A Family of Error Correcting Codes

Ashleigh Meyers
Point Loma Nazarene University
San Diego, CA

April 30, 2018

Abstract

Error correcting codes (ECC) protect the integrity of a message by detecting and correcting errors that occur in digital communication channels. Cyclic codes are examples of ECC of fixed length n. Cyclic codes of length n are constructed by factoring the polynomial x^n+1. In this paper we construct another family of codes by factoring the polynomial $x^n+x^{n-1}+1$. We give the generating and check matrices of these codes and their dimension.

Contents

1 Introduction

In virtually all forms of digital communication, there is a transmission process that is required to take the message from the sender and deliver it to the receiver. The original message to be sent is usually composed of alphabetical characters, binary or decimal digits; however, before it can be delivered to the receiver, it must be transformed by the encoder into a form that the destination storage medium finds acceptable. For our purposes, we will be working with codes composed of binary characters. As we will later see, we can detect and correct errors in the transmitted message by using the structure and properties of certain polynomials. So the first task is to associate a polynomial to a binary message. For example, the polynomial $1 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 1$ will be associated to the binary message 1101.

Using the associated polynomial, we can perform operations and utilize certain properties of polynomials in order to check if any errors were made and if so, correct the errors, thus making the transmission more reliable. This is done by adding redundancies to the code before transmission. By repeating parts of the message, it is easier to deduce what the original message was, in the case that errors occur.

For instance, suppose a message was sent as a response to a question either with Y for yes or N for no. If the symbol is received incorrectly, the receiver will have no way of knowing if that was the intended response or if the answer was warped in transmission. To make it possible to know if an error occurred, the sender could add an additional symbol to the message - YY for yes and NN for no. Now if a symbol is warped in transmission, the receiver will know since YN and NY are not possible codewords; however, with a code only having one correct and one incorrect symbol, the receiver cannot know which one is correct. In order for the receiver to be able to detect not only that an error occurred, but also be able to discern where the error occurred, the original message will have to have an additional redundancy with the possible codewords being either YYY or NNN. Then, if NNY is received, the receiver can deduce that the original message was NNN because it is more likely that just one error occurred.

2 Background

To even begin constructing a code in which error correction can occur, the underlying structure of the code must first be understood. In this section we will review the mathematical background necessary for the construction and study of the codes.

2.1 Finite Rings and Finite Fields

Definition 1. A finite commutative ring R is a non-empty set endowed with two operation addition and multiplication satisfying the following axioms:

Axiom 1 Addition is commutative: $a + b = b + a$ for all a and b in R.

Axiom 2 Addition is associative: $(a + b) + c = a + (b + c)$ for all a, b and c in R.

Axiom 3 Multiplication is commutative: $a \cdot b = b \cdot a$ for all a and b in R

Axiom 4 Multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot a)$ for all a b and c in R

Axiom 5 Multiplication distributes over sum: $a \cdot (b + c) = a \cdot b + a \cdot c$ for all a, b and c in R.

Axiom 6 There is a unique element 0 in R such that $a + 0 = 0 + a = a$ for all a in R

Axiom 7 For each a in R there is a unique element x in R such that $a + x = x + a = 0$

Axiom 8 There is a unique element $1 \neq 0$ in R such that $a \cdot 1 = 1 \cdot a = a$ for all a in R

Definition 2. An ideal I in a ring R is a subset of R such that

1. For all a and b in I, $a + b$ is in I.
2. For all a in I and for all x is in R, $x \cdot a$ is in I.

Definition 3. A finite integral domain D is a finite ring satisfying the condition: if a and b are elements of D and $a \cdot b = 0$ then either $a = 0$ or $b = 0$.

Definition 4. A finite field with q elements $\mathbb{F}_q$ is ring such that each element of $\mathbb{F}$ that is not equal to 0 has a multiplicative inverse.

The unique structure of finite fields allows the possibilities of finite patterns to be controlled and therefore is useful in the construction of codes. In order to design codes in which errors are easily detectable and correctable, the code alphabet is given the structure of a finite field $\mathbb{F}_q$.

