ABSTRACT

IDEMPOTENTS IN CYCLIC CODES

by

Benjamin Brame

April 9, 2012

Chair: Dr. Zachary Robinson

Major Department: Mathematics

Cyclic codes give us the most probable method by which we may detect and correct data transmission errors. These codes depend on the development of advanced mathematical concepts. It is shown that cyclic codes, when viewed as vector subspaces of a vector space of some dimension n over some finite field $\mathbb{F}$, can be approached as polynomials in a ring. This approach is made possible by the assumption that the set of codewords is invariant under cyclic shifts, which are linear transformations. Developing these codes seems to be equivalent to factoring the polynomial $x^n - x$ over $\mathbb{F}$. Each factor then gives us a cyclic code of some dimension k over $\mathbb{F}$.

Constructing factorizations of $x^n - 1$ is accomplished by using cyclotomic polynomials and idempotents of the code algebra. The use of these two concepts together allows us to find cyclic codes in $\mathbb{F}^n$. Hence, the development of cyclic codes is a journey from codewords and codes to fields and rings and back to codes and codewords.

IDEMPOTENTS IN CYCLIC CODES

A Thesis

Presented to

The Faculty of the Department of Mathematics

East Carolina University

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts in Mathematics

by

Benjamin Brame

April 9, 2012

Copyright 2012, Benjamin Brame

IDEMPOTENTS IN CYCLIC CODES

by

Benjamin Brame

APPROVED BY:

DIRECTOR OF THESIS:

Dr. Zachary Robinson

COMMITTEE MEMBER:

Dr. Chris Jantzen

COMMITTEE MEMBER:

Dr. Heather Ries

COMMITTEE MEMBER:

Dr. David Pravica

CHAIR OF THE DEPARTMENT
OF MATHEMATICS:

Dr. Johan Hattingh

DEAN OF THE
GRADUATE SCHOOL:

Dr. Paul Gemperline

ACKNOWLEDGEMENTS

First and foremost I must thank my fiance, Sheila Best. This work would not have been possible without her love, understanding and support. I thank my parents for their guidance and support throughout my graduate work. Thanks must be extended to my brother who has been a rock and calming voice through the many challenges I have faced over the past two years. All of my friends and family have been essential to success in my studies. In particular, Dr. Isaac Bruck offered words of support and encouragement, without which I would have gone crazy a year ago. Thank you to the mathematics department support staff for your assistance. You have made so many things easy in getting through graduate school. To each of my fellow mathematics graduate students, and in particular, my fellow graduate teaching assistants, thank you for the laughs, encouragement and mutual frustration. Thank you to all math faculty members. Your understanding and teaching has been fundamental to all of our success. Finally, I must thank my thesis director, Dr. Zachary Robinson. This work is the culmination of his guidance.

TABLE OF CONTENTS

CHAPTER 1: Introduction

Reliable data transmission is essential in the modern world. For instance, cellular technology depends on data transmission and reception. The devices we use for data storage even employ some form of data transmission. However, no transmission medium is completely reliable. Any type of communication is susceptible to noise corruption or other form of imperfection.

Though coding theory is closely related to cryptography, there is a fundamental difference between the two disciplines; cryptography employs coding to protect messages from interception while coding theory employs coding to increase the reliability of message transmission. Thus, one of the central ideas in coding theory is reduction of noise corruption in a transmission. It is therefore imperative to develop means by which errors in transmission can be detected and, hopefully, resolved. This is accomplished by employing error-correcting codes.

Suppose we want to send a message $\mathbf{t} = t_1 t_2 ... t_k$ where each t_i is a symbol from an alphabet $\mathbb{A}$. We then define $\mathbf{z}(\mathbf{t}) = z_1 z_2 ... z_n$ as a function of the message $\mathbf{t}$ such that $n \geq k$.

For example, let $\mathbb{F}_2$ be the field of two elements, 0 and 1. Consider the mapping $\mathbf{z}(\mathbb{F}_2^8) \longrightarrow \mathbb{F}_2^{16} : t \mapsto (t, t)$.

Note that $\mathbf{z}(\mathbb{F}_2^8)$ is an 8-dimensional $\mathbb{F}_2$-vector subspace of $\mathbb{F}_2^{16}$. The image of $\mathbf{z}$ is called the code, and the elements of the image are called codewords. Now consider the cyclic shift operator $\sigma : \mathbb{F}_2^{16} \longrightarrow \mathbb{F}_2^{16}$, which permutes the coordinates by a cyclic shift of order 16. Note that the code is invariant under σ, i.e., $\sigma(\mathbf{z}(\mathbb{F}_2^8)) = \mathbf{z}(\mathbb{F}_2^8)$. Hence, the term "cyclic" is used to describe such codes.

Definition 1.1. A code is a set $\mathcal{C}$ such that all $\mathbf{c} \in \mathcal{C}$ are codewords (also called words).

It is clear that $\mathcal{C}$ is a subset of the set of all n-tuples, strings of symbols of length n, in the alphabet $\mathbb{A}$. That is $\mathcal{C} \subseteq \mathbb{A}^n$. Because all coding devices are finite machines, our alphabet must be finite. Generally alphabets are taken to be the integers modulo a prime number p ($\mathbb{Z}_p$). As we will see in §2.2, this choice of $\mathbb{Z}_p$ gives us a finite field. Thus, our codes are subsets of the vector space $\mathbb{F}_p^n$. We will always assume p is a prime and $q = p^k$.

We refer to codes constructed from a finite field $\mathbb{F}_q$ as *q-ary* codes. The most widely used and well known alphabet is the binary alphabet, $\mathbb{F}_2$, giving rise to binary codes. However, ternary codes and quaternary codes, codes in $\mathbb{F}_3$ and $\mathbb{Z}_4$ respectively, are extensively studied as well, though $\mathbb{Z}_4$ is not a field. We will make use of the algebraic structure to obtain results about codes.

CHAPTER 2: Structure of Finite Fields

2.1 Basic Definitions

We begin our review of field structures with a formal definition.

Definition 2.1. A *field* $\mathbb{F}$ is a set of elements together with two defined operations:

(i) Addition: $\mathbb{F} \times \mathbb{F} \xrightarrow{+} \mathbb{F} : (x, y) \mapsto x + y$

and

(ii) Multiplication: $\mathbb{F} \times \mathbb{F} \xrightarrow{\times} \mathbb{F} : (x, y) \mapsto xy$

that satisfies the following axioms:

(i) $\mathbb{F}$ is an abelian group, $\mathbb{F}^+$, under addition. There is an additive identity, denoted $0_{\mathbb{F}}$.

(ii) $\mathbb{F}^\times = \mathbb{F} - \{0\}$ is an abelian group where multiplication is associative and commutative. The multiplicative identity is denoted $1_{\mathbb{F}}$.

(iii) The distributive law holds: $(x + y)z = xz + yz$, for all $x, y, z \in \mathbb{F}$.

(iv) $0 \neq 1$.

Though fields can hold an infinite number of elements, we focus on fields with a finite number of elements. It is important to note here that any field is a ring. Using this fact, we can now take advantage of a particular homomorphism. Throughout the development of our ideas in the next section we will use this homomorphism extensively.

Theorem 2.2. *There is a unique homomorphism $\varphi : \mathbb{Z} \to R$ from the ring of integers to R defined by*

$\varphi(a) = a \cdot 1_R$.

Proof. Let $\varphi : \mathbb{Z} \to R$. Let $\varphi(a) = a \cdot 1_R$ and $\varphi(b) = b \cdot 1_R$ for $a, b \in \mathbb{Z}$. This gives us:

$$\begin{aligned}\varphi(a+b) &= (a+b) \cdot 1_R \\ &= (a \cdot 1_R + b \cdot 1_R \\ &= \varphi(a) + \varphi(b).\end{aligned}$$

Likewise, we see that

$$\begin{aligned}\varphi(ab) &= (ab) \cdot 1_R \\ &= (a \cdot 1_R)(b \cdot 1_R) \\ &= \varphi(a) \cdot \varphi(b).\end{aligned}$$

For uniqueness, observe that $\varphi(1) = 1_R$ and $\varphi(0) = 0_R$. This, by definition, makes the homomorphism unique. □

This ring homomorphism allows us to discuss the correspondence between the integers and any finite field since, again, any field is a ring. In particular, this theorem gives us exactly one such correspondence. Hence, we may use the homomorphism unambiguously.

Because a code is defined partly by its alphabet, it is important to know the number of elements in the alphabet. As we define our alphabet as a finite field, we define the number of elements in such a field.

Definition 2.3. The number of elements in a field $\mathbb{F}$ is called the *order* of the field.

We denote a finite field of order q as $\mathbb{F}_q$. The order of a field is not the only useful way to describe a field. We also need to know the characteristic.

Definition 2.4. The least positive integer $c \in \mathbb{F}$ for which $\varphi(c) = 0$, where φ is the ring homomorphism $\varphi : \mathbb{Z} \to \mathbb{F}$, is called the *characteristic* of the field. We will denote the characteristic of a field $\mathbb{F}$ as $char(\mathbb{F})$.

When n is the least positive integer for which $\alpha^n = 1$, $\alpha \in \mathbb{F},/$ we call n the multiplicative *order of* α, denoted $|\alpha|$. The order of α is the number of distinct powers of α.

2.2 Basic Results

We find many results relating to finite fields useful in studying codes. The following, supplied with proofs, will be used throughout our discussion.

As noted earlier, in defining our alphabet as the integers modulo p, our choice of p as a prime is not arbitrary as it offers us the luxury of defining our alphabet as an abelian group. We will see shortly that this allows us to use $\mathbb{Z}_p$ as a field.

The integers taken by themselves do not satisfy all field axioms as they do not have multiplicative inverses since $\mathbb{Z}$ is not closed under division. To form a field, we must define a correspondence under which the integers have multiplicative inverses. Hence, we introduce the idea of *congruence classes*. The set of these classes is denoted $\mathbb{Z}_m$ where m is an integer. Under modular arithmetic, an integer b belongs to a congruence class, $\overline{r}$, in $\mathbb{Z}_m$ if $b = mq + r$ where $0 \leq r < m$.

