Chapter 1
Introduction
1

Introduction

1.1 Digital Communication

In digital communication system, the information to be communicated is converted into binary form. The process of converting information into binary form is called source encoding. Most of the times unnecessary bits are present in the converted message and it is important to represent the digitized signal by as few bits as possible. The source encoder removes the unnecessary bits. This converted message is transmitted through the medium or channel. In the receiver end the decoder converts the binary form of message into original one. Most of the times noise is present in the channel and as a result the message received by the receiver is different from the message that was sent. Thus it becomes important to detect and correct errors while transmitting a message through a noisy communication channel. A Satellite communication link, high frequency radio link, or telephone line are some examples of communication channels. Thermal noise, lightning, human error etc are different types of noises. In digital communication, we have to send a picture or voice message through a noisy communication channel.

The idea of error correction and detection technique is to add some extra bits to the converted message in the binary form so that the original message can be recovered if
not too many errors have occurred. The process of adding extra bits or redundancy to the original message is called channel encoding. We have given the block diagram of a digital communication system in Fig. 1.1.

1.2 Error-correction Technologies in Digital Communication System

The principle of error correction technologies is to break up a picture or voice message into small parts and represent each of the parts by a sequence of zeros and ones of same length in most of the cases. The binary strings are often chosen to achieve some additional goal such as to detect or correct errors that might be caused by noise when the information is sent over a noisy channel. For example, to apply error correction technology while sending the picture in Fig. 1.2 through a noisy communication channel the picture is divided into 7X7 small squares. Each of the small square is called a pixel. The pixels (picture elements) of the image could be sent over the channel by coding a white pixel with 000000, a black pixel with 111111 and a gray pixel with 000111. Now the receiver knows the size of the image which is 7X7 and the receiver also knows that the pixels are being sent row by row in order of increasing column number. Thus the receiver can accurately decode the picture if not too many errors have occurred during the transmission process.

The Hamming distance between two strings of equal length is the number of positions at which the corresponding symbols are different. Here Hamming distance between any pair of codes is at least 3, so if no more than one error has occurred while transmitting any code word,
then received code word can be checked and if errors have occurred, they can be corrected so that the original image can be reconstructed.

1.3 Relation between Codes and Geometry

There is a relation between codes and finite geometry. Codes can be constructed using finite geometry. For example, we consider the diagram in Fig. 1.3, which represents a finite geometry known as projective geometry. It has exactly 7 points and 7 lines with 3 points on every line. In this finite geometry two points determine a unique line but every pair of lines has a point in common. It has also relation with balance block design. Now we can construct a matrix of zeros and ones that represents this plane by thinking of the columns of the matrix as representing the points, and the rows of the matrix as representing the lines. For a particular row, the entry in a column is 1 if that point is on the line which the row represents and a 0 otherwise. For example for $L_1$, we would get the entries:

1101000

This is because this line contains the points $P_1$, $P_2$, and $P_4$ and, thus, there are 1’s in column one, two, and four. We continue the process for the other 6 lines and get the following 7X7 array of zeros and ones.

110100
0110100
Fig. 1.3 Projective geometry

0011010
0001101
1000110
0100011
1010001

By treating the rows of the matrix above as binary strings we get the Hamming distance between any pair of these binary strings is at least 3. Thus, we can think of these 7 rows as being the code words of a binary error correction code which will correct up to one error per code word. One can add additional binary strings of length 7 to the strings above and still keep the distance between the strings at least three. We can do this by creating a new string from each string above by changing the ones in the row to zeros and the zeros in the row to ones. Now we have 14 sequences of binary digits of length 7 where each of the pairs of sequences has Hamming distance at least three. Finally, we can add the two additional strings 0000000 and 1111111 and maintain this property. Thus, we have the remarkably large collection of binary strings (16 strings), each pair of which has distance at least three. Thus, we have a 16 code word code which will correct 1 error. There can be no longer collection of code words for a code with code words of length 7 that corrects one error [64].
1.4 Examples of Error-correcting Codes with Applications

**Hamming codes**: The nascent computer industry and the phone industry were among the very earliest users of error correction technologies. For example, data is moved around often within a computer. Computer memory systems use Hamming codes to prevent errors occurring in some of these situations.

