In chapter three we have treated the problem of factorization in \( \mathbb{Z}[[x]] \). Like the factorization in \( \mathbb{Z}[x] \) and \( \mathbb{Q}[x] \), the factorization in \( \mathbb{Z}[[x]] \) is still not completely solved. \( \mathbb{Z}[[x]] \) is a UFD. If the constant term of a power series is prime, then the power series is irreducible. Again a formal power series is invertible if the constant term is a unit. In [8] Birmajer and Gil proved that a non-invertible power series is reducible if the constant term is not a prime power. They have given an algorithm to factorise a non-invertible power series whose constant term is not a prime power. By induction it can be proved that any non-invertible power series whose constant term is not a prime power can be reduced to product of power series whose constant terms are prime powers. As \( \mathbb{Z}[[x]] \) is a UFD, this factorization is unique and our problem of factorization in \( \mathbb{Z}[[x]] \) reduces to factorise power series whose constant term is a prime power. In chapter three we have discussed some irreducibility criterion for power series with constant term prime square as given by Birmajer and Gil[8]. In [9], [10], [11] Birmajer, Gil and Weiner have given some irreducibility criterion and algorithm for factorization of power series whose constant term is a prime power. Still the problem of factorization in \( \mathbb{Z}[[x]] \) is unsolved and there are lots of scope to work in this direction.

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. In chapter four we have constructed an isomorphism between $\frac{R_{m u}[x]}{<x^{m+1} u>}$ and $\frac{R_{m u}[x]}{<x^m u>}$ 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 $\frac{R_{m u}[x]}{<x^u m-1>}$. Then by taking projection of the co-efficients of the elements of the ring $\frac{R_{m u}[x]}{<x^u m-1>}$ we have proved that cyclic codes of length $mn$ over the finite chain ring $R_i$ corresponds to $u-$constacyclic code of length $m$ over $\frac{R_{i u}[x]}{<x^u i-1>}$. It may be possible to establish a relation between the total number of ideals of the ring $\frac{R_{i u}[x]}{<x^u i-1>}$ and total number of ideals of the ring $\frac{R_{i u}[x]}{<x^u -1>}$ [x]. Hence a relation between the total number of ideals of the ring $\frac{R_{i u}[x]}{<x^u -1>}$ and $\frac{R_{i u}[x]}{<x^u i-1>}$. If one of $m$ or $n$ say $m = rs$ is a composite number where $r \neq 1, s \neq 1$ then we can apply the theorem for $r$ and $s$. Repeating this process our problem reduces to establish a relation between the total number of ideals of the ring $\frac{R_{i u}[x]}{<x^u i-1>}$ and total number of ideals of the ring $\frac{R_{i u}[x]}{<x^u -1>}$ where $m$ and $n$ both are prime. It would be interesting to establish such relations. It will give us relation between total number of cyclic codes of length $m$ over $R_i$ and total number of cyclic codes of length $mn$ over $R_i$

Again in chapter four, considering both $n$ and $m$ as odd we have proved that $u-$constacyclic codes of length $m$ over $\frac{R_{m u}[x]}{<x^u -1>}$ corresponds to $u-$constacyclic code of length $m$ over $\frac{R_{m u}[x]}{<x^u +1>}$. Thus corresponding to every cyclic code of odd length $mn$ over $R_{\infty}$ there exists a negacyclic code of same length over $R_{\infty}$. Still we have not been able to find any counter example to disprove that $u-$constacyclic codes of length $m$ over $\frac{R_{m u}[x]}{<x^u -1>}$ corresponds to $u-$constacyclic code of length $m$ over $\frac{R_{m u}[x]}{<x^u +1>}$, when at least one of $m$ or $n$ is even. Nor we have been able to construct any isomorphism between $\frac{R_{m u}[x]}{<x^u -1>}$ and $\frac{R_{m u}[x]}{<x^u +1>} \quad \text{to prove that} \quad u-$constacyclic codes of length $m$ over $\frac{R_{m u}[x]}{<x^u -1>}$ corresponds to $u-$constacyclic code of length $m$ over $\frac{R_{m u}[x]}{<x^u +1>}$, when either $m$ or $n$ or both are even. We are still investigating this problem and propose to study in this direction.

Coding theory is a vast area. It has connection with different branches of mathematics like 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 in coding theory. Their solutions would lead to further study.

(ii) **Fermat Problems:** These are difficult problems in coding theory and they are unsolved.
for a significant period of time. Many coding theorists tried to solve these problems but failed.
In the conference paper [25] Dougherty, Kim and Sole have discussed many open problems in coding theory. We shall discuss some of the open problems and try to understand them. We propose to study these open problems in future.

**Fundamental Problem of Coding Theory:** It is a Hilbert problem. It can be stated in many ways.

**Open Problem 1(a)**[25] For a fixed $n, \, d$ and $\mathbb{F}_q$, find $A(n, \, d)$, the largest $M$ such that there exists a code $C \subset \mathbb{F}_q^n$ with $|C| = M$.