We cannot assume that every congruence class under $\mathbb{Z}_m$ has a multiplicative inverse. For instance, $\overline{3}$ does not have a multiplicative inverse modulo 6. But we find an interesting result when we let $\mathbb{Z}_p$ be of prime order. Under this restriction, every nonzero congruence class modulo p has an inverse, and hence makes $\mathbb{Z}_p$ a field, denoted $\mathbb{F}_p$.

Theorem 2.5. *For every prime p, the integers modulo p, $\mathbb{Z}_p$, is a field $\mathbb{F}_p$ with p*

elements. We call $\mathbb{F}_p$ *a prime field.*

Proof. As $\mathbb{Z}_p$ is a ring, it suffices to show that each element $j = 0, 1, ..., p-1$ has an inverse. We denote multiplication modulo p by $\times$ and proceed by induction.

1. $j = 1$ has an inverse element as $1^{-1} = 1$

2. Suppose $j > 1$ and all inverses $1^{-1}, 2^{-1}, ..., (j-1)^{-1}$ exist. Using the division algorithm and denoting the quotient by k and the remainder by r we have $p = jk + r$, or $p - r = jk$. Hence we have

$$-r = j \times k.$$

However, $0 < r < j$. Hence $p \neq jk$. By the induction hypothesis, r^{-1} exists. This implies that the inverse to j is $-k \times r^{-1}$ as

$$j \times (-k \times r^{-1}) = -(j \times k) \times r^{-1} = -(-r) \times r^{-1} = r \times r^{-1} = 1.$$

□

Given on the next page are the addition and multiplication tables for $\mathbb{F}_2$, the binary system. We see that 1 has a multiplicative inverse. We need not consider 0 under multiplication as seen in the previous theorem.

Addition:

+	0	1
0	0	1
1	1	0

Multiplication:

·	0	1
0	0	0
1	0	1

Using $\mathbb{F}_2$ is quite advantageous. When we consider congruence classes, we need only consider $\overline{0}$ and $\overline{1}$. Under this modular arithmetic, we can greatly reduce our computations. The majority of codes use a binary alphabet.

We have now defined an infinite number of finite fields. The homomorphism φ given in Theorem 2.2 can now be defined as a map from the integers to $\mathbb{Z}_p$, where p is a prime. We use this unique homomorphism to prove many of the following theorems.

Theorem 2.6. *The characteristic of any finite field must be a prime p.*

Proof. Let $\mathbb{F}_q$ be a finite field with $p = char(\mathbb{F}_q)$. Let φ be the unique ring homomorphism from $\mathbb{Z}$ to $\mathbb{F}_q$. Assume p is not prime. Then there exist prime integers m and n such that $1 < n, m < p$ and $p = nm$. Then $0 = \varphi(mn) = \varphi(m)\varphi(n) = 0$. This implies that either $\varphi(m) = 0$ or $\varphi(n) = 0$. In either case, as $n < p$ and $m < p$, one must be the characteristic of the field, contradicting the fact that p is the characteristic. Hence, p is prime. □

We now introduce the concept of *subfields*. Subfields are subsets of a field that satisfy the field axioms. The smallest subfield of a field is the prime subfield.

Theorem 2.7. *For any finite field $\mathbb{F}$, there exists a subfield $\mathcal{P} \subseteq \mathbb{F}$ such that $\mathcal{P} \cong \mathbb{Z}_p$. We call $\mathcal{P}$ the prime subfield.*

Proof. Let $\mathbb{F}$ be a finite field with $p = char(\mathbb{F})$, for p a prime, and φ be the unique ring homomorphism from $\mathbb{Z}$ to $\mathbb{F}$. Set $\mathcal{P} = \varphi(\mathbb{Z})$. Then $\mathcal{P} = Im(\varphi)$, hence $\mathcal{P} \cong \mathbb{Z}_p$. Now let Q be a subfield of $\mathbb{F}$. Since $1_F \subseteq Q$, it follows that $\mathcal{P} \subseteq Q$. Thus Q contains a subfield $\mathcal{P}$ such that $\mathcal{P} \cong \mathbb{Z}_p$. □

By this point, it should come as no surprise that finite fields are constructed within the prime numbers. This turns out to be true even if the number of element is not

a prime number. That is, if the order of a field is not prime, it is still related to a prime.

Theorem 2.8. *The order of a finite field $\mathbb{F}_q$ is a power of a prime p.*

Proof. Let $char(\mathbb{F}_q) = p$. By Theorem 2.7, there is a subfield $\mathcal{P}$ of $\mathbb{F}_q$ such that $\mathcal{P} \cong \mathbb{Z}_p$. Hence, $\mathbb{F}_q$ is a vector space over $\mathcal{P}$ and as $\mathbb{F}_q$ is finite, it must be a finite dimensional vector pace over $\mathcal{P}$. Thus, as a $\mathcal{P}$-vector space, $\mathbb{F}_q \cong \mathcal{P}^n$. This proves $q = p^n$. □

This result has a consequence that allows us to ultimately derive the idea by which we may define the generators for our cyclic codes. As $q = p^n$, we know that $gcd(q, q-1) = 1$. Thus, there is an element in $\mathbb{F}_q$, namely $q-1$, that generates all elements in the field except 0. This element is known as a *primitive element.*

Theorem 2.9. *Let $\mathbb{F}_q$ be a finite field. Then $\mathbb{F}_q$ must contain a primitive field element of order $q-1$ whose powers are all non-zero.*

Proof. Let q be the number of non-zero field elements in $\mathbb{F}_q$ and let α be a field element of order n, $n > 1$. As each of the n powers of α is distinct and is non-zero, $n \leq q-1$. Now let β be another non-zero field element and let β have order m. If $m \nmid n$ then $\beta^{(n,m)}$ has order $m/(n,m)$ which is relatively prime to n. So $\alpha\beta^{(n,m)}$ has order $nm/(n,m)$ which exceeds n, a contradiction. Hence, $m|n$. Therefore, every non-zero element in $\mathbb{F}_q$ is a root of the polynomial $x^n - 1$ which has at most n roots in the field. Hence, $q-1 \leq n$ and since $n \leq q-1$ we conclude that $n = q-1$. □

We use this idea of a primitive field element to show generators. This will be an important concept as the focus of this paper is ultimately on generators of a code.

Adding m-tuples in $\mathbb{F}_q$ is quite easy. However, multiplying m-tuples in $\mathbb{F}_q$ is difficult. It becomes necessary to define a means by which we may multiply these

elements and affix this new form of the elements to the m-tuples. We begin with restricting our field and viewing it as a group. Let $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$. It is obvious that $\mathbb{F}_q^*$ is a group. In fact, it is an abelian group under multiplication. We then have the following:

Theorem 2.10. *Let $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$. Then the following are true:*

(i) The group $\mathbb{F}_q^*$ is cyclic with order $q-1$.

(ii) If γ is a generator of of this cyclic group, then

$\mathbb{F}_q = \{0, 1 = \gamma^0, \gamma, \gamma^2, ..., \gamma^{q-2}\}$, *and*

$\gamma^i = 1$ *if and only if* $(q-1)|i$.

Proof. (i) Observe that $\mathbb{F}_q^*$ is a product of cyclic groups of orders $p_1, p_2, ..., p_a$, such that $p_j | p_{j+1}$ for $1 \leq j < a$ and $p_1 p_2 ... p_a = q-1$. This gives us $\alpha^{p_a} = 1$ for all $\alpha \in \mathbb{F}_q^*$, implying that $x^{p_a} - 1$ has at least $q-1$ roots, which is not possible unless $a = 1$ and $p_a = q-1$. Thus, $\mathbb{F}_q^*$ is cyclic.

(ii) This follows quickly from the definition of cyclic groups.

□

We have now introduced polynomials. The natural progression is to find a way to solve polynomials. We now define the basic idea for solving polynomials.

Definition 2.11. If $f(x)$ is a polynomial over a field F, $\alpha \in F$, and $f(\alpha) = 0$, then α is called a *root* of $f(x)$.

The following corollary is a generalization of Fermat's theorem.

Corollary 2.12. *Every element in $\mathbb{F}_q$ must satisfy the equation $x^q - x = 0$.*

Proof. As shown in the proof of 2.7, since $\mathbb{F}_q$ has order q all non-zero elements satisfy $x^{q-1} - 1 = 0$. The zero element satisfies $x = 0$. Hence, all field elements satisfy $x(x^{q-1} - 1) = x^q - x = 0$. □

We expand finite fields of order q to obtain important fields used in building codes. Here it is important to define two useful algebraic terms.

Definition 2.13. Let $f(x)$ be a nonconstant polynomial in F. A *splitting field* for $f(x)$ over F is an extension field $\mathcal{K}$ such that:

(i) $f(x)$ factors into linear monic factors in $\mathcal{K}$: $f(x) = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$ for $\alpha_i \in \mathcal{K}$, and

(ii) $\mathcal{K}$ is generated by the roots of $f(x)$: $\mathcal{K} = \mathbb{F}(\alpha_1, \alpha_2, ..., \alpha_n)$.

Before we proceed further, we introduce a concept that helps us in factoring polynomials under modular operations. This idea will be generalized §5.1.

Theorem 2.14. *Let $\mathbb{F}_q$ be a field with characteristic $char(\mathbb{F}_q) = p$ and let $a \in \mathbb{F}_q$. Then we have*

$(x - a)^q = x^q - a^q$.

Proof. Let a be an element in $\mathbb{F}_q$. We can write $(x-a)^p = \sum_{i=0}^{k} \binom{p}{k} (-a)^k x^{p-k}$, where $\binom{p}{k}$ is the binomial coefficient. We see that

$$\binom{p}{k} = \frac{p(p-1)...(p-k+1)}{1 \cdot 2 \cdot ... \cdot k}.$$

If $0 < k < p$ it is obvious that the numerator has a factor of p while the denominator does not, hence $\binom{p}{k} \equiv 0 \pmod{p}$. If, however, $k = 0$ or $k = p$ we have $\binom{p}{0} = \binom{p}{p} = 1$ so that $(x - a)^p = x^p - a^p$. □

Much of code development depends on the relationship between two fields. We like to think of a pair of fields with one contained in the other. That is, if $\mathbb{F}$ is a field, we define a larger field K for which $\mathbb{F} \subset K$. We call K an *extension field* containing $\mathbb{F}$.