**Reed-Solomon codes** [64]: We can take the example of audio compact discs and those that are used in conjunction with computers. It is known that Reed-Solomon codes are used for some compact discs although some of the systems used in these technologies are proprietary.

**Turbo codes** [64]: There are error correcting codes which do not employ the idea of separate code words of the same length, where the code word has information symbols and some other symbols present for the error correction capability. For example, convolutional codes can be thought of as sending information as a stream of symbols where "check symbols" are entered into the stream being sent from time to time. The output from the encoder of a message divided into k-tuples depends on the current k-tuple being processed as well as on some of the prior message k-tuples. The output from pieces are longer than the input pieces to incorporate the error correction capability. Turbo codes are examples of these kind of codes.

**Reed-Muller codes**: In 1965 the Mariner spacecraft mission took photographs (without color) of Mars successfully. The pictures were 200x200 with each pixel being assigned one of 64 brightness levels (six bits). Transmission of a single picture took about 8 hours as the data was transmitted at about 8 bits per second. In the year 1972 Mariner 9 went into orbit around Mars. This time the spacecraft used a Reed-Muller code having 6 information bits and 26 additional bits to provide error correction (the code words were 32 bits long) and therefore the picture quality was better than before. Although transmission speed now was up to about 16000 bits per second, the individual images were larger, and so about 100000 bits per second were being acquired by the cameras. This meant that the images were stored for transmission.

**Spherical codes**: Rover spacecraft was launched in the year 2011 and landed on Mars successfully in 2012. A specific kind of code called the spherical codes was used in this mission and much better quality picture of the surface of Mars was received by NASA.
Fig. 1.4 Picture of Mars surface taken by Mariner 4, 1965

Fig. 1.5 Picture of Mars surface taken by Rover, 2012
1.5 Historical Development of Error-correcting Codes

In 1947, Dr. Hamming constructed the first error-correcting code namely “Hamming code” and introduced the idea of error-correcting codes. Later in the year 1950, Hamming published a paper entitled, Error detecting and error correcting codes in The Bell System Technical Journal[48]. In the year 1948, C E Shannon published a paper[83] in the same journal The Bell System Technical Journal entitled A mathematical theory of communication. In this paper he proved that better codes really exist. Till then everybody considered information theory as an engineering discipline. In his revolutionary paper Shannon proved that we can transmit digital information almost without error up to a computable maximum rate though a communication channel for given degree of noise contamination of the channel. This is called Noisy-channel coding theorem of Shannon and it’s proof is probabilistic. This theorem guarantees the existence of such good codes but he had not constructed any code which proves his result. In coding theory researchers actually try to meet the demand of Noisy-channel coding theorem of Shannon.

In the year 1949, M J E Golay constructed the (23, 12) Golay code and published an article on digital coding in the Proceedings of the IEEE[45]. “BCH codes” are a generalization of Hamming codes. They were independently discovered by Bose and Ray-Chaudhuri[14] in 1960 and by Hocquenghem[53] in 1959. The dual of Hamming codes are called Hadamard codes and its generalization are called “Reed-Muller codes”. Reed-Muller codes were first introduced by Muller[68] in the year 1954 but he had not studied decoding algorithm of these codes. In the same year Reed has given an efficient decoding algorithm of Reed-Muller codes[77]. In 1960 Reed and Solomon introduced the Reed-Solomon codes[78]. These are optimal codes and require a large alphabet size.

