methodology.

1.1 Background information

Definition 1.1.1. *[18] Let A be a finite set. A code is a non-empty subset of the set A^n of n-tuples of elements from A. Let C be a code constructed by elements of A. If C is a code of length n and size $|C|$, then C is an $(n, |C|)$ code. Members of the code space are words, those belonging to C being codewords. If A has m elements, then C is said to be an m-ary code. If $|A|$ =2, then C is a binary code and the set A=$\{0, 1\}$.*

1.1.1 Types of Computer Errors

According to Williams [49] in digital transmission systems, an error occurs when a bit is altered between transmission and reception, that is a binary 1 is transmitted and a binary 0 is received or a binary 0 is transmitted and a binary 1 is received. Two general types of errors can occur; single bit (random) errors and burst (compound) errors. A single bit error is an isolated error condition that alters one bit but does not affect nearby bits. A burst error of length b is a continuous sequence of b - bits in which the first and the last bits and any number of intermediate bits are received in error.

1.1.2 Error detection, correction and control

Definition 1.1.2. *[31] Error detection is the ability to identify presence of errors caused by noise or other impairments during transmission from the transmitter to the receiver.*

Error correction is the ability to reconstruct the original, error free data.

Error control is the ability to detect and correct errors using a given code.

According to Moschoyiannis [28] the fundamental tool used in the study of error control is the algebraic structure of groups and fields. Rings of polynomials are significant in the study of algebraic codes and can be used to define some classes of error control codes.

Error control coding started in the late 1940's and early 1950's by the works of Shannon [41], Hamming [16] and Golay [15]. Shannon [41] introduced the basic theory on bounds for communication. He showed that it is possible to get low error probability using coding on any channel, provided that the bit-rate is below a channel-specific parameter called the **capacity** of the channel. He did not show how that could be accomplished. His paper gave rise to two research fields, namely Information Theory which deals with bounds on performance and Coding Theory which deals with methods to achieve good communication using codes. Hamming [16] published his construction of a class of single-error-correcting binary codes in 1950. Golay [15] obtained a generalization of the construction to any alphabet of prime size. Both Hamming's original binary codes and Golay's generalizations are called **Hamming codes**.

The discoveries made by Hamming [16] and Golay[15] initiated research activities among mathematicians who were interested in investigating the algebraic and combinatorial aspects of code vectors. Coding theory consists of two parts; code construction and development of decoding methods [18].

Shubhangi, *etal* [43] noticed that polynomial algebra plays an important role in the construction of generators for error correcting codes and in analyzing code parameters. In the study of polynomial rings the factorization of $x^n - 1$ has been done but the generators of corresponding codes have not been fully characterized.

In the work of Hall [18] the quotient ring $F_2^n\,[x]/\langle x^n - 1\rangle$ has been used to study cyclic codes. In this research we use the same ring to generate polynomial codes, discuss their suitability for error control and characterize them.

In the work of Adams [1] it is demonstrated that $\mathbb{Z}_n$ is a field if and only if n is prime.

The polynomial analogue of prime is irreducibility. Most of the available codes for error control such as Hamming [16], BCH [5], cyclic [25] Reed Muller [29] and Reed Solomon [35] are constant length codes and cannot control errors in variable length codes. They are also limited since they are only capable of controlling random errors. According to Richa and Bhudhev [36] development of variable length code has been too slow due to lack of mathematical tools. Variable length codes can control both random errors and burst errors and have an additional advantage of compressing data by way of shortening codes.

The tools we have used to characterize our results include kissing numbers, lattices and isometries.

Definition 1.1.3. *Wheeler [47] Kissing number is the number of $n-$ spheres which can be arranged so that they all touch another central sphere of the same size. It is given by:* $T(\Lambda) =| \{x \in \Lambda : \|x\| = d_{min}(\Lambda)\} |$.

A kissing number determines the maximum number of nearest neighbors a given code is likely to have. In error control coding a higher kissing number means a code has very many useful neighbors and can be easily decoded using minimum distance decoding.

According to Wheeler [47] the hyper volume and hyper surface area of sphere packing reduces significantly as n increases. Thus for the candidate polynomial ring $F_2^n\,[x]/\langle x^n-1\rangle$, we have $lim._{n\to\infty}$hyper surface area $\to 0$ and $lim._{n\to\infty}$hyper volume $\to 0$. In such a case the kissing numbers become very large. Hence too much kissing goes on as n approaches infinity. Therefore as $n \to \infty$, we are bound to get better codes for the purpose of error control.

1.1.3 Ideals in a commutative ring

Definition 1.1.4. *[39]*

A non-empty subset I of a ring $F_2^n\,[x]/\langle x^n-1\rangle$ is an ideal of $F_2^n\,[x]/\langle x^n-1\rangle$ if and only if:

(i) $0 \in I$

(ii) $\forall a, b \in I,\ a \pm b \in I$

(iii) $\forall a \in I$ *and* $r \in F_2^n\,[x]/\langle x^n - 1\rangle,\ ra \in I$.

The ring $F_2^n\,[x]/\langle x^n - 1\rangle$ itself and the subset consisting of 0 alone, denoted by $\{0\}$, are ideals in this ring called *trivial* or *improper ideals.* An ideal $I \neq F_2^n\,[x]/\langle x^n - 1\rangle$ is a *proper* ideal (see Olege, *etal* [32]).

Since $F_2^n\,[x]/\langle x^n - 1\rangle$ is commutative then $ar = ra$. An ideal I has closure if $a \pm b \in I$, for all $a, b \in I$. An ideal I absorbs elements from $F_2^n\,[x]/\langle x^n - 1\rangle$, if $ra, ar \in I$ for all $a \in I$ and for all $r \in F_2^n\,[x]/\langle x^n - 1\rangle$.

The left principal ideal of a ring R is a subset of R of the form RI=$\{aI$: a∈$R\}$. The right principal ideal of a ring R is a subset of the form IR=$\{Ia$: a∈$R\}$. A two-sided principal ideal is a subset of the form $RIR = \{aIa : a \in R\}$. In a commutative ring, these three types of ideals coincide.

1.2 Statement of the Problem

Shannon [41] proposed a model for generating codes which were both efficient and reliable. He also proved the existence of these codes without necessarily pointing to a specific structure (algebraic or otherwise) to obtain them. Richa and Bhudev [36] observed that developments in the study of variable length codes had shown little growth citing lack of mathematical tools as one of the hindrances. Koopman [21] constructed cyclic redundancy codes but these deal with missing or rejected data but not integrity mechanism which involve correctness of data. The factorization of the polynomial $x^n - 1$ has been done, however the generators of codes of ideals of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ have not been fully characterized. Shanon [41] provided neither the technique nor the methodology of obtaining these codes. In this research, we expand classical coding theory by allowing alphabets that are ideals of rings to describe generators of codes of ideals of polynomial rings. In particular we propose error control coding by principal ideals of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$. To this end, we investigate and characterize the generators of codes of ideals of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ for error control.

1.3 Objectives

1.3.1 General Objective

To investigate and characterize generators of codes of ideals of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ for error control.

1.3.2 Specific Objectives

(i) To apply algebraic coding theory to the generators of codes of ideals of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$.

(ii) To investigate generators of codes of ideals of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ for error control.

(iii) To characterize generators of codes of ideals of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ for error control.

1.4 Significance of the study

The results of this study add to the body of knowledge in algebraic coding theory by investigating and characterizing generators of codes of ideals of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ for error control. In particular generators of codes of the candidate polynomial ring can be characterized for error control using lattices and isometries.

1.5 Methodology

Principles of maximum likelihood decoding, minimum distance decoding, incomplete minimum distance decoding, features of an optimal code, efficiency and reliability of code vectors were used to apply algebraic coding theory to the generators of codes of ideals of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$. Principal Ideal Domains, Unique Factorization Domains and chain conditions were used to investigate the properties of the candidate ring. Modulo multiplication, cyclic shifts, irreducible polynomials and an on-line tool, www.quickmath.com were used to investigate the generators of codes of ideals of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$. Shannon's Theorem [41] and Manin's bound [26] were used to construct a code region for ideals of the polynomial ring. As an example we constructed the code region of $F_2^{31}[x]/\langle x^{31} - 1\rangle$ using MATLAB. Lattices and isometries were used to characterize generators of codes of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ for error control.

CHAPTER TWO

LITERATURE REVIEW

In this chapter, we give a review of the literature related to our work. The chapter presents definitions and concepts that are required in subsequent chapters. It has five sections; Section 2.1 presents an introduction to ideals in algebraic number fields, Section 2.2 deals with Noetherian rings, Section 2.3 principal ideals, Section 2.4 tackles cyclic codes and Section 2.5 deals with error control coding.

2.1 Introduction to ideals in algebraic number fields

Kummer [22] introduced the concept of an ideal complex number with the aim of preserving the notion of unique factorization in rings of algebraic integers. Dedekind [11] showed that any ideal in the ring of integers of any algebraic number field could be written uniquely as a product of prime ideals.

According to Miranda [27], the motivation for studying ideals in polynomial rings was to prove Fermat's Last Theorem. By this Theorem, $x^n + y^n = z^n$ has no solution for positive integers $x, y, z \in \mathbb{Z}$ if $n > 2$. After three and a half centuries, this Theorem was completely proved by Wiles [48] using ring homomorphism and application of modularity conjecture for semi-stable elliptic curves. Rotman [39] defined an ideal by characterizing it as a sub-ring whose elements on being multiplied by any ring element, remain in the sub-ring. .

2.2 Noetherian rings

Definition 2.2.1. *[37] A ring R is Noetherian if it satisfies the following three equivalent conditions:*

(i) Every ideal of R is finitely generated.

(ii) Every nonempty set of ideals of R has a maximal element.

(iii) Every ascending chain of ideals of R stabilizes.

Noether developed rings which reproduced themselves. The ideals of these rings also reproduced themselves. In a Noetherean ring every ideal is a finite intersection of other ideals and homomorphic images of Noetherean rings are also Noetherean. Aryasomayajula *eta* [3] showed that given a proper ideal $I_p \lhd R$, the quotient ring R/I_p is Noetherian.

2.3 Principal ideals

Definition 2.3.1. *[39]*

Let $F_2^n\,[x]/\langle x^n - 1\rangle$ be a commutative ring with unity and let $g \in F_2^n\,[x]/\langle x^n - 1\rangle$. The set $\langle g\rangle = \{rg|\ r \in F_2^n\,[x]/\langle x^n - 1\rangle\}$ is an ideal of $F_2^n\,[x]/\langle x^n - 1\rangle$ called the principal ideal generated by g. The element g is the generator of the principal ideal.

So, I is a principal ideal of a commutative ring $F_2^n\,[x]/\langle x^n - 1\rangle$ with unity if there exists $g \in I$ such that for all $g \in I$ we have $rg \in F_2^n\,[x]/\langle x^n - 1\rangle$ for some $r \in F_2^n\,[x]/\langle x^n - 1\rangle$.

In a Principal Ideal Domain every ideal is principal. If $\mathbb{F}$ is a field then every ideal I in $\mathbb{F}$ is a principal ideal. If a polynomial ring $F\,[x]/\langle x^n - 1\rangle$ is irreducible over $\mathbb{F}$ then $F\,[x]/\langle x^n - 1\rangle$ becomes a field. According to Ronald, *etal* [38], given some $\mathbb{Z}$-basis of an ideal we should be able to find a sufficiently shorter generator g which is not necessarily g itself. In this case we can explore polynomial rings with many shorter generators and determine their suitability for error control.

2.4 Cyclic codes

Definition 2.4.1. *[1]*

A linear code C of length n is cyclic if it is invariant under any cyclic shift:

That is a code C is cyclic if :

(i) C is linear.

(ii) Any cyclic shift of a codeword in C is also a codeword.

Xing and Ling [51] demonsrated the fact that every cyclic code consists of polynomials as well as codewords. Hall [18] showed that for every codeword a=(a_0, a_1,...,a_i,...a_{n-2}, a_{n-1})$\in$ $\mathbb{F}^n$, we have a corresponding polynomial $a(x) = \Sigma_{i=0}^{n-1} a_i x^i \in \mathbb{F}^n[x]$, (for all $i = 1, 2, 3, ...$, n is the length of the code vectors). If c is a codeword of the code C, then we call $c(x)$ the corresponding code polynomial. The shifted codeword $\tilde{c}$ has the corresponding code polynomial $\tilde{c}(x)$=$c_{n-1}x^{n-1}$ + $c_0 x$ + $c_1 x^2$ + ... + $c_i x^{i+1}$ + ... + $c_{n-2}x^{n-1}$. This means that $\tilde{c}(x)$ has degree less than n. By application to the candidate ring, $\tilde{c}(x)$ and $xc(x)$ are isomorphic in the ring of polynomials $F_2^n\,[x]/\langle x^n - 1\rangle$, in which arithmetic is done modulo $(x^n - 1)$.

According to Prange [34] for each polynomial $f(x)$$\in$$\mathbb{F}^n[x]$, $f(x)$$\in$$C/(x^n$-1). That is, for any $a_i \in \mathbb{F}^n$, $\Sigma_{i=0}^{n-1} a_i x_i c(x) \in C$ mod$(x^n - 1)$. Hence, for every polynomial $a(x)$= $\Sigma_{i=0}^{n-1} a_i x_i$$\in$ $\mathbb{F}^n[x]$, the product $a(x)c(x)$$\in$ C. Since the code C is linear and closed under polynomial addition, the polynomial presentation of a cyclic code is an ideal of the ring $F_2^n\,[x]/\langle x^n - 1\rangle$.

It was shown by Xing and Ling [51] that a cyclic code is an ideal in a polynomial ring over a finite field. It is characterized by its generator polynomial, $g(x)$. In a polynomial ring $F\,[x]/\langle x^n - 1\rangle$, cyclic codes form a group of the roots $x^n - 1$, hence they are also called group algebra codes. According to Suat and Yildz [44] for any polynomial ring $R_n = F_q\,[x]/\langle x^n - 1\rangle$ there is a bijective correspondence between the vectors of $\mathbb{F}_q^n$ and residue classes of polynomials in R_n.

The first codes which were ever used for error detection were cyclic codes. According to Hall [18] every code can be represented by a set of polynomials called *polycodewords.*

The work of Hai, *etal* [17] on combinatorics shows that the weight distribution of cyclic codes is desirable in establishing the error correction capability of cyclic codes. Thus all constacyclic codes in the same equivalence class of cyclic codes share the same weight distribution, (see Hai,*etal* [17]). Like cyclic codes, e-constacyclic codes of length n over $\mathbb{F}_q$ are ideals of the quotient ring $F_q[x]/\langle x^n - e\rangle$. When $e = 1$ constacyclic codes are reduced to cyclic codes. Two cyclic codes C_1 and C_2 are of the same quality if there exists a mapping $\varphi : C_1 \mapsto C_2$ which preserves the Hamming distance. Mappings with this property are called *isometries* and the codes involved are said to be *equivalent.*

2.5 Error Control coding

Shannon [41] showed that it is possible to achieve reliable communication over a noisy channel provided that the source's entropy is lower than the channel's capacity. He did not explicitly state how channel capacity could be practically reached, only that it was attainable. Hamming [16] and Golay [15] developed the first practical error control schemes. According to Wicker [50], one major drawback with the Hamming code was that it could only control one error.

Golay code [15] addressed this drawback by generalizing the construction of the Hamming code. In the process he discovered two other codes; the first was the binary Golay code which is capable of controlling up to three errors and the second was the ternary Golay code which has the ability to control up to two errors.

The history of error control coding can be broadly divided into two; pre-turbo code and post-turbo code. Turbo codes were invented by Berrou and Glavieux [4]. Prior to this invention, no one really knew how to get close to the theoretical performance limits proposed by Shannon [41]. Algebraic codes such as Reed-Solomon [35] and Bose, Chaudhuri and Hocquenghem (BCH) codes [5] build algebraic structure into the code such that the code can be decoded using algorithms for solving systems of equations. All error control algorithms utilize one basic principle: that is redundancy is added to information in order to detect and correct any errors.

2.5.1 Construction, development and application of error control codes

The general techniques for constructing Hamming and Golay codes were the same (see Olege, *etal* [32]). They involved grouping q-ary symbols into blocks of k and then adding $n-k$ check symbols to produce an n symbol code word. The resulting code has the ability to control up to t errors, and has a code rate of $\frac{k}{n}$. A code of this type is called a *block code*, and is referred to as a (q, n, k, t)- block code, where q is the alphabet of the code, n is the length, k is the rate and t is the maximum number of errors the code can control. Hamming and Golay codes are linear since the modulo-q sum of any two code-words is itself a code - word.

The next main class of linear block codes to be discovered were the Reed-Muller codes, which were first described by Muller [29] in the context of Boolean logic design. These codes were more superior to the Golay codes since they allowed more flexibility in the size of the codeword and the number of controllable errors per codeword.

Next came the discovery of cyclic codes by Prange [34]. These are linear block codes that possess the additional property that any cyclic shift of a code- word is also a code-word. According to Olege, *etal* [32] this property suggests that cyclic codes can be specified by a polynomial of degree $n - k$, denoted by $g(x)$ (where $g(x)$ is the *generator polynomial*).

Castagnoli, Braeuer, and Herrman [7] developed another class of Cyclic Codes called *Cyclic Redundancy* Check (CRC) codes. These have a desirable ability of increasing the number of detectable errors and are basically used to detect single and double bit errors. For this reason, CRC codes are primarily used for error detection applications rather than for error control.

Bose, Ray-Chaudhuri and Hocquenghem [5] discovered BCH codes. They have length $n = q^m - 1$, where m is an integer valued design parameter. The number of errors that the binary $(q = 2)$ BCH code can control is $t = (n - k)$. BCH codes were extended to the non-binary case $(q \neq 2)$ by Reed and Solomon [35]. Reed Solomon (RS) codes constituted a major advancement because their non-binary nature allows for protection against bursts of errors. However, it was not until Rubal and Gupta [40] introduced an efficient decoding algorithm that RS codes began to find practical applications. In their paper on the application of error control to communication, Rubal and Gupta [40] observed that RS codes have found extensive applications in such systems as Compact Disk (CD) players, Digital Video Decoder (DVD) players, and the Cellular Digital Packet Data (CDPD).

In the work of Olege, *etal* [32], three drawbacks are pointed out when block codes are in use. First, the entire code word must be received before decoding is completed. This introduces intolerable lateness into the system particularly for large block lengths. Second the block code requires frame synchronization and third most algebraic-based decoders for block codes work with hard- decisions rather than with soft-decision decoding. With hard-decision decoding typical for block codes, the output of the channel is taken to be binary while with soft-decision decoding the channel output is continuous-valued.