Definition 5. Let $\mathbb{F}_q$ be a finite field. **The ring of polynomials** with coefficients in $\mathbb{F}_q$ and denote by $\mathbb{F}_q[x]$ is the set

$$\mathbb{F}_q[x] = \left\{ a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n \,|\, a_0, a_1, \ldots, a_n \text{ are in } \mathbb{F}_q \text{ and } a_n \neq 0. \right\}$$

The operations are addition and multiplication of polynomials.

2.2 Constructions

There are a variety of types of fields to consider within code theory. We will use the binary field $\mathbb{F}_2$.

Definition 6. As a set, **the binary field** is $\mathbb{F}_2 = \{0, 1\}$. Addition is defined as $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, and $1 + 1 = 0$. Multiplication is defined as $0 \cdot 0 = 0$, $0 \cdot 1 = 1 \cdot 0 = 0$, and $1 \cdot 1 = 1$.

2.3 Building the Code

Definition 7. A **binary word** w of length n is a vector

$$w = [w_0, w_1, \ldots, w_{n-1}]$$

where each w_i is in the binary field $\mathbb{F}_2$. That is, each w_i is either 0 or 1.
The set of all the binary words of lenght n will be denoted by $\mathbb{F}_2^n$.
Binary words can be added coordinate by coordinate. Also, if a word is multiplied by 0 the result is the zero word $[0, 0, 0, \ldots, 0]$ and if the word is multiplied by 1 then the result is the same word.

Definition 8. A **binary linear code** C of length n is a set

$$C = \{c_1, c_2, c_3, \ldots, c_M\}$$

such that the sum of any two code words is a code word in C. C is also called a block code of length n.

3 Introduction to Error-Correcting Codes

The main objective behind the process of Error-Correcting Codes is that the errors in a received message are corrected.

The way in which a message is sent is in a block code C, which is a set of M codewords.

$$C = \{c_1, c_2, ..., c_M\}$$

$$c_i = \left[c_{i0}, c_{i1}, c_{i2}, ..., c_{i(n-1)}\right]$$

3.1 Properties

The ability to perform computations on codewords is essential because useful codes can only be constructed through certain algebraic methods. This concept was developed by Richard Hamming in the 1950's and his ideas and the codes he constructed set the foundation for ECC and thus paved the way for the construction error correcting codes. No matter how complex or different newly created error correcting codes may seem, they all boil down to the same basic principles.

Definition 9. The **weight** *w(x)* of a word $x \in \mathbb{F}_2^n$ is the number of 1's in x.

Definition 10. Suppose we are given two words x and $y \in \mathbb{F}_2^n$

$$x = x_1x_2...x_n \qquad y = y_1y_2...y_n$$

The **Hamming distance** $d(x, y)$ is the number of $i\,(1 \leq i \leq n)$ such that $x_i \neq y_i$. In other words, it is the number of places where x and y differ. See page 95 in [1].

For example, let the following words be in $\mathbb{F}_2^7$ be

$$x = 1110101 \quad y = 0110100 \quad z = 1000111$$

The words x and y differ in the first and last bits only, therefore $d(x, y) = 2$. Similarly, $d(x, z) = 3$ and $d(y, z) = 5$.

The distance of a code is a key component in many aspects, but is useful to know when considering the efficiency of a code, especially in regards to how many errors can be detected and corrected. To see how the distance affects this, it must first be understood how it is determined whether a code has an error. After the encoding and transmission of the message, the encoded message is decoded and received. With the message in the form of a matrix, another matrix, known as the **parity check matrix**, is multiplied with the received message and a product of 0 will indicate that no errors were made.

Definition 11. A matrix H over $\mathbb{F}_2$ with m rows and n columns is the **parity check matrix** (or **check matrix**) for the linear code C if and only if for all $x \in C$ $Hx = 0$.

While the parity check matrix is able to accomplish error detection, the structure of it also determines how many errors are able to be corrected.