In 1957, while working at the Air Force Cambridge Research Center, Dr. Prange invented cyclic codes[72]. Later in the year 1958 he had also invented the quadratic residue codes[73]. Both BCH and Reed-Solomon codes are cyclic codes. The concept of cyclic shift of code words was first introduced by Hocquenghem, Bose and Ray-Chaudhuri. Reed-Solomon codes have large Hamming distance and efficient decoding algorithm was given by Berlekamp[4] and Massey[66]. Berlekamp was the first to study Negacyclic codes over finite fields[4], [5]. While BCH codes are binary cyclic codes, Reed-Solomon codes are non-binary. Reed-Solomon codes became more popular with the development of efficient decoding algorithm together with more powerful computers. Reed-Solomon codes are used in satellite communication, data storage system, space communication etc. Binary quadratic residue codes are very powerful class of cyclic codes. But their decoding algorithm are very
difficult. The block size of quadratic residue codes are selected depending upon \( n = 8t \pm 1 \), where \( t \) is the error correction capacity.

The repeated-root codes were discovered when the length \( n \) of the code is divisible by the characteristic \( p \) of the field. This was first studied by Berman[6] in 1967 and then by several authors such as Massey, Costello and Justesen[65], Falkner, Kowol, Heise and Zehendner[42], and Van Lint[89].

Professor emeritus Robert G Gallager[43] of Massachusetts Institute of Technology was credited for the discovery of LDPC (Low-density parity check) codes. He was the first to propose these codes in the year 1963. These are linear error correcting codes and can be constructed using a sparse bipartite graph. LDPC codes are important as they can meet the demand of Noisy-channel coding theorem of Shannon. These codes were remained unknown to the researchers untill its rediscovery in the year 1996. In the year 1991, Turbo codes were discovered and it was observed that these codes nearly fulfill the expectation of Shannon’s Noisy-channel coding theorem. But the first paper on Turbo codes was published in the year 1993 by Claude Berrou[7]. The fundamental patent application for Turbo codes was filled by Claude Berrou in April, 1991 and he is the sole inventor of these codes. Turbo codes have similar performance as LDPC codes. Both Turbo codes and LDPC codes are used in 3G/4G mobile communication and satellite communication. It is only after the discovery of these two codes and the study of iterative decoding algorithms of these codes, most of the researchers tried to discover codes that fulfill the expectation of Shannon’s Noisy-channel coding theorem.

Singleton bound was given by Richard Collom Singleton in the year 1964[84]. Codes meeting this bound are called MDS codes. Reed-Solomon codes and their extended codes are examples of non-trivial MDS codes. In the year 1968, P. F. Preparata found a class of non-linear double-error correcting codes called Preparata codes[76]. Preparata codes are non-linear over \( GF(2) \), but linear over \( \mathbb{Z}_4 \). In the 1970’s Goppa[46] invented a class of linear codes called Goppa codes. The Goppa codes meets the famous Gilbert-Varshamov bound asymptotically and hence important in the technical point of view.

For scientific and financial computing data corruption is not tolerated. Error-correcting code memory in a computer can detect and correct most common kind of internal data corruption. In modern time error-correcting codes(ECC) are widely used in the system reliability and data integrity of computer semiconductor memory systems. ECCs are now
becoming more cost-effective means of maintaining a high level of system reliability[58], [59], [79].

### 1.6 Recent Development in Error-correcting Codes

Most important development in error-correcting codes took place during the 1990’s. More and more researchers entered into this field and made some ground breaking discoveries. Calderbank and Sloane[18] in the year 1995 have given the structure of cyclic codes over $\mathbb{Z}_p$, and in 1997 Kanwar and Lopez-Permouth[55] have given an alternative proof. The structure theorems in [18] and [55] were extended by Norton and Salagean[70] by using a different technique in 2000. Dinh and Lopez-Permouth[21] in 2004 generalised the structure of cyclic codes to finite chain rings. The general properties of cyclic codes over $\mathbb{Z}_n$ were studied by Dougherty and Park[29] using discrete Fourier transform in the year 2007.

