T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

FONKSİYON CİSİMLERİ VE KODLAR HAKKINDA

ENGİN ŞENEL

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

Tez Danışmanı: Doç. Dr. FİGEN ÖKE

EDİRNE-2017

T.Ü. Fen Bilimleri Enstitüsü onayı

Prof. Dr. Murat YURTCAN
Fen Bilimleri Enstitüsü Müdürü

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

Prof. Dr. Hülya İŞCAN (V.)
Anabilim Dalı Başkanı

Bu tez tarafımca okunmuş, kapsamı ve niteliği açısından bir Yüksek Lisans tezi olarak kabul edilmiştir.

Doç. Dr. Figen ÖKE
Tez Danışmanı

Bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Matematik Anabilim Dalında bir Yüksek Lisans tezi olarak oy birliği ile kabul edilmiştir.

Jüri Üyeleri	İmza
Prof. Dr. Ahmet Sinan ÇEVİK	
Doç. Dr. Figen ÖKE	
Doç. Dr. Yasemin ÇENGELLENMİŞ	

Tarih: 31/07/2017

T.Ü. FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK YÜKSEK LİSANS PROGRAMI

DOĞRULUK BEYANI

İlgili tezin akademik ve etik kurallara uygun olarak yazıldığını ve kullanılan tüm literatür bilgilerinin kaynak gösterilerek ilgili tezde yer aldığını beyan ederim.



31/07/2017

Engin ŞENEL

Yüksek Lisans Tezi
Fonksiyon Cisimleri ve Kodlar Hakkında
T.Ü. Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

ÖZET

Bu tez dört bölümden oluşmaktadır. İlk bölümde, tezin yazımında kullanılacak olan fonksiyon cismi teorisine cebirsel yaklaşım hakkında bilgi verilmiştir. Kodlama teorisinin tarihsel gelişim süreci hakkında bilgi verildikten sonra, fonksiyon cismi teorisiyle olan ilişkisinden bahsedilmiştir. Son olarak, cebirsel geometrik kodların özellikleri ve kodlama teorisindeki yeri ve öneminden bahsedilmiştir.

İkinci bölümde, cebirsel yaklaşım kullanılarak fonksiyon cismi teorisinin temel kavramları ve teoremleri verilmiştir. Bu bölümde ana amaç Riemann-Roch teoreminin kanıtını vermektir. Ek olarak, cebirsel geometrik kodların inşası için gerekli olan altyapı oluşturulmuştur.

Üçüncü bölümde, kodlama teorisiyle ilgili temel bilgiler verildikten sonra, cebirsel geometrik kodlar incelenmiştir ve parametreleriyle ilgili temel bilgiler verilmiştir. Reed-Solomon, BCH ve "klasik" Goppa kodlarının, cebirsel geometrik kodlar olarak temsil edilebileceği gösterilmiştir. Ardından, kodların asimptotik teorisiyle ilgili temel kavramlar ve sınırlar verildikten sonra asimptotik Tsfasman-Vladut-Zink Sınırı verilmiştir. Son olarak, bir divizörün tabanı kavramı incelenmiştir ve bu kavram yardımıyla cebirsel geometrik kodların tasarlanmış uzaklığı üzerinde elde edilen literatürdeki bir dizi gelişme incelenmiştir.

Yıl : 2017
Sayfa Sayısı : 90
Anahtar Kelimeler : Fonksiyon Cisimleri, Riemann-Roch Teoremi, Cebirsel Geometrik Kodlar, Reed-Solomon Kodları, BCH Kodları, Goppa Kodları, Kodların Asimptotik Teorisi, Cebirsel Geometrik Kodların Minimum Uzaklığı

Master Thesis
Function Fields and Codes
Trakya University Institute of Natural Sciences
Department of Mathematics

ABSTRACT

This thesis consists of four chapters. In the first chapter, information about the algebraic approach to the function field theory to be used in writing the thesis is given. After giving information about the historical development process of coding theory, its relationship with the function field theory is discussed. Finally, the properties of algebraic geometric codes and their place and importance in coding theory are mentioned.