Theorem 12. *Let H be a check matrix for a binary code C. Then the **minimum distance** $d(C)$ of C, is equal to the minimum number of linearly dependent columns of H.*

Proof. See page 153 in [1]. □

In other words, the minimum distance of a code C is the smallest Hamming distance between distinct code words of C [4]. For instance, let B be a code containing the two words from an earlier example - YYY and NNN. Then $d(B) = 3$ since the codewords vary in all three positions. In this case, the code could detect if one or two errors had been made if the received message contained at least one of each letter. However, only in the instance of one error occurring can it be corrected successfully. If the received word was YYN, the conclusion would be that the intended message was YYY. However, if the original message was NNN and the received message was also YYN, then the conclusion that the original message was YYY would be false. Due to the exceedingly low probability of two errors occurring in a code of length three, this is a satisfactory method of correcting errors, but also has an opportunity of the correction method to be improved.

With the minimum distance known, utilizing the triangle inequality will determine the maximum number of errors that can be accurately corrected. With the minimum distance of three in the example above, it is clear by the triangle inequality that no more than one error could be corrected. In regards to larger codes, a similar argument holds true. [4]

Theorem 13. *The code C corrects all errors of weight up to t if and only if C has minimum distance $2t + 1$.*

Proof. See page 18 in [4] □

4 The Family of Cyclic Codes Associated to $x^n + 1$

The way in which we are able to check codes for errors is by putting them in the format of matrices. To do so, the structure of a cyclic code is used, which can be thought of in a few ways. A cyclic code is created by taking a factor $g(x) = g_0 + g_1 \cdot x \cdots + g_{n-k} \cdot x^{n-k}$ of the polynomial $x^n + 1$ and creating a matrix associated to this polynomial. The first row of the matrix corresponds to the coefficients of the polynomial, the next row of the matrix corresponds to the coefficients of the polynomial multiplied by x, thus increasing each power of x by one and shifting each coefficient of the polynomial over by one. In simpler terms, the coefficients of the polynomial are shifted over one for each row, or the coefficients are "cycling" through for k shifts construct the matrix. The **cyclic shift** of a word is obtained by taking the last digit of the word and moving it to the beginning, with all other digits moving one position to the right. See page 102 [5]

For example, 01011 is a cyclic shift of 10110. Other examples include...

codeword	10110	111000	0000	1011
shift	01011	011100	0000	1101

A code C is said to be a **cyclic code** if the cyclic shift of each codeword is also a codeword. [5]

For a cyclic code, the polynomial $x^n + 1$ is split into two factors $g(x)$ and $h(x)$ in which one is used for the generating matrix $g(x)$ and the other for the parity check matrix $h(x)$. Each one has this cyclic property to form each matrix and holds the property $G \cdot H = 0$.

Theorem 14. *For the cyclic codes corresponding to the polynomial $x^n + 1$, factor $x^n + 1$ as $g(x) \cdot h(x)$:*

$$x^n + 1 = g(x) \cdot h(x) = (g_0 + g_1 x + ... + g_{n-k} x^{n-k}) \cdot (h_0 + h_1 x + ... + h_k x^k)$$

The polynomial $g(x)$ is used to create the generating matrix G with k rows. To be able to check if a received word is a codeword, a parity check matrix will need to be constructed. The parity check matrix H will have $n-k$ columns and must satisfy the equation $G \cdot H = \mathbf{0}$, where $\mathbf{0}$ is the zero matrix of size $k \times (n-k)$. The matrices G and H below satisfy this equation

$$G \cdot H = \begin{bmatrix} g_0 & g_1 & g_2 & g_3 & \cdots & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & 0 & 0 \\ 0 & 0 & g_0 & g_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 \\ 0 & 0 & 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} \end{bmatrix} \cdot \begin{bmatrix} h_k & 0 & 0 & \cdots & 0 & 0 \\ h_{k-1} & h_k & 0 & \cdots & 0 & 0 \\ h_{k-2} & h_{k-1} & h_k & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ h_0 & h_1 & h_2 & \cdots & h_{k-1} & h_k \\ 0 & h_0 & h_1 & \cdots & h_{k-2} & h_{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & h_0 & h_1 \\ 0 & 0 & 0 & \cdots & 0 & h_0 \end{bmatrix} = \mathbf{0}$$