In [49] Hammons, Kummar, Calderbank, Sloane and Sole proved that a binary polynomial that generates the cyclic Hamming code of length 7 can be lifted to be a polynomial over $\mathbb{Z}_4$ that generates the octacode, which is equivalent to the binary nonlinear Nordstrom-Robinson code. In [18] structure of cyclic codes of length $n$ over the $p$-adic integers was studied by Calderbank and Sloane and the structure of cyclic codes of length $n$ over the $p$-adic integers was obtained, where $\text{gcd}(n, p) = 1$. They have also given the description of the lifts of codes of length $n$ over $\mathbb{Z}_p$ to $\mathbb{Z}_{p^n}$ and to the $p$-adics was also given. In 2005, Dougherty, Kim and Park[24] investigated these codes and found the weight enumerators of this class of codes.

Cyclic codes, negacyclic codes and constacyclic codes are widely studied in coding theory due to the rich algebraic structure of these codes. Codes like BCH, Kerdock, Golay, and Preparata are either cyclic codes or constructed from cyclic codes. All $\lambda$-cyclic codes over a finite field of length $n$ are classified as ideals of the ring $\frac{\mathbb{F}[x]}{<x^n-\lambda>}$, where $\mathbb{F}$ is a finite field. In the year 2000, Norton and Salagean[70] studied the structure of linear and cyclic codes over finite chain rings. In 2008, Zhu and Kai[96] obtained the structure of dual and self-dual negacyclic codes of even length over $\mathbb{Z}_2^n$.

Dinh and Lopez-Permouth[21] in the year 2004 published a paper on structure of Cyclic and negacyclic codes over finite chain rings. Dougherty, Liu, and Park[28] in 2011 defined a series of finite chain rings and introduced the concept of $\gamma$-adic codes over formal power series rings. In 2011 Dougherty and Liu[27] have given the concept of $\lambda$-cyclic code of...
length $n$ over formal power series rings. They established a relation between cyclic codes and negacyclic codes over formal power series rings. They obtained a relation between cyclic codes over formal power series rings and cyclic codes over finite chain rings. Dougherty and Ling[26] in the year 2006 proved that a cyclic shift in $\mathbb{Z}_4^{2^k n}$ corresponds to a $u$—constacyclic shift in $\left(\frac{\mathbb{Z}_4[u]}{<u^{2^k} - 1>}\right)^n$ by constructing a module isomorphism between $\left(\frac{\mathbb{Z}_4[u]}{<u^{2^k} - 1>}\right)^n$ and $\mathbb{Z}_4^{2^k n}$.

In [28] Dougherty, Liu, and Park defined MDS codes over $R_\infty$ to be the codes satisfying the bound $d \leq n - k + 1$, where $d$ is the minimum Hamming weight of the code, $k$ is the rank of the code, and $n$ is the length of the code. Here it is shown that lifts of MDS codes are MDS codes.

In [86] in the year 2013, Sobhani and Molakarimi constructed a one-to-one correspondence between cyclic codes of length $2n$ over the ring $R_{k - 1, m}$ and cyclic codes of length $n$ over the ring $R_{k, m}$ for odd $n$ and determined the number of ideals of the ring $R_{2, m}$ and $R_{3, m}$. Hence in [86] they have obtained the number of cyclic codes of odd length over $R_{2, m}$ and $R_{3, m}$ as a corollary.