Kazakov [20] showed that in order to achieve the performance bounds predicted by Shannon [41] a continuous-valued channel output is required. While block codes can achieve impressive performance, they are typically not very power efficient and therefore exhibit poor performance when the signal-to-noise ratio is low. The poor performance of block codes at low signal to noise ratio is not a function of the code itself but a function of the sub optimality of hard-decision decoding.

Elias [14] introduced convolution codes to solve the drawbacks of block codes. By segmenting data into distinct blocks, convolution codes add redundancy to a continuous stream of input data by using a linear shift register. Each set of n output bits is a linear combination of the current set of k input bits and the m bits stored in the shift register. The total number of bits that each output depends on is called the *constraint length* and is denoted by κ_c. The rate of the convolution encoder is the number of data bits κ taken in by the encoder in one coding interval divided by the number of code bits n output during the same interval. Just as the data is continuously encoded it can also be continuously decoded.

Convolution codes have been used by several deep space exploration such as Voyager and Pioneer. West [46] has shown that a sub-class of convolution codes has become a standard for commercial satellite communication applications. In the work of Olege, *etal* [32] we note that all the second generation digital cellular standards incorporate convolution coding.

The major weakness of convolution codes is their susceptibility to burst errors. They have properties that are complimentary to those of Reed-Solomon codes [35]. Wicker [40] observed that while convolution codes are susceptible to burst errors, RS codes handle burst errors quite well. Ungerboeck [45] discovered Trellis Coded Modulation (TCM) which use convolution codes and multidimensional signal constellations to achieve reliable communications over band limited channels. TCM have enabled telephone modems to break the 9600 bits per second (bps) barrier. These codes are used in high speed modems and satellite communication applications,(see Rubal and Gupta [40]). TCM comes close to achieving Shannon's promise of reliable communications at channel capacity.

Berrou and Glavieux [4] discovered Turbo codes. The performance of Turbo codes has helped in narrowing the gap between practical coding systems and Shannon's theoretical limit. A turbo code is the parallel concatenation of two or more component codes. In its original form, the constituent codes were from a subclass of convolution codes. The optimal (maximal likelihood) decoding of turbo codes is complicated and impractical. Although turbo codes approach the capacity limit more closely than any other codes, they have a problem of error propagation which makes their practical implementation difficult.

Shannon's model [41] was developed using error coding techniques based on algebraic coding theory. According to his Theorem, given a code with a code rate that is less than the communication channel capacity, a code exists for a block length of n bits with code rate that can be transmitted over the channel with an arbitrarily small probability of error. Theoretically, we should be able to devise a coding scheme for a particular communication channel for any error rate, but so far no one has been able to develop a block code that satisfies Shannon's Theorem.

In the work of Castagnoli, Braeuer, and Herrman [7], we observe that a polynomial's effectiveness is evaluated by computing weights for that polynomial. A critical measurement of polynomial effectiveness for general purpose computing is the Hamming Distance (HD). Each undetectable error pattern is itself a codeword. This also means that determining the minimum HD for a polynomial is equivalent to determining the lowest non-zero weight for that polynomial.

Castagnoli, Braeuer, and Herrman [7] conjectured that there exist techniques of evaluating the weights of polynomials based on prime factorization characteristics. Alderson [2] introduced one of the techniques of using geometric construction on optimal optical orthogonal codes. Kazakov [20] developed cyclic codes based upon polynomials over finite fields. Charles [9] improved on Prange's work [25] to show that polynomial addition and multiplication of cyclic codes were closed in polynomial rings.

According to Brookshear [6] a code is suitable for computer application if and only if it is expressed in binary form or easily convertible into binary symbols. This is because computers have circuits which are either on or off. This gives them two states to work from, to make calculations and run to processes.

Castagnoli, Braeuer, and Herrman [7] filtered cyclic redundancy codes within the code region of 32-bit for greater HD. It singled out a class of polynomials of {1,3,28} with HD=6 as the best polynomial for the purpose of preserving message length while detecting errors at the same time. This was however a CRC Code and could not be used for error control.

Daniele and Feige [10] observed that it is possible to construct lattices from generators of codes if each polycodeword is considered to be a sphere with some metric distance from the other. The characterization of codes using kissing numbers is significant in determining the number of neighbors a central sphere would have. This finds its application in minimum distance decoding for the candidate polynomial ring. In this thesis we have determined minimum distance using weights.

Huffman and Pless [19] observed that real life applications of error control codes include and not limited to modern communication, such as digital radio and television, cellphone communication, mobile money transfer, mobile banking and deep space communication.

2.5.2 Shortcomings in the present error control codes

Richa and Bhudev [36] on the "generation of variable length error control codes" observed that developments in the study of variable length codes had shown little growth citing lack of mathematical tools as one of the hindrances. Most useful data has variable length yet the Galois Field [15] which has been used to generate codes for a long time gives codes of fixed length. Koopman [21] constructed cyclic redundancy codes but these deal with missing or rejected data but not integrity mechanism which involve correctness of data.

CHAPTER THREE

APPLICATION OF ALGEBRAIC CODING THEORY TO IDEALS OF THE POLYNOMIAL RING $F_2^n\,[x]/\langle x^n - 1\rangle$

This chapter addresses the first specific objective of this research. It has six sections; Section 3.1 deals with properties of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$. Section 3.2 deals with application of maximum likelihood decoding to codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$, Section 3.3 deals with application of minimum distance decoding to codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$, Section 3.4 addresses application of incomplete minimum distance decoding to codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$, Section 3.5 application of features of an optimal code to codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ and Section 3.6 measurement of efficiency and reliability of codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$. These sections are addressed in an analogous manner to the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$. We illustrate this using values of n as composite integer and also as a prime number then generalize the results to any values of n.

3.1 Properties of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$

Proposition 3.1.1. *Let I be a maximal ideal over the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$. The following statements are equivalent:*

(i) I is Noetherian.

(ii) Every chain of subsets $(I_0) \subseteq (I_1) \subseteq (I_2) \subseteq ... \subseteq (I_n)$ stabilizes at some I_n.

(iii) Every non-empty collection of subsets of I has a maximal ideal.

Proof

(i) ⇒ (ii). Let I be Noetherian. Then we have the chain $(I_0) \subseteq (I_1) \subseteq (I_2) \subseteq ... \subseteq (I_n)$. We can write $I' = \bigcup I_i \subset I$ which is finitely generated since I is Noetherian. Let the generator elements be $I_1, I_2, ..., I_n$. Each of these elements is contained in the union of I_n. Therefore $I' \subset I_n$ hence $I_n = I'$

(ii)$\Rightarrow$ (i). Assume that the ascending chain condition exists. Let $I' \subset I_n$ be any subset of I. Define a chain of subsets $(I_0) \subseteq (I_1) \subseteq (I_2) \subseteq ... \subseteq (I')$ as follows; $I_0 = \{0\}$. Let $I_{n+1} = I_n + x(F_2^n[x]/\langle x^n - 1\rangle)$ for some $x \in (I' - I_n)$ if such an x exists. Suppose such an x does not exist take $I_{n+1} = I_n$. Clearly $I_0 = \{0\}, I_1$ is generated by some non-zero element of I', I_2 is I_1 with some element of I' not in I_1 until the chain stabilizes. By construction we have an ascending chain which stabilizes at some finite point by ascending chain condition. Hence I' is generated by n elements since $I' = I_n$.

(i) $\Rightarrow$ (iii). If I is Noetherian then it has a maximal ideal. To see this let P be a set of all the proper ideals in the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ containing I_p where I_P is any proper ideal in this ring. Already we know that $P \neq \emptyset$ since $I_P \in P$. Since $F_2^n[x]/\langle x^n - 1\rangle$ is Noetherian the maximum condition gives a maximal element $I \in P$. We should show that I is a maximal ideal in $F_2^n[x]/\langle x^n - 1\rangle$. Suppose there is a proper ideal J with $I \subseteq J$. Then $I_P \subseteq J$ and hence $J \in P$. Therefore maximality of I gives $I = J$ and so I is a maximal ideal in $F_2^n[x]/\langle x^n - 1\rangle$.

(ii) $\Rightarrow$ (iii). If (iii) is false there is a non-empty subset S of $F_2^n[x]/\langle x^n - 1\rangle$ with no maximal element and inductively we can construct a non -terminating strictly increasing chain in S. (iii)$\Rightarrow$(ii). The set $\{x_{(m)} : m \geq 1\}$ has a maximal element which is I. □

Proposition 3.1.2. *$F_2^n[x]/\langle x^n - 1\rangle$ is a Unique Factorization Domain.*

Proof

Let $t \in F_2^n[x]/\langle x^n - 1\rangle$. Then t is irreducible if and only if t is prime. We have to show the following two claims:

(i) if t is prime then t is irreducible.

(ii) if t is irreducible then t is prime.

For claim (i) suppose that t is prime and $t = uv$, for all $t, u, v, \in F_2^n[x]/\langle x^n - 1\rangle$. We should prove that either u or v is a unit. Using the definition of prime, t divides either u or v. Suppose t divides u then we have $u = tw \Rightarrow u = uvw \Rightarrow u(1 - vw) = 0 \Rightarrow vw = 1$, for all $t, u, v \in F_2^n[x]/\langle x^n - 1\rangle$ and some $w \in F_2^n[x]/\langle x^n - 1\rangle$. Since $F_2^n[x]/\langle x^n - 1\rangle$ is an integral domain v is a unit. This same argument holds if we assume t divides v, thus t is irreducible. For claim (ii) let t be irreducible and t divides uv. Then $uv = tw$ for some $w \in F_2^n[x]/\langle x^n - 1\rangle$. By a property of unique factorization domain, we decompose t, u, v into products of irreducible elements, say (t_i, u_i, v_i) upto the units (a, b, c). Hence $a \cdot t_1 ... a \cdot t_n = b \cdot u_i ... u_n = c \cdot v_i ... v_n$. This factorization is unique and therefore t must be associated to some u_i or v_i implying that t divides u or v. □

Example 3.1.1. *Consider the ideals corresponding to the polynomial ring $F_2^7[x]/\langle x^7 - 1\rangle$. We have:*

$I_1 = 0$

$I_2 = 1$

$I_3 = x + 1$

$I_4 = x^3 + x + 1$

$I_5 = x^3 + x^2 + 1$

$I_6 = x^4 + x^3 + x^2 + 1$

$I_7 = x^4 + x^2 + x + 1$

$I_8 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

where each of the I_i's $(i = 1, 2, 3, ..., 8)$ is a principal ideal of this ring. We then have the chain:

$(I_1) \subseteq (I_2) \subseteq (I_3) \subseteq (I_4) \subseteq (I_5) \subseteq (I_6) \subseteq (I_7) \subseteq (I_8)$

Generally, for any polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ we can develop the chain $(I_1) \subseteq (I_2) \subseteq (I_3) \subseteq ... \subseteq (I_j)$ where j is the total number of principal ideals in the candidate polynomial ring hence $I_{i+1} \mid I_i$, for all $I_i \in F_2^n[x]/\langle x^n - 1\rangle$. The prime factors of I_{i+1} contain prime factors of I_j. Already I_j has a unique factorization into many finite prime factors which end up being the same and so the chain stabilizes or terminates.

By Proposition 3.1.1 and 3.1.2 the ring $F_2^n[x]/\langle x^n - 1\rangle$ is Noetherian. It is also a Unique Factorization Domain.

The polynomial I_j is the maximal ideal of the candidate ring.

Proposition 3.1.3. *$F_2^n\,[x]/\langle x^n - 1\rangle$ satisfies the descending chain condition on principal ideals.*

Proof

Using Example 3.1.1 and rearranging the ideals from maximal to the least we have: $(I_j) \supseteq (I_{j-1}) \supseteq (I_{j-2}) \supseteq \ldots \supseteq (I_1)$ which also terminates or stabilizes. □

By Proposition 3.1.3 the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ is Artinian.

Proposition 3.1.4. *Let (I_n) be a family of ideals such that $(I_n) \geq (I_m)$ for some fixed $(I_m) \in (I)$, if:*

(i) (I_m) is true and ((I_m) true means its fixed in (I_n), false means its varying in (I_n))

(ii) (I_n) is true $\Rightarrow$ (I_{n+1}) is true, then (I_n) is true for all $n \geq m$.

Proof

Let $I_c \in F_2^n\,[x]/\langle x^n - 1\rangle$ be a family of all principal ideals for which (I_n) is false. If (I_c) is empty there is nothing to prove. Otherwise there is the smallest ideal $(I_k) \subseteq (I_c)$. From (i) $(I_k) > (I_m)$ and so we have some (I_{k-1}). But $(I_{k-1}) < (I_k)$ implies that $(I_{k-1}) \notin (I_c)$ since (I_k) is the smallest ideal in (I_c). Hence (I_{k-1}) is true. From (ii) $(I_k) = (I_{([k-1]+1)})$ is true and this contradicts $(I_k) \in (I_c)$ which claims that (I_k) is false. □

3.2 Application of Maximum Likelihood Decoding to Codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$

Definition 3.2.1. *[8]*

Let C be a linear code over $\mathbb{F}_q$ and u a vector in the code space $\mathbb{F}_q^n$. The Maximum Likelihood Decoding problem is to find a code $v \in C$ such that:

$d_c(v, u) = d_c(u, c) = min\{d_c(u, c)\}$ for all $c \in C$.

On an mSC (p), the probability of receiving v after the transmission of u is given by $P(\frac{v}{u}) = p^{d_c} q^{n-d_c}$, (where d_c is the Hamming Distance between u and v, p is transition parameter such that $p + q = 1$ and n is the length of the code).

Definition 3.2.2. *[13] A Fermat prime is a prime of the form $2^{2^n}+1$ where n is itself prime. A Mersenne prime is one of the form 2^n-1 for some prime n. A safe prime is a prime number of the form $2p+1$ where p is also prime.*

Consider the set of generators of the polynomial ring $F_2^6\,[x]/\langle x^6-1\rangle$. Here $n=6$ which is a composite integer. The code generated is given by

$$C = [000000, 000001, 000011, 000101, 001001, 010101, 001001, 011011, 111111].$$

Suppose a codeword 010101 was transmitted on a BSC (0.02) and two codewords, 000001 and 111111 were received. Then we have $P(000001|010101)$ $=q^4p^2\approx$ 0.000368947264, while $P(111111|010101)$ $=q^3p^3\approx$ 0.000007529536; it would therefore be efficient to decode 010101 to 000001.

Suppose $n=7$ which is a safe prime. This would give the polynomial ring
$F_2^7\,[x]/\langle x^7-1\rangle$. The code generated is given by

$$C = [0000000, 0000001, 0000011, 0001011, 0001101, 0011101, 0010111, 1111111].$$

Consider a codeword 0000011 transmitted on a BSC (0.03) and the two codewords, 0001011 and 1111111 are received. We have $P(0001011|0000011)$ $=q^6p^1\approx$ 0.02498916, while $P(1111111|0000011)$ $=q^2p^5\approx$ 0.00000002286387; it would be efficient to decode 0000011 to 0001011.

Hence principles of maximum likelihood decoding are applicable to the polynomial ring $F_2^n[x]\text{mod}(x^n-1)$ for prime values of n and for composite values of n.

3.3 Application of Minimum Distance Decoding to Codes of the polynomial ring $F_2^n\,[x]/\langle x^n-1\rangle$

Definition 3.3.1. *[42]*

A code vector v is said to have undergone minimum distance decoding if and only if, when v is received, it is decoded to a codeword u that minimizes the Hamming distance $d_c(u,v)$.

Consider the set of generators of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ in which $n = 5$ which is a safe prime. The code generated is represented by

$$C = [00000, 00011, 00101, 00110, 01100, 01010, 11000, 11111].$$

Suppose we want to decode 01100 to any of the other codewords in C we must compute minimum distance as follows:

$d_c(01100, 00000) = 2$

$d_c(01100, 00011) = 2$

$d_c(01100, 00101) = 2$

$d_c(01100, 00110) = 2$

$d_c(01100, 01010) = 2$

$d_c(01100, 11111) = 3$

Hence it would be more efficient to decode 01100 to any of the codewords in C except to 11111.

Consider the set of codes generated by the polynomial ring $F_2^6[x]/\langle x^6 - 1\rangle$ in which $n = 6$ which is composite. The code is represented by

$$C = [000000, 000001, 000011, 000101, 010101, 001001, 011011, 111111].$$

Suppose we want to decode 111111 to any of the other codewords in C we must compute minimum distance d_c as follows:

$d_c(111111, 000000) = 6$

$d_c(111111, 000001) = 5$

$d_c(111111, 000011) = 4$

$d_c(111111, 000101) = 4$

$d_c(111111, 010101) = 3$

$d_c(111111, 001001) = 4$

$d_c(111111, 011011) = 2$

Therefore it would be more efficient to decode 111111 to 011011.

Hence principles of Minimum Distance Decoding are applicable to the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ for prime values of n as well as for composite values of n.

Proposition 3.3.1. *Let $p < \frac{1}{2}$ where $p + q = 1$. Then maximum likelihood decoding and minimum distance decoding are equivalent.*

Proof

Let the the probability of receiving v after the transmission of u be given by $P(\frac{v}{u}) = p^{d_c}q^{n-d_c}$, (where d_c is the Hamming Distance between u and v, p is transition parameter such that $p+q = 1$ and n is the length of the code). Minimizing the quantity $P(\frac{v}{u})$ $= p^{d_c}q^{n-d_c}$ is equivalent to minimizing d_c. □

3.4 Application of Incomplete Minimum Distance Decoding to Codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$

Definition 3.4.1. *[42]*

Incomplete Minimum Distance Decoding for a received codeword v, occurs when it is decoded to a codeword u that minimizes the Hamming distance or when decoded to the error detected symbol η.

Consider a set of generators of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ in which $n = 5$, which is a safe prime. It was observed for instance in Section 3.3 that 01100 could be decoded to any of the codewords in C except to 11111. By Incomplete Minimum Distance Decoding, 01100 could also be decoded to the error detected symbol η. In this case the minimum distance cannot be determined.

Hence principles of Incomplete Minimum Distance Decoding are applicable to the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ for prime values of n as well as for composite values of n.

3.5 Application of Features of an optimal code to codewords of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$

According to Huffman and Pless [19], an (n, m, d_c) - code is a code of length n containing m words and having minimum distance d_c. Thus for instance, in the polynomial ring

$F_2^7\,[x]/\langle x^7-1\rangle$, $n=7, m=8, d_c=7$, hence it is a $(7,8,7)$ -code, while for the polynomial ring $F_2^{30}\,[x]/\langle x^{30}-1\rangle$, $n=30, m=31, d_c=30$, hence it is a $(30,31,30)$- code. A good code is one with small n for fast transmission of messages, large m to enable transmission of wide variety of messages and large d_c to detect and correct a large number of errors. Generally good codes are those whose value of m and d_c are large relative to values of n.