Proof. See Theorem 4.2.7 in [3] □

4.1 Properties

Let C be an $[n, k]$ cyclic code over $\mathbb{F}_2$. If a codeword

$$c = [c_0, c_1, \ldots, c_{n-1}]$$

is in C we associate to c the poynomial

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$$

in $\mathbb{F}_2[x]$.

Definition 15. A polynomial $g(x)$ in $\mathbb{F}_2[x]$ is a **monic** if the coefficient of the highest power of x is 1.

Theorem 16. *Let $g(x)$ be the monic polynomial of lowest degree in C. Then the following properties hold:*

1. *$g(x)$ divides $c(x)$ for every $c \in C$*
2. *$g(x)$ divides $x^n + 1$ in $\mathbb{F}_2[x]$*
3. *$k = n - \deg(g(x))$*

Part 1 of the above theorem says that every $c(x)$ is a multple of the monic polynomial $g(x)$. The polynomial $g(x)$ will be called the **generating** polynomial of C. Also, part 2 of the theorem indicates that to understand and build cyclic codes, we must first understand the divisors of $x^n + 1$.

For the polynomials we are working with, the codes rely on on fields that have p^d elements, or more specifically, 2^d elements. As we have seen, this is dependent upon the primitive element, which in this case is the irreducible polynomial $f(x)$. The **generator polynomial** is the monic polynomial that divides the polynomial that generates the code and is unique; this is then used to construct the **generator matrix** $g(x)$.

For cyclic codes, n is taken to be odd (in the binary case) because the polynomial $x^n + 1$ has derivative $n \cdot x^{n-1} = x^{n-1}$ and since the greatest common divisor of the polynomial and its derivative is equal to 1, that will ensure that the polynomial does not have common factors.

5 The Family of Codes Associated to $x^n + x^{n-1} + 1$

Theorem 17 (Main Theorem)**.** *For the family of codes corresponding to the polynomial $x^n + x^{n-1} + 1$, factor $x^n + x^{n-1} + 1$ as $g(x) \cdot h(x)$:*

$$x^n + x^{n-1} + 1 = g(x) \cdot h(x) = (g_0 + g_1 x + ... + g_{n-k}x^{n-k}) \cdot (h_0 + h_1 x + ... + h_k x^k)$$

The polynomial $g(x)$ is used to create the generator matrix G with k rows. To be able to check if a received word is a codeword, a parity check matrix will need to be constructed. The parity check matrix H will have $n-k$ columns and must satisfy the equation $G \cdot H = \mathbf{0}$, where $\mathbf{0}$ is the zero matrix of size $k \times (n-k)$. The matrices G and H below satisfy this equation

$$G \cdot H = \begin{bmatrix} g_0 & g_1 & g_2 & g_3 & \dots & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & \dots & 0 & 0 \\ 0 & 0 & g_0 & g_1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & g_0 & g_1 & \dots & g_{n-k} & 0 \\ 0 & 0 & 0 & g_0 & \dots & g_{n-k-1} & g_{n-k} \end{bmatrix} \cdot \begin{bmatrix} h_k & 0 & 0 & \dots & 0 & 1 \\ h_{k-1} & h_k & 0 & \dots & 0 & 0 \\ h_{k-2} & h_{k-1} & h_k & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ h_0 & h_1 & h_2 & \dots & h_{k-1} & h_k \\ 0 & h_0 & h_1 & \dots & h_{k-2} & h_{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & h_0 & h_1 \\ 0 & 0 & 0 & \dots & 0 & h_0 \end{bmatrix} = \mathbf{0}$$