### 1.7 Objective

In coding theory we apply algebraic techniques to detect and correct communication errors caused by noise while transmitting through a noisy communication channel. Each code word of an error-correcting code is a finite sequence of symbols taken from a finite set. The finite set of symbols is called alphabet and generally it is taken to be the set $\mathbb{F}_q = \{0, 1, \ldots, q - 1\}$ with $q$ prime power, which is a field. All the code words of a code are taken to be of same length in general. A sub-space of a vector space over a finite field of dimension $n$ is called a linear code, or generalizing the concept, a $R$—submodule $C$ of the $R$—module $R^n$ is called a linear code of length $n$ over $R$, where $R$ is a ring. If $n$ is the length of a codeword of a code, $M$ is the total number of code words of a code and $d$ is the minimum distance between any two code words of the code, then $n, M, d$ are called the parameters of a code. A code with parameters $n, M$ and $d$ is called an $(n, M, d)$—code. A good $(n, M, d)$—code has small $n$, large $M$ and large $d$. The main coding theory problem is to optimize one of the parameters $n, M$, $d$ for given values of the other two. This problem is fundamental to the theory of error correcting codes as the transmission speed increases for small $n$, we can detect and correct more errors for large $d$ and more information can be communicated when the number of code words $M$ is more.
If \( q \) is the size of alphabet of a given code and for given values of \( n \) and \( d \), the largest possible size \( M \) for which there exists an \( (n, d) \)-code is denoted by \( A_q(n, d) \). \( A_q(n, d) \) does not depend on the choice of alphabet. It depends on the size of alphabet, \( n \) and \( d \). Much effort has been made by the coding theorists to determine this value of \( A_q(n, d) \). But they got success to find some bounds only. We can restrict ourselves to linear codes only. If \( q \) is a prime power and given values of \( n \) and \( d \), the largest possible size \( q^k \) for which there exists an \( [n, k, d] \)-code is denoted by \( B_q(n, d) \). The objective of error correcting code is to determine the values of \( A_q(n, d) \) and \( B_q(n, d) \). Though it is a tough job to find these values, Some well known bounds have been determined.

If \( q > 1 \) is an integer and \( n \) and \( d \) are integers such that \( 1 \leq d \leq n \), then

\[
\frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i} \leq A_q(n, d) \tag{1.1}
\]

\[
A_q(n, d) \leq \frac{q^n}{\sum_{i=0}^{\left\lfloor (d-1)/2 \right\rfloor} \binom{n}{i} (q-1)^i} \tag{1.2}
\]

\[
A_q(n, d) \leq q^{n-d+1} \tag{1.3}
\]

Bound 1.1 is a lower bound and is called sphere-covering bound and bound 1.2 is an upper bound and is called Hamming bound or sphere-packing bound. The upper bound 1.3 is called Singleton bound.

If \( q > 1 \) is an integer and \( n \) and \( d \) are integers satisfying \( nr < d \), where \( r = 1 - q^{-1} \), then

\[
A_q(n, d) \leq \left\lfloor \frac{d}{d-rn} \right\rfloor \tag{1.4}
\]

The bound 1.4 is called Plotkin bound. In table 1.1, 1.2 and 1.3, we have discussed sphere covering bounds, Hamming bounds, Singleton bounds and Plotkin bounds for \( A_2(n, 3) \), \( A_2(n, 5) \) and \( A_2(n, 7) \).

We are interested to study cyclic codes over finite chain rings over finite fields in this research work. Our objective is to determine all the cyclic codes of given length over a finite chain ring over a finite field. Every ideal of the ring \( \frac{R_i[x]}{<x^a-1>} \) corresponds to a cyclic code of length \( n \) over the finite chain ring \( R_i \) over a finite field \( \mathbb{F} \). So if we can determine the total number of ideals of the ring \( \frac{R_i[x]}{<x^a-1>} \) and the structure of the ideals of the same ring, it will give us the answer of our problem. The structure of ideals of the ring \( \frac{R_i[x]}{<x^a-1>} \) are given by the
Table 1.1 Bounds for $A_2(n, 3)$

<table>
<thead>
<tr>
<th>$n$</th>
<th>Sphere-covering</th>
<th>Hamming</th>
<th>Singleton</th>
<th>Plotkin</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>5</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>9</td>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>16</td>
<td>32</td>
<td>16</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>28</td>
<td>64</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td>51</td>
<td>128</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>19</td>
<td>93</td>
<td>256</td>
<td>-</td>
</tr>
<tr>
<td>11</td>
<td>31</td>
<td>170</td>
<td>512</td>
<td>-</td>
</tr>
<tr>
<td>12</td>
<td>52</td>
<td>315</td>
<td>1024</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 1.2 Bounds for $A_2(n, 5)$