Any element in a field $\mathbb{F}$ that is the root of a polynomial with coefficients in $\mathbb{F}$ is said to be *algebraic* over $\mathbb{F}$.

Definition 2.15. An extension $\mathbf{A}_p$ of the field $\mathbb{F}_p$ is an *algebraic closure* if each non-constant polynomial in $\mathbb{F}_p[x]$ has a root in $\mathbf{A}_p$. This means $\mathbb{F}_p$ is a subfield of $\mathbf{A}_p$. We will henceforth denote an algebraic closure of $\mathbb{F}_p$ as $\mathbf{A}_p$.

Theorem 2.16. *Any field F has an algebraic closure.*

Proof. We can extend F to an algebraically closed extension field K. Let $H = \{\alpha \in K | \alpha \text{ is algebraic over } F\}$. Then H is a field and is algebraic. Let $f(x)$ be any non-constant polynomial in $H[x]$. Hence, $f(x)$ has a root, δ in K. We must show that $\delta \in H$.

As δ is algebraic over H, we have that $H(\delta)/H$ is algebraic. In addition, H/F is algebraic. Hence, $H(\delta)/F$ is algebraic. This implies that δ is algebraic over F and so is in H. □

The following corollary allows us to define longer codes based on p.

Corollary 2.17. *For any prime p and positive integer k, there exists a finite field $\mathcal{P}$ with $q = p^k$ elements that is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.*

Proof. Let $\mathbf{A}_p$ be an algebraic closure of the field $\mathbb{F}_p$. Let $\mathcal{K} \subseteq \mathbf{A}_p$ be the splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. Let $\mathcal{C}$ be the set of all roots of the polynomial $x^{p^n} - x$ in $\mathcal{K}$. Then $\mathcal{C}$ has exactly p^n elements. Furthermore, $\mathcal{C}$ contains $\mathbb{F}_p$ and is a

subfield of $\mathbf{A}_p$ since, by Theorem 2.14, $(\gamma + \lambda)^{p^n} = \gamma^{p^n} + \lambda^{p^n}$. Hence, $\mathcal{C}$ is exactly the splitting field of $\mathcal{K}$. That is, $\mathcal{K}$ is finite of order p^n.

Let $\mathcal{K} \subset \mathbf{A}_p$ be a finite field with q elements. By Corollary 2.12, the elements of $\mathcal{K}$ are roots of $x^q - x$. Hence, $\mathcal{K}$ is the splitting field of $x^q - x$ over $\mathbb{F}_p$. $\square$

CHAPTER 3: Algebraic Coding Theory

We have laid the groundwork for algebraic coding theory. Additional structure is needed to fully develop our codes. Defining our codes as vectors and ultimately polynomials allows us to algebraically manipulate our codes to construct them more easily. Here we introduce concepts that simplify code development.

3.1 Field and Vector Space Structure Underlying Codes

A natural progression is to examine subsets of elements from finite fields. We will call the elements of $\mathbb{F}_p$ scalars and the set of all ordered n-tuples over $\mathbb{F}_p$ will now be denoted $\mathbb{F}_p^n$ and its elements called vectors. We equip $\mathbb{F}_p^n$ with the usual addition and scalar multiplication:

(i) vector addition: if $\mathbf{x} = (x_1, x_2, ..., x_n) \in \mathbb{F}_p^n$ and $\mathbf{y} = (y_1, y_2, ..., y_n) \in \mathbb{F}_p^n$ then

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n),$$

and

(ii) scalar multiplication: if $\mathbf{x} = (x_1, x_2, ..., x_n) \in \mathbb{F}_p^n$ and $a \in \mathbb{F}_p$ then

$$a \cdot \mathbf{x} = (ax_1, ax_2, ..., ax_n).$$

Definition 3.1. Let $\mathbb{F}$ be a field. A *vector space*, or linear space, is a set L with the operations of addition, $+$, and scalar multiplication, $\cdot$, satisfying the following axioms:

(i) $(L, +)$ is a commutative group,

(ii) For each scalar s in $\mathbb{F}$ and each vector $\mathbf{v}$ in L, $\cdot$ assigns a unique vector $s \cdot \mathbf{v}$. (Henceforth, $s \cdot \mathbf{v}$ will be denoted $s\mathbf{v}$),

(iii) associativity: $(st)\mathbf{v} = s(t\mathbf{v})$ for all scalars s, t in $\mathbb{F}$ and all vectors $\mathbf{v}$ in L,

(iv) distributivity: $s(\mathbf{u} + \mathbf{v}) = s\mathbf{u} + s\mathbf{v}$ and $(s + t)\mathbf{v} = s\mathbf{v} + t\mathbf{v}$ for all scalars s, t in $\mathbb{F}$ and all vectors $\mathbf{u}, \mathbf{v}$ in L,

(v) $1\mathbf{v} = \mathbf{v}$ for all vectors $\mathbf{v}$ in L where 1 is the unit of $\mathbb{F}$.

We can derive further properties of vector spaces from the above axioms. Namely,

- $0\mathbf{v} = 0$ for each vector $\mathbf{v}$ in L,
- $(-1)\mathbf{v} = -\mathbf{v}$ for each vector $\mathbf{v}$ in L,
- $s\mathbf{0} = \mathbf{0}$ for each scalar s in $\mathbb{F}$.

Returning to our definition of a code, if we let $\mathcal{C}$ be a code in an alphabet $\mathbb{A} = \mathbb{F}_q$, we can regard our codeword $\mathbf{c}$ as a vector in the vector space $\mathbb{F}_q^n$ of all n-tuples over the finite field $\mathbb{F}_q$. An (n, M) code $\mathcal{C}$ over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$ of size M. A codeword $\mathbf{c}$ in $\mathcal{C}$ is a vector $(a_1, a_2, ..., a_n)$ which we write in the form $a_1a_2...a_n$. However, recall that we renumber our vector coordinate spaces to $a_0a_1...a_{n-1}$.

The usefulness of a code is limited without affixing additional structure. As we are working in vector spaces, the most common additional structure to require is linearity.

Definition 3.2. Let $\mathbb{F}_q^n$ be a vector space over $\mathbb{F}_q$. Let $\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_k$ be vectors in $\mathbb{F}_q^n$ and $\delta_1, \delta_2, ..., \delta_k$ be elements in $\mathbb{F}_q$. Then the vector $\mathbf{c} = \delta_1\mathbf{c}_1 + \delta_2\mathbf{c}_2 + ... + \delta_n\mathbf{c}_n$ is called a *linear combination* of the $\mathbf{c}_i$'s over $\mathbb{F}_q$.

Taking linear combinations in $\mathbb{F}_q^n$ affords us the opportunity to impose even more structure on our vector space.

Definition 3.3. A *linear code* is the set of all k linear combinations in $\mathbb{F}_q^n$. If $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$ then $\mathcal{C}$ is called an $[n, k]$ linear code, or more commonly an $[n, k]$ code. An $[n, k]$ code has q^k codewords.

While it is possible to construct codes with codewords of variable length, we will focus on codes in which all codewords are of the same length. These types of codes are called *block codes*. Block codes are the most widely used form of coding for error correction.

CHAPTER 4: Cyclic Codes

We now begin our investigation of cyclic codes. Cyclic codes were first studied in the 1950's. The present day theory has produced a class of codes that offer the greatest probability of error detection and correction. As we proceed we will express our codewords and code as rings and polynomials. While a cyclic code is a linear code, we impose a cyclic structure on the code to obtain a more useful code structure.

4.1 Basic Definition of Cyclic Codes

A cyclic code begins with a cyclic shift of a linear code. That is, we wish to rearrange the codewords. Performing such an operation allows us to study codes with cyclic traits. The development of such codes begins with the idea of a cyclic group. It is evident that our field $\mathbb{F}_q$ is a cyclic group under addition. If we set $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$, then $\mathbb{F}_q^*$ is a cyclic group under multiplication. In fact, these groups are abelian groups. We use their cyclic structure to ultimately form a ring which gives us simplified algorithms for defining a cyclic code.

The general idea of a cyclic shift is given below. Though a more formal definition is discussed later in this section, the following informal definition will suffice for our general development of the idea of a cyclic code.

Definition 4.1. Given a codeword $c_0c_1...c_{n-2}c_{n-1}$ of length n, the *right cyclic shift* is $c_{n-1}c_0c_1...c_{n-2}$. Likewise, the *left cyclic shift* is $c_1c_2...c_{n-1}c_0$.

These cyclic shifts represent a special form of a linear code. Namely, since our code is linear, all cyclic shifts of a codeword must be codewords in the code.

Definition 4.2. A linear $[n, k]$-code $\mathcal{C}$ over $\mathbb{F}_q^n$ is a *cyclic code* if for each vector $\mathbf{c} = c_0...c_{n-2}c_{n-1}$ in $\mathcal{C}$ the vector $c_{n-1}c_0...c_{n-2}$, obtained from $\mathbf{c}$ by the cyclic shift of

coordinates is also in $\mathcal{C}$.

Cyclic codes are an invaluable tool in error correction. This general definition gives us the platform whereby we may discuss some general traits of a cyclic code. The cyclic shift is paramount to the idea of these types of codes. In general, all cyclic shifts result in a subset of $\mathcal{C}$. The fact that $\mathcal{C}$ is linear means that we can use linear combinations to develop more codewords from these cyclic shifts. That is, a k-dimensional code in $\mathbb{F}_q^n$ is set of linear combinations of cyclic shifts in $\mathcal{C}$. Here we begin the algebraic development of these ideas.

We define $\sigma : \mathcal{C} \longrightarrow \mathcal{C} : \mathbf{c}_i \mapsto \mathbf{c}_{i+1} \pmod{n}$ where each $i \in \{0, 1, ..., n-1\}$. This clearly defines a cyclic shift.