Proof. Let X be a matrix such that $G \cdot H = X$. Thus, X will have the form

$$\begin{bmatrix} x_{00} & x_{01} & x_{02} & x_{03} & \dots & x_{0(n-k)} \\ x_{10} & x_{11} & x_{12} & x_{13} & \dots & x_{1(n-k)} \\ x_{20} & x_{21} & x_{22} & x_{23} & \dots & x_{2(n-k)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{k0} & x_{k1} & x_{k2} & x_{k3} & \dots & x_{k(n-k)} \end{bmatrix}$$

Therefore, the entries of X satisfy the equations below

$$g_0 h_k + g_1 h_{k-1} + g_2 h_{k-2} + g_3 h_{k-3} + \dots 0 \cdot 0 + 0 \cdot 0 = x_{00}$$
$$0 \cdot h_k + g_0 h_{k-1} + g_1 h_{k-2} + g_2 h_{k-3} + \dots 0 \cdot 0 + 0 \cdot 0 = x_{10}$$
$$0 \cdot h_k + 0 \cdot h_{k-1} + g_0 h_{k-2} + g_2 h_{k-3} + \dots 0 \cdot 0 + 0 \cdot 0 = x_{20}$$
$$\vdots$$
$$g_0 \cdot 1 + \dots + g_{n-k-1} \cdot h_k + g_{n-k} \cdot h_{k-1} \dots + 0 \cdot h_0 = x_{0(n-k)}$$

We observe that $g_{n-k+i} = 0$, for $i \geq 1$. To ensure that $G \cdot H$ produces the $\mathbf{0}$ matrix, each entry of X must equal 0.

When multiplying the two factors $g(x)$ and $h(x)$ of the polynomial $x^n + x^{n-1} + 1$ we obtain

$$g_0 h_0 + (g_0 h_1 + g_1 h_0)x + \dots + (g_{n-k-1} h_k + g_{n-k} h_{k-1})x^{n-1} + (g_{n-k} h_k)x^n$$

Since $g(x) \cdot h(x) = x^n + x^{n-1} + 1$, it is clear that the only coefficients equal to 1 are those of x^n, x^{n-1} and 1. Thus, the corresponding coefficients of the expanded product must satisfy

$$g_0 h_0 = 1, \quad (g_{n-k-1} h_k + g_{n-k} h_{k-1}) = 1, \quad g_{n-k} h_k = 1,$$

and the remaining coefficients must be equal to zero.

Note that if $g_i h_j$ appears as a term of the coefficient of x^r, then $i + j = r$. Looking at the matrix multiplication that produces the entries of X, the only problematic entry is $x_{0(n-k)}$; this will always be the case since each term $g_i h_j$ in the coefficient satisfies $i + j = n - 1$ and thus $x_{0(n-k)}$ would equal 1. However, by always placing a 1 in the $n - k$ position of the first row of H, $x_{0(n-k)}$ will equal the coefficient of x^{n-1} plus $g_0 \cdot 1$, which equal to $1 + 1 = 0$. With this modification of the matrix H, all entries of X will be equal to zero. This proves that H is a parity check matrix for the code generated by G. □

Example 18. Consider codes associated with the polynomial $x^{12} + x^{11} + 1$. Since there are three factors of this polynomial and only two factors can be considered here - one for the generating matrix and one for the parity check matrix - there are $2^3 = 8$ possible codes associated with this polynomial with the factorization

$$x^{12} + x^{11} + 1 = (x^3 + x + 1) \cdot (x^4 + x + 1) \cdot (x^5 + x^4 + x^3 + x^2 + 1)$$

By taking different possibilities of combining these three factors into two, differently structured codes can be created, but will all be done in the same process, resulting in codes able to detect if errors occurred in transmission.