<table>
<thead>
<tr>
<th>$n$</th>
<th>Sphere-covering</th>
<th>Hamming</th>
<th>Singleton</th>
<th>Plotkin</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>6</td>
<td>16</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>11</td>
<td>32</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>18</td>
<td>64</td>
<td>12</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>30</td>
<td>128</td>
<td>24</td>
</tr>
<tr>
<td>12</td>
<td>6</td>
<td>51</td>
<td>256</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 1.3 Bounds for $A_2(n, 7)$

<table>
<thead>
<tr>
<th>$n$</th>
<th>Sphere-covering</th>
<th>Hamming</th>
<th>Singleton</th>
<th>Plotkin</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>3</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>5</td>
<td>16</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>8</td>
<td>32</td>
<td>4</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>13</td>
<td>64</td>
<td>4</td>
</tr>
</tbody>
</table>
generators of the ideals. The general idea for determination of the ideals of the ring \( R_\infty[x]/_{x^n-1} \) is to determine the structure of the ideals of the ring \( R_\infty[x]/_{x^n-1} \). Since the formal power series ring \( R_\infty \) over a finite field \( \mathbb{F} \) is the natural extension of the finite chain ring \( R_t \), we can take projection of the coefficients of the elements of the ring \( R_\infty[x]/_{x^n-1} \) onto the ring \( R_t[x]/_{x^n-1} \). Thus any property satisfied by the ring \( R_\infty[x]/_{x^n-1} \) will also be satisfied by the ring \( R_t[x]/_{x^n-1} \) under the projection mapping. Therefore we determine the generators of the ideals of the ring \( R_\infty[x]/_{x^n-1} \) and then by taking projection we can determine the generators of the ideals of the ring \( R_t[x]/_{x^n-1} \). In some cases it is possible to determine the total number of ideals of the ring \( R_\infty[x]/_{x^n-1} \). Again the generators of the ideals of the ring \( R_\infty[x]/_{x^n-1} \) are given by the factors of the polynomial \( x^n - 1 \). Thus factorization in \( R_\infty[x] \) is an important topic. Again factorizatin in formal power series ring \( R_\infty \) over a finite field \( \mathbb{F} \) are closely related with factorizatin in formal power series ring with integer coefficients. In the third chapter of this thesis we have treated the problem of factorization in \( \mathbb{Z}[x] \). In this research work, we have adopted a completely different approach to determine the structure of the ideals of the ring \( R_\infty[x]/_{x^n-1} \).

In the fourth chapter of this thesis, we have constructed an isomorphism between \( R_\infty[x]/_{x^n-1} \) and \( R_t[x]/_{x^n-1} \) and proved that cyclic codes of composite length \( mn \) over the formal power series ring \( R_\infty \) corresponds to \( u \)-constacyclic code of length \( m \) over \( R_t[x]/_{x^n-1} \). By taking projection it is proved that cyclic codes of length \( mn \) over the finite chain ring \( R_t \) corresponds to \( u \)-constacyclic code of length \( m \) over \( R_t[x]/_{x^n-1} \). Hence we have determined the types of ideals of the ring \( R_\infty[x]/_{x^n-1} \) as well as the ring \( R_t[x]/_{x^n-1} \) that will give us cyclic codes over \( R_\infty \) and \( R_t \) respectively. In the fifth chapter of our thesis, we have defined a bijective mapping \( \Phi_t \) on \( R_\infty \), where \( R_\infty \) is the formal power series ring over a finite field \( \mathbb{F} \). The inverse of \( \Phi_t \) has been determined and hence proved that \( \Phi_t \) is bijective. \( \Phi_t \) preserves addition but does not preserve multiplication, thus it is not an isomorphism. It is proved that a cyclic shift in \( (\mathbb{F})^n \) corresponds to a \( \Phi_t \)-cyclic shift in \( (R_\infty)^n \) by defining a mapping from \( (R_\infty)^n \) onto \( (\mathbb{F})^n \).