Example 4.3. Consider a binary codeword $\mathbf{c} = 0100$ in a cyclic code $\mathcal{C}$. Each cyclic shift of 0100 must also be in $\mathcal{C}$. Hence, $1000, 0001, 0010$ must also be in $\mathcal{C}$.

There are n cyclic shifts in this code. A cyclic code contains all n cyclic shifts of a codeword. It is helpful to think of all coordinate positions in terms of modular arithmetic where once we reach $n-1$ we begin our next coordinate with 0. This idea is used extensively in translating our codeword to polynomial form.

When studying finite fields we can represent the elements in polynomial form. As a vector space is defined over a field, we can define our vectors in polynomial form. That is to say, there is a bijective correspondence between $\mathbf{c} = c_0c_1c_2...c_{n-1}$ and the polynomial $c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]$ of degree at most $n-1$.

Example 4.4. The following gives examples of codewords in $\mathbb{F}_2^7$. Here our coefficients are binary digits and our codewords are of length 7. The codewords are defined with the constant as the leftmost coordinate position, c_0.

Polynomial	Codeword
$1 + x + x^3 + x^5 + x^6$	1101011
$1 + x^5$	1000010
$1 + x^2 + x^4 + x^6$	1010101

We can consider our code $\mathcal{C}$ as a subset of $\mathbb{F}_q[x]$ where $\mathbb{F}_q[x]$ is the set of polynomials in x with coefficients in $\mathbb{F}_q$. This suggests that the proper context for studying cyclic codes is the residue class ring

$$\mathcal{R}_n = \mathbb{F}_q[x]/(x^n - 1).$$

4.2 Additional Structures of $\mathcal{C}$ Yield a Ring

We now consider two linear maps:

$$\pi : \mathbb{F}_q[x] \longrightarrow \mathbb{F}_q[x]/(x^n - 1)$$

and

$$\varphi : \mathcal{C} \longrightarrow \mathbb{F}_q[x] : c_0 ... c_{n-1} \mapsto \sum_{i=0}^{n-1} c_i x^i.$$

Theorem 4.5. *If $\mathcal{C}$ is an $[n, k]$ cyclic code and $\boldsymbol{c} = c_0 c_1 ... c_{n-1}$ a codeword in $\mathcal{C}$, then the map*
$\overline{\varphi} : \mathcal{C} \longrightarrow \mathbb{F}_q[x]/(x^n - 1) : \boldsymbol{c} \mapsto \pi \circ \varphi(\boldsymbol{c})$ *is an injective linear map.*

Proof. We know that $\overline{\varphi}$ is linear because $\overline{\varphi} = \vartheta \circ \varphi$ and the composition of linear maps is a linear map. Hence, it remains to show that $Ker\ \overline{\varphi} = \mathbf{0}$.

Let $\mathbf{c} = c_0c_1...c_{n-1}$ be a codeword in $\mathcal{C}$. Suppose $\overline{\varphi}(\mathbf{c}) = 0$. Then $\pi(\varphi(c)) = 0$. But $Ker(\pi) = k(x^n - 1)$ where k is some integer. This implies that $\overline{\varphi} = 0$ if and only if$\varphi(\mathbf{c}) = k(x^n - 1)$. But, as the $dim(\mathcal{C}) < n$, we must have that $\mathbf{c} = 0$, proving that $Ker\overline{\varphi} = 0$. □

Recall that $\sigma : \mathcal{C} \longrightarrow \mathcal{C} : \mathbf{c}_i \mapsto \mathbf{c}_{i+1}$, and consider the correspondence $\mu_x : \mathcal{R}_n \longrightarrow \mathcal{R}_n : c(x) \mapsto xc(x)$. We see that μ_x is bijective and corresponds to a cyclic shift as for $\mathbf{c} = c_0c_1...c_{n-1}$ and $c(x) = c_0 + c_1x + ... + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}$ we have $xc(x) = c_{n-1} + c_0x + ... + c_{n-2}x^{n-1}$ which corresponds to $c_{n-1}c_0...c_{n-2} = \sigma(\mathbf{c})$. This gives us the commutative diagram given below.

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\overline{\varphi}} & \mathbb{F}_q[x]/(x^n-1) \\ \Big\downarrow{\scriptstyle \sigma} & & \Big\downarrow{\scriptstyle \mu_x} \\ \mathcal{C} & \xrightarrow{\overline{\varphi}} & \mathbb{F}_q[x]/(x^n-1) \end{array}$$

Theorem 4.6. *Let $\mathbf{c}$ be a codeword in a code $\mathcal{C}$ and $\mathbb{F}_q$ be a field. Then*

$$\overline{\varphi} \circ \sigma(\mathbf{c}) = \mu \circ \overline{\varphi}(\mathbf{c}).$$

Proof. This follows from the □

Example 4.7. Here we consider cyclic shifts for $n = 7$ and a codeword $\mathbf{c} = 1011000$. Then $c(x) = 1 + x^2 + x^3$.

Codeword	Polynomial (mod (x^7-1))
$\mathbf{c} = 1011000$	$c(x) = 1 + x^2 + x^3$
$\sigma(\mathbf{c}) = 0101100$	$\mu_x(c(x)) = x + x^3 + x^4$
$\sigma^2(\mathbf{c}) = 0010110$	$\mu_x{}^2(c(x)) = x^2 + x^4 + x^5$
$\sigma^3(\mathbf{c}) = 0001011$	$\mu_x{}^3(c(x)) = x^3 + x^5 + x^6$
$\sigma^4(\mathbf{c}) = 1000101$	$\mu_x{}^4(c(x)) = 1 + x^4 + x^6$
$\sigma^5(\mathbf{c}) = 1100010$	$\mu_x{}^5(c(x)) = 1 + x + x^5$
$\sigma^6(\mathbf{c}) = 0110001$	$\mu_x{}^6(c(x)) = x + x^2 + x^6$
$\sigma^7(\mathbf{c}) = 1011000 = \mathbf{c}$	$\mu_x{}^7(c(x)) = 1 + x^2 + x^3 = c(x)$

By Theorem 4.5 we see that the code $\mathcal{C}$ is an ideal of $\mathcal{R}_n$. Thus, studying cyclic codes in $\mathbb{F}_q^n$ is equivalent to studying ideals in $\mathcal{R}_n$.

4.3 Ideals

Studying our codes as ideals in $\mathcal{R}_n$ allows some freedom to explicitly define our codes. That is, we define our codes over some polynomial and mod out over the ideal, leading to unique polynomials containing the coordinates of our codewords.

Definition 4.8. A set I of elements in $\mathcal{R}_n$ is known as an *ideal* if it satisfies the following two conditions:

(i) If a is in I then ab is in I for all b in $\mathcal{R}_n$, and

(ii) If a and b are in I then $a + b$ and $a - b$ are also in I.

With vectors corresponding to polynomials in $\mathcal{R}_n$ as defined above, the following result is important.

Theorem 4.9. *A set of elements I in $\mathcal{R}_n$ corresponds to a cyclic code $\mathcal{C}$ if and only if I is an ideal of $\mathcal{R}_n$.*

Proof. Suppose I is a set of elements in $\mathcal{R}_n$ that corresponds to a cyclic code $\mathcal{C}$. If $c_1(x)$ and $c_2(x)$ are in I, then so are $c_1(x) + c_2(x)$ and $c_1(x) - c_2(x)$ by definition of a

code. As a cyclic shift corresponds to multiplication by x if $c(x)$ is in I, we have that $(c(x))x$ is also in I as is $(c(x)x)x = (c(x))x^2$ and so on. Let $b(x)$ be a polynomial in $\mathcal{R}_n$. Then $a(x)b(x) = b_0a(x) + b_1a(x)x + ... + b_{n-1}a(x)x^{n-1}$ which is also in I as each element in the sum is in I. Hence, I is an ideal.

On the other hand, if I is an ideal in $\mathcal{R}_n$, then the polynomials in I clearly correspond to the vectors in a cyclic code $\mathcal{C}$. □

This tells us that in finding the ideals of a ring we can generate cyclic codes specific to that ring. However, it is important to note that $\mathbb{F}_p[x]$ forms not only a ring, but a commutative ring with unity. A commutative ring with unity satisfies all the field axioms with the exception that the nonzero elements do not necessarily have multiplicative inverses. In addition, $\mathbb{F}_p[x]$ is an integral domain. An integral domain is a commutative ring with unity such that the product of any two nonzero elements in the ring is also nonzero. We now show that the ideals of a residue ring $\mathcal{R}_n$ are principal ideals.

Definition 4.10. An ideal I in R_n is a *principal ideal* if every element in I is a multiple of a fixed polynomial $g(x)$.

If I is principal, then $I = \{c(x)g(x)|c(x) \in \mathcal{R}_n\}$. A *principal ideal ring* (PIR) is a ring in which all ideals are principal.

To consider our codewords as polynomials with our codes as ideals we must introduce an additional definition.

Definition 4.11. A *monic polynomial* is a polynomial in which the leading coefficient is 1.

Theorem 4.12. *If $\mathcal{C}$ is an ideal (cyclic code of length n) in $\mathcal{R}_n = \mathbb{F}_p[x]/(x^n - 1)$, let $g(x)$ be the monic polynomial of smallest degree in $\mathcal{C}$. Then $g(x)$ is uniquely determined and $\mathcal{C} =< g(x) >$.*

Proof. It suffices to show that $\mathcal{R}_n$ is a PIR and that the monic generator of smallest degree is unique in an ideal.

Let $g(x)$ the monic polynomial of smallest degree in $\mathcal{C}$ and let $c(x)$ be any other polynomial in $\mathcal{C}$. By the division algorithm, $c(x) = g(x)q(x) + r(x)$ where the degree of $r(x)$ is less than the degree of $g(x)$. As $\mathcal{C}$ is an ideal, $r(x)$ is in $\mathcal{C}$.But as $g(x)$ is of lowest degree, $r(x) = 0$. So $c(x) = g(x)q(x)$ and, hence, $\mathcal{R}_n$ is a PIR.