Define $A_q(n,1)$ as the maximum m such that (n,m,d_{max})-code exists. Determining the values of $A_q(n,1)$ is the main coding problem.

Theorem 3.5.1. *[24] For any set of codewords C of a q-ary of length n over a finite set A the following statements hold:*

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

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

Proof

(a) Suppose C is the set of all codewords of length n. Then $C=A^n$. Any two distinct codewords must differ in at least one position. The minimum distance between two such words is at least 1. A q-ary code of length n cannot be bigger than this.

(b) Suppose C is a q-ary code with parameters (n,m,n). The minimum distance between two such words is n if any two distinct codewords of C differ in all n positions. Therefore the entries in fixed positions of m codewords must be different. This implies that $A_q(n,n)\leq q$ (i)

But the q-ary repetition code has parameters (n,q,n). This yields

$A_q(n,n)\geq q$ (ii)

Combining (i) and (ii) we have $A_q(n,n)=q$. □

3.6 Measurement of Efficiency and Reliability of codewords of the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$

Definition 3.6.1. *[51]*

Efficiency of a code is a function of its information rate κ. *The dimension of a code* k *is the number of symbols which carry information as opposed to redundancy. Normalized dimension or rate* κ *of an m-ary code* C *of length* n *is the ratio* $\frac{k}{n}$ *of message symbols to coded symbols. A code is said to be reliable when its minimum distance* $d_c \geq 2$.

Table 1: Comparison of Efficiency and reliability of code vectors for the polynomial ring $F_2^6[x]/\langle x^6 - 1\rangle$

Code vector	δ	$\delta_C = \frac{\delta}{n}$	**Reliability %**	$\kappa_C = \frac{\kappa}{n}$	**Efficiency %**
000000	0	0	0	1.000	100
000001	1	0.1667	16.67	0.8333	83.33
000011	2	0.3333	33.33	0.6667	66.67
000101	2	0.3333	33.33	0.6667	66.67
001001	2	0.3333	33.33	0.6667	66.67
010101	3	0.5000	50.00	0.5000	50.00
011011	4	0.6667	66.67	0.3333	33.33
111111	6	1.00	100	0.00	0.00

Table 2: Comparison of Efficiency and reliability of code vectors for the polynomial ring $F_2^7\,[x]/\langle x^7 - 1\rangle$

Code vector	δ	$\delta_C = \frac{\delta}{n}$	**Reliability %**	$\kappa_C = \frac{\kappa}{n}$	**Efficiency %**
0000000	0	0	0.00	1.0000	100
0000001	1	0.1429	14.29	0.8571	85.71
0000011	2	0.2857	28.57	0.7142	71.42
0001011	3	0.4286	42.86	0.5714	57.14
0001101	3	0.4286	42.86	0.5714	57.14
0011101	4	0.5714	57.14	0.4286	42.86
0010111	4	0.5714	57.14	0.4286	42.86
1111111	7	1.0000	100	0.00	0.00

From Tables 1 and 2, its clear that as efficiency increases the code becomes more unreliable.

According to Shannon [41] we need to evaluate information content and error performance of any given codeword. High rate codewords are desirable since they employ a more efficient use of redundancy than lower rate codewords. Error correcting capabilities must also be considered when choosing a code for a particular application. A rate 1 code has the optimal rate but has no redundancy and hence not suitable for error control. Generally given a q-ary (n, m, d)-code C we define the rate of C to be $\frac{\log_q m}{n}$. We can then deduce that; $\lim_{n\to\infty} \frac{\log_q m}{n} = 0$

This trend of efficiency and reliability is applicable to the polynomial ring
$F_2^n\,[x]/\langle x^n - 1\rangle$ for any values of $n \geq 2$ for all $n \in \mathbb{N}$.

CHAPTER FOUR

GENERATORS OF CODES OF IDEALS OF THE POLYNOMIAL RING $F_2^n\,[x]/\langle x^n-1\rangle$ FOR ERROR CONTROL

This chapter presents the second and third specific objectives of this research. It has nine sections; Section 4.1 deals with the generators of codes of the polynomial ring $F_2^n\,[x]/\langle x^n-1\rangle$ using modulo multiplication, Section 4.2 deals with the generators of codes of the polynomial ring $F_2^n\,[x]/\langle x^n-1\rangle$ using cyclic shifts, Section 4.3 generators of codes of the polynomial ring $F_2^n\,[x]/\langle x^n-1\rangle$ using irreducible polynomials, Section 4.4 generators of codes of the polynomial ring $F_2^n\,[x]/\langle x^n-1\rangle$ using an online tool, Section 4.5 characterization of the set $I(C)$ of polynomials, Section 4.6 addresses error control with the proposed code, Section 4.7 deals with the construction of the proposed code of the candidate polynomial ring, Section 4.8 Residue classes and Section 4.9 presents the characterization of codes of the polynomial ring $F_2^n\,[x]/\langle x^n-1\rangle$.

4.1 Generators of codes of the polynomial ring $F_2^n\,[x]/\langle x^n-1\rangle$ obtained by multiplication mod (x^n-1)

Consider the polynomial ring $F_2^3\,[x]/\langle x^3-1\rangle$ in which $n=3$ which is a safe prime. Let $\langle g(x)\rangle$=$\langle 1+x^2\rangle$. The generator polynomials of this ring are given by the set R_3 =$\{0,1,x,1+x,x^2,1+x^2,x+x^2,1+x+x^2\}$. Let $r(x)$ be any of the elements of R_3. The computation of $r(x)\langle g(x)\rangle/(x^3-1)$ is as follows:

$0(1+x^2)=0$

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

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

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

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

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

$(x{+}x^2)(1{+}x^2)=x^4{+}x^3{+}x^2{+}x=x(x^3){+}x^3{+}x^2{+}x=x{+}1{+}x^2{+}x=2x{+}1{+}x^2=1{+}x^2$

$(1+x+x^2)(1+x^2) = x^4+x^3+x+1 = x(x^3)+x^3+x+1 = x+1+x+1 = 2x+2 = 0$

The *polycodewords* in this polynomial ring are given by the set $P_c = \{0, 1+x, x^2+x, 1+x^2\}$. These *polycodewords* correspond to the code vectors in C given by
$C = [000, 011, 110, 101]$ which is $\mathbb{V}(3, 2)$.

For composite n, consider the polynomial ring $F_2^6[x]/\langle x^6-1\rangle$. Let $\langle g(x)\rangle$=$\langle 1+x\rangle$. The generator polynomials of this ring are given by $R_6 = \{0, 1, x+1, x^2+1, x^3+1, x^2+x+1, x^4+x^2+1, x^4+x^3+x+1, x^5+x^4+x^3+x^2+x+1\}$. We determine $r(x)\langle g(x)\rangle/(x^6-1)$, for all $r(x) \in R_6$ as follows:

$0(1+x) = 0$

$1(1+x) = 1+x$

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

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

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

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

$(1+x)(x^4+x^2+1) = x^5+x^4+x^3+x^2+x+1$

$(1+x)(x^4+x^3+x+1) = x^5+x^3+x^2+1$

$(1+x)(x^5+x^4+x^3+x^2+x+1) = x^6+1$

The *polycodewords* in this polynomial ring are given by the set $P_c = \{0, 1+x, x^2+1, x^3+x^2+x+1, x^4+x^3+x+1, x^3+1, x^5+x^4+x^3+x^2+x+1, x^5+x^3+x^2+1, x^6+1\}$. These *polycodewords* correspond to the code vectors in C given by
$C = [000000, 000011, 000101, 001111, 011011, 001001, 111111, 101101]$ which is $\mathbb{V}(6, 2)$. This can be done for any polynomial ring $F_2^n[x]/\langle x^n-1\rangle$ in which n is either a positive prime or a positive composite integer.

4.2 Generators of codes of the polynomial ring $F_2^n[x]/\langle x^n-1\rangle$ using cyclic shifts

Definition 4.2.1. *[51] A cyclic shift to the right of the n-tuple vector* $c = (c_0, c_1, c_2, ..., c_{n-1})$ *is given by* $C^R = (c_{n-1}, c_0, c_1, c_2, ..., c_{n-2})$. *The left cyclic shift is given by* $C^L = (c_1, c_2, ..., c_{n-1}, c_0)$.

Suppose for instance we have a polynomial code $c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1}$. If $c(x)$ is multiplied by $x/(x^n - 1)$ we get $\tilde{c}(x) = (c_0x + c_1x^2 + ... + c_{n-1}x^n)/(x^n - 1)$. The codeword associated with $\tilde{c}(x)$ is $(c_{n-1}, c_0, ..., c_{n-2})$. The polynomial code $\tilde{c}(x)$ is the right cyclic shift of $c(x)$.

For instance the codewords of the polynomial ring $F_2^5\,[x]/\langle x^5 - 1\rangle$ using cyclic shifts are determined as follows:

Let the generator polynomial $g(x) = 1 + x$ corresponding to the codeword $c = 00011$ from $C = \{00000, 00011, 00101, 00110, 01100, 01010, 11000, 11111\}$ which is the set of codewords of the polynomial ring $F_2^5\,[x]/\langle x^5 - 1\rangle$. Multiplying $g(x)$ by x we obtain another generator polynomial $g(x)x = \tilde{g}(x) = x + x^2/(x^5 - 1)$. The polynomial $\tilde{g}(x)$ is the generator for the code vector 00110 which is in C. The codeword 00110 is the left cyclic shift of 00011.

Suppose we have the generator polynomial $p(x) = x+x^2$. The codeword corresponding to $p(x)$ in C is 00110. If $p(x)$ is multiplied by x we get another generator polynomial $\tilde{p}(x)$ $= x^2 + x^3/(x^5 - 1)$. The polynomial $\tilde{p}(x)$ is the generator for the codeword 01100 which is in C. The codeword 01100 is the left cyclic shift of 00110.

4.3 Generators of codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ obtained by irreducible polynomials

Definition 4.3.1. *[12]*

A polynomial in indeterminate x over $F_2^n\,[x]/\langle x^n - 1\rangle$ is irreducible if it has degree at least one and is not a product of polynomials of smaller degree.

Proposition 4.3.1. *Let the polynomial $\rho(x) \in F_2^n\,[x]\,/\langle x^n - 1\rangle$. If deg $\rho(x) = 1$ then $\rho(x)$ is irreducible.*

Proof

Suppose $\rho(x) = g(x), h(x)$ for some $g(x), h(x) \in F_2^n\,[x]/\langle x^n - 1\rangle$. Then deg $(g(x))$+deg$(h(x)) =$ 1. Therefore the degrees of $g(x)$ and $h(x)$ are 0 and 1. Hence one of them is a unit. □

Consider the polynomial ring $F_2^6\,[x]/\langle x^6 - 1\rangle$. The irreducible generator polynomials of this ring are $(x+1)^2(x^2+x+1)^2$. The polycodewords of this polynomial ring are given by the set $P_c = \{0, 1, x+1, x^2+1, x^3+1, x^2+x+1, x^4+x^2+1, x^4+x^3+x+1, x^5+x^4+x^3+x^2+x+1\}$

This gives the codewords given by

$$C = [000000, 000001, 000011, 000011, 000101, 010101, 001001, 010101, 011011, 111111]$$

which is $\mathbb{V}(6, 2)$.

Suppose n was prime, say $n = 5$. Our polynomial ring would be $F_2^5\,[x]/\langle x^5 - 1\rangle$. This has the irreducible generator polynomials as $(x+1)(x^4+x^3+x^2+x+1)$. The polycodewords of this ring are given by the set $P_c = \{0, x+1, x^2+1, x+x^2, x^2+x^3, x^3+x^4, x^4+x^3+x^2+x+1\}$

This gives the code vectors of $C = [00000, 00011, 00101, 00110, 01100, 01010, 11000, 11111]$ which is $\mathbb{V}(5, 2)$.

This can be done for any polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ for all $n \in \mathbb{N}$.

4.4 Generators of codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ obtained using an online tool

As the values of n increase it becomes increasingly difficult to accurately determine the irreducible generator polynomials of the said n. In such a case an on-line tool was used to determine the irreducible generator polynomials which when analyzed provide the code vectors as required.

Consider the polynomial ring $F_2^{11}\,[x]/\langle x^{11} - 1\rangle$ where $n = 11$ which is a safe prime. The irreducible generator polynomials obtained by the on-line tool are $x+1$ and $x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$. These are also the polycodewords of $F_2^{11}\,[x]/\langle x^{11} - 1\rangle$. The code vectors are given by $C = [00000000000, 00000000011, 11111111111]$.

Suppose n was composite say $n = 9$. We shall have the polynomial ring
$F_2^9\,[x]/\langle x^9 - 1\rangle$. The irreducible generator polynomials obtained by the on-line tool are $x+1, x^2+x+1$ and x^6+x^3+1. The code vectors provided by these generator polynomials

are [000000011,000000111,001001001,000001001,011011011,111111111] which is $\mathbb{V}(9,2)$.

4.5 Characterization of the set $I(C)$ of polynomials

The set $I(C)$ consists of principal ideals generated by an element $\langle g(x)\rangle$

Any generator polynomial $g(x)$ of $F_2^n\,[x]/\langle x^n-1\rangle$ provides principal ideals.

Theorem 4.5.1. *Let $g(x) \in F_2^n\,[x]/\langle x^n-1\rangle$ be an irreducible and monic factor of x^n-1. The following statements are equivalent:*

(i) $g(x)$ is a generator polynomial of $F_2^n\,[x]/\langle x^n-1\rangle$.

(ii) $\langle g(x)\rangle$ is a generator of the set of ideals $I(C) \in F_2^n\,[x]/\langle x^n-1\rangle$.

Proof

(i) ⇒ (ii). Suppose $g(x)$ is a generator polynomial of $F_2^n\,[x]/\langle x^n-1\rangle$ and is a factor of x^n-1. Then $p(x)g(x) = x^n-1$ for some $p(x) \in F_2^n\,[x]/\langle x^n-1\rangle$. Hence $\langle g(x)\rangle$ is a generator of the set of ideals $I(C) \in F_2^n\,[x]/\langle x^n-1\rangle$.

(ii) ⇒ (i). Suppose that $\langle g(x)\rangle$ is a generator of the set of ideals $I(C) \in F_2^n\,[x]/\langle x^n-1\rangle$. Then any element of $I(C)$ would be given by $p(x)g(x)$ for some $p(x) \in F_2^n\,[x]/\langle x^n-1\rangle$. Hence there exists some $h(x) \in F_2^n\,[x]/\langle x^n-1\rangle$ such that any element of $I(C)$ is given by $p(x)h(x) = x^n-1$. Hence $g(x)$ is the generator polynomial of $F_2^n\,[x]/\langle x^n-1\rangle$. □

Proposition 4.5.1. *For a given polynomial code $P_c \in F_2^n\,[x]/\langle x^n-1\rangle$ the generator polynomial $g(x)$ is unique.*

Proof

Assume the polynomial code $P_c \in F_2^n\,[x]/\langle x^n-1\rangle$ has two generator polynomials $g(x)$ and $g(x)'$. Since $g(x)'$ is the other generator polynomial then $g(x)$ is a multiple of $g(x)'$. This means $g(x)' = h(x)g(x)'$ is a multiple of $g(x)$, for some $h(x) \in F_2^n\,[x]/\langle x^n-1\rangle$. We can also write $g(x)' = r(x)g(x)$ for some $r(x) \in F_2^n\,[x]\,/\langle x^n-1\rangle$. Hence $h(x)r(x) = 1 \Rightarrow h(x)$ $= r(x) = 1$ (since $r(x)$ and $h(x)$ are monic). Equivalently $g(x) = g(x)'$.

Definition 4.5.1. *[51]*

Given the generator polynomial $g(x) \in F_2^n[x]/\langle x^n - 1\rangle$, then $g(x)$ divides $x^n - 1$. Therefore $h(x) = \frac{x^n-1}{g(x)}$ is the parity check polynomial.

The parity check polynomial confirms the accuracy of the generator polynomial.

4.6 Error Control with the proposed code

The proposed error control code is an ideal of the polynomial ring, (see Olege, *etal* [32]). Our candidate polynomial ring was $F_2^n[x]/\langle x^n - 1\rangle$ for all $n \in \mathbb{N}$. This is a polynomial in indeterminate x with coefficients from $\mathbb{F}_2$. We appreciate the fact that any polynomial ring $F_q^n[x]/\langle x^n - 1\rangle$ would provide any codes. However to be used for error control q must be prime. This would turn all the non-zero elements in $\mathbb{F}_q$ to have multiplicative inverses which is a requirement for error control. The choice of $q = 2$ in this research was motivated by the fact that we needed to generate binary codes to match the current computer architecture. The length of the code n can take any positive integral values as desired. This ring has a rich algebraic structure, generates codes of variable length n and does not lead to cascaded bit errors. In their work, Nechaev and Tzypyshev [30] showed that we can out perform finite field linear codes by using codes over rings while relying on the Hamming distance.

Lemma 4.6.1. *Let $u, v, w \in P_c$ where P_c is a polynomial code in the polynomial ring $F_2^n[x]/(x^n - 1)$. Let d_c be the Hamming distance between the codewords in P_c. Then the following properties hold:*

(i) $d_c(u, v) \geq 0$

(ii) $d_c(u, v) = 0$ if and only if $u = v$

(iii) $d_c(u, v) = d_c(v, u)$

(iv) $d_c(u, w) \leq d_c(u, v) + d_c(v, w)$

Proof

(i) $d_c(u, v) =| u - v |\geq 0$

(ii) $d_c(u,v) = 0$ implies that $\mid u - v \mid= 0$ which implies that $u = v$. Conversely if $u = v$ then $d_c(u,v) = d_c(u,u) =\mid u - u \mid=\mid 0 \mid= 0$

(iii) $d_c(u,v) =\mid u - v \mid=\mid -(v-u) \mid=\mid v - u \mid= d_c(v,u)$.

(iv) Let $u = (u_1, u_2, ..., u_n), v = (v_1, v_2, ..., v_n), w = (w_1, w_2, ..., w_n)$. Then $d_c(u,w)$ is the number of places in which u and w differ. Denote this set by φ. Then
$d_c(u,v) =\mid \varphi \mid=\mid j : u_j \neq w_j \mid$ for all $j = 1, 2, 3, ..., n$. Let the set $A = \{j : u_j \neq w_j$ and $u_j = v_j\}$ and the set $B = \{j : u_j \neq v_j$ and $u_j = w_j\}$. Then the sets A and B are disjoint. Hence $d_c(u,w) =\mid A \mid + \mid B \mid= \varphi$. Therefore $\mid B \mid\leq d_c(u,v)$. Suppose $j \in A$ then $v_j = u_j \neq w_j$ and hence $\mid A \mid\leq d_c(v,w)$. This implies that $d_c(u,w) \leq d_c(u,v) + d_c(v,w)$.
□

The pair (P_c, d_c) is a metric space.