In the second chapter, basic concepts and theorems of function field theory are given using algebraic approach. The main purpose of this chapter is to prove the Riemann-Roch theorem. In addition, the infrastructure necessary for the construction of algebraic geometric codes is established.

In the third chapter, after giving basic information about coding theory, algebraic geometric codes are studied and basic information about their parameters is given. It has been shown that, Reed-Solomon, BCH and "classical" Goppa codes can be represented as algebraic geometric codes. Next, the asymptotic Tsfasman-Vladut-Zink Bound has been given after the basic concepts and bounds related to the asymptotic theory of codes have been given. Finally, the concept of the floor of a divisor is studied and a number of developments on the designed distance of algebraic geometric codes in the literature that obtained with the help of this concept are investigated.

Year : 2017
Number of Pages : 90
Keywords : Function Fields, Riemann-Roch Theorem, Algebraic Geometric Codes, Reed-Solomon Codes, BCH codes, Goppa Codes, Asymptotic Theory of Codes, Minimum Distance of Algebraic Geometric Codes

ÖNSÖZ

Beni bu heyecan verici konuya yönlendirerek ufkumu açan, yardımlarını ve ilgisini esirgemeyen değerli hocam Doç. Dr. Figen Öke'ye en içten saygı ve teşekkürlerimi sunarım.

Engin ŞENEL

İÇİNDEKİLER

ÖZET ..... **i**
ABSTRACT ..... **ii**
ÖNSÖZ ..... **iii**
İÇİNDEKİLER ..... **iv**
SİMGELER DİZİNİ ..... **v**
ŞEKİLLER LİSTESİ ..... **vii**
TABLOLAR LİSTESİ ..... **viii**
1. GİRİŞ **1**
2. FONKSİYON CİSİMLERİ **4**
2.1 Fonksiyon Cisimleri **4**
2.2 Rasyonel Fonksiyon Cismi **10**
2.3 Riemann-Roch Teoremi **12**
2.4 Weil Diferansiyellerinin Yerel Bileşenleri **25**
3. CEBİRSEL GEOMETRİK KODLAR **27**
3.1 Kodlar **27**
3.2 Cebirsel Geometrik Kodlar **29**
3.3 Rasyonel Cebirsel Geometrik Kodlar **38**
3.4 Tsfasman-Vladut-Zink Teoremi **49**
3.5 Cebirsel Geometrik Kodların Minimum Uzaklığı için Taban Sınırları **54**
4. SONUÇLAR VE TARTIŞMA **75**
KAYNAKLAR **76**
ÖZGEÇMİŞ **78**
BİLİMSEL FAALİYETLER **79**

SİMGELER DİZİNİ

$\widetilde{K}$	: $F\ /\ K$ fonksiyon cisminin sabitlerinin cismi
$\mathcal{P}_F$	: $F\ /\ K$ fonksiyon cisminin placelerinin kümesi
$\mathcal{O}_P$	: P place'inin değerlendirme halkası
v_P	: P place'ine karşılık gelen değerlendirme
F_P	: P place'inin rezidü cismi
$x(P)$	: $x \in \mathcal{O}_P$ elemanının modülo P ye göre kalan sınıfı
$degP$	: P place'inin derecesi
$Div(F)$	: $F\ /\ K$ fonksiyon cisminin divizör grubu
$suppD$	: D divizörünün support'u
$degD$	: D divizörünün derecesi
$(x)_0$	: x elemanının kök divizörü
$(x)_\infty$	: x elemanının kutup divizörü
(x)	: x elemanının esas divizörü
$Princ(F)$	: $F\ /\ K$ fonksiyon cisminin esas divizörlerinin grubu
$Cl(F)$	: $F\ /\ K$ fonksiyon cisminin divizör sınıf grubu
$[D]$	: D nin divizör sınıfı
$D_1 \sim D_2$	: Divizörlerin denkliği
$\mathcal{L}(A)$	: A divizörünün Riemann-Roch uzayı
$\ell(A)$	: $\mathcal{L}(A)$ Riemann-Roch uzayının boyutu
g	: $F\ /\ K$ fonksiyon cisminin cinsi
$i(A)$	: A nın özellik indeksi
$\mathcal{A}_F$	: F/K fonksiyon cisminin adele uzayı
Ω_F	: $F\ /\ K$ fonksiyon cisminin Weil diferansiyellerinin uzayı
(ω)	: ω Weil diferansiyelinin divizörü
ω_P	: ω Weil diferansiyelinin yerel bileşeni