If $g(x)$ and $h(x)$ are monic polynomials of the same degree and both are in C, then $g(x) - h(x)$ is a polynomial in C of lower degree than either. But this is not possible as $g(x)$ has the smallest degree by assumption. Hence, $g(x)$ is the unique monic polynomial of smallest degree in C and $C =< g(x) >$. □

We now further the idea of a monic polynomial of least degree and show that it is essential to deriving codes from our ring $\mathcal{R}_n$.

Theorem 4.13. *If C is an ideal in $\mathcal{R}_n$, the unique monic polynomial, $g(x)$, of C of smallest degree divides $(x^n - 1)$, and conversely, if $g(x)$ in C divides $(x^n - 1)$, then $g(x)$ has the lowest degree in $< g(x) >$.*

Proof. First suppose $g(x)$ is the monic polynomial of least degree in C. By the division algorithm, $(x^n - 1) = g(x)q(x) + r(x)$ where, again, the degree of $r(x)$ is less than the degree of $g(x)$. Now we have $r(x) = -g(x)q(x)$ modulo $(x^n - 1)$ so that $r(x)$ is in $< g(x) >$, a contradiction unless $r(x) = 0$. Hence, $g(x)$ divides $(x^n - 1)$.

Now suppose $g(x)$ divides $(x^n - 1)$ and $h(x)$ is in $< g(x) >$ but has lower degree than $g(x)$. Then $h(x) = c(x)g(x) + (x^n - 1)d(x)$ in $F[x]$ since $h(x)$ is in C. But as $g(x)$ divides $(x^n - 1)$ it must also divide $h(x)$, a contradiction. Hence, $g(x)$ has the lowest degree in $< g(x) >$. □

This theorem tells us that in order to construct a cyclic code we have to be able

to factor $(x^n - 1)$. This, however, can be very difficult. When considering binary codes, we assume n is odd as, in that case, $(x^n - 1)$ has distinct factors.

CHAPTER 5: Factoring $x^n - 1$

5.1 Minimal Polynomials

We now introduce the idea of minimal polynomials which leads us to cyclotomic polynomials. These polynomials will play a central not only in factoring $x^n - 1$, but also in generators of cyclic codes and cyclic code idempotents. To fully develop these notions we must introduce new concepts.

Definition 5.1. A polynomial $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_{n-1} x^{n-1}$ in a ring $F[x]$ for F a field is said to be an *irreducible polynomial* if it cannot be factored into polynomials of lower degree.

Definition 5.2. An element $\xi \in \mathbb{F}_p$ is an *nth root of unity* if $\xi^n = 1$. If $\xi^s \neq 1$ for $0 < s < n$, then ξ is called a primitive nth root of unity.

Definition 5.3. Let $\mathbb{F}_q$ be a field where $q = p^r$ and α an element in $\mathbb{F}_q$. The *minimal polynomial* $\mathcal{M}_\alpha(x)$ in $\mathbb{F}_q[x]$ is the monic polynomial of smallest degree with α as a root. It is called the minimal polynomial of α over $\mathbb{F}_q$.

Next we note some basic facts about minimal polynomials.

Theorem 5.4. *Let $\mathbb{F}_{q^t}$ be an extension field of $\mathbb{F}_q$ and let α be an element of $\mathbb{F}_{q^t}$ with minimal polynomial $\mathcal{M}_\alpha(x)$ in $\mathbb{F}_q[x]$. The following are true:*

(i) $\mathcal{M}_\alpha(x)$ is irreducible over $\mathbb{F}_q$.

(ii) If $g(x)$ is any polynomial in $\mathbb{F}_q[x]$ satisfying $g(\alpha) = 0$, then $\mathcal{M}_\alpha(x) | g(x)$.

(iii) $\mathcal{M}_\alpha(x)$ is unique.

Proof. (i) If $\mathcal{M}_\alpha(x)$ is reducible then $\mathcal{M}_\alpha(x) = s(x)t(x)$ for some $s(x), t(x) \in \mathbb{F}_q[x]$. But $\mathcal{M}_\alpha(\alpha) = 0$. Hence, $s(\alpha)t(\alpha) = 0$. Both $s(x)$ and $t(x)$ are polynomials of lower degree than $\mathcal{M}_\alpha(x)$. Hence, we reach a contradiction as $\mathcal{M}_\alpha(x)$ is the minimal polynomial. Thus, $\mathcal{M}_\alpha(x)$ is irreducible.

(ii) By polynomial division, $g(x) = q(x)\mathcal{M}_\alpha(x) + r(x)$ for $q(x), r(x) \in \mathbb{F}_q[x]$ where the degree of $r(x)$ is between 0 and the degree of $\mathcal{M}_\alpha(x)$. As $g(\alpha) = 0$ and $\mathcal{M}_\alpha(\alpha) = 0$, we have $r(\alpha) = 0$. So $r(x) = 0$. Hence, $\mathcal{M}_\alpha(x)|g(x)$.

(iii) Suppose $f_1(x)$ and $f_2(x)$ are minimal polynomials of the same degree. Then $f(x) = f_1(x) - f_2(x)$ would be a nonzero polynomial of smaller degree. But as $f(\alpha) = 0$ we have a contradiction of the minimality of $f_1(x)$ and $f_2(x)$. Hence, the minimal polynomial is unique.

□

We now want to explicitly factor our polynomials in $\mathcal{R}_n$. The following theorems help us define a process for finding the factors of a polynomial in $\mathcal{R}_n$.

Theorem 5.5. *Let $f(x)$ be a polynomial in $\mathbb{F}_q[x]$ and let α be a root of $f(x)$ in a field extension $\mathbb{F}_{q^t}$. Then we have:*

(i) $f(x^q) = f(x)^q$, and

(ii) α^q is also a root of $f(x)$ in $\mathbb{F}_q$.

Proof. (i) This is a generalization of Theorem 2.14.

(ii) In particular, based on (i), we have $f(\alpha_i^q) = f(\alpha_i)^q = 0$, so (ii) holds.

□

If we apply this theorem repeatedly we see that $\alpha, \alpha^q, \alpha^{q^2}, ...$ are all roots of $\mathcal{M}_\alpha(x)$. This sequence will stop after r terms where $\alpha^{q^r} = \alpha$. That is, if α is a root of the polynomial $x^n - 1$, then $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ are all roots of $x^n - 1$. The following theorem follows directly from 5.6.

Theorem 5.6. *Let $f(x)$ be a monic irreducible polynomial over $\mathbb{F}_q$ of degree r. Then the following hold:*

(i) all the roots of $f(x)$ are in $\mathbb{F}_{q^r}$ and in any field containing $\mathbb{F}_q$ along with a root of $f(x)$,

(ii) $f(x) = \prod_{i=1}^{r}(x - \alpha_i)$, where $\alpha_i \in \mathbb{F}_{q^r}$ for $1 \leq i \leq r$, and

(iii) $f(x)|(x^{q^r} - x)$.

In particular, as minimal polynomials over $\mathbb{F}_q$ are monic, we have the following.

Theorem 5.7. *Let $\mathbb{F}_{q^t}$ be a field extension over $\mathbb{F}_q$ and α an element in $\mathbb{F}_{q^t}$ with minimal polynomial $\mathcal{M}_\alpha(x)$ in $\mathbb{F}_q[x]$. Then the following are true:*

(i) $\mathcal{M}_\alpha(x)|(x^{q^t} - x)$.

(ii) $\mathcal{M}_\alpha(x)$ has distinct roots all lying in $\mathbb{F}_{q^t}$.

(iii) The degree of $\mathcal{M}_\alpha(x)$ divides t.

(iv) $x^{q^t} - x = \prod_{\alpha} \mathcal{M}_\alpha(x)$, where α runs through some subset of $\mathbb{F}_{q^t}$ which enumerates the minimal polynomials once.

(v) $x^{q^t} - 1 = \prod_{f} f(x)$, where f runs through all monic irreducible polynomials whose degree divides t.

Proof. (i) follows from theorem 5.5(ii). The q^t elements of $\mathbb{F}_{q^t}$ are the roots of $x^{q^t}-x$, hence $x^{q^t}-x$ has distinct roots. So (i) and theorem 5.7(i) imply (ii). Since any nonconstant polynomial is the product of irreducible polynomials of distinct powers, we have $x^{q^t}-x=\prod_{i=1}^{n} p_i(x)$, where each $p_i(x)$ is irreducible over $\mathbb{F}_q$. This implies that each $p_i(x)$ is distinct since $x^{q^t}-x$ has distinct roots. We can assume, by scaling each $p_i(x)$, that they are monic. So, $p_i(x)=\mathcal{M}_\alpha(x)$ for any $\alpha\in\mathbb{F}_{q^t}$ with $p_i(\alpha)=0$. Hence, (iv) holds. If $\mathcal{M}_\alpha(x)$ has degree m, then adjoining α to $\mathbb{F}_q$ gives the subfield $\mathbb{F}_{q^m}=\mathbb{F}_{p^{km}}$, or $\mathbb{F}_{q^t}=\mathbb{F}_{q^{km}}$, which implies $mr|mt$ and, hence, (iii) holds. Part (v) follows since every monic polynomial of degree m dividing t is a factor of $x^{q^t}-x$ by theorem 5.7(iii). □

Every factorization of the polynomial x^q-x partitions the elements in a finite field of order q. If we let $x^q-x=g(x)h(x)$ then every element in the field is either a root of $g(x)$ or $h(x)$. We know that $x^q-x=x(x^{q-1}-1)$ so that we can separate the zero elements from the nonzero elements. We now have left to separate the nonzero elements according to their orders by factoring $x^{q-1}-1$. This is a special case of x^n-1.

5.2 Cyclotomic Cosets

Referring back to theorem 5.6 we know that $f(x^q)=f(x)^q$ and that if α is a root of $f(x)$ in some field extension $\mathbb{F}_{q^t}$, then α is also a root in $\mathbb{F}_q$. So we see that $\alpha,\alpha^q,\alpha^{q^2},...$ are all roots of $\mathcal{M}_\alpha(x)$. This sequence stops after d terms for $\alpha^{q^d}=\alpha$.