Proposition 4.6.1. *Over the ring $F_2^n\,[x]/\langle x^n - 1\rangle$ Hamming distance is translation invariant. In particular for linear codes, the minimum weight equals minimum distance.*

Proof

Let P_c be the set of linear polycodewords in $F_2^n\,[x]/\langle x^n - 1\rangle$. Let $u, v, w \in P_c$. Then $d_c(u,v) = d_c(u-w, v-w)$ for all $u, v, w \in P_c$. Let $v = w$, then
$d_c(u,v) = d_c(u-v, v-v) = d_c(u-v, 0)$. □

Proposition 4.6.2. *Let n be fixed and α be the cardinality of a sphere of radius $d_{max} - 1$ about any point $u \in F_2^n\,[x]/\langle x^n - 1\rangle$. A code (n, κ, d_{max}) exists for all values of $\alpha < q^{n-\kappa+1}$. In brief $n = d_{max} = W_{max}$.*

Proof

By allowing mathematical induction for $k-1$ we have the map $u \mapsto (u, u, ...u, 0, 0, ..., 0)$ from $R \mapsto R^n$ (where $R = F_2\,[x]/\langle x^n - 1\rangle$) defining a code with maximum weight W_{max} where W_{max} is the maximum number of non-zero components in each element of the range. Suppose we have another code C with parameters $(n, \kappa - 1, d_{max})$. Since $\mid C \mid= q^{k-1}$, we have $\alpha. \mid C \mid< q^{n-k+1}.q^{k-1} = q^n$.

On the other hand suppose $u \notin C$. This would mean $d(u, v) > d_{max}$ for all $v \in C$. Let a code B=span $\{C, z\}$. Consider an element e of weight $W_{max} < d_{max}$ in B. Then we have $e - v + nz$ for every $v \in C$, $n \in \mathbb{N}$ and $z \in R$. Dividing by $-n$ we have $-en^{-1} - v' - z$ where $v' \in C$. This means that $d_{max}(v', z) - W_{max}(-n^{-1}) = W_{max}(e) < d_{max}$ which is a contradiction. Hence the maximum weight of an element of B is equivalent to the maximum weight of an element of C, implying that they have the same maximum distance. □

4.7 Construction of the proposed code of the candidate ring

The procedure for construction of the proposed code involves the following steps:

Step 1: Select the desired length n. This selection can be random or deterministic.

Step 2: Determine the generator polynomials. These are the principal ideals for the selected length n.

Step 3: Determine the parity check polynomial. For both prime and composite values of n in the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ the parity check polynomial turned out to be $x + 1$.

Step 4: Perform multiplication modulo$(x^n - 1)$ for all the ideals obtained in order to determine the polycodewords.

Step 5: Determine the codewords corresponding to the polycodewords obtained in Step 4.

Step 6: The set C consisting of all the codewords obtained in Step 5 is the proposed code of the candidate ring.

Table 3: Factorization of $x^n - 1$ over $\mathbb{F}_2^n$ for selected n

n	x^n+1	Complete factorization of $x^n - 1$ over $\mathbb{F}_2^n$
11	$x^{11}+1$	$(x+1)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
15	$x^{15}+1$	$(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$
17	$x^{17}+1$	$(x+1)(x^8+x^7+x^6+x^4+x^2+x+1)(x^8+x^5+x^4+x^3+1)$
21	$x^{21}+1$	$(x+1)(x^2+x+1)(x^3+x^2+1)(x^3+x+1)$ $(x^6+x^5+x^4+x^2-1)(x^6+x^4+x^2+x+1)$
30	$x^{30}+1$	$(x+1)^2(x^2+x+1)^2(x^4+x+1)^2(x^4+x^3+1)^2(x^4+x^3+x^2+x+1)^2$
31	$x^{31}+1$	$(x+1)(x^5+x^2-1)(x^5+x^3+1)(x^5+x^3+x^2+x+1)$ $(x^5+x^4+x^2+x+1)(x^5+x^4+x^3+x+1)(x^5+x^4+x^3+x^2+1)$

From Table 3 the parity check polynomial for $x^n + 1$ is $x + 1$.

Theorem 4.7.1. *Let a polynomial $\sigma(x) \in F_2^n[x]$ be irreducible. Then the polynomial ring $F_2^n[x]/\langle\sigma(x)\rangle$ is a field.*

Proof

Let $r(x)$ be a non-zero element of $F_2^n[x]/\langle\sigma(x)\rangle$. If $r(x)$ is co-prime to $\sigma(x)$ then we can find polynomials $\alpha(x)$ and $\beta(x)$ such that $r(x)\alpha(x)+\sigma(x)\beta(x) = 1$. But $r(x)\alpha(x) \equiv 1 \bmod \sigma(x)$ implies that $r(x)$ has a multiplicative inverse $\alpha(x)/\sigma(x)$. □

Proposition 4.7.1. *A polynomial code $P_c \in F_2^n\,[x]/\langle x^n - 1\rangle$ can control up to e errors if and only if $d_{max} \geq 2e + 1$.*

Proof

Suppose P_c cannot control up to e errors. Then there exists a pattern of at most e errors which changes the code vector u into a code vector v for all $u, v \in P_c$. Since we can change u into v using a maximum of e errors, we have $d_{max}(u, v) \leq e$. Suppose it was not possible to change v then we have a code vector $w \neq u$ with $d_{max}(w, v) \leq d_{max}(u, v)$ for some $w \in P_c$. Hence $d_{max}(w, v) \leq e$. By triangle inequality $d_{max}(u, v)+d_{max}(v, w) \leq e+e = 2e$ which contradicts $d_{max} \geq 2e+1$. □

For instance to determine the minimum value of d_{max} a code should have to be selected for error control, we take:

$\Rightarrow d_{max} = 2e + 1$

$\Rightarrow$ for $e = 1$

$d_{max} = 3$

Proposition 4.7.2. *A polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ generates an error control code for $n \geq 3$.*

Proof

Assume the contrary that the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ does not generate error control codes. Then $F_2^n[x]/\langle x^n - 1\rangle$ has a maximum Hamming distance $d_{max} < 3$ for all the codewords it generates. But the most optimal codeword generated by $F_2^n[x]/\langle x^n - 1\rangle$ has $d_{max} = n \geq 3$. This contradicts the original assumption. Hence $F_2^n[x]/\langle x^n - 1\rangle$ generates an error control code. □

Suppose we want to show the maximum number of errors the code generated by $F_2^{11}[x]/\langle x^{11} - 1\rangle$ can control. Then;

$2e + 1 = d_{max}$ (where e is the maximum number of errors this code can control)

$\Rightarrow 2e + 1 = 11$

$\Rightarrow e = 5$

Table 4: Generator Polynomials of $F_2^{11}[x]/\langle x^{11} - 1\rangle$

Generator Polynomial	**Corresponding Codeword, C**
0	00000000000
1	00000000001
$x + 1$	00000000011
$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4$ $+x^3 + x^2 + x + 1$	11111111111

From Table 4 the codewords in C are ideals of the polynomial ring $F_2^{11}[x]/\langle x^{11}-1\rangle$. Here $m=4, n=11$ (which is a safe prime), $W_{max}=11$,
$d_{max}=11, (n, m, d_{max})=(11,4,11)$.

Again by Proposition 4.7.1 this code can control up to five errors.

Table 5: Generator Polynomials of $F_2^{15}[x]/\langle x^{15}-1\rangle$

Generator Polynomial	**Corresponding Codeword, C**
0	000000000000000
1	000000000000001
$x+1$	000000000000011
x^2+x+1	000000000000111
x^4+x+1	000000000001011
x^4+x^3+1	000000000011001
$x^4+x^3+x^2+x+1$	000000000011111
x^3+1	000000000001001
x^5+x^3+x+1	000000000101011
$x^5+x^4+x^2+1$	000000000110101
x^5+1	000000000100001
$x^6+x^5+x^4+x^3+1$	000000001111001
x^7+x^3+x+1	000000010001011
$x^6+x^3+x^2+x+1$	000000001001111
$x^{12}+x^9+^6+x^3+1$	001001001001001
$x^7+x^6+x^4+x+1$	000000011010001
$x^6+x^4+x^3+x^2+1$	000000001011101
x^7+1	000000010000001

$x^8 + x^2 + 1$	000000100000101
$x^9 + x^8 + x^3 + x^2 + x + 1$	000001100001111
$x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$	000010100110111
$x^5 + x^4 + x + 1$	000000000110011
$x^{11} + x^{10} + x^8 + x^6 + x^4 + x^3 + 1$	000110101011001
$x^8 + x^4 + x^2 + x + 1$	000000100010111
$x^9 + x^8 + x^5 + x^4 + x^3 + 1$	000001100111001
$x^{11} + x^{10} + x^8 + x^6 + x^4 + x^3 + 1$	000110101011001
$x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$	000000110111011
$x^8 + x^7 + x^6 + x^4 + 1$	000000111010001
$x^7 + x^6 + x^4 + 1$	000000011010001
$x^8 + x^4 + x^2 + x + 1$	000000100010111
$x^7 + x^6 + x^5 + x^2 + x + 1$	000000011100111
$x^9 + x^6 + x^5 + x^4 + x + 1$	000001001110011
$x^9 + x^8 + x^5 + x^4 + x^3 + 1$	000001100111001
$x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$	000010100110111
$x^7 + x^6 + x^5 + x^2 + x + 1$	000000011100111
$x^7 + x^3 + x + 1$	000000010001011
$x^9 + x^6 + x^5 + x^4 + x + 1$	000010001110011
$x^7 + x^6 + x^4 + 1$	000000011010001
$x^9 + x^8 + x^5 + x^3 + 1$	000001100111001
$x^7 + x^6 + x^4 + 1$	000000011010001
$x^{10} + x^8 + x^7 + x^5 + x^4 + 1$	000010110110001

$x^{10}+x^7+x^6+x^2+x+1$	000010011000111
$x^{10}+x^9+x^7+x^6+x^2+x+1$	000011011000111
$x^{10}+x^9+x^8+x^6+x^5+x^2+1$	000011101100101
$x^{10}+x^8+x^4+1$	000010100010001
$x^{10}+x^9+x^8+x^6+x^4+x^2+x+1$	000011101010111
$x^{11}+x^{10}+x^6+x^5+x+1$	000010001100011
$x^{11}+x^{10}+x^9+x^8+x^6+x^4+x^3+1$	0000111101011001
$x^9+x^7+x^6+x^3+x^2+1$	000001011001101
$x^{11}+x^8+x^7+x^5+x^3+x^2+x+1$	000100110101111
$x^{13}+x^{11}+x^8+x^6+x^5+1$	010100101100001
$x^{13}+x^{12}+x^{10}+x^9+x^7+x^6+x^4+x^3+x+1$	011011011011011
$x^9+x^7+x^6+x^3+x^2+1$	000001011001101
x^7+x^3+x+1	000000010001011
$x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7 +x^6+x^5+x^4+x^3+x^2+x+1$	111111111111111

From Table 5 the codewords in C are ideals of the polynomial ring $F_2^{15}\,[x]/\langle x^{15}-1\rangle$. We have $m=55, n=15$ (which is composite), $W_{max}=15, d_{max}=15$,

$(n,m,d_{max})=(15,55,15)$,

By Proposition 4.7.1 this code can control up to seven errors.

Table 6: Generator Polynomials of $F_2^{17}[x]/\langle x^{17}-1\rangle$

Generator Polynomial	**Corresponding Codeword, C**
0	00000000000000000
1	00000000000000001
$x+1$	00000000000000011
$x^8+x^7+x^6+x^4+x^2+x+1$	00000000111010111
$x^9+x^7+x^5+x^4+x^3+1$	00000001010111001
$x^8+x^5+x^4+x^3+1$	00000000100111001
$x^9+x^8+x^6+x^3+x+1$	00000001101001011
$x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9$ $+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$	11111111111111111

From Table 6 the codewords in C are ideals of the polynomial ring $F_2^{17}[x]/\langle x^{17}-1\rangle$. Again, here $m=8, n=17$ (which is a Fermat prime), $W_{max}=17, d_{max}=17$, $(n,m,d_{max})=(17,8,17)$.

By Proposition 4.7.1 this code can control up to eight errors.

Table 7: Generator Polynomials of $F_2^{21}[x]/\langle x^{21}-1\rangle$

Generator Polynomial	**Corresponding Codeword, C**
0	000000000000000000000
1	000000000000000000001
$x+1$	000000000000000000011
x^2+x+1	000000000000000000111
x^3+x^2+1	000000000000000001101
x^3+x+1	000000000000000001011

$x^6+x^5+x^4+x^2+1$	00000000000000111011
$x^6+x^4+x^2+x+1$	00000000000001010111
x^3+1	00000000000000001001
x^4+x^2+x+1	00000000000000010111
$x^4+x^3+x^2+1$	00000000000000011111
$x^7+x^4+x^3+x^2+1$	00000000000010011111
$x^7+x^6+x^5+x^4+x^3+1$	00000000000011111001
x^5+x+1	00000000000000100011
x^5+x^4+1	00000000000000110001
$x^8+x^6+x^3+x+1$	00000000000101001011
$x^9+x^7+x^6+x^5+x^3+x^2+x+1$	00000000001011111111
$x^8+x^7+x^5+x^2+1$	00000000000110100101
$x^6+x^5+x^2+1$	00000000000001100101
x^6+x^4+x+1	00000000000001010011
$x^9+x^8+x^7+x^6+x^3+x^2+1$	00000000001111011101
$x^6+x^5+x^4+x^3+x^2+x+1$	00000000000001111111
x^9+x^3+1	00000000001000001001
x^9+x^3+1	00000000001000001001
x^7+1	00000000000010000001
$x^{10}+x^9+x^4+x^3+x+1$	00000000011000011011
$x^{10}+x^7+x^6+x^4+x^2+1$	00000000100011010101
x^8+x^7+x+1	00000000000110000011
$x^9+x^8+x^5+x^4+x^2+x+1$	00000000001100110111

$x^9 + 1$	000000000001000000001
$x^{10} + x^8 + x^6 + x^4 + x^3 + 1$	000000000010101011001
$x^{12} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^3 + x + 1$	000000001101101101011
$x^{13} + x^{12} + x^{11} + x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$	000000111001101111101
$x^{14} + x^9 + x^8 + x^4 + 1$	000000100001100010001
$x^{15} + x^{14} + x^{11} + x^{10} + x^8 + x^7 + x^4$ $+x^3 + x^2 + x + 1$	000001100110110011111
$x^{15} + x^{14} + x^{13} + x^{12} + x^{10} + x^9 + x^7$ $+x^6 + x^5 + x^2 + 1$	000001111011011100101
$x^{15} + x^{14} + x^{13} + x^{12} + x^{10} + x^9 + x^8$ $+x^5 + x^4 + x^2 + 1$	000001111011100110101
$x^{18} + x^{15} + x^{12} + x^9 + x^6 + x^3 + 1$	001001001001001001001
$x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14}$ $+... + x^2 + x + 1$	111111111111111111111

From Table 7 the codewords in C are ideals of the polynomial ring $F_2^{21}\,[x]/\langle x^{21} - 1\rangle$. Again, here $m = 39, n = 21$(which is composite)$, W_{max} = 21, d_{max} = 21,$ $(n, m, d_{max}) = (21, 39, 21)$.

By Proposition 4.7.1 this code can control up to a maximum of ten errors.

For instance, to show the maximum number of errors e a code generated by say $F_2^{30}\,[x]/\langle x^{30} - 1\rangle$ can control, we have;

$$\begin{aligned} 2e + 1 &= d_{max} \text{ (where e is the maximum number of errors this code can control)} \\ &\Rightarrow\ 2e + 1 = 30 \\ &\Rightarrow\ e = 14 \end{aligned}$$

This is because the errors controlled cannot be fractions.

Table 8: Generator Polynomials of $F_2^{30}[x]/\langle x^{30}-1\rangle$

Generator Polynomial	**Corresponding Codeword, C**
0	000000000000000000000000000000
1	000000000000000000000000000001
$x+1$	000000000000000000000000000011
x^2+1	000000000000000000000000000101
x^2+x+1	000000000000000000000000000111
x^4+x^2+1	000000000000000000000000010101
x^4+x+1	000000000000000000000000010011
x^8+x^2+1	000000000000000000000100000101
x^4+x^3+1	000000000000000000000000011001
x^8+x^6+1	000000000000000000000101000001
$x^4+x^3+x^2+x+1$	000000000000000000000000011111
$x^8+x^6+x^3+x^2+1$	000000000000000000000101001101
x^3+1	000000000000000000000000001001
x^4+x+1	000000000000000000000000011011
$x^5+x^4+x^3+x^2+x+1$	000000000000000000000000111111
x^6+1	000000000000000000000001000001
$x^5+x^4+x^2+1$	000000000000000000000000110101
$x^6+x^4+x^3+x^2+x+1$	000000000000000000000001011111
$x^6+x^5+x^4+x^3+1$	000000000000000000000001111001
x^7+x^3+1	000000000000000000000010001011
$x^8+x^7+x^4+x^3+x^2+1$	000000000000000000000110011101

$x^8 + x^6 + x^5 + x^3 + x^2 + x + 1$	000000000000000000000101101111
$x^9 + x^8 + x^7 + x^5 + x^4 + 1$	000000000000000000001110110001
$x^7 + x^6 + x^4 + x + 1$	000000000000000000010011010011
$x^{12} + x^{10} + x^8 + x^6 + 1$	000000000000000001010101000001
$x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x + 1$	000000000000000011111111000011
$x^{14} + x^6 + x^2 + 1$	000000000000000100000001000101
$x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{14} + x^6 + x^5 + x^4$ $+x^3 + x^2 + x + 1$	000000000111110100000001111111
$x^{24} + x^{20} + x^{16} + x^{14} + x^{10} + x^6 + x^2 + 1$	000001000100010100010001000101
$x^{28} + x^{27} + x^{26} + x^{25} + x^{23} + x^{22} + x^{21} + x^{19} + x^{15}$ $+x^{13} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x + 1$	011110111010001011100101010011
$x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + ... + x^8$ $+x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	111111111111111111111111111111

From Table 8 the codewords in C are ideals of the polynomial ring $F_2^{30}[x]/\langle x^{30} - 1\rangle$. Again here $m = 31, n = 30$ (which is composite), $W_{max} = 30, d_{max} = 30$, $(n, m, d_{max}) = (30, 31, 30)$.