1. Take the generating polynomial $g(x)$ to be the product of the first two factors

$$g(x) = (x^3 + x + 1) \cdot (x^4 + x + 1) = x^7 + x^5 + x^3 + x^2 + 1$$

and the check polynomial $h(x)$ is taken to be the remaining factor

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

Let $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_7 x^7$ and $h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_5 x^5$. The generating matrix for the code is

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & 0 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & 0 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & 0 & 0 \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & 0 \\ 0 & 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 \end{bmatrix} =$$

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

and parity check matrix for the code is

$$H = \begin{bmatrix} h_5 & 0 & 0 & 0 & 0 & 0 & 1 \\ h_4 & h_5 & 0 & 0 & 0 & 0 & 0 \\ h_3 & h_4 & h_5 & 0 & 0 & 0 & 0 \\ h_2 & h_3 & h_4 & h_5 & 0 & 0 & 0 \\ h_1 & h_2 & h_3 & h_4 & h_5 & 0 & 0 \\ h_0 & h_1 & h_2 & h_3 & h_4 & h_5 & 0 \\ 0 & h_0 & h_1 & h_2 & h_3 & h_4 & h_5 \\ 0 & 0 & h_0 & h_1 & h_2 & h_3 & h_4 \\ 0 & 0 & 0 & h_0 & h_1 & h_2 & h_3 \\ 0 & 0 & 0 & 0 & h_0 & h_1 & h_2 \\ 0 & 0 & 0 & 0 & 0 & h_0 & h_1 \\ 0 & 0 & 0 & 0 & 0 & 0 & h_0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

To ensure that H is a parity check matrix for G, it must be the case that $G \cdot H = \mathbf{0}$. According to Theorem 14, the only problematic position of X would be $x_{0,12}$ had there not been a 1 placed in the $(n-k)^{th} = 7^{th}$ position of the first row of H. The calculation of $x_{0,12}$ is taken to be

$$g_0 \cdot 1 + g_1 \cdot 0 + g_2 \cdot 0 + g_3 \cdot 0 + g_4 \cdot 0 + g_5 \cdot 0 + g_6 h_5 + g_7 h_4 + g_8 h_3 + g_9 h_2 + g_{10} h_1 + g_{11} h_0$$

$$= g_0 \cdot 1 + g_6 h_5 + g_7 h_4 + g_8 h_3 + g_9 h_2 + g_{10} h_1 + g_{11} h_0$$

By the theorem, it is clear that $g_6 h_5 + g_7 h_4 + g_8 h_3 + g_9 h_2 + g_{10} h_1 + g_{11} h_0$ is the coefficient of x^{11} and thus equal to 1. Since $g_0 = 1$, $x_{0,12} = 1 + 1 = 0$ and therefore the required property for this code is satisfied.

2. For another one of the eight possible codes for this polynomial, take $g(x)$ to be

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

and h(x) to be the product of the remaining two factors

$$h(x) = (x^4 + x + 1) \cdot (x^5 + x^4 + x^3 + x^2 + 1) = x^9 + x^8 + x^7 + x^4 + x^2 + x + 1$$

Let $g(x) = g_0 + g_1 x + g_2 x^2 + g_3 x^3$ and $h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_9 x^9$.
The generating matrix for the code is

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & g_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & g_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & g_3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & g_0 & g_1 & g_2 & g_3 \end{bmatrix} =$$

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

and parity check matrix for the code is

$$H = \begin{bmatrix} h_9 & 0 & 1 \\ h_8 & h_9 & 0 \\ h_7 & h_8 & h_9 \\ h_6 & h_7 & h_8 \\ h_5 & h_6 & h_7 \\ h_4 & h_5 & h_6 \\ h_3 & h_4 & h_5 \\ h_2 & h_3 & h_4 \\ h_1 & h_2 & h_3 \\ h_0 & h_1 & h_2 \\ 0 & h_0 & h_1 \\ 0 & 0 & h_0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Similarly to part 1, it must be satisfied that $G \cdot H = \mathbf{0}$ and can be checked by ensuring that $x_{0,12} = 0$. Note for this example, the 1 has been placed in the $(n-k)^{th} = 3^{rd}$ position of the first row of H. The calculation of $x_{0,12}$ is taken to be

$$g_0 \cdot 1 + g_1 \cdot 0 + g_2 h_9 + g_3 h_8 + 0 \cdot h_7 + 0 \cdot h_6 + 0 \cdot h_5 + 0 \cdot h_4 + 0 \cdot h_3 + 0 \cdot h_2 + 0 \cdot h_1 + 0 \cdot h_0$$

$$= g_0 \cdot 1 + g_2 h_9 + g_3 h_8$$

By the theorem, it is clear that $g_2 h_9 + g_3 h_8$ is the coefficient of x^{11} and thus equal to 1. Since $g_0 = 1$, $x_{0,12} = 1 + 1 = 0$ and therefore the required property for this code is satisfied.