$d(a,b)$	: Hamming uzaklığı
$wt(a)$	: $a \in \mathbb{F}_q{}^n$ vektörünün ağırlığı
$d(C)$	: C kodunun minimum uzaklığı
$[n,k,d]$	: Parametreleri n, k, d olan kod
$< a,b >$	: $\mathbb{F}_q{}^n$ üzerindeki doğal iç çarpım
$C^{\perp}$	: C kodunun duali
$C_{\mathcal{L}}(D,G)$	: D ve G divizörleri ile ilişkili bir fonksiyonel cebirsel geometrik kod
$C_{\Omega}(D,G)$	: D ve G divizörleri ile ilişkili bir rezidü cebirsel geometrik kod
$GRS_k(\alpha,v)$	: Genelleştirilmiş Reed-Solomon kodu
$C\|_{\mathbb{F}_q}$	: Alt cisim alt kod
$A(q)$	: Ihara sabiti
$R(C)$	: C kodunun haberleşme oranı
$\delta(C)$	: C kodunun göreceli minimum uzaklığı
$H_q(x)$	: q-entropi fonksiyonu

ŞEKİLLER LİSTESİ

Şekil 3.1 51
Şekil 3.2 54
Şekil 3.3 59
Şekil 3.4 64

TABLOLAR LİSTESİ

Tablo 3.1 74

BÖLÜM 1

GİRİŞ

Fonksiyon cismi teorisine cebirsel ve geometrik olmak üzere iki farklı yaklaşım mevcuttur. Cebirsel yaklaşım, geometrik yaklaşımdan daha elementer olmakla birlikte teorinin temel sonuçlarının daha kolay bir şekilde elde edilmesini sağlamaktadır. Cebirsel yaklaşım belirgin olarak ilk defa R. Dedekind ve H. Weber tarafından [1] de verilmiştir. Bu daha sonra K. Hensel ve G. Landsberg tarafından Theorie der algebraischen Funktionen einer Variabeln (Leipzig, 1902) adlı kitabın yazılmasına ilham vermiştir. Yirminci yüzyılın ilk yarısında bu konu E. Artin, H. Hasse, F. K. Schmidt ve A. Weil tarafından geliştirilmiştir. Günümüzde en fazla kullanılan kaynaklar [2], [3] ve [4] dır.

Bu yaklaşımın diğer bir avantajı, fonksiyon cismi teorisinin kodlama teorisi ile olan ilişkisinin sunumunu kolaylaştırmasıdır.

1948 yılında Claude Shannon tarafından yazılan "A mathematical theory of communication" adlı makalede gürültülü bir iletişim kanalında uygun şifreleme ve deşifreleme teknikleri kullanılırsa sağlıklı bir iletişim kurulabileceğinden bahsedilmiştir. Bu kodlama teorisinin başlangıcı olarak kabul edilir. Kodlama teorisi verilerin bir noktadan diğer bir noktaya aktarımı ve bu aktarım sırasında bozulan verilerin onarılması ile ilgilenir. Bu nedenle kodlama teorisi çoğu uygulamada matematik, bilgisayar bilimi ve mühendisliğin buluşma noktası olmuştur.