By Proposition 4.7.1 this code can control up to fourteen errors.

Table 9: Generator Polynomials of $F_2^{31}[x]/\langle x^{31} - 1\rangle$

Generator Polynomial	**Corresponding Codeword**
0	0000000000000000000000000000001
1	0000000000000000000000000000001
$x + 1$	0000000000000000000000000000011
$x^5 + x^2 + 1$	0000000000000000000000000100101
$x^5 + x^3 + 1$	0000000000000000000000000101001

$x^5+x^3+x^2+x+1$	0000000000000000000000000101111
$x^5+x^4+x^2+x+1$	0000000000000000000000000110111
$x^5+x^4+x^3+x+1$	0000000000000000000000000111011
$x^5+x^4+x^3+x^2+x+1$	0000000000000000000000000111111
$x^6+x^5+x^3+x^2+x+1$	0000000000000000000000001101111
$x^6+x^5+x^4+x^3+x+1$	0000000000000000000000000111111
$x^6+x^5+x^4+1$	0000000000000000000000001110001
$x^6+x^4+x^3+1$	0000000000000000000000001011001
$x^6+x^3+x^2+1$	0000000000000000000000001001101
x^6+x^2+x+1	0000000000000000000000001000111
$x^{10}+x^8+x^7+x^5+x^3+x^2+1$	0000000000000000000010110101101
$x^{11}+x^{10}+x^9+x^7+x^5+x^4+x^2+x+1$	0000000000000000000111010110111
$x^{10}+x^8+x^6+x^5+x^4+x+1$	0000000000000000000010101110011
$x^{11}+x^{10}+x^9+x^8+x^7+x^4+x^2+1$	0000000000000000000001111100101
$x^{10}+x^9+x^3+x+1$	0000000000000000000011000001011
$x^{11}+x^9+x^4+x^3+x^2+1$	0000000000000000000101000011101
$x^{10}+x^9+x^8+x^7+x^5+x^4+x^2+x+1$	0000000000000000000011110110111
$x^{11}+x^7+x^6+x^4+x^3+1$	0000000000000000000100011011001
$x^{10}+x^9+x^8+x^6+x^5+1$	0000000000000000000011101100001
$x^{11}+x^8+x^6+x^5+x^2+1$	0000000000000000000100101100101
$x^{10}+x^7+x^5+x^4+x^2+x+1$	0000000000000000000010010110111
$x^{11}+x^{10}+x^8+x^7+x^6+x^4+x^3+1$	0000000000000000000110111011001
$x^{10}+x^9+x^8+x^6+x^5+x^3+x^2+x+1$	0000000000000000000011101101111

$x^{11}+x^8+x^7+x^5+x^4+1$	00000000000000000000010110110001
$x^{10}+x^9+x^7+x+1$	00000000000000000010011010000011
$x^{11}+x^9+x^8+x^7+x^2+1$	00000000000000000000101110000101
$x^{10}+x^9+x^5+x^2+x+1$	00000000000000010101011000100111
$x^{11}+x^9+x^6+x^5+x^3+1$	00000000000000000000101001101001
$x^{15}+x^7+x^3+x+1$	00000000000000001000000010001011
$x^{16}+x^{15}+x^8+x^7+x^4+x^3+x^2+1$	00000000000000110000000111011101
$x^{15}+x^{14}+x^{13}+x^{12}+x^{10}+x^9$ $+x^8+x^5+x^4+x+1$	00000000000001111011011100110011
$x^{16}+x^{12}+x^{11}+x^8+x^6+x^4+x^2+1$	00000000000000010001100101010101
$x^{10}+x^9+x^8+x^7+x^6+x^4+x^3+x^2+1$	00000000000000000000001111011101
$x^{11}+x^6+x^5+x^2+x+1$	00000000000000000001000001100111
$x^{15}+x^{14}+x^{13}+x^9+x^8+x^3+1$	00000000000000001110001100001001
$x^{16}+x^{13}+x^8+x^4+x^3+x+1$	00000000000000010010000100011011
$x^{15}+x^{14}+x^9+x^7+x^4+x^2+1$	00000000000000000110000010010101
$x^{16}+x^{14}+x^{10}+x^9+x^8$ $+x^7+x^5+x^4+x^3+x^2+x+1$	00000000000000010100011110111111
$x^{10}+x^6+x^5+x^4+1$	00000000000000000000010001110001
$x^{11}+x^{10}+x^7+x^4+x+1$	00000000000000000000110010010011
$x^{15}+x^{12}+x^{11}+x^9+x^8+x^7$ $+x^4+x^2+1$	00000000000000001001101110010101
$x^{16}+x^{15}+x^{13}+x^{11}+x^{10}$ $+x^7+x^5+x^4+x^3+x+1$	00000000000000011010110010111111
$x^{15}+x^{13}+x^{11}+x^8+x^7+x^6$ $+x^4+x^3+1$	00000000000000001010100111011001

$x^{16}+x^{15}+x^{14}+x^{13}+x^{12}$ $+x^{11}+x^{9}+x^{6}+x^{5}+x^{3}+x+1$	0000000000000011111101001101011
$x^{15}+x^{13}+x^{12}+x^{7}+x^{6}+x^{5}+x^{4}$ $+x^{3}+x^{2}+x+1$	0000000000000001011000011111111
$x^{16}+x^{15}+x^{14}+x^{12}+x^{8}+1$	0000000000000011101000100000001
$x^{10}+x^{8}+x^{7}+x^{5}+x^{3}+1$	0000000000000000000010110101001
$x^{11}+x^{10}+x^{9}+x^{7}+x^{6}+x^{5}+x^{4}$ $+x^{3}+x+1$	0000000000000000000111011111011
$x^{15}+x^{13}+x^{10}+x^{9}+x^{5}+x^{3}+x^{2}+1$	0000000000000001010011000101101
$x^{16}+x^{15}+x^{14}+x^{13}+x^{11}+x^{9}$ $+x^{6}+x^{5}+x^{4}+x^{2}+x+1$	0000000000000011110101001110111
$x^{15}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{6}+1$	0000000000000001001110111000001
$x^{15}+x^{14}+x^{11}+x^{10}+x^{7}+x^{6}+x^{5}+x^{3}$ $+x^{2}+x+1$	0000000000000001100110011101111
$x^{15}+x^{14}+x^{12}+x^{8}+1$	0000000000000001101000100000001
$x^{16}+x^{14}+x^{12}+x^{10}+x^{8}+x^{5}+x^{4}+1$	0000000000000010101010100110001
$x^{16}+x^{15}+x^{13}+x^{10}+x^{9}+x^{6}+x+1$	0000000000000011010011001000011
$x^{15}+x^{5}+x^{4}+x^{2}+x+1$	0000000000000001000000000110111
$x^{20}+x^{19}+x^{18}+x^{16}+x^{15}+x^{12}$ $+x^{11}+x^{10}+x^{4}+x^{2}+1$	0000000001101011001110000010101
$x^{20}+x^{19}+x^{17}+x^{12}+x^{11}+x^{9}$ $+x^{8}+x^{5}+x^{3}+x^{2}+1$	0000000000110100001101100101111
$x^{21}+x^{17}+x^{16}+x^{13}+x^{8}+x^{6}$ $+x^{5}+x^{4}+1$	0000000000110100001101100101111
$x^{21}+x^{18}+x^{17}+x^{15}+x^{13}+x^{5}$ $+x^{4}+x^{3}+x^{2}+1$	0000000010001101010000000111111
$x^{21}+x^{19}+x^{18}+x^{15}+x^{13}+x^{11}$ $+x^{10}+x^{9}+x^{7}+x^{5}+x+1$	0000000001011001010111010100011

$x^{25}+x^{23}+x^{21}+x^{20}+x^{19}+x^{17}+x^{15}+x^{13}$ $+x^{13}+x^{12}+x^{10}+x^{9}+x^{8}+x^{7}+x^{4}+x^{3}+x+1$	0000010101110101011011110011011
$x^{26}+x^{25}+x^{22}+x^{19}+x^{18}+x^{17}$ $+x^{16}+x^{15}+x^{13}+x^{8}+x^{7}+x^{3}+x+1$	0000110010001111010000110001011
$x^{30}+x^{24}+x^{22}+x^{21}+x^{20}+x^{14}+x^{12}+x^{11}$ $+x^{20}+x^{10}+x^{9}+x^{8}+x^{7}+x^{6}+x^{5}$ $+x^{4}+x^{3}+x^{2}+1$	0000001011100000101111111111111
$x^{30}+x^{29}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{23}$ $+x^{20}+x^{19}+x^{18}+x^{17}+x^{8}+x^{7}+x^{6}$ $+x^{5}+x^{2}+1$	1111111111111100000000111100101
$x^{30}+x^{29}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{23}$ $+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}$ $+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^{9}+x^{8}+x^{7}$ $+x^{6}+x^{5}+x^{4}+x^{3}+x^{2}+x+1$	1111111111111111111111111111111

The codewords in C are ideals of the polynomial ring $F_2^{31}\,[x]/\langle x^{31}-1\rangle$. We have $m=71, n=31$ (which is a Mersenne prime), $W_{max}=31$, $d_{max}=31, (n,m,d_{max})=(31,71,31)$.

Table 10: Analysis of (n,m,d_{max}) of $F_2^{n}\,[x]/\langle x^{n}-1\rangle$

n	11	15	17	21	30	31
m	4	55	7	39	31	71
d_{max}	11	15	17	21	30	31

GAP Software was used to confirm that all the repetition codes of odd length addressed in this research were perfect, (see Olege, $etal$[33]).

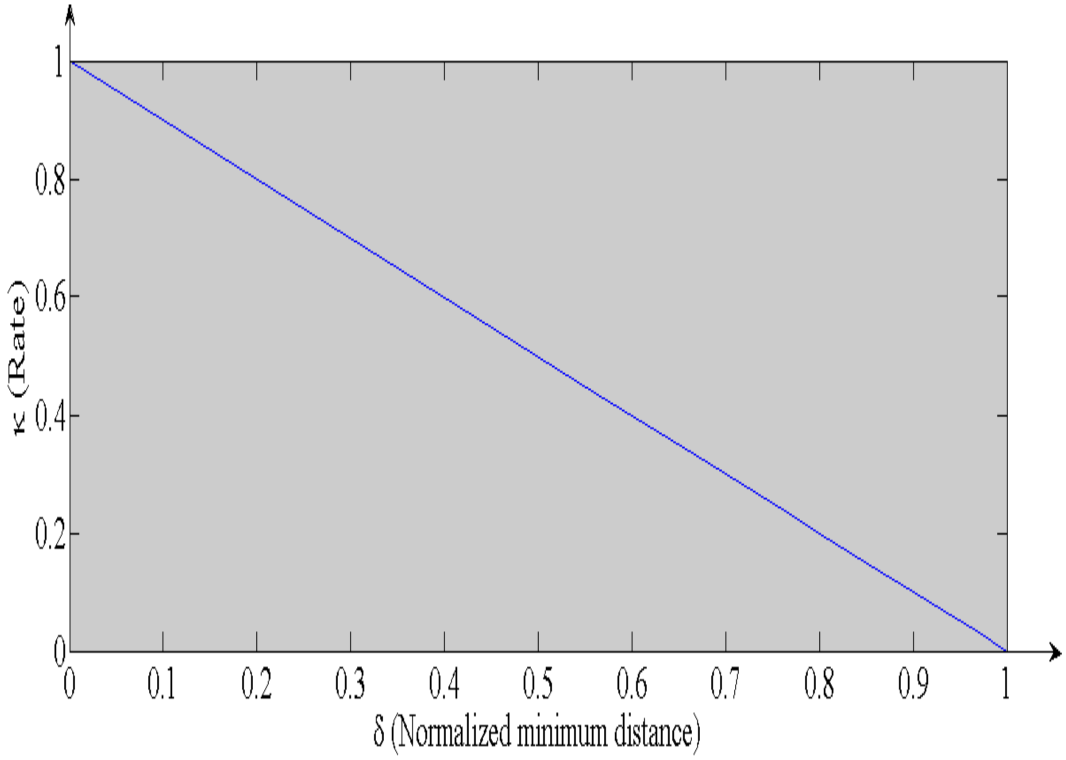
Remark 4.7.1. *There is no standard formula for determining the value of m for an arbitrary value of n. It was also observed that for the optimal codewords $n=W_{max}=d_{max}$.*

Table 11: Relationship between κ_c and δ_c for $F_2^{31}[x]/\langle x^{31}-1\rangle$

Weight	0	1	2	3	4	5	6	7	8
d	0	1	2	3	4	5	6	7	8
δ_c	0.000	0.0333	0.0667	0.1000	0.1333	0.1667	0.20007	0.2333	0.2667
κ_c	1.000	0.9677	0.9333	0.9000	0.8667	0.8333	0.8000	0.7667	0.7333

Weight	10	11	12	13	17	18	20	30	31
d	10	11	12	13	17	18	20	30	31
δ_c	0.333	0.3548	0.3871	0.4333	0.5667	0.5806	0.6452	0.6129	1.0000
κ_c	0.6667	0.6452	0.6129	0.5633	0.4333	0.4194	0.3548	0.3871	0.0000

Figure 1: Graph of the Code Region of $F_2^{31}[x]/\langle x^{31}-1\rangle$



According to Olege, *etal* [32], we could graph in $[0,1] \times [0,1]$, all the pairs (δ_c, κ_c) determined by some code $C \in F_2^n[x] \bmod(x^n-1)$, but some of these correspond to codes which are not practical. For instance, the length 1 binary code $C = [0,1]$ has $(\delta_c, \kappa_c) = (1, 1)$ but it can neither detect nor correct any error. The results become more meaningful when the length n is large enough.

Therefore, instead of graphing all attainable pairs (δ_c, κ_c), we adopted the other extreme and considered only those pairs that could be obtained by codes of arbitrarily large n. The point $(\delta, \kappa) \in [0, 1] \times [0, 1]$ belongs to this code region if and only if there is a sequence (C_n) of codewords C with unbounded length n for which $\delta = \lim_{n\to\infty} \delta(C_n)$ and $\kappa = \lim_{n\to\infty} \kappa(C_n)$. The code region is the set of all accumulation points in $[0, 1] \times [0, 1]$ of the graph of determined pairs (δ_c, κ_c).

By Manin Theorem [26] there is a continuous, non increasing function f_m on the interval [0, 1] such that the point (δ, κ) is in the code region if and only if $0 \leq \kappa \leq\ f_m$.

In their work Olege, *etal* [32] pointed out that if the point (δ, κ) is in the code region, then this region should contain as well the points, (δ', κ) for $\delta' < \delta$, corresponding to codes with the same rate but smaller distance and also the points (δ, κ') for $\kappa' < \kappa$, corresponding to codes with the same distance but smaller rate. Thus for any point in the code region, the rectangle with corners $(0, 0), (0, \kappa), (\delta, \kappa)$ and $(\delta, 0)$ is contained within the boundaries of the code region.

4.8 Residue classes

Definition 4.8.1. *[9] An ideal J of R defines a partition of R into disjoint cosets, residue classes modulo J. This forms a ring; when addition and multiplication are defined as follows.*

$(a + J) + (b + J) = (a + b) + J$

$(a + J)(b + J) = (ab) + J$

This ring is called the residue class ring and is denoted as R/J.

Thus the residue class ring $R_s = \mathbb{F}(x)/\langle x^n - 1\rangle = \{f : f + (x^n - 1) \mid f \in \mathbb{F}_q(x)\}$ with null $\bar{f_0}.\ \bar{f_1} = f_0, \bar{} f_1, f_0, f_1 \in \mathbb{F}_q(x)$.

A codeword c means a vector $c = (c_0, c_1, ..., c_{n-1}) \in \mathbb{F}_q^n$, or c is an element of the residue class $c = c(x) + (x^n - 1)$ $\in$Res$_{q,n}$, where $c(x)$ is the uniquely defined polynomial $\Sigma_{i\in n} c_i x^i$ of degree less than n, which is the canonical representation of this residue class.

Example 4.8.1. *Binary cyclic codes of length 7 amounts to listing all ideals of $Res_{2,7} = \mathbb{F}_2^7(x)/\langle x^7 - 1\rangle$ where $x^7 - 1 \equiv (x+1)(x^3+x+1)(x^3+x^2+1)$. Let $a(x) = (x+1), \phi_1(x) = (x^3+x+1), \phi_2(x) = (x^3+x^2+1)$. Then $g(x) = a(x)\phi_1(x)\phi_2(x)$ generates (0). The three irreducible factors determine $2^3 = 8$ cyclic codes (if (0) is included).*

Theorem 4.8.1. *Let $f_1 \in \mathbb{F}_2^n$. Then the residue class ring $\mathbb{F}_2^n/\langle f_1\rangle$ is a field if and only if f_1 is irreducible over $\mathbb{F}_2^n$.*

Proof

Assume that f_1 is irreducible. We should show that each non-zero element $f_2 + f_3 \in \mathbb{F}_2^n/\langle f_1\rangle$ has a multiplicative inverse. This implies that $\mathbb{F}_2^n/\langle f_1\rangle$ is a field. Let $\bar{f}_2 = \bar{f}_1 + \bar{f}_3$ for each $\bar{f}_1, \bar{f}_3 \in \mathbb{F}_2^n$. If $\bar{f}_2 \neq \bar{0}$, then $f_2 \notin f_1$ implying that the $\gcd(f_1, f_2) = 1$. Therefore $f_1u + f_2v = 1$, for some $u, v \in \mathbb{F}_2^n$ and hence $\overline{f_2u} = \bar{f}_2\bar{u} = \bar{1}$. Hence $u + f_1$ is the inverse of $f_1 + f_2$.

Conversely suppose f_1 is reducible say $f_1 = \alpha\beta$ for some $\alpha\beta \in \mathbb{F}_2^n$ of positive degree. Then 0 <degree α, degree β <degree f_1 and therefore f_1 divides α or β. Hence $\bar{\alpha}, \bar{\beta} \neq 0$ but $\bar{\alpha}\bar{\beta} = \bar{f}_1 = \bar{0}$, implying that $f_2 + f_3 \in \mathbb{F}_2^n/\langle f_1\rangle$ is not an integral domain and therefore not a field. □

4.9 Characterization of codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$.

Definition 4.9.1. *[10]*

A lattice $\bigwedge$ is a discrete additive subgroup of $\mathbb{R}^n$. That is $\bigwedge \subseteq \mathbb{R}$ satisfying the following properties:

(i) $\bigwedge$ is closed under addition and subtraction.

(ii) There exists an $\epsilon > 0$ such that any two distinct lattice points $x \neq y$ are at a distance at least $\mid x - y \mid \geq \epsilon$.