Recall that there must exist a primitive element γ in $\mathbb{F}_q$ of order $q-1$ such that γ generates all elements except 0 in $\mathbb{F}_q$. Then we know $\alpha=\gamma^s$ for some positive integer s. Thus $\alpha^{q^d}=\alpha$ if and only if $(\gamma^s)^{q^d}=\gamma^s$, or, $\gamma^{sq^d-s}=1$. But $sq^d\equiv s \pmod{q^t-1}$. We can now define q-cyclotomic cosets.

Definition 5.8. A *q-cyclotomic coset* is the set $C_s = \{s, sq, ..., sq^{d-1}\} \pmod{q^t - 1}$, where d is the smallest positive integer such that $sq^d \equiv s \pmod{q^t - 1}$. These sets partition $\{0, 1, 2, ..., q^t - 2\}$ into disjoint sets. We list cyclotomic cosets with members only given once and represented by the smallest element of the coset.

Example 5.9. We wish to compute the 2-cyclotomic cosets modulo 15. We get:

For $s = 1$:

$\{1, 2, 4, 8, 16 \equiv 1\}$ which gives us $C_1 = \{1, 2, 4, 8\}$.

Since 2 is in C_1, we need not compute a coset for $s = 2$.

For $s = 3$:

$\{3, 6, 12, 24 \equiv 9, 18 \equiv 3\}$, which gives us $C_3 = \{3, 6, 9, 12\}$.

For $s = 5$:

$C_5 = \{5, 10\}$.

For $s = 7$:

$C_7 = \{7, 11, 13, 14\}$.

The 2-cyclotomic coset for 0 is always $\{0\}$.

The roots of $\mathcal{M}_\alpha(x) = \mathcal{M}_{\gamma^i}(x)$ include $\{\gamma^i | i \in C_s\}$. Hence, we know all of the roots. Furthermore, this tells us that the size of C_s is the degree of $\mathcal{M}_{\gamma^i}(x)$.

We will further use these ideas in the following sections.

5.3 Cyclotomic Polynomials

Let us assume that our field has an element ε of order n. Then $1, \varepsilon, \varepsilon 2, ..., \varepsilon^n$ are all roots of $x^n - 1 = 0$ by Corollary 2.12. Note that $x^n - 1$ has degree n. Hence, this factors into, at most, n roots. This implies that all the powers of ε must contain all nth roots of unity. This leads us to the following result.

Theorem 5.10. $x^n - 1 = \prod_{i=0}^{n-1}(x - \varepsilon^i) = \prod_{i=1}^{n}(x - \varepsilon^i)$.

Proof. This follows quickly from the above discussion. As ε is a root in our field, each power of ε, $\{1, \varepsilon, \varepsilon^2, ..., \varepsilon^{n-1}\}$ must all be roots satisfying the equation $\prod_{i=1}^{n-1} x - \varepsilon^i = 0$. □

Now consider the polynomial $x^n - 1$ where $n = kd$. Then we have $\varepsilon^k, \varepsilon^{2k}, ..., \varepsilon^{nk}$ must all be roots of $x^d - 1 = 0$. As this polynomial has order d it can have no more than d roots. Hence, the powers of ε include all dth roots of unity. This means that any element whose order divides n must be a power of ε. Conversely, the order for every power of ε must divide n.

Corollary 5.11. *If ε is a field element of order d and $d|n$ then*

$$x^n - 1 = \prod_{d,d|n} \quad \prod_{\varepsilon}(x - \varepsilon)$$

Definition 5.12. The polynomial whose roots are field elements of order d is called the cyclotomic polynomial. We denote this $\mathcal{Q}^{(d)}(x)$.

As an immediate consequence we get:

Corollary 5.13. $x^n - 1 = \prod_{d,d|n} \mathcal{Q}^{(d)}(x)$.

We now introduce a form of the Moebius inversion formula. We use this formula without proof although one may find a proof in [2]. We first define the Moebius function:

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1 \\ (-1)^k & \text{if } d \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{if } d \text{ contains any repeated prime factors} \end{cases}$$

This gives us the Moebius multiplicative inversion formula:

If $f(n) = \prod_{d,d|n} g(d)$

then

$$g(m) = \prod_{n,n|m} f(n)^{\mu(m/n)}.$$

Applying this formula we have:

Corollary 5.14. $\mathcal{Q}^{(n)}(x) = \prod_{d,d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d,d|n} (x^{n/d} - 1)^{\mu(d)}$

This allows us to deduce many properties of cyclotomic polynomials:

Theorem 5.15. *If p is prime and $p \nmid m$ then*

$\mathcal{Q}^{(mp^k)}(x) = \mathcal{Q}^{(pm)}(x^{p^{k-1}})$.

Proof. We have:

$$\begin{aligned}\mathcal{Q}^{(mp^k)}(x) &= \prod_{d,d|p^k m} (x^{mp^k/d} - 1)^{\mu(d)} \\ &= \prod_{d,d|pm} [(x^{p^k})^{m/d} - 1]^{\mu(d)} = \mathcal{Q}^{(pm)}(x^{p^{k-1}})\end{aligned}$$

□

Theorem 5.16. *If p is prime and $p \nmid m$ then*

$$\mathcal{Q}^{(pm)}(x) = \frac{\mathcal{Q}^{(m)}(x^p)}{\mathcal{Q}^{(m)}(x)}$$

Proof. We have:

$$\mathcal{Q}^{(pm)}(x) = = \left[\prod_{d,d|m} (x^{pm/d} - 1)^{\mu(d)}\right] \left[\prod_{d,d|pm,d\nmid m} (x^{pm/d} - 1)^{\mu(d)}\right]$$

$$= \left[\prod_{d,d|m} [(x^p)^{m/d} - 1]^{\mu(d)}\right] \left[\prod_{d,d|m} (x^{m/d} - 1)^{-\mu(d)}\right]$$

$$= \frac{\mathcal{Q}^{(m)}(x^p)}{\mathcal{Q}^{(m)}(x)}$$

□

The following are given without proofs which can be found in [2].

Theorem 5.17. *If* $n = \prod_i p_i^{e_i}$, *where the* p_i *are primes, then*

$deg\mathcal{Q}^{(n)}(x) = \varphi(n)$,

where $\varphi(n)$ *is Euler's phi function,*

$\varphi(n) = \prod_i p_i^{e_i - 1}(p_i - 1)$.

Theorem 5.18. *If* $n \geq 2$, *then*

$$\mathcal{Q}^{(n)}(x) = \prod_{d,d|n} (1 - x^{n/d})^{\mu(d)}.$$

Theorem 5.19. *If* $n \geq 3$ *and odd, then*

$$\mathcal{Q}^{(2n)}(x) = \mathcal{Q}^{(n)}(-x).$$

Theorem 5.20. *If* $n \geq 2$, *then*

$$x^{\varphi(n)}\mathcal{Q}^n(x^{-1}) = \mathcal{Q}^{(n)}(x).$$

Any finite field contains $\varphi(q-1)$ primitive field elements. This means that the degree of a cyclotomic polynomial can be determined easily. Namely, if the order of α is n then the order of α^k is also n provided $(n, k) = 1$. This gives us

$$\mathcal{Q}^{(n)}(x) = \prod_{(k,n)=1, 1 \leq k < n} (x - \alpha^k).$$

Using the properties of cyclotomic polynomials makes calculations easier. We may reduce our calculations to the case $n > 1$ to get

$$\mathcal{Q}^{(n)}(x) = \prod_{d,d|n} (1 - x^{n/d})^{\mu(d)} \pmod{x^{\varphi(n)/2+1}}.$$

The following is a list of $Q^{(n)}(x)$ and $\varphi(n)$ for $1 \leq n \leq 10$:

n	$\mathcal{Q}^{(n)}(x)$	$\varphi(n)$
1	$x-1$	1
2	$x+1$	1
3	x^2+x+1	2
4	x^2+1	2
5	$x^4+x^3+x^2+x+1$	4
6	x^2-x+1	2
7	$x^6+x^5+x^4+x^3+x^2+x+1$	6
8	x^4+1	4
9	x^6+x^3+1	6
10	$x^4-x^3+x^2-x+1$	4

5.4 Explicit Factorization of $x^n - 1$

Explicitly factoring $x^n - 1$ is now made easier by using cyclotomic cosets and cyclotomic polynomials. We have now seen the power of using cyclotomic polynomials to factor $x^n - x$. Consider the binary polynomial $x^{2^4} - x = x^{16} - x$. To factor it, we first find the 2-cyclotomic cosets modulo 15 since we will be factoring $x^{15} - 1$. We get (from Example 5.9):

$C_1 = \{1, 2, 4, 8\}$.

$C_3 = \{3, 6, 9, 12\}$.

$C_5 = \{5, 10\}$.

$C_7 = \{7, 11, 13, 14\}$, and

$C_0 = \{0\}$.

By our earlier discussion about cyclotomic cosets, we now know that there are three polynomials of order 4, a polynomial of order 2, and a polynomial of order 1.

Next we find the cyclotomic factorization. We will use $\mathcal{Q}^{(d)}(x)$ for all d such that $d|15$.This gives us:

$$x^{16} - x = x(x^{15} - 1)$$

$$= x\mathcal{Q}^{(1)}(x)\mathcal{Q}^{(3)}(x)\mathcal{Q}^{(5)}(x)\mathcal{Q}^{(15)}(x)$$

$$= x(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^8-x^7+x^5-x^4+x^3-x+1)$$

To see that $\mathcal{Q}^{(15)}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ we have:

$$\mathcal{Q}^{(15)}(x) = \frac{x^{15}-1}{\mathcal{Q}^{(3)}(x)\mathcal{Q}^{(5)}(x)}$$

$$= \frac{x^{15}-1}{\mathcal{Q}^{(3)}(x)(x^5-1)}$$

$$= \frac{x^{10}+x^5+1}{\mathcal{Q}^{(3)}(x)}$$

$$= \frac{x^{10}+x^5+1}{x^2+x+1}$$

$$= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

Recall that the 2-cyclotomic cosets modulo 15 are $\mathcal{C}_0 = \{0\}, \mathcal{C}_1 = \{1,2,4,8\}, \mathcal{C}_3 = \{3,6,9,12\}, \mathcal{C}_5 = \{5,10\}, \mathcal{C}_7 = \{7,11,13,14\}$. Hence, we must have 5 irreducible polynomials in the factorization of $x^{15}-1$ and by the properties of cyclotomic cosets, three of these polynomials must have degree 4.