### 1.8 Outcome of Our Present Work

Rings and modules are abstract algebraic structures. Rings are divided into two classes, namely, commutative and non-commutative. While the ring of integers and the rings of polynomials are central to the development of commutative ring theory, attempts to extend the complex numbers to various hypercomplex number systems is responsible for the development of non-commutative ring theory. In 1908 Joseph Wedderburn and in 1928 Emil Artin identified various hypercomplex numbers with matrix rings. In 1920, Emmy Noether, and W. Schmeidler published a landmark paper about the theory of ideals. In this paper, they defined
left and right ideals in a ring. In the following year, Noether published a paper, "Idealtheorie in Ringbegrifneh" which was called revolutionary by the noted algebraist Irving Kaplansky. In this paper she analyzed the ascending chain conditions with regard to ideals. In a module over a ring the scalars are the elements of an arbitrary given ring (with identity). Thus a module is a generalization of the notion of vector space over a field. Here multiplication is defined between elements of the ring and elements of the module. Many mathematicians were involved in the development of the theory of rings and modules. Rings and modules have wide applications in different areas. They have major application in the mathematical theory of error-correcting codes. A sub-module of a module is called a linear code. Again a cyclic code of length \( n \) over a finite field \( \mathbb{F} \) can be viewed as an ideal of the ring \( \mathbb{F}[x]_{<x^n-1>} \). In this study we are interested in the application of rings and modules in error-correcting codes. Thus the study of sub-modules of some particular kind of modules and ideals of some special rings play a vital role in our present work.

The first chapter of this thesis is an introductory one. In the second chapter, we have discussed some basic results and important definitions with examples required for our further study which are available in the literature. The whole chapter is divided into two sections. While some definitions and results from rings and modules are included in the first section required for the study of error-correcting codes, in the second section we have given the basic definitions and some fundamental results of coding theory. We have included some lemmas and theorems in this chapter which we have proved in alternative methods.

Some results of the third chapter of this thesis have been presented as a paper entitled, "Factorization in Formal Power Series Ring with Integer Coefficients" in the UGC Sponsored National Seminar on "Mathematics-Its Interdisciplinary Approaches in Modern Curriculum" organised by the Department of Mathematics, Devicharan Barua Girls’ College, Jorhat, Assam from 30th to 31st August, 2013 in collaboration with Devicharan Barua Girls’ High School, Jorhat. We have published the contents of this chapter in the paper, "Some Classes of Irreducible Eliments in Formal Power Series Ring over the Set of Integers" in the "International Journal of Mathematical Archive."

In the third chapter we have considered the problem of factorization in \( \mathbb{Z}[[x]] \). The formal power series ring \( \mathbb{Z}[[x]] \) is the natural extension of the polynomial ring \( \mathbb{Z}[x] \). The basic difference between the factorization in \( \mathbb{Z}[x] \) and \( \mathbb{Z}[[x]] \) is that while \( 6 + x + x^2 \) is irreducible in \( \mathbb{Z}[x] \), it is reducible in \( \mathbb{Z}[[x]] \) as a power series over \( \mathbb{Z} \) is reducible if the constant term of the power series is not a prime power. Again \( 2 + 7x + 3x^2 = (2 + x)(1 + 3x) \) is reducible in
\[ \mathbb{Z}[x] \text{ but irreducible in } \mathbb{Z}[[x]] \text{ as } 1 + 3x \text{ is a unit in } \mathbb{Z}[[x]]. \] Factorization in \( \mathbb{Z}[[x]] \) is still a topic of research and it is not completely solved in most of the cases.