In order to study their lattice properties we shall treat polynomial codes as spheres. Let a packing $P \subset \mathbb{R}^n$ contain spheres centered at u and v. Suppose this is true, then there is also a sphere centered at either $u+v$ or $u-v$.

Claim 4.9.1. *We claim that the minimum Hamming distance d_c induces a metric in the code space.*

Proposition 4.9.1. *Suppose $1 \leq c < \infty$ and d_c is the minimum Hamming distance of polynomial codes $u, v \in F_2^n\,[x]/\langle x^n-1\rangle$ given by $d_c(u,v) = (\sum_{i=1}^n \mid u_i - v_i \mid^c)^{\frac{1}{c}}$ for $u=(u_1,u_2,...,u_n)$ and $v=(v_1,v_2,...,v_n)$. Then, the induced metric in the code space is given by $d_c(u,v) = (\sum_{i=1}^n d(u_i,v_i)^c)^{\frac{1}{c}}$.*

Proof

Suppose $u=(u_1,u_2,...,u_n)$ and $v=(v_1,v_2,...,v_n)$ for all $u,v \in F_2^n\,[x]/\langle x^n-1\rangle$. The metric induced by d_c is given by $d_c(u,v)$= inf.$d(u',v')$; where $u'=u+qe, v'=v+qz$ for all $e,z \in F_2^n\,[x]/\langle x^n-1\rangle$ =(inf $\{\sum_{i=1}^n \mid u_i - v_i - q(z_i - e_i) \mid^c, e,z \in F_2^n\,[x]/\langle x^n-1\rangle\})^{\frac{1}{c}}$

$= (\sum_{i=1}^n \mid u_i - v_i - q(\frac{u_i-v_i}{q}) \mid^c)^{\frac{1}{c}}$. (i)

Equation (i) is minimum when $= (\sum_{i=1}^n \mid u_i - v_i - qA_i \mid^c)^{\frac{1}{c}}$, for $A_i = \mid \frac{u_i-v_i}{q} \mid$.

Suppose $\alpha_i = (\frac{u_i-v_i}{q})$ for $i=1,2,3,...,n$. Since $0 \leq \mid u_i - v_i \mid \leq q$, it follows that $-1 \leq \frac{u_i-v_i}{q}$ and $\alpha_i \in \{-1,0,1\}$. If $\alpha^i = 0$ for some i then $\frac{-q}{2} \leq u_i - v_i \leq \frac{q}{2}$. In such a case min $\{\mid u_i - v_i \mid, q- \mid u_i - v_i \mid\} = \mid u_i - v_i \mid$.

If $\alpha_i = 1$ for some i then $\frac{-q}{2} \leq u_i - v_i \leq q$ and min $\{\mid u_i - v_i \mid, q- \mid u_i - v_i \mid\} = q- \mid u_i - v_i \mid$ and $\mid u_i - v_i \mid = u_i - v_i$. If $\alpha_i = -1$ for some i then $-q \leq u_i - v_i \leq \frac{-q}{2}$ and min $\{\mid u_i - v_i \mid, q- \mid u_i - v_i \mid\} = q- \mid u_i - v_i \mid$ and $\mid u_i - v_i \mid = u_i - v_i$ and hence
$d_c(u,v) = (\sum_{i=1}^n d(u_i,v_i)^c)^{\frac{1}{c}}$. □

Proposition 4.9.2. *Suppose $\bigwedge_C$ is a $q-$ array lattice and $v=(v_1,v_2,...,v_n)^e \in \mathbb{R}^n$ is the received vector. Let $v \in \mathbb{R}^n$, $C \in F_2^n\,[x]/\langle x^n-1\rangle$ and $c \in C, c=(c_1,c_2,...,c_n)^e$, $0 \leq c_i < q$, a neighbor codeword to u. Considering the induced metric $d_c \in F_2^n\,[x]/\langle x^n-1\rangle$ another neighbor $z \in \bigwedge_C$ is given by $(z_1,z_2,...,z_n)^e$ where $z_i = c_i + qA_i$ for $A_i = \mid \frac{v_i-u_i}{q} \mid$ for $i=1,2,3,...,n$.*

Proof

We should show that if $u \in C$ and $z = u+qA$, for $A_i =\mid \frac{v_i-u_i}{q} \mid$, then $d(v,z) = d_c(v,z)$. We know that $c \in C$ satisfies $d_c(v,c)$=min$\{d_c(v,u), u \in C\}$. For $A_i =\mid \frac{v_i-u_i}{q} \mid$ it follows that $d(v, c+qA_i) = d_c(v,c) \leq \min\{d(v,u+qe), u \in C, e \in F_2^n\,[x]/\langle x^n-1\rangle$. Hence $c+qA_i$ is the neighbor of $\bigwedge_C$ that minimizes the distance $d_c(v,u)$. □

Our next problem is the characterization of perfect codes generated by the candidate ring.

We already know that perfect codes satisfy the sphere packing bound with equality, (see Hall [18]).

Proposition 4.9.3. *Given the range $1 \leq n < \infty$ perfect codes exist in the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$ induced by the metric d_c for $\kappa_c = 1$ and any $\ell = 2n+1$.*

Proof

If $n = 1$ the result is clear. Suppose $1 < n < \infty$. The inequality $\mid u_1 \mid^n + \cdots + \mid u_n \mid^n \leq 1$ has $2n+1$ integer solutions namely $u_i = \pm 1$ and $u_j = 0$ for all $j \neq i$ and $u_i = 0$ for all i. Define $\aleph_n(n,1)$ to be the number of points in $F_2^n\,[x]/\langle x^n - 1\rangle$ inside a sphere centered at the origin. Then $\aleph_n(n,1) = 2n+1 = \aleph_1(n,1)$. But there exists at least one perfect code $C \subseteq F_2^n\,[x]/\langle x^n - 1\rangle$ in the metric d_c satisfying the proposition. It follows that this code must also be perfect in the metric d_c for any $1 < n < \infty$, because $\mid C \mid \aleph_n(n,1) =\mid C \mid \aleph_1(n,1) = 2^n$. □

The perfect codes characterized by Proposition 4.9.3 are trivial. The next problem is to characterize non- trivial perfect codes of the candidate polynomial ring.

Proposition 4.9.4. *For an odd integer $\alpha > 1 \in F_2^n\,[x]/\langle x^n - 1\rangle$ and any integer $\beta > 1 \in F_2^n\,[x]/\langle x^n - 1\rangle$, there exists a non-trivial perfect code $C \subseteq F_2^n\,[x]/\langle x^n - 1\rangle$ in the metric $d_\infty(u,v)$ if and only if $q = \alpha\beta$.*

Proof

By the sphere packing bound [51] we know that a code $C \subseteq F_2^n\,[x]/\langle x^n - 1\rangle$ with minimum distance $2\kappa + 1$ is perfect if and only if:

$\mid C \mid (2\kappa+1)^n = q^n$. This implies that $\mid C \mid = \frac{q^n}{(2\kappa+1)^n}$. This means q must have an odd factor and so $q \neq 2^n$. If q is prime then $2\kappa+1 = q$ which gives a perfect trivial code. Thus there is no perfect code for prime q or composite q, a power of 2.

Suppose $q = \alpha\beta$. Let the code C be generated by the vectors $\{(\alpha, 0..., 0), (0, \alpha, 0, 0, ..., 0), ..., (0, ..., 0, \alpha)\} \in C \subseteq F_2^n\,[x]/\langle x^n - 1\rangle$. Therefore $\mid C \mid = \beta^n$. Suppose $e \in F_2^n\,[x]/\langle x^n - 1\rangle$. If $e = \beta n + v$, for $0 \leq v < \beta$ then $e(0, ..., \alpha, 0, ..., 0) = v(0, ..., \alpha, ...0)$. In this case the minimum distance d_c=min$\{d_\infty(u, v), u, v \in C, u \neq v\} = \alpha$. This implies that $\kappa_c = \frac{\alpha-1}{2}$. Since $\aleph_\infty(n, \kappa_c) = (2\kappa+1)^n = \alpha^n$, it follows that $\mid C \mid \aleph_\infty(n, \kappa_c) = \alpha^n\beta^n = q^n$ for $1 <\mid C \mid< q^n$. This code is perfect and non-trivial. □

Remark 4.9.1. *There are no perfect codes of length $n \in \mathbb{N}$ and $\kappa_c > 1$.*

Such a code cannot be plotted within the proposed code region of $F_2^n\,[x]/\langle x^n - 1\rangle$. The major feature of such a code is the message length which is greater than the length of the code.

Let W_{11} denote a polynomial code generated by $b(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Its generator matrix is

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

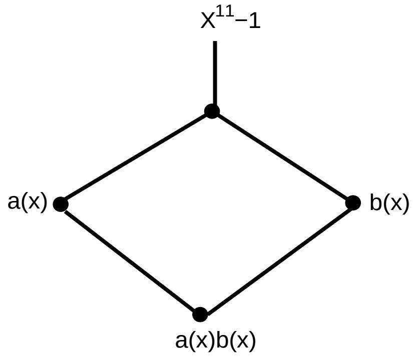
and hence (11, 1) is a repetition code.

The cyclic code C_{11} with generator polynomial $a(x) = x + 1$ is $(11, 10)$ code. From the generator polynomial we obtain a generator matrix which can be transformed into a systematic generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Hence C_{11} is isometric to a parity check code. It consists of all even weight vectors in $\mathbb{F}_2^{11}$.

Figure 2: Lattice diagram of the generators of $x^{11} - 1$



Definition 4.9.2. *[10] A geometric lattice is a regular arrangement of points in an n-dimensional Euclidean space. A polyhedron is a solid in three dimensions whose surface is made up of a number of polygonal surfaces.*

Geometrically Figure 2 is a lattice diagram with 4 lattice points. In this research each lattice point is a codeword. The shape of this geometric lattice is a rhombus.

Let W_{15} denote a cyclic code which is generated by $d_1(x)d_2(x)d_3(x)d_4(x) = (x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1) = x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$. Its generator matrix is $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ and hence W_{15} is a (15, 1) repetition code. The cyclic code S_4 with generator polynomial

$a(x)d_1(x)d_2(x)d_4(x) = x^{11}+x^{10}+x^9+x^8+x^6+x^4+x^3+1$ is a (15, 4) code with generator matrix

$$\begin{bmatrix} 1&0&0&1&1&0&1&0&1&1&1&1&0&0&0 \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ 0&0&1&0&0&1&1&0&1&1&1&1&0&1&0 \\ 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \end{bmatrix}$$

which is the check matrix of the fourth order binary Hamming-code and so S_4 is a binary simplex code. The cyclic code S_4' with generator polynomial $a(x)d_1(x)d_3(x)d_4(x) = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$ is also (15, 4) code which is isometric to S_4. The cyclic code C_{15} with generator polynomial $a(x) = x + 1$ is (15, 14) code. From its generator polynomial we obtain a generator matrix that can be transformed using elementary row transformations into the systematic generator matrix

$$\begin{bmatrix} 1&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&1 \end{bmatrix}$$

Hence C_{15} is isometric to a parity check code. It consists of all even weight vectors in $\mathbb{F}_2^{15}$.

The cyclic code H_8 generated by $d_3(x)d_4(x) = x^8 + x^5 + x^3 + 1$ is (15, 7) code with generator matrix

$$\begin{bmatrix} 1&0&0&1&0&1&0&0&1&0&0&0&0&0&0\\ 0&1&0&0&1&0&1&0&0&1&0&0&0&0&0\\ 0&0&1&0&0&1&0&1&0&0&1&0&0&0&0\\ 0&0&0&1&0&0&1&0&1&0&0&1&0&0&0\\ 0&0&0&0&1&0&0&1&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&0&1&0&1&0&0&1&0\\ 0&0&0&0&0&0&1&0&0&1&0&1&0&0&1 \end{bmatrix}$$

Now $H_8^{\perp}$ has the generator polynomial $a(x)d_1(x)d_2(x) = x^7 + x^3 + x + 1$ so that $H_8^{\perp}$ is the simplex code S_8, hence H_8 is a Hamming code.

Generator matrix for $a(x)$

$$\begin{bmatrix} 1 & 1 \end{bmatrix}$$

Generator matrix for $d_1(x)$

$$\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

Generator matrix for $d_2(x)$

$$\begin{bmatrix} 1&0&0&1&1\\ 1&1&0&0&1\\ 1&1&1&0&0\\ 0&1&1&1&0\\ 0&0&1&1&1 \end{bmatrix}$$

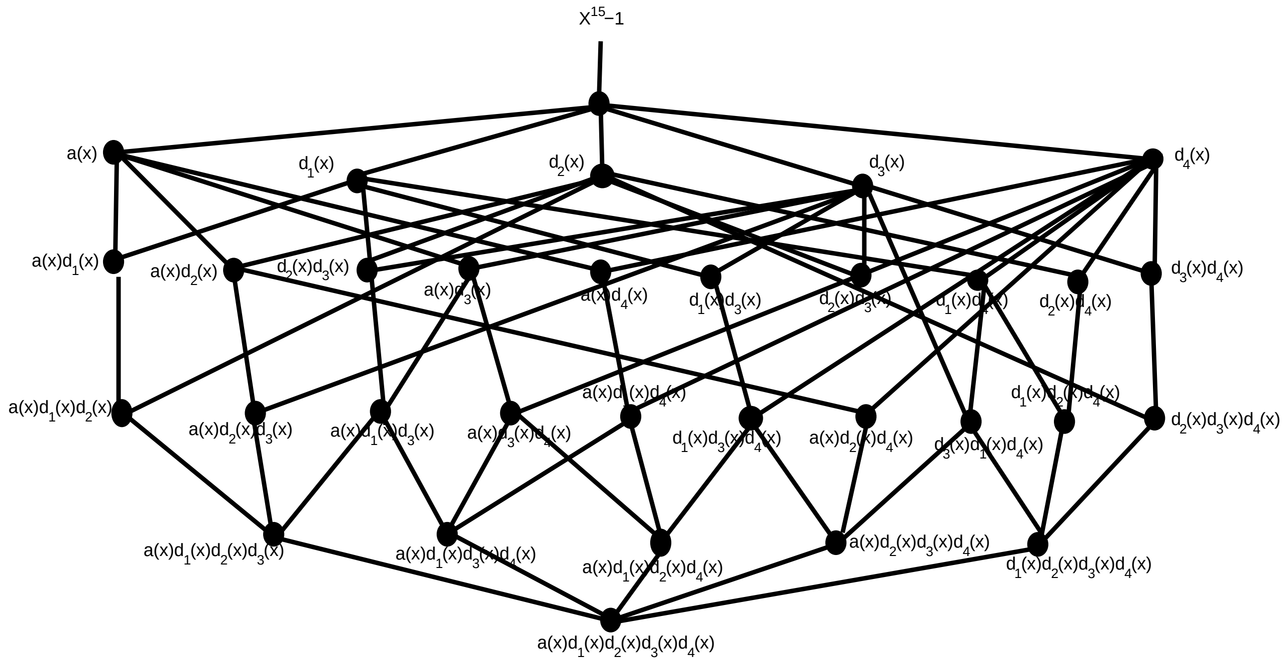
Generator matrix for $d_3(x)$

$$\begin{bmatrix} 1&1&0&0&1\\ 1&1&1&0&0\\ 0&1&1&1&0\\ 0&0&1&1&1\\ 1&0&0&1&1 \end{bmatrix}$$

Generator matrix for $d_4(x)$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Figure 3: Lattice diagram of the generators of $x^{15} - 1$



Geometrically this is a closed lattice diagram with 57 lattice points. It is a polyhedron with 57 vertices.

Let W_{17} denote a cyclic code generated by

$$t_1(x)t_2(x) = x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1.$$

This has the generator matrix $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ and hence W_{17} is (17, 1) repetition code. The cyclic S_8 code with generator polynomial $a(x)t_1(x) = (x+1)(x^8+x^7+x^6+x^4+x^2+x+1) = x^9+x^6+x^5+x^4+x^3+1$ is (17, 8) code with generator matrix

$$\begin{bmatrix}
1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1
\end{bmatrix}$$

This is the check matrix of the eighth order binary Hamming-code and so S_8 is a binary simplex code. The cyclic code S'_8 with generator polynomial $a(x)t_2(x) = x^9 + x^8 + x^6 + x^3 + x + 1$ is also (17, 8) which is isometric to S_8. The cyclic code C_{17} with generator polynomial $a(x) = x + 1$ is (17, 16) code. From the generator polynomial we obtain a generator matrix that can be transformed into the systematic generator matrix by row transformations.

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1
\end{bmatrix}$$

A cyclic code H_8 generated by $t_1(x) = x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$
is a (17, 9)-code with generator matrix

$$\left[\begin{array}{ccccccccccccccccc}
1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1
\end{array}\right]$$

The matrix $H_8^{\perp}$ has the generator polynomial $x^9 + x^8 + x^6 + x^3 + x + 1$ so that $H_8^{\perp}$ is the simplex code H_8, hence H_8 is a Hamming code.

Generator polynomials:

$$\begin{aligned}
a(x) &= x + 1 \\
t_1(x) &= x^8 + x^7 + x^6 + x^4 + x^2 + x + 1 \\
t_2(x) &= x^8 + x^5 + x^4 + x^3 + 1
\end{aligned}$$

Generator matrix for $a(x)$

$$\left[\begin{array}{cc} 1 & 1 \end{array}\right]$$

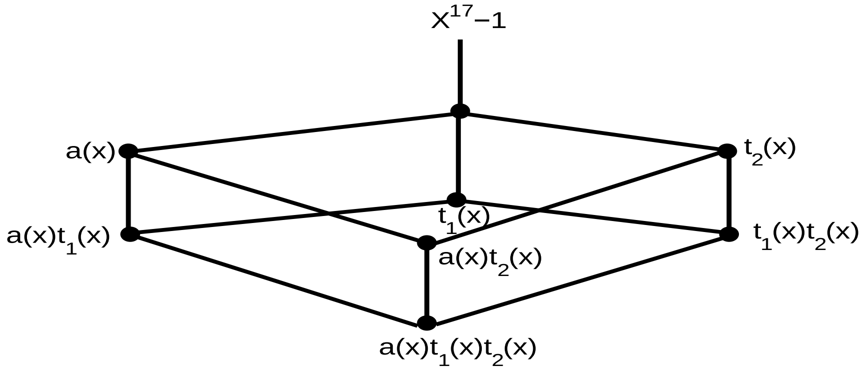
Generator matrix for $t_1(x)$

$$\left[\begin{array}{ccccccccc}
1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1
\end{array}\right]$$

Generator matrix for $t_2(x)$

$$\left[\begin{array}{ccccccccc}
1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1
\end{array}\right]$$

Figure 4: Lattice diagram of the generators of $x^{17}-1$



Geometrically this is a lattice diagram with 8 lattice points. It is a cuboid. Let W_{21} denote a cyclic code generated by $\gamma_1(x)\gamma_2(x)\gamma_3(x)\gamma_4(x)\gamma_5(x) = x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^{9}+x^{8}+x^{7}+x^{6}+x^{5}+x^{4}+x^{3}+x^{2}+x+1$. This has the generator matrix $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ and hence W_{21} is (21, 1) repetition code. The cyclic code S_9 with generator polynomial $\gamma_1(x)\gamma_3(x)\gamma_4(x)\gamma_5(x) = (x+1)(x^2+x+1)(x^3+x^2+1)(x^3+x+1)(x^6+x^5+x^4+x^2-1)$ $= x^{12}+x^9+x^8+x^4+x^3+x^2+x+1$ is (21, 9) code with generator matrix

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1
\end{bmatrix}$$

This is the check matrix of the ninth order binary Hamming-code and so S_9 is a binary simplex code. The cyclic code S_9' with generator polynomial $a(x)\gamma_1(x)\gamma_3(x)\gamma_5(x)$ $= x^{12}+x^{11}+x^{10}+x^9+x^5+x^3+x+1$ is also (21, 9) code which is isometric to S_9.