Now we know that in $\mathbb{F}_2[x]$, $\mathcal{Q}^{(15)}(x)$ must factor into two irreducible polynomials of degree 4. Hence, we must have two polynomials of the form $x^4+ax^3+bx^2+c^x+1$. Note here that 1 is not a root of this polynomial. Thus, $a+b+c=1$, which means either one of a, b, c is 1 or all three are 1. But as $\mathcal{Q}^{(5)}(x) = x^4+x^3+x^2+x+1$ it cannot be the case that all three are 1. This leaves us with only three possible polynomials: x^4+x^2+1, x^4+x^3+1, or x^4+x+1. But we see that $x^4+x^2+1 = (x^2+x+1)^2$. Hence, the only remaining choices give us our factorization of $^{(15)}(x)$:

$\mathcal{Q}^{(15)}(x) = (x^4+x^3+1)(x^4+x+1)$

Through this process we obtain the complete factorization of $x^{16} - x$ over $\mathbb{F}_2$:

$x^{16} - x = x(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$

We now show the roots with associated minimal polynomial and 2-cyclotomic coset.

Roots	Minimal Polynomial	2-cyclotomic Coset
0	x	
1	$x+1$	$\{0\}$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	x^4+x+1	$\{1,2,4,8\}$
$\alpha^3, \alpha^6, \alpha^{\cdot}\alpha^{12}$	$x^4+x^3+x^2+x+1$	$\{3,6,9,12\}$
α^5, α^{10}	x^2+x+1	$\{5,10\}$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	x^4+x^3+1	$\{7,11,13,14\}$

This process illustrates the power of cyclotomic cosets and cyclotomic polynomials. Using the results of this factorization we are able to define and find generator polynomials, the building blocks for cyclic codes.

CHAPTER 6: Generator Polynomials and Idempotents

6.1 Generator Polynomials

As was seen in section 3.5, the polynomial $g(x)$ in I generates all polynomials in $\mathcal{R}_n$. It is a monic polynomial that divides $x^n - 1$. The polynomial $g(x)$ is called a *generator* of I. This is denoted by $I =< g(x) >$. It is not necessarily the case that $g(x)$ is the only polynomial that generates I. As every cyclic code $\mathcal{C}$ is an ideal, there is a generator polynomial for every cyclic code $\mathcal{C}_i$.

Because we are computing our cyclic codes as ideals in $\mathcal{R}_n$, there is a bijective correspondence between the nonzero cyclic codes and the divisors of $x^n - 1$. Under this correspondence, if $\mathcal{C}_i \in \mathcal{R}_n$ are cyclic codes where i runs through the number, z, of q-cyclotomic polynomials, then there are 2^z cyclic codes. Furthermore, the dimensions of the cyclic codes are all possible sums of the sizes of the q-cyclotomic cosets. Because $\mathcal{R}_n = \mathbb{F}_q[x]/(x^n-1)$, the generator polynomial of the zero cyclic code is $x^n - 1$.

Let us consider the generator polynomials of $(x^7-1) = (x+1)(x^3+x+1)(x^3+x^2+1)$ over $\mathbb{F}_2$. We have:

i	dim	$g_i(x)$
0	0	$1 + x^7$
1	1	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
2	3	$x^4 + x^3 + x^2 + 1$
3	3	$x^4 + x^2 + x + 1$
4	4	$x^3 + x + 1$
5	4	$x^3 + x^2 + 1$
6	6	$x + 1$
7	7	1

This factorization gives us eight binary codes $\mathcal{C}_i$ of length 7 and more than one generator for $x^9 - 1$

6.2 Idempotents

We move on now to the idea of idempotents. These elements of a ring reduce the computations for factoring $x^n - 1$ and simplify the process for finding cyclic codes.

Definition 6.1. An element e of a ring is called an *idempotent* if $e^2 = e$.

Though a simple definition, the power of these ring elements becomes clear as we extend the idea of generator polynomials.

We note here that the idempotent for the zero cyclic code is 0 and the generator for $\mathcal{R}_n$ is 1.

Theorem 6.2. *Let $\mathcal{C}$ be a cyclic code in $\mathcal{R}_n$. Then we have the following:*

(i) There is a unique idempotent $e(x) \in \mathcal{C}$ where $\mathcal{C} =< e(x) >$, and

(ii) $\mathcal{C} =< e(x) >$ if and only if $e(x)$ is a unity of $\mathcal{C}$, i.e., $c(x)e(x) = c(x)$.

Proof. We consider the nonzero codes since, if $\mathcal{C}$ is the zero code, both *(i)* and *(ii)* are trivial.

We will prove *(ii)* first. Let $e(x)$ be a unity in $\mathcal{C}$. Then as $\mathcal{C}$ is an ideal, $e(x) \subseteq \mathcal{C}$. Let $c(x) \in \mathcal{C}$, then $e(x)c(x) = c(x) \in \mathcal{C}$. This implies that $< e(x) >= \mathcal{C}$. Now suppose $e(x)$ is an idempotent such that $\mathcal{C} = e(x)$. For some $g(x) \in \mathcal{C}$, every element $c(x) \in \mathcal{C}$ can be written as $c(x) = g(x)e(x)$. But this gives us $c(x)e(x) = g(x)(e(x))^2 = g(x)e(x) = c(x)$. Hence, $e(x)$ is a unity in $\mathcal{C}$.

Now we use *(ii)* to prove *(i)*. If $e_1(x)$ and $e_2(x)$ are generating idempotents of $\mathcal{C}$, then they are both unities. We also have that $e_1(x) = e_1(x)e_2(x) = e_2(x)$. This shows that a generating idempotent is unique, hence we have left to prove that there exists such an idempotent.

Suppose $g(x)$ is the generator polynomial in $\mathcal{C}$. Then $g(x)|(x^n - 1)$. Using polynomial factorization we let $f(x) = (x^n - 1)/g(x)$, giving us $\gcd((g(x), f(x)) = 1$ in

$\mathbb{F}_q[x]$ since $x^n - 1$ has distinct roots. Now using the Euclidean Algorithm we have polynomials $c(x), d(x) \in \mathbb{F}_q[x]$ such that $c(x)g(x)+f(x)d(x) = 1$. Let $e(x) = c(x)g(x)$ (mod $(x^n - 1)$). Then in $\mathcal{R}_n$ $(e(x))^2 \equiv (c(x)g(x))(1 - d(x)f(x)) \equiv c(x)g(x) \equiv e(x)$ (mod $(x^n - 1)$) since $g(x)f(x) = x^n - 1$. Now let $c(x) \in \mathcal{C}$ with $c(x) = h(x)g(x)$. This implies $c(x)e(x) \equiv h(x)g(x)(1 - d(x)f(x)) \equiv h(x)g(x) \equiv c(x)$ (mod $(x^n - 1)$). Hence, $e(x)$ is a unity in $\mathcal{C}$. □

This proof tells us that we can find the idempotent for code from a generator polynomial by employing the Euclidean algorithm. That is, we solve the polynomial equation $c(x)g(x) + d(x)f(x) = 1$ where $f(x) = (x^n - 1)/g(x)$, which gives us $gcd(f(x), g(x)) = 1$. Using the Euclidean algorithm we can get the polynomials $c(x)$ and $d(x)$ that solve the polynomial equation. This gives us $e(x) = c(x)g(x)$ (mod $x^n - 1$).

Theorem 6.3. *Let $e(x)$ be the generating idempotent for a cyclic code $\mathcal{C}$ over $\mathbb{F}_q$. Then $gcd(e(x), x^n - 1)$ is the generator polynomial in $\mathbb{F}_q[x]$.*

Proof. Let $g(x)$ be the generator polynomial for $\mathcal{C}$ with $f(x) = \gcd((e(x), x^n - 1)$ in $\mathbb{F}_q[x]$. We have $f(x)|e(x)$, implying $e(x) = f(x)h(x)$. BY Theorem 6.3 (i), $\mathcal{C} =< e(x) >$. Hence, every element of $\mathcal{C}$ is a multiple of $f(x)$. Thus, $\mathcal{C} \subseteq< f(x) >$.

By theorem 6.1 $g(x)|(x^n - 1)$ and $g(x)|e(x)$ since $e(x) \in \mathcal{C}$. Then $g(x)|f(x)$ which implies $f(x) \in \mathcal{C}$. Hence, $< f(x) >\subseteq \mathcal{C}$. So $\mathcal{C} =< f(x) >$. As $f(x)$ is a monic divisor generating $\mathcal{C}$, we have $f(x) = g(x)$. □

Example 6.4. The following table includes all cyclic codes $\mathcal{C}_i$ of length 7 over $\mathbb{F}_2$ listed with their generator polynomials $g_i(x)$ and generating idempotents $e_i(x)$.

i	dim	$g_i(x)$	$e_i(x)$
0	0	$1+x^7$	0
1	1	$x^6+x^5+x^4+x^3+x^2+x+1$	$x^6+x^5+x^4+x^3+x^2+x+1$
2	3	$x^4+x^3+x^2+1$	$x^6+x^5+x^3+1$
3	3	x^4+x^2+x+1	x^4+x^2+x+1
4	4	x^3+x+1	x^4+x^2+x
5	4	x^3+x^2+1	$x^6+x^5+x^3$
6	6	$x+1$	$x^6+x^5+x^4+x^3+x^2+x$
7	7	1	1

Though we can use idempotents to find generating polynomials utilizing the Euclidean algorithm, there is another way to employ idempotents in factoring x^n-1.