5.1 Comparing cyclic codes and codes generated by $x^n + x^{n-1} + 1$

The table below shows the corresponding polynomials for the cyclic codes of length n up to length $n = 19$ and the factorization in the ring $\mathbb{F}_2[x]$.

Degree	Polynomial	Factors
1	$x+1$	$(x+1)$
3	x^3+1	$(x+1)\cdot(x^2+x+1)$
5	x^5+1	$(x+1)\cdot(x^4+x^3+x^2+x+1)$
7	x^7+1	$(x+1)\cdot(x^3+x+1)\cdot(x^3+x^2+1)$
9	x^9+1	$(x+1)\cdot(x^2+x+1)\cdot(x^6+x^3+1)$
11	$x^{11}+1$	$(x+1)\cdot(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$
13	$x^{13}+1$	$(x+1)\cdot(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+$ $+x^5+x^4+x^3+x^2+x+1)$
15	$x^{15}+1$	$(x+1)\cdot(x^2+x+1)\cdot(x^4+x+1)\cdot$ $\cdot(x^4+x^3+1)\cdot(x^4+x^3+x^2+x+1)$
17	$x^{17}+1$	$(x+1)\cdot(x^8+x^5+x^4+x^3+1)\cdot(x^8+x^7+x^6+x^4+x^2+x+1)$
19	$x^{19}+1$	$(x+1)\cdot(x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+$ $+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$

Note that there are no cyclic codes of even length listed. When n is even, codes of the form x^n+1 always have repeated roots in their factorization and because this repeated factor causes difficulties in not only encoding and decoding, but also error correcting, these factorizations have been omitted. However, it is clear after examining the codes generated by $x^n + x^{n-1} + 1$ below that cases in which n is even, the factorizations do not produce a repeated root and can thus be utilized for error correcting purposes.

The table below shows the corresponding polynomials for the family of codes based on $x^n + x^{n-1} + 1$ of length n up to length $n = 19$ and the factorization in the ring $\mathbb{F}_2[x]$.

Degree	Polynomial	Factors
2	$x^2 + x + 1$	$(x^2 + x + 1)$
3	$x^3 + x^2 + 1$	$(x^3 + x^2 + 1)$
4	$x^4 + x^3 + 1$	$(x^4 + x^3 + 1)$
5	$x^5 + x^4 + 1$	$(x^2 + x + 1) \cdot (x^3 + x + 1)$
6	$x^6 + x^5 + 1$	$(x^6 + x^5 + 1)$
7	$x^7 + x^6 + 1$	$(x^7 + x^6 + 1)$
8	$x^8 + x^7 + 1$	$(x^2 + x + 1) \cdot (x^6 + x^4 + x^3 + x + 1)$
9	$x^9 + x^8 + 1$	$(x^9 + x^8 + 1)$
10	$x^{10} + x^9 + 1$	$(x^3 + x^2 + 1) \cdot (x^7 + x^4 + x^3 + x^2 + 1)$
11	$x^{11} + x^{10} + 1$	$(x^2 + x + 1) \cdot (x^9 + x^7 + x^6 + x^4 + x^3 + x + 1)$
12	$x^{12} + x^{11} + 1$	$(x^3 + x + 1) \cdot (x^4 + x + 1) \cdot (x^5 + x^4 + x^3 + x^2 + 1)$
13	$x^{13} + x^{12} + 1$	$(x^5 + x^4 + x^2 + x + 1) \cdot (x^8 + x^5 + x^3 + x + 1)$
14	$x^{14} + x^{13} + 1$	$(x^2 + x + 1) \cdot (x^5 + x^2 + 1) \cdot (x^7 + x^5 + x^2 + x + 1)$
15	$x^{15} + x^{14} + 1$	$(x^{15} + x^{14} + 1)$
16	$x^{16} + x^{15} + 1$	$(x^8 + x^5 + x^3 + x^2 + 1) \cdot (x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1)$
17	$x^{17} + x^{16} + 1$	$(x^2 + x + 1) \cdot$ $\cdot(x^3 + x^2 + 1) \cdot (x^{12} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1)$
18	$x^{18} + x^{17} + 1$	$(x^5 + x^3 + 1) \cdot (x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^6 + x^5 + x^3 + 1)$
19	$x^{19} + x^{18} + 1$	$(x^3 + x + 1) \cdot (x^4 + x^3 + 1) \cdot (x^5 + x^4 + x^3 + x + 1) \cdot$ $\cdot(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1)$