The cyclic code C_{21} with generator polynomial $a(x) = x + 1$ is (21, 20) code. From the generator polynomial we obtain a generator matrix that can be transformed into the systematic generator matrix by row transformations.

$$\left[\begin{array}{ccccccccccccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1
\end{array}\right]$$

Hence C_{21} is isometric to a parity check code. It consists of all even weight vectors in $\mathbb{F}_2^7$.

A cyclic code H_{12} generated by $a(x)\gamma_1(x)\gamma_3(x)\gamma_5(x) = x^{12}+x^{11}+x^{10}+x^9+x^5+x^3+x+1$ is a (21, 9)-code with generator matrix

$$\begin{bmatrix} 1&1&0&1&0&1&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&1&1&0&1&0&1&0&0&0&1&1&1&1&0&0&0&0&0&0&0 \\ 0&0&1&1&0&1&0&1&0&0&0&1&1&1&1&0&0&0&0&0&0 \\ 0&0&0&1&1&0&1&0&1&0&0&0&1&1&1&1&0&0&0&0&0 \\ 0&0&0&0&1&1&0&1&0&1&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&1&1&0&1&0&1&0&0&0&1&1&1&1&0&0&0 \\ 0&0&0&0&0&0&1&1&0&1&0&1&0&0&0&1&1&1&1&0&0 \\ 0&0&0&0&0&0&0&1&1&0&1&0&1&0&0&0&1&1&1&1&0 \\ 0&0&0&0&0&0&0&0&1&1&0&1&0&1&0&0&0&1&1&1&1 \end{bmatrix}$$

The matrix $H_{12}^{\perp}$ has the generator polynomial $\gamma_2(x)\gamma_4(x) = x^9+x^8+x^5+x^4+x^2+x+1$ so that $H_{12}^{\perp}$ is the simplex code H_{12}, hence H_{12} is a Hamming code.

Generator polynomials:

$a(x) = x + 1$

$\gamma_1(x) = x^2 + x + 1$

$\gamma_2(x) = x^3 + x + 1$

$\gamma_3(x) = x^3 + x^2 + 1$

$\gamma_4(x) = x^6 + x^5 + x^4 + x^2 - 1$

$\gamma_5(x) = x^6 + x^4 + x^2 + x + 1$

Generator matrix for $a(x)$

$$\begin{bmatrix} 1 & 1 \end{bmatrix}$$

Generator matrix for $\gamma_1(x)$

$$\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

Generator matrix for $\gamma_2(x)$

$$\begin{bmatrix} 1&0&1&1 \\ 1&1&0&1 \\ 1&1&1&0 \\ 1&0&1&1 \\ 0&1&1&1 \end{bmatrix}$$

Generator matrix for $\gamma_3(x)$

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Generator matrix for $\gamma_4(x)$

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Generator matrix for $\gamma_5(x)$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Let W_{30} denote a cyclic code generated by $a(x)\lambda_1(x)^2\lambda_2(x)^2\lambda_3(x)^2\lambda_4(x)^2 = x^{29}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^{9}+x^{8}+x^{7}+x^{6}+x^{5}+x^{4}+x^{3}+x^{2}+x+1$. This has the generator matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Hence W_{30} is (30, 1) repetition code. A cyclic code S_{15} with generator polynomial $a(x)\lambda_1(x)\lambda_2(x)\lambda_3(x)^2 = x^{15}+x^{13}+x^{9}+x^{8}+x^{7}+x^{6}+x^{4}+x^{2}+x+1$ is (30, 15) code with generator matrix

$$\begin{bmatrix}
1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&1&1&1&1&0&0&0&1&0&1
\end{bmatrix}$$

This is the check matrix of the fifteenth order binary Hamming-code and hence S_{15} is a binary simplex code. The cyclic code S'_{15} with generator polynomial $a(x)\lambda_1(x)\lambda_3(x)^2\lambda_4(x)$ $= x^{15}+x^{14}+x^{12}+x^{11}+x^{10}+x^{9}+x^{5}+x^{2}+x+1$ is also a (30, 15) code which is isometric to S_{15}. The cyclic code C_{30} with generator polynomial $a(x) = x+1$ is (30, 29) code. From the generator polynomial we obtain a generator matrix that can be transformed into the systematic generator matrix by row transformations.

$$\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1
\end{bmatrix}$$

Therefore C_{30} is isometric to a parity check code and consists of all even weight vectors in $\mathbb{F}_2^{30}$. The cyclic code H_{15} generated by $a(x)\lambda_1(x)\lambda_3(x)^2\lambda_4(x) = x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^5 + x^2 + x + 1$ is a (30, 16)-code with generator matrix

$$\begin{bmatrix}
1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&0&1&1
\end{bmatrix}$$

Now $H_{15}^{\perp}$ has the generator polynomial $a(x)\lambda_1(x)\lambda_3(x)^2\lambda_4(x) = x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^5 + x^2 + x + 1$ so that $H_{15}^{\perp}$ is the simplex code H_{15}, hence H_{15} is a Hamming code.

Generator polynomials:

$$\begin{array}{rcl}
a(x) & = & (x+1) \\
a(x)^2 & = & (x+1)^2 = x^2+1 \\
\lambda_1(x) & = & (x^2+x+1) \\
\lambda_1(x)^2 & = & (x^2+x+1)^2 = x^4+x^2+1 \\
\lambda_2(x) & = & (x^4+x+1) \\
\lambda_2(x)^2 & = & (x^4+x+1)^2 = x^8+x^2+1 \\
\lambda_3(x) & = & (x^4+x^3+1) \\
\lambda_3(x)^2 & = & (x^4+x^3+1)^2 = x^8+x^6+1 \\
\lambda_4(x) & = & (x^4+x^3+x^2+x+1)
\end{array}$$

$$\begin{aligned}\lambda_4(x)^2 &= (x^4+x^3+x^2+x+1)^2\\ &= x^8+x^6+x^4+x^2+1\end{aligned}$$

Generator matrix for $a(x)$

$$\begin{bmatrix} 1 & 1 \end{bmatrix}$$

Generator matrix for $\lambda_1(x)$

$$\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

Generator matrix for $(\lambda_1(x))^2$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Generator matrix for $\lambda_2(x)$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ & & & & \end{bmatrix}$$

Generator matrix for $(\lambda_2(x))^2$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Generator matrix for $\lambda_3(x)$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Generator matrix for $(\lambda_3(x))^2$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Generator matrix for $\lambda_4(x)$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Generator matrix for $(\lambda_4(x))^2$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Let W_{31} denote a cyclic code generated by $\mu_1(x)\mu_2(x)\mu_3(x)\mu_4(x)\mu_5(x)\mu_6(x) = x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. This has the generator matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Hence W_{31} is (31, 1) repetition code. A cyclic code S_{15} with generator polynomial $a(x)\mu_1(x)\mu_2(x)\mu_3(x) = x^{16} + x^{15} + x^8 + x^7 + x^4 + x^3 + x^2 + 1$ is (31, 15) code with generator matrix

$$\begin{bmatrix}
1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1
\end{bmatrix}$$

This is the check matrix of the fifteenth order binary Hamming-code and hence S_{15} is a binary simplex code. The cyclic code S^1_{16} with generator polynomial $a(x)\mu_1(x)\mu_2(x)\mu_4(x) = x^{16} + x^{12} + x^{11} + x^8 + x^6 + x^4 + x^2 + 1$ is also a (31, 15) code which is isometric to S_{15}. The cyclic code C_{31} with generator polynomial $a(x) = x + 1$ is (31, 30) code. From the generator polynomial we obtain a generator matrix that can be transformed into the systematic generator matrix by row transformations.

$$\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1
\end{bmatrix}$$

Therefore C_{31} is isometric to a parity check code and consists of all even weight vectors in $\mathbb{F}_2^{31}$. The cyclic code H_{15} generated by $\mu_4(x)\mu_5(x)\mu_6(x) = x^{15}+x^{14}+x^{13}+x^{11}+x^{10}+1$ is a (31, 16)-code with generator matrix

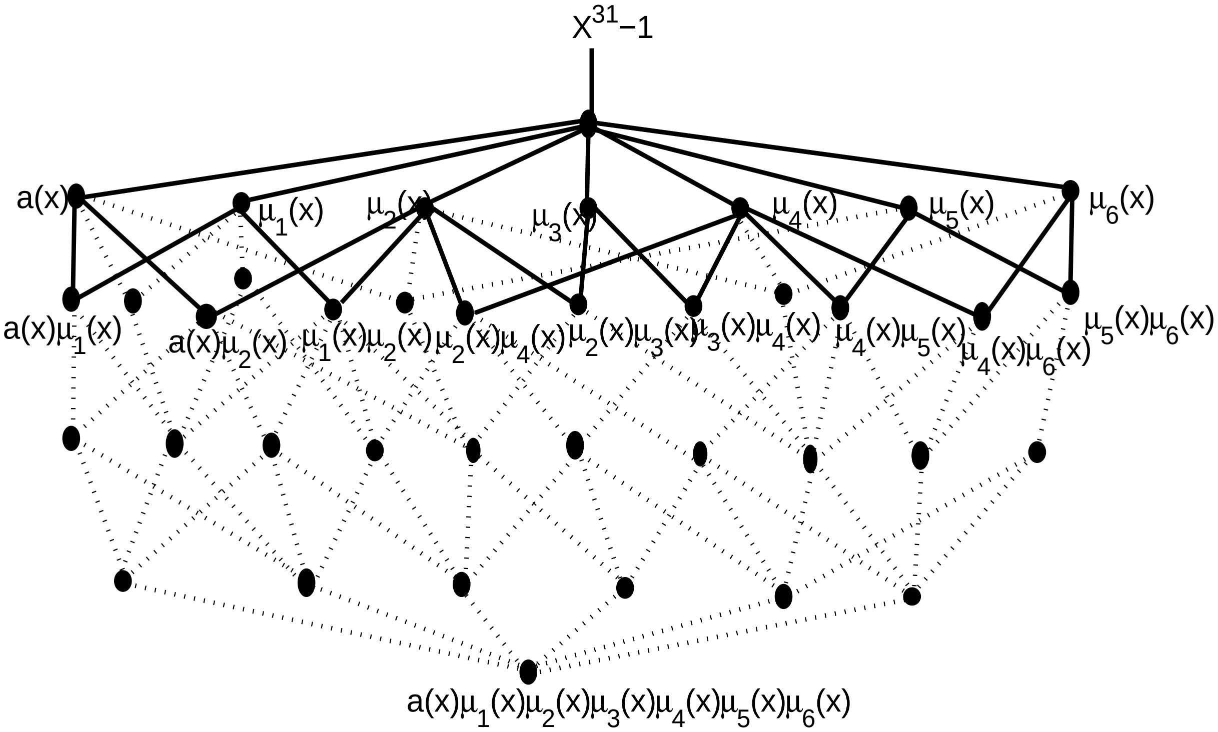
$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1
\end{bmatrix}$$

Now $H_{15}^{\perp}$ has the generator polynomial $a(x)\mu_1(x)\mu_2(x)\mu_3(x) = x^{16} + x^{15} + x^8 + x^7 + x^4 + x^3 + x^2 + 1$ so that $H_{15}^{\perp}$ is the simplex code S_{15}, hence H_{15} is a Hamming code.

Generator polynomials:

$$\begin{aligned}
a(x) &= x + 1 \\
\mu_1(x) &= x^5 + x^2 - 1 \\
\mu_2(x) &= x^5 + x^3 + 1 \\
\mu_3(x) &= x^5 + x^3 + x^2 + x + 1 \\
\mu_4(x) &= x^5 + x^4 + x^2 + x + 1 \\
\mu_5(x) &= x^5 + x^4 + x^3 + x + 1 \\
\mu_6(x) &= x^5 + x^4 + x^3 + x^2 + 1
\end{aligned}$$

Figure 5: Lattice diagram of the generators of $x^{31}-1$



Geometrically this is a lattice diagram with 71 lattice points. It is a polyhedron with 71 vertices.

Generator matrix for $a(x)$

$$\begin{bmatrix} 1 & 1 \end{bmatrix}$$

Generator matrix for $\mu_1(x)$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & -1 \\ -1 & 1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 1 & 0 & 0 & 1 \\ 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 \end{bmatrix}$$

Generator matrix for $\mu_2(x)$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Generator matrix for $\mu_3(x)$

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Generator matrix for $\mu_4(x)$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Generator matrix for $\mu_5(x)$

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Generator matrix for $\mu_6(x)$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Theorem 4.9.1. *Let W_n denote a code with generator polynomial $g(x) = g_0(x) + g_1(x) + g_2(x^2) + ... + g_{n-k}(x^{n-k})$, the generator matrix is given by*

$$G = \begin{bmatrix} g_0 & g_1 & . & . & . & g_{n-k} & 0 & 0...0 \\ 0 & g_0 & g_1 & . & . & . & g_{n-k} & 0...0 \\ 0 & . & . & . & . & & . & . \\ . & & . & . & . & . & . & . \\ . & & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & . & g_{n-k} \end{bmatrix}$$

Proof

We should show that:

(i) $g_0(x) + g_1(x) + g_2(x^2) + ... + g_{n-k}(x^{n-k})$ forms a basis of W_n.

(ii)$dim.(W_n) = k$.

For part (i) the vectors $g_0(x), g_1(x), g_2(x^2), ..., g_{n-k}(x^{n-k})$ are linearly independent. If not we must have a set of coefficients $\{\alpha_i\}$ such that $\alpha_o g_0(x) + \alpha_1 g_1(x) + \alpha_2 g_2(x^2) + ... + \alpha_k g_{n-k}(x^{n-k}) = 0$. But this product has degree $k - 1 + n - k = n - 1 < n$, which cannot be $= 0$ mod$(x^n - 1)$ unless all the $\alpha_i = 0$. Suppose we have $w(x)$ in W_n, then $w(x) = \alpha(x)g(x)$. Assume $\alpha(x)$ has degree $< k-1$. Then $w(x)$ can be written as a linear combination of $x^i g(x)$ for $0 < i < k-1$. The set of all the linear combinations $\{x^i g(x)\}$ is a basis for W_n.

For part (ii) suppose we have two polynomials $p_1(x) \neq p_2(x)$ with degree $p_i(x) \leq k-1$ (for $i = 1, 2$) and $g(x)p_1(x) \neq g(x)p_2(x)$. The set $\tau = \{g(x)p(x) : p(x) \in F_q^n[x]/\langle x^n - 1\rangle$, degree $p(x) \leq k - 1\}$ has q^k elements and is a subset of the ideal $\langle g(x)\rangle$.

Conversely for any codeword $g(x)r(x)$ (for some $r(x) \in F_q^n[x]/\langle x^n - 1\rangle$), we have $g(x)r(x) = y(x)(x^n - 1) + z(x)$ (for some $z(x) \in F_q^n[x]/\langle x^n - 1\rangle$). This means $z(x) = g(x)r(x) - y(x)(x^n - 1)$. Therefore $g(x)$ divides $z(x)$. Let $z(x) = g(x)t(x)$ for some polynomial $t(x) \in F_q^n[x]/\langle x^n - 1\rangle$. This implies that degree $t(x) < k$ and hence $z(x) \in \tau$. Equivalently, $\tau = \langle g(x)\rangle$. Hence the dimension of the code is given by $\log_q|\tau| = k$. □

Proposition 4.9.5. *Let $S_k(q)$ be a simplex code. Then $S_k(q)$ is a constant weight code with parameters $[(q^k - 1)/q - 1, k, q^{k-1}]$.*

Proof

Let $H_k^{\perp}(q)$ be a Hamming code. We know that the simplex code $S_k(q)$ and the Hamming code $H_k^{\perp}(q)$ are dual codes. $H_k(q)$ is a parity check matrix of $H_k^{\perp}(q)$ and the generator matrix of $S_k(q)$.

Consider a parity check matrix $H_k(q)$ with redundancy k. The rank of this matrix $=$ dimension $=k$. Let u be a non zero codeword of the simplex code $S_k(q)$. We have $u - mH_k(q)$ for some non-zero $m \in F_q^n[x]/\langle x^n - 1\rangle$. Let $h_i^{\perp}(q)$ be the i^{th} column of $H_k(q)$ (for $i = 1, 2, 3, ...$). Then $\Sigma u_i = 0$ if and only if $mh_i = 0$. Let $mv = 0$ for some $v \in F_q^n[x]/\langle x^n - 1\rangle$ be a non-trivial homogeneous linear equation. This equation has q^{k-1} solutions. The solutions $(q^{k-1})/q - 1$ such that v^T is a column of $H_k(q)$ is a non-zero multiple of v^T. Hence the number of zeros of u is $(q^{k-1} - 1)/q - 1$. Therefore the weight of u is the number of non-zeros which is q^{k-1}. □

Proposition 4.9.6. *For a polynomial code $P_c \in F_2^n[x]/\langle x^n - 1\rangle$ the the following statements are equivalent*

(i) Hamming weight of P_c is isomorphic to the homogeneous weight.

(ii) Homogeneous weight of P_c is isomorphic to the Hamming weight .