Tüm kodlar matematiksel bir yapı kullanılarak oluşturulur. Kodlama teorisi 1940'lı yılların sonunda başladığında kullanılan ana matematiksel teknik lineer cebirdi. Daha sonra halka teorisi kullanıldı, özellikle polinom halkaları ve kesir halkaları teorisi. 1970'li yıllarda V. D. Goppa cebirsel fonksiyon cisimlerinin belli divizörleri ile kodların ilişkilendirilebileceğini göstermiştir [5]. Böylece cebirsel geometrinin bu eski

disipliniyle, kodlama teorisi arasında bir ilişkinin olduğunu göstermiştir. Bu nedenle bu kodlara, cebirsel geometrik kodlar denir. Bu güzel keşif, Reed-Solomon, BCH ve "klasik" Goppa kodlarının olası genelleştirmelerinin uzun seneler düşünülmesi sonucu meydana gelmiştir.

Cebirsel geometrik kodların özellikleri, ilgili fonksiyon cisminin özellikleri ile yakından ilgilidir. Bu da ilgili fonksiyon cismi uygun bir şekilde seçildiğinde çok iyi parametrelere sahip kodların elde edilmesini sağlamaktadır. Cebirsel geometrik kodların diğer bir özelliği de parametreleri hakkında, ünlü Riemann-Roch teoremi yardımıyla bir yorumda bulunulabilmesidir. Tüm fonksiyon cismi teorisi ağırlıklı olarak Riemann-Roch teoremine dayanmaktadır.

Kodların asimptotik teorisi, bir kodun göreceli minimum uzaklığı ve haberleşme oranı arasındaki birleşik ilişkinin doğal limitlerinin belirlenmesi ile ilgilenir. Kodların asimptotik teorisindeki en önemli konulardan biri iyi parametrelere sahip kodların varlığının belirlenmesidir. Asimptotik Gilbert-Varshamov Sınırı 1952'de bulunmuştur. Bu sınır iyi parametrelere sahip kodların varlığını kanıtlamaktadır. Bu keşiften sonraki 30 yıl boyunca bu sınırı geçebilecek herhangi bir kod ailesi bulunamamıştır. Bu nedenle kodlama teorisiyle ilgilenen çoğu bilim insanı bu sınırın geçilemeyeceğini düşünmüştür. 1982 yılında M. A. Tsfasman, S. G. Vladut ve T. Zink tarafından belli cebirsel geometrik kodların bu sınırı geçtiği gösterilmiştir [6]. Cebirsel geometrik kodların birçok ilginç özelliği olsa da önemi bu noktadan sonra anlaşılmıştır ve bu tarihten itibaren kodlama teorisiyle ilgilenen bilim insanları tarafından yoğun olarak çalışılmıştır.

İkinci bölümde fonksiyon cismi teorisine cebirsel yaklaşımda bulunularak temel kavramlar ve teoremler verilecektir. Genel anlamda fonksiyon cisimleri için verilen kavramlar rasyonel fonksiyon cisimleri üzerinde incelenecekdir. Bu bölümdeki temel amaç Riemann-Roch teoremini ve kanıtını vermektir. Daha sonra Rieman-Roch teoreminin sonuçları üzerinde durulacaktır. Bu bölümdeki diğer bir amaç cebirsel geometrik kodların inşasında kullanılacak alt yapıyı hazırlamaktır.

Üçüncü bölümde kodlama teorisi ile ilgili gerekli bilgiler verildikten sonra Reed-Solomon kodları tanıtılacaktır. Reed-Solomon kodları, cebirsel geometrik kodların yapısının anlaşılabilmesi açısından çok önemlidir. Bunun ardından cebirsel geometrik kodlar incelenmiş ve bu kodların paremetreleri üzerindeki temel sınırlar verilmiştir.

Bu aşamadan sonra rasyonel fonksiyon cisimlerinden alınan divizörler ile oluşturulan rasyonel cebirsel geometrik kodlar incelenecektir. Rasyonel fonksiyon cisminin, fonksiyon cisimlerinin en basit örneği olması nedeniyle bu kodlar çok daha somut ve ayrıntılı olarak incelenebilecektir. Burada Reed-Solomon, BCH ve "klasik" Goppa kodlarının, rasyonel cebirsel kod olarak temsil edilebileceği gösterilecektir.