Suppose we want to factor x^7-1 over $\mathbb{F}_2$. Let $e(x)$ be an idempotent in $\mathbb{F}_2[x]/(x^7-1)$. It is easy to see that if x is in $e(x)$, then so too must be x^2. Likewise, $(x^2)^2 = x^{s2^2}$ must also be in $e(x)$. Then $((x^2)^2)^2 = x^{2^3}$ must also be in $e(x)$. But, as we are factoring x^7-1, $x^{2^3} = x^8 \equiv x \pmod 7$, we need not go any further. Note here that one of the 2-cyclotomic cosets modulo 7 is $C_1 = \{1,2,4\}$.

Hence, for $x \in e(x)$ we have $x^{s2^{r-1}} \in e(x)$ where r is the smallest integer for which $s2^r \cong s \pmod{x^n-1}$. This implies that to form an idempotent in $\mathbb{F}_2[x]/(x^n-1)$ we can form the coefficients for our polynomial from the 2-cyclotomic cosets. Our idempotents are all possible combinations of the 2-cyclotomic cosets modulo n.

Since our 2-cyclotomic cosets modulo 7 are $C_0 = \{0\}, C_1 = \{1,2,4\}, C_3 = \{3,5,6\}$, the possible combinations are:

$\{0\}, \{1,2,4\}, \{3,5,6\}, \{0,1,2,3\}, \{0,3,5,6\}, \{0,1,2,3,4,5,6\}, \{1,2,3,4,5,6\}$, and 1.

Hence, our idempotents are:

$e_0(x) = 0$,

$e_1(x) = x^6+x^5+x^4+x^3+x^2+x+1$,

$e_2(x) = x^6 + x^5 + x^3 + 1,$

$e_3(x) = x^4 + x^2 + x + 1,$

$e_4(x) = x^4 + x^2 + x,$

$e_5(x) = x^6 + x^5 + x^3,$

$e_6(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x,$ and

1, as seen in Example 6.4.

Therefore, we can find generator polynomials by forming idempotents from our 2-cyclotomic cosets and using the Euclidean algorithm to find $gcd(e_i(x), x^n - 1)$.

We have now defined two methods, using cyclotomic polynomials and using idempotents, for finding generator polynomials of cyclic codes. In the next section, we will develop a $[9, 4]$ binary cyclic code using both methods.

CHAPTER 7: A $[9, 4]$ Binary Cyclic Code

To begin the development of our $[9, 4]$ binary cyclic code, we note that we will be forming 9-dimensional vectors over $\mathbb{F}_2$. That is we will be mapping $\mathbb{F}_2^4 \to \mathbb{F}_2^9$.

We start by finding our 2-cyclotomic cosets.

We have:

(i) For $s = 1$: $\{1, 2, 4, 8, 16 \equiv 7, 14 \equiv 5, 10 \equiv 1\} \Rightarrow C_1 = \{1, 2, 4, 5, 7, 8\}$.

(ii) For $s = 3$: $\{3, 6, 12 \equiv 3\} \Rightarrow C_3 = \{3, 6\}$

We now know that $x^9 - 1$ factors into three polynomials, one of degree 6, one of degree 2, and $C_0 = x + 1$.

We will proceed by using cyclotomic polynomials to factor $x^9 - 1$. We have: $\mathcal{Q}^{(9)}(x) = \mathcal{Q}^{(1)}(x)\mathcal{Q}^{(3)}(x)\mathcal{Q}^{(9)}(x)$

Which gives us $\mathcal{Q}^{(9)}(x) = (x + 1)(x^2 + x + 1)\mathcal{Q}^{(9)}(x)$.

But, $\mathcal{Q}^{(9)}(x) = \mathcal{Q}^{(3)}(x^3) = x^6 + x^3 + 1$.

Hence, $x^9 - 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$.

We can now form our generator polynomials:

i	dim	$g_i(x)$
0	0	$x^9 + 1$
1	1	$(x^6 + x^3 + 1)(x^2 + x + 1) = x^8 + x^7 + ... + x + 1$
2	2	$(x^6 + x^3 + 1)(x + 1) = x^7 + x^6 + x^4 + x^3 + x + 1$
3	3	$x^6 + x^3 + 1$
4	6	$(x^2 + x + 1)(x + 1) = x^3 + 1$
5	7	$x^2 + x + 1$
6	8	$x + 1$
7	9	1

Finally we will use the generator polynomial $g(x) = x^3 + 1$ to form our code:

Messages	Code Vector	Code Polynomial
0000	000000000	$0 = 0 \cdot g(x)$
1000	100100000	$1 + x^3 = 1 \cdot g(x)$
0100	010010000	$x + x^4 = x \cdot g(x)$
1100	110011000	$1 + x + x^3 + x^4 = (1 + x) \cdot g(x)$
0010	001001000	$x^2 + x^5 = x^2 \cdot g(x)$
1010	101101000	$1 + x^2 + x^3 + x^5 = (1 + x^2) \cdot g(x)$
0110	011011000	$x + x^2 + x^4 + x^5 = (x + x^2) \cdot g(x)$
1110	111111000	$1 + x + x^2 + x^3 + x^4 + x^5 = (1 + x + x^2) \cdot g(x)$
0001	000100100	$x^3 + x^6 = x^3 \cdot g(x)$
1001	100000100	$1 + x^6 = (1 + x^3) \cdot g(x)$
0101	010110100	$x + x^3 + x^4 + x^6 = (x + x^3) \cdot g(x)$
1101	110010100	$1 + x + x^4 + x^6 = (1 + x + x^3) \cdot g(x)$
0011	001101100	$x^2 + x^3 + x^5 + x^6 = (x^3 + x^2) \cdot g(x)$
1011	101001100	$1 + x^2 + x^5 + x^6 = (1 + x + x^2) \cdot g(x)$
0111	011111100	$x + x^2 + x^3 + x^4 + x^5 + x^6 = (x + x^2 + x^3) \cdot g(x)$
1111	111011100	$1 + x + x^2 + x^4 + x^5 + x^6 = (1 + x + x^2 + x^3) \cdot g(x)$

This gives us a complete $[9, 4]$ cyclic code.

Now, we proceed using idempotents to find our generator polynomial. We already know that we have three cyclotomic cosets. Hence, we need only find all possible combinations of these cosets. We get:

$\{0\}, \{1, 2, 4, 5, 7, 8\}, \{3, 6\}, \{0, 1, 2, 4, 5, 7, 8\}, \{0, 3, 6\}, \{1, 2, 3, 4, 5, 6, 7, 8\},$

$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, and 1.

We use the Euclidean algorithm to find $gcd(e_i(x), x^9 - 1)$. Hence, our idempotents are:

$e_0(x) = 0,$

$e_1(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8,$

$e_2(x) = x + x^2 + x^4 + x^5 + x^7 + x^8,$

$e_3(x) = 1 + x^3 + x^6,$

$e_4(x) = x^3 + x^6,$

$e_5(x) = 1 + x + x^2 + x^4 + x^5 + x^7 + x^8,$

$e_6(x) = x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8$, and

$e_7(x) = 1,$

where each $e_i(x)$ corresponds to $g_i(x)$ for $i \in \{0, ..., 7\}$. We have now arrived at our generator polynomials, which are the same for both methods.

CHAPTER 8: Conclusion

The use of cyclic codes is crucial to our society. These codes are found in every facet of life, from computers to phones to ATM's and even cars. Thus, it is imperative to find a means by which we may construct these codes without performing rigorous "guess and check" methods. Defining these codes as algebraic structures affords us the opportunity to simplify the computations.

In particular, by defining our codes with an alphabet of integers in modular arithmetic, we are able to view our alphabet as a field and all codewords as vectors in a vector space over the field. This is an obvious leap to make since codes are given as a sequence of digits over some length. Mathematically, this is the definition of a vector space, provided the alphabet is a field. In addition, we can use this vector space and define our codewords as polynomials in a ring. The advantage to such an action is that our codewords can then be defined as polynomials in the ideals of a ring.

The idea of defining codewords in the ideal of a ring hinges on the ability to completely factor the ideal. We develop a progression of ideas that allows us to identify factors of the ideal and, hence, our codewords. Thus completes the trip from codewords to codes, to fields, to vector spaces and rings, and back to codes and codewords.

There are two methods by which we factor $x^n - 1$: using cyclotomic polynomials and using generating idempotents. When factoring $x^n - 1$, the use of cyclotomic polynomials is a less rigorous method for small enough values of n. However, for larger values of n, the use of idempotents in factorization is the preferred approach, especially given the computer programs that can be utilized for finding $gcd(e(x), x^n - 1)$. This completes the trip from codewords to code to polynomial and back to codes and codewords.

Though we define methods for simplifying the development of a code, the ideas used in such a development are complex. The use of advanced algebraic and number theoretical notions is essential to defining and developing these codes. Hence, cyclic codes and, indeed codes in general, are an excellent example of the link between information theory and mathematics. Therefore, we see that such seemingly theoretical concepts lead directly to ideas and processes that affect our everyday lives.

REFERENCES

[1] Artin, M. (1991). *Algebra*. Prentice-Hall, Upper Saddle River, NJ, first edition.

[2] Berlekamp, E. R. (1968). *ALgebraic Coding Theory*. McGraw-Hill, New York, first edition.

[3] Blake, I. F. and Mullin, R. C. (1975). *The Mathematical Theory of Coding*. Academic Press, New York, first edition.

[4] Gallian, J. A. (2006). *Contemporary Abstract Algebra*. Brooks/Cole, Belmont, CA, seventh edition.

[5] Hill, R. (1986). *A First Course in Coding Theory*. Oxford, New York, first edition.

[6] Huffman, W. C. and Pless, V. (2003). *Fundamentals of Error-Correcting Codes*. Cambridge, New York, first edition.

[7] Pless, V. (1998). *In troduction to the Theory of Error-Correcting Codes*. Wiley, New York, third edition.

[Poli and Huguet] Poli, A. and Huguet, L. *Error Correcting Codes Theory and Applications*. Prentice Hall, Englewood Cliffs, NJ PAGES = v+508, ISBN = 0-13-284894-5, MRCLASS = 11Txx, MRNUMBER = MR1429394 (97i:11115),, first edition.

[9] Strayer, J. K. (1994). *Elementary Number Theory*. Waveland, Long Grove, IL, first edition.