The value of $A(n, \, d)$ is known for many cases when values of $n$ and $d$ are given over various small fields. But in most of the cases the problem is unsolved. We can rephrase the problem by holding fixed any two parameters.

Much attention is given to linear version of the problem which is stated as follows:

**Open Problem 1.(b)**[25] For a fixed $n, \, d$ and $\mathbb{F}_q$, find $k[n, \, d]$, the largest integer $k \leq n$ such that there exists a linear code $C \subset \mathbb{F}_q^n$ with $dim(C) = k$ and minimum weight $d$.

Most general version of fundamental theorem of coding theory is stated as follows:

**Open Problem 1.(c)**[25] Given a finite metric space $X^n$ and a metric $D$, fix $n$ and $d$. Find the largest $M$ such that there exists a code $C \subset X^n$, with minimum distance $d$, and $M = |C|$.

**MDS and MDR Codes:** At first we shall discuss some theorems, then state the open problem related to MDS and MDR codes. It connects finite geometry with codes.

**Theorem**[25] Let $C$ be a code over an alphabet $A$ with length $n$, minimum distance $d$ and size $k = \log_{|A|}(C)$. Then $d \leq n - k + 1$. Codes meeting this bound are called Maximum Distance Separable (MDS) codes.

**Theorem**[25] A set of $s$ mutually orthogonal Latin squares (MOLS) of order $q$ is equivalent to an $MDS[s+2, \, q^2, \, s+1]$ code over $\mathbb{F}_q$.

The problem of determining when a set of $s$ MOLS exist has been open since 1782. If we consider the algebraic structure of codes over rings, a stronger bound can be made for codes over a principal ideal ring.

**Theorem**[25] Let $C$ be a linear code over a principal ideal ring, then $d(c) \leq n - k + 1$ where $k$ is the rank of the code.

The linear Codes meeting the above bound are called Maximum Distance with respect to Rank (MDR). If a code is MDR (when it is not also MDS), it indicates that the code is
optimal and thus there can be no linear MDS code with the same parameters.

**Open Problem 2**[25] Find and classify all MDS and MDR codes over various classes of alphabets.

**Doubly-even binary codes:** This problem asks whether there exists extremal doubly-even binary self-dual codes of length a multiple of 24. It is a Fermat problem. Many coding theorists have tried to solve it, but failed. The standard techniques do not seem to be able to solve it. If all the weights of a binary self-dual code are congruent to $0$ $(mod$ $4)$ then the code is said to be *Type II*, otherwise *Type I*. Weights of *Type II* codes are doubly-even.

**Open Problem 3**[25] Does there exist a *Type II* [72, 36, 16] code?

Some of the coding theorists have declared monetary prizes for the solution of the above problem. N J A Sloane have offered: $10$ and S T Dougherty have offered $100$ for the existence; M Harada have offered $200$ for the nonexistence. The general conditions for the prizes is that they will be paid only once and the solution must be accepted by the mathematical community.

**Spherical codes:** Coding theory has connection with physics also. The question of distribution of $n$ points on a unit sphere such that they maximize the minimum distance between any pair of points remains open for a long period of time. In this case the maximum distance is called covering radius and the related configuration is called Spherical codes. In the year 1943, a Hungarian Mathematician Fejes Toth proved that for $n$ points there always exist two points whose distance $d$ is

$$d \leq \sqrt{4 - \cos^2 \left( \frac{\pi n}{6(n-2)} \right)}$$  \hspace{1cm} (6.1)

and the limit is exact for $n = 3, 4, 6, 12$

Spherical codes or spherical packing are equivalent to Thomson problem. It states that what will be the position of equilibrium of $n$ electrons if we allow them to move on the surface of a unit sphere and repelling each other by an inverse square law. For two points for maximum distance between them they must be located at the two opposite ends of a diameter. For four points, they should be located at the polyhedron vertices of an inscribed regular tetrahedron. For six points, the solution is an inscribed regular octahedron and for 12 points it is an inscribed regular icosahedron. Still there is no unique best solution for $n = 5$. For eight points, the best solution is not the polyhedron vertices of a cube. For eight points, the best
solution is the vertices of a square antiprism with equal polyhedron edges.

In algebraic coding theory researchers try to find codes that can meet the demand of Noisy-channel coding theorem of Shannon. Robert G Gallager[43] was the first to propose the LDPC (Low-density parity check) codes in the year 1963 in his Doctoral thesis. 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 until its rediscovery in the year 1996. Gallager proposed some encoding and decoding algorithm for LDPC codes. But his algorithms were difficult. This was the reason why these codes remained unknown for more than 30 years after their discovery. As some efficient decoding algorithm was developed for these codes, they became popular. So for every code some efficient decoding and encoding algorithm is necessary. There are so many good codes available in the literature developed by the coding theorists. But nobody has developed efficient encoding and decoding algorithm for these codes. Thus they are not implemented in the practical field. It will be interesting to study some of these codes and try to develop encoding and decoding algorithms for these codes.