In the first section of the third chapter we have discussed the invertible and irreducible polynomials over various integral domains. In the second section we have discussed the invertible and irreducible power series over \( \mathbb{Z}, \mathbb{Q}, \mathbb{R} \) and \( \mathbb{C} \). In the third section we have discussed the fact that \( \mathbb{Z}[[x]] \) is a UFD. It does not follow from the fact that \( R[x] \) is a UFD when \( R \) is a UFD. In [82] Samuel proved that it is possible for \( R[[x]] \) not to be a UFD even if \( R \) is a one. \( \mathbb{Z}[[x]] \) is a UFD follows from the fact that \( \mathbb{R}[[x]] \) is a UFD when \( \mathbb{R} \) is a PID. In this chapter we have proved that the problem of factorization in \( \mathbb{Z}[[x]] \) reduces to factorization of power series where the constant term is a prime power. In the last section we have discussed some irreducibility criterion of formal power series over the set of integers.

A part of the fourth chapter has been presented as a paper entitled, "Some Results on Cyclic Codes over Formal Power Series Rings and Finite Chain Rings." in the, "National Conference on Mathematics and Its Applications-2016" jointly organised by Cotton College State University and Cotton College, Guwahati. The fourth chapter is communicated as a paper entitled, "Projection of Cyclic Codes over Formal Power Series Rings onto Cyclic Codes over Finite Chain Rings" for publication in some reputed journals.

In the fourth chapter of this thesis, we have constructed an isomorphism between \( \frac{R_{\omega}[x]}{<x^{m}-u>} \) and \( \frac{R_{\omega}[x]}{<x^{m}-1>} \) and proved that cyclic codes of composite length \( mn \) over the formal power series ring \( R_{\omega} \) corresponds to \( u-\text{constacyclic code of length } m \) over \( \frac{R_{\omega}[x]}{<x^{m}-1>} \). Then by taking projection we have proved that cyclic codes of length \( mn \) over the finite chain ring \( R_{i} \) corresponds to \( u-\text{constacyclic code of length } m \) over \( \frac{R_{i}[x]}{<x^{m}-1>} \). We have also determined the types of ideals of the ring \( \frac{R_{\omega}[x]}{<x^{m}-u>} \) as well as the ring \( \frac{R_{i}[x]}{<x^{m}-u>} \) that will give us cyclic codes over \( R_{\omega} \) and \( R_{i} \) respectively. Here, considering both \( m \) and \( n \) as odd numbers we have proved that \( u-\text{constacyclic codes of length } m \) over \( \frac{R_{\omega}[x]}{<x^{m}-1>} \) corresponds to \( u-\text{constacyclic code of length } m \) over \( \frac{R_{i}[x]}{<x^{m}+1>} \). Thus corresponding to every cyclic code of odd length \( mn \) over \( R_{\omega} \) there exists a negacyclic code of same length over \( R_{i} \).

The contents of the fifth chapter was presented in the national conference on, "Recent Trends of Mathematics and its Applications-2014" organized by Department of Mathematics Rajiv Gandhi University, Rono Hills, Arunachal Pradesh, as a paper entitled, "A Study of Cyclic Codes Via a Surjective Mapping." The same paper with slight modifica-
tion is accepted for publication in the journal "MATEMATIKA".

In the fifth chapter of our thesis, we have defined a bijective mapping $\Phi_I$ on $R_\infty$, where $R_\infty$ is the formal power series ring over a finite field $\mathbb{F}$. The inverse of $\Phi_I$ has been determined and hence proved that $\Phi_I$ is bijective. $\Phi_I$ preserves addition but does not preserve multiplication, thus it is not an isomorphism. It is proved that a cyclic shift in $(\mathbb{F})^n$ corresponds to a $\Phi_I$-cyclic shift in $(R_\infty)^n$ by defining a mapping from $(R_\infty)^n$ onto $(\mathbb{F})^n$.

We have concluded the thesis with future scope. Coding theory is a vast area. It has connection with finite geometry, combinatorics and lattice theory. There are many open problems in coding theory. They are classified into two categories:

(i) **Hilbert Problems**: These are fundamental questions whose solutions would lead to further study.

(ii) **Fermat Problems**: These are difficult problems in coding theory that have defied solution for a significant period of time.

In this chapter we have discussed some of the open problems and proposed to study those problems in future.