Proof

(i)⇒ (ii) Let $f^n(u) = f(x_1) + ... + f(x_n)$ for all $f^n(u) \in I$ where I is an ideal in $F_2^n[x]/\langle x^n - 1\rangle$. Then;

$$\begin{aligned}
(\Sigma f^n)u &= \frac{1}{R_n u}\Sigma_{v\in R_n} f^n v \text{ for all } f^n(v) \in R_n \textit{ and } R_n = F_2^n[x]\langle x^n - 1\rangle \\
&= \frac{1}{R_n u}\Sigma_{v\in R_n}\Sigma_{i=1}^n f^n(v_i) \\
&= \Sigma_{i=1}^n \frac{1}{R_n u_i}\Sigma_{v\in R_n} f^n(u_i) \\
&= \Sigma_{i=1}^n(\Sigma f)(u_i) \\
&= (\Sigma f)^n(u)
\end{aligned}$$

(ii)⇒ (i) Let $f^n(v) = f(x_1) + ... + f(x_n)$ for all $f^n(v) \in I$ where I is an ideal in

$F_2^n[x]/\langle x^n - 1\rangle$. Then;

$$\begin{aligned}
(\Sigma f^n)v &= \frac{1}{R_n v}\Sigma_{v\in R_n} f^n u \text{ for all } f^n(u) \in R_n \; and \; R_n = F_2^n[x]/\langle x^n - 1\rangle \\
&= \frac{1}{R_n v}\Sigma_{u\in R_n}\Sigma_{i=1}^n f^n(u_i) \\
&= \Sigma_{i=1}^n \frac{1}{R_n v_i}\Sigma_{u\in R_n} f^n(v_i) \\
&= \Sigma_{i=1}^n (\Sigma f)(v_i) \\
&= (\Sigma f)^n(v)
\end{aligned}$$

□

Proposition 4.9.7. *Let W_n be a cyclic code with a check polynomial $h(x) = h_0 + h_1(x) + ... + h_k x^k$. Then W_n has dimension k with the parity check matrix given by:*

$H=$

$$\begin{bmatrix}
h_k & h_{k-1} & . & . & .h_0 & .0 & 0 & . & . & . & 0 \\
0 & h_k & h_{k-1} & . & . & h_0 & 0 & . & . & . & 0 \\
. & . & . & . & . & . & .h_0 & . & . & & . \\
. & & . & . & . & . & . & h_0 & . & . & . \\
. & & & . & . & . & . & . & . & . & . \\
0 & 0 & . & . & . & 0 & h_k & h_{k-1} & . & . & .h_0
\end{bmatrix}$$

Proof

Let the degree of the generator matrix $= n - k$. The dimension of this code is k. Let $u = c_0 + c_1(x) + c_2(x^2) + ... + c_n(x^{n-1})$ for some $u \in F_q^n[x]/\langle x^n - 1\rangle$. Then $u(x)h(x) = 0$. For $d = k, k+1, ..., n-1$ we have $\Sigma c_i h_j = 0$ (for $i + j = d$). These code-vectors are orthogonal to the linear combinations of the rows of H. Hence $C^\perp$ contains the span of the rows of H. Since $hk = 1$, the rank of $h = n - k$. This generates a linear subspace of $C^\perp$, implying that H is the parity check matrix for the check polynomial $h(x)$. □

4.9.1 Syndromes of the simplex codes in the candidate ring

Definition 4.9.3. *[51] Let C be an (n, κ, d) code over $F_2^n[x]/\langle x^n - 1\rangle$ and let H be a parity check matrix for C. For any $w \in F_2^n[x]/\langle x^n - 1\rangle$ the syndrome of w is the codeword $S(w) = wH^T \in F_2^{n-k}[x]/\langle x^n - 1\rangle$.*

Proposition 4.9.8. *[51] Let $u, v \in C$, where C is a codeword generated by $F_2^n\,[x]/\langle x^n - 1\rangle$. The following statements are equivalent.*

(i) u and v are in the same coset.

(ii) u and v have the same syndrome

Proof

(i)$\Longrightarrow$(ii). Suppose u and v belong to the same coset. Then $u = z_1 + e$ and $v = z_2 + e$ for $z_1, z_2 \in C$ and $e \in F_2^n\,[x]/\langle x^n - 1\rangle$. The syndrome corresponding to u is given by $Hu^T = H(z_1 + e)^T = He^T$.

The syndrome corresponding to v is given by $Hv^T = H(z_2 + e)^T = He^T$. Hence the syndrome of u and v are the same.

(ii)$\Longrightarrow$(i). Suppose u and v have the same syndrome. Then
$Hu^T = Hv^T = H(u - v)^T = 0 \Longrightarrow (u - v) \in C$. Since $u - v$ is a codeword then u and v must belong to the same coset. □

The following result summarizes the findings in this thesis.

Theorem 4.9.2. *Consider the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$. Any code generated in this ring satisfies the following properties;*

(a) There is no standard formula for enumerating the codewords.

(b) Let $p < \frac{1}{2}$ where $p + q = 1$. Then maximum likelihood decoding and minimum distance decoding are equivalent.

(c) Let n be fixed and α be the cardinality of a sphere of radius $d_{max} - 1$ about any point $u \in F_2^n\,[x]/\langle x^n - 1\rangle$. A code (n, κ, d_{max}) exists for all values of $\alpha < q^{n-\kappa+1}$. In brief $n = d_{max} = W_{max}$

(d) Let $g(x) \in F_2^n\,[x]/\langle x^n - 1\rangle$ be an irreducible and monic factor of $x^n - 1$. The following statements are equivalent:

(i) $g(x)$ is a generator polynomial of $F_2^n\,[x]/\langle x^n - 1\rangle$.

(ii) $\langle g(x)\rangle$ is a generator of the set of ideals $I(C) \in F_2^n\,[x]/\langle x^n - 1\rangle$.

(e) A polynomial code $P_c \in F_2^n\,[x]/\langle x^n - 1\rangle$ can control up to e errors if and only if

$d_{max} \geq 2e + 1$.

(f) A polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ generates an error control code for $n \geq 3$.

(g) Suppose $1 \leq c < \infty$ and d_c is the minimum Hamming distance of polynomial codes $u, v \in F_2^n[x]/\langle x^n - 1\rangle$ given by $d_c(u, v) = (\sum_{i=1}^{n} \mid u_i - v_i \mid^c)^{\frac{1}{c}}$ for $u = (u_1, u_2, ..., u_n)$ and $v = (v_1, v_2, ..., v_n)$. Then, the induced metric in the code space is given by $d_c(u, v) = (\sum_{i=1}^{n} d(u_i, v_i)^c)^{\frac{1}{c}}$.

(h) Suppose $\bigwedge_C$ is a $q-$ array lattice and $v = (v_1, v_2, ..., v_n)^e \in \mathbb{R}^n$ is the received vector. Let $v \in \mathbb{R}^n$, $C \in F_2^n[x]/\langle x^n - 1\rangle$ and $c \in C, c = (c_1, c_2, ..., c_n)^e$, $0 \leq c_i < q$, a neighbor codeword to u. Considering the induced metric $d_c \in F_2^n[x]/\langle x^n - 1\rangle$ another neighbor $z \in \bigwedge_C$ is given by $(z_1, z_2, ..., z_n)^e$ where $z_i = c_i + qA_i$ for $A_i = \mid \frac{v_i - u_i}{q} \mid$ for $i = 1, 2, 3, ..., n$.

(i)Given the range $1 \leq n < \infty$ perfect codes exist in the polynomial ring $F_2^n[x]/\langle x^n - 1\rangle$ induced by the metric d_c for $\kappa_c = 1$ and any $\ell = 2n + 1$.

(j) For an odd integer $\alpha > 1 \in F_2^n[x]/\langle x^n - 1\rangle$ and any integer $\beta > 1 \in F_2^n[x]/\langle x^n - 1\rangle$, there exists a non-trivial perfect code $C \subseteq F_2^n[x]/\langle x^n - 1\rangle$ in the metric $d_\infty(u, v)$ if and only if $q = \alpha\beta$.

(k) For a polynomial code $P_c \in F_2^n[x]/\langle x^n - 1\rangle$ the Hamming weight of P_c is isomorphic to the homogeneous weight.

Proof

Result (a) is observed from the illustrations in $F_2^n[x]/\langle x^n - 1\rangle$ where $n = 11, 15, 21, 30, 31$.

For the rest of the results refer to Theorem 4.5.1 and Propositions 3.3.1, 4.6.2, 4.7.1, 4.7.2, 4.9.1, 4.9.2, 4.9.3, 4.9.4 and 4.9.6.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

This chapter has two sections. Section 5.1 presents conclusion of our results. Section 5.2 provides recommendations for future research.

5.1 Conclusion

In this research we have applied some aspects of algebraic coding theory namely; principles of maximum likelihood decoding, minimum distance decoding, incomplete minimum distance decoding, features of an optimal code, efficiency and reliability of code vectors to the generators of codes of the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$. We have investigated the generators of codes of ideals of the polynomial ring obtained by modulo multiplication, cyclic shifts, irreducible polynomials, and an on-line-tool WWW.quickmath.com. The on-line tool was capable of providing generators of codes of any variable length n. A procedure for constructing the proposed code has been outlined. The code generators were characterized as complex lattices whose kissing numbers increased with increasing values of n. For a given n, the various code generators were isomorphic to their simplex generator matrices. It was established that a code of length n is suitable for error control if and only if the maximum Hamming distance $d_{max} \geq 3$. Table 10 revealed that there is a one to one correspondence between n and d_{max} for the codes generated by the polynomial ring $F_2^n\,[x]/\langle x^n - 1\rangle$. All the code generators have a parity check polynomial of $(x + 1)$. From Graph 1, the codes generated form a Shannon's code region as traced out by Manin's bound [26].

5.2 Recommendations

We believe there are many other optimal codes within the code region of $F_2^n\,[x]/\langle x^n - 1\rangle$ which could be found by examining all polynomials without being limited to those with certain theoretical properties for instance computing exact weight as has been done in this research. The ring $F_2^n[x]/\langle x^n - 1\rangle$ is an inexhaustible tank containing any binary polycodewords one can think of. We strongly recommend that any future search for optimal polynomial codes should be done using this ring. Other generators of codes of polynomial rings could be found by use of another polynomial ring $F_q^n[x]/\langle x^n - 1\rangle$ for prime $q \neq 2$.

REFERENCES

[1] Adams, S. S. (2008), *Introduction to Coding Theory,* (3rd ed.), Cornel University Press, Berlin.

[2] Alderson, T. L. (2008), Geometric constructions of optimal optical orthogonal codes*Advances in mathematics of communication* Vol. 2, No. **4**, 451-467.

[3] Aryasomayajula, A., Biswas, I., Morye, A.S., and Parameswaran, A. J. (2017), *Analytic and Algebraic Geometry*, Springer, Singapore.

[4] Berrou, C. Glavieux, A. (1966), Near optimum error correcting coding and decoding: Turbo-codes, *IEEE Trans. Commun.*, Vol. 44, No. **10**, 1261-1271.

[5] Bose R. C. and Ray-Chaudhuri, D. K. (1960), On a class of error correcting binary group codes, Information and control, Vol. 3, 68-79.

[6] Brookshear, J. (2000), *Computer science: an overview* (6th ed.), Addison Wesley.

[7] Castagnoli, G., Braeuer, S. and Herman, M. (1993), Optimization of cyclic redundancy-check codes with 24 and 32 parity bits, *IEEE Trans. on communications,* Vol. 41, No. **6**, 883-892.

[8] Cesar, F. C., Nestor R. B., and Araceli N. P.(2007), Maximum Likelihood Decoding on a Communication Channel, *Journal of Information Control*, Vol. 16, No. **18**, 55-57.

[9] Charles, C. (2000), *Abstract Algebra* (2nd.ed.) , McGraw Hill publishing Company, New York, USA.

[10] Daniele, M. and Feige, U. (2004), The inapproximability of lattice and coding problems with preprocessing, *Journal of Computer and System Sciences*, Vol. 69, No. **1**, 45-69.

[11] Dedekind, R. (1876), *Algebraic number theory and foundations of real numbers*, Frentice Berlin Germany.

[12] Driver, E., Leonard, P. A. and Williams K. S.(2005), Irreducible quartic polynomials with factorization modulo p, *Amer.maths. monthly,* Vol.112 No.**10**, 876-890.

[13] Dubner, H. and Gallot, Y. (2002), Distribution of generalized Fermat prime numbers, *Math. Comp.* Vol.71, No.**238**, 825-832.

[14] Elias, P. (1955), Coding for noisy channels *IRE Conv. Record,* Vol.4, 37-47.

[15] Golay, M. J. E. (1949), Notes on digital coding, *Proc. IEEE,* Vol. 37, 657

[16] Hamming, R. W. (1950), Error detecting and error correcting codes, *Bell Syst. Tech. J.Vol.* 29, 147-150.

[17] Hai, Q. D. Chengju, L. and Qin, Y. (2014), Recent progress on weight distributions of cyclic codes over finite fields, *Journal of algebra combinatorics discrete structures and application*, Vol. 2, No.**1**, 39-63.

[18] Hall, J. (2003), *Algebraic Coding Theory*, Michigan State University U.S.A.

[19] Huffman, W. C. and Pless, V. (2003), *Fundamentals of Error-Control Coding*, Cambridge University Press, New York, USA.

[20] Kazakov, P.(2001), Fast Calculation on the Number of Minimum Weight Words of CRC Codes, *IEEE Trans.Inf. Theory,* Vol. 47, No. **3**, 1190-1195.

[21] Koopman, P. (2014), Software and digital systems program, data integrity techniques (Contract DTFACT-11-C-00005) *Brendan Hall Honeywell Laboratories.*

[22] Kummer, E. (1847), *The theory of ideals*, Indian Institute of Technology, Bombay University of New South Wales, New Delhi India, 31-157.

[23] Leo, C. (2004), *Modern algebra and the rise of mathematical structures* (2nd ed.), Birkhauser Verlag, Basel.

[24] Macwilliams, F. J. and Sloane, N. J. A. (1981), *Theory of error correcting codes*, North Holland publishing company.

[25] Manish, G. Bhullar, J. S. and Vinocha, O. P. (2010), On the Combination of Five Cyclic Code Int. *J. Contemp. Math. Sciences,* Vol. 5, No. **33**, 1627 - 1635.

[26] Manin, Y.I. (2016). Error correcting codes and neural networks, Sel. Math. New Ser. https://doi.org/10.1007/s00029-016-0284-4.

[27] Miranda, E. S. (2012), A note on Jacobson rings and generalizations, East-West JM Vol.14, No.**1**, 37-42.

[28] Moschoyiannnis, S. K. (2001), *Group theory and error detecting/correcting codes.* (SCOMP-TC-02-01) School of electronics computing and mathematics, Department of computing, University of Surrey.

[29] Muller, D. E. (1954), Application of boolean algebra to switching circuit design, *IEEE Trans. on computers,* Vol.3, No. **3**, 6-12.

[30] Nechaev, A. A. and Tzypyshev, V. N. (2000), Artinian bimodule with quasi-Frobenius canonical bimodule, Proc. Int. Workshop devoted to 70th anniversary of scientific algebraic workshop of Moscow State University, 39-40.

[31] Olege, F., Aywa, S., Rao G. K. R. and Wanambisi, A. W. (2013), Ideals the polynomial ring $F_2^n[x]$ mod $(x^n - 1)$ for error control in computer applications, *Journal of mathematical theory and modelling* Vol. 3, No. **7**, 55-63.

[32] Olege, F., Oduor, M. O., Aywa, S. and Okaka, A. C. (2016), Characterization of codes of ideals the polynomial ring $F_2^{30}[x]$ mod $(x^{30} - 1)$ for error control in computer applications, Journal of advances in mathematics Vol. 12, No. **5**, 6238-6247.

[33] Olege, F., Oduor, M. O., Aywa, S. and Okaka, A. C. (2016), Perfect repetition codes of ideals the polynomial ring $F_2^n[x]$ mod $(x^n - 1)$ for error control in computer applications, *Journal of mathematics and statistical sciences* Vol. 2016, No. **10**, 579-605.

[34] Prange, E. (1957), Cyclic Error-correcting codes in two symbols, Air Force cambridge Research centre, cambridge, MA, Tech. Rep. AFCRS-TN-57-103.

[35] Reed, I. S. and Solomon, G. (1960), Polynomial codes over certain finite fields, *Journal of Applied Mathematics*, Vol. 8, No. **2**, 300-304.

[36] Richa, G. and Bhudev S. (2012), Generation of variable length error correcting codes over using constant length error correcting codes, *International journal of emerging trends in engineering and development*, Vol. 1, No. **2**, 269-279.

[37] Roger, W. and Sylvia W. (2010), *Prime ideals in Noetherian rings*, A survey in ring and module theory 175, Trends in maths, Birkhouse/Springer Basel AG, Basel.

[38] Ronald, C., Ducas, L., Chris, P. and Oded, R. (2016), Recovering short generators of principal ideals in cyclotomic rings, a paper presented at the annual international conference on the theory and application of cryptographic techniques.

[39] Rotman, J. (2003), *Advanced Mordern Algebra*, (2nd ed.), Prentice Hall.

[40] Rubal, C. and Gupta, V. (2011), Error control techniques and their applications, *International journal of computer applications in engineering science*, Vol. 1, No.**2**, 187-191.

[41] Shannon, C. E. (1948), A mathematical theory of communication Bell Syst. *Tech. J.,* Vol. 27, 379-423, 623-656.

[42] Sidorenko, V. Chabaan, A. Senger, C. Bossert, M. (2009), On extended Forney Kovalev generalised minimum distance decoding, *IEEE International symposium on information theory,* Seoul, Korea.

[43] Shubhangi, S. Zeev, D. Swastik, K. and Madhu, S. (2013), Extensions to the Method of Multiplicities, with applications to Kakeya Sets and Mergers, *Journal of society for industrial and applied mathematics*, Vol. 42, No.**6**, 2305-2328.

[44] Suat, K. and Yildz, B. (2014), A new construction for the extended binary Golay code, *Journal of applied mathematics and information science*, Vol. 8 No.**1**, 69-72.

[45] Ungeboeck, G. and Csajka, I. (1976), "On improving data link performance by increasing the channel alphabet and introducing sequence coding," in Proc., IEEE Int. symp. on information theory, (Ronney, Sweden).

[46] West, J. (2008), Commercializing Open Science: Deep Space Communications as the Lead Market for Shannon Theory, *Journal of management studies* Vol. 45 No.**8**, 39-63.

[47] Wheeler, N. (2004), Upper bound on the number $N-$ spheres that can simultaneously kiss a central sphere, *Journal of science news* Vol.166, No.**14**.

[48] Wiles, A. (1995), Modular elliptic curves and Fermat's Last Theorem, *Annals of mathematics* Vol. 142, 443-551.

[49] Williams, S. (2007), *Data and computer communication*, (8th ed.), Prentice Hall USA.

[50] Wicker, S. (1995), *Error control systems for digital communication and storage,* Englewood Cliffs, NJ: Prenctice Hall, Inc.

[51] Xing, C. and Ling, S. (2004), *Coding Theory: A first course*, New York, Cambridge University Press.