Example 19. Let $n = 5$ for both $x^n + 1$ and $x^n + x^{n-1} + 1$ in order to compare the different codes produced.

1. Consider the polynomial $x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$.

   The cyclic code C with generating polynomial $g(x) = 1 + 1 \cdot x$ and check polynomial $h(x) = 1 \cdot x^4 + 1 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x + 1$ has the following generating matrix G and check matrix H

   $$G \cdot H = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

   Looking at the codewords of G and its combinations, the minimum distance oc C is $d(C) = 2$.

2. Consider the polynomial $x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$.

   The code C with generating polynomial $g(x) = 1 + 1 \cdot x + 1 \cdot x^3$ and check polynomial $h(x) = 1 \cdot x^2 + 1 \cdot x + 1$ has the following generating matrix G and check matrix H

   $$G \cdot H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

   Looking at the codewords of G and its linear combinations, the minimum distance of C is $d(C) = 3$.

6 Future Research

For the codes based on these polynomials, great progress has been made in regards to their construction and properties. After observing the construction for the cyclic codes corresponding to $x^n + 1$, a similar construction was made for the family of codes corresponding to $x^n + x^{n-1} + 1$. Using this new polynomial, we were able to find a method to determine if any errors were made by constructing their check matrix. However, there is still much to done. For each specific case of these codes, the minimum distance can be calculated. What still remains to be found though is a general formula for minimum distance for all codes of these forms. Knowing the minimum distance is critical in order to determine how many errors can be corrected. Once the minimum distance is determined, a method to correct errors remains to be found. We did not address this problem.

7 Conclusion

While the concept of Error Correcting Codes has been around for over half a century, the foundational properties and structures have been used to create new codes with new possibilities. They all serve the same purpose - to deliver messages in a secure, efficient and reliable manner. The structure of these codes is designed to transmit the original message in the most accurate way possible while still keeping its confidentiality. To make these codes reliable, algebraic computations are performed to add indicators in the case of an error occurring, as well as including the correction tools that are necessary.

By using the polynomial $x^n + 1$ to create a cyclic code, messages are sent in a reliable and secure method. Developing upon this, polynomials of new forms can be used to create codes in a similar way but allowing for a variety of new codes. Now, an error detection method has been discovered for the family of codes corresponding to $x^n + x^{n-1} + 1$. To correct the errors and thus further the functionality of these codes constructed the parity check matrix. The construction of the parity matrix is the main contribution of our work.

References

[1] Norman L. Biggs. *Codes: An Introduction to Commmunication and Cryptography*, Springer, London. 2008

[2] Jorn Justesen, Tom Hoholdt. *A Course in Error-Correcting Codes*, European Mathematical Society, 2004

[3] W. Cary Huffman, Vera Pless. *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2010

[4] Oliver Pretzel *Error-Correcting Codes and Finite Fields*, Oxford University Press Inc., New York, 1992

[5] D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, J.R. Wall *Coding Theory: The Essentials*, Marcel Dekker, Inc., 1991