Üçüncü bölümdeki en temel amaçlardan biri de Tsfasman-Vladut-Zink Sınırı ve kanıtını vermektir. Bu amaçla kodların asimptotik teorisi ile ilgili temel kavram ve sınırlar verilmiştir. Daha sonra Tsfasman-Vladut-Zink Sınırının, Gilbert-Varshamov Sınırını geçtiği gösterilmiştir.

Cebirsel geometrik kodların, tasarlanmış uzaklığını geliştirmek için kullanılan başlıca iki yöntem vardır. Üçüncü bölümün son kısmında bu yöntemlerden biri olan taban sınırı incelenecektir. Taban sınırının temeli, farklı divizörlerin Riemann-Roch uzayının aynı olmasına dayanmaktadır. Bu nedenle taban sınırının kanıtında Riemann-Roch teoremi çok önemli bir rol oynamaktadır. Ayrıca yine bu kısımda taban sınırı üzerinde elde edilen bir dizi gelişme verilmiştir. Bu gelişmelerde fonksiyon cismi teorisinin temel tanım ve teoremlerinin yanı sıra, divizörler üzerindeki çeşitli varsayımlar kullanılmıştır.

Bu çalışma boyunca [2] de verilen notasyonlar kullanılacaktır.

BÖLÜM 2

FONKSİYON CİSİMLERİ

Bu bölümde cebirsel fonksiyon cismi teorisinin temel tanımları ve sonuçları üzerinde durulacaktır. Bu bölüm boyunca K herhangi bir cismi gösterecektir.

2.1 Fonksiyon Cisimleri

2.1.1 Tanım: $x \in F$, K cismi üzerinde transandant bir eleman olmak üzere, F, $K(x)$ cisminin sonlu bir cebirsel genişlemesi ise F cismine K cismi üzerinde tek değişkenli bir cebirsel fonksiyon cismi denir. Bu cebirsel fonksiyon cismi $F\ /\ K$ ile gösterilir ve kısaca fonksiyon cismi denir [2].

Cebirsel elemanların toplamları, çarpımları ve tersleri de cebirsel olduğundan $\widetilde{K} = \{z \in F \mid z,\ K$ üzerinde cebirsel bir elemandır $\}$ kümesi F nin bir alt cismidir. $\widetilde{K}$, $F\ /\ K$ nın sabitlerinin cismi olarak isimlendirilir. $K \subseteq \widetilde{K} \subsetneq F$ olmakla beraber $F\ /\ \widetilde{K}$, $\widetilde{K}$ üzerinde bir fonksiyon cismidir. Eğer $\widetilde{K} = K$ ise K, F te cebirsel olarak kapalıdır (veya K, F nin tam sabit cismidir) denir.

2.1.2 Not: $F\ /\ K$ bir fonksiyon cismi ve $z \in F$ olmak üzere, z nin K üzerinde transandant olması için gerekli ve yeterli koşul $F\ /\ K(z)$ genişlemesinin sonlu olmasıdır [2].

2.1.3 Tanım: K üzerinde transandant olan herhangi bir $x \in F$ elemanı için $F = K(x)$ ise $F\ /\ K$ fonksiyon cismine, rasyonel fonksiyon cismi denir [2].

Değerlendirme, place ve ayrık değerlendirme kavramları herhangi bir cisim üzerinde tanımlanabilmesine rağmen bu çalışmada yalnızca fonksiyon cismi üzerinde tanımlanacaktır.

2.1.4 Tanım: $F\ /\ K$ fonksiyon cisminin aşağıdaki özellikleri sağlayan bir $\mathcal{O} \subseteq F$ halkasına değerlendirme halkası denir:

(1) $K \subsetneq \mathcal{O} \subsetneq F$

(2) Her $z \in F$ için $z \in \mathcal{O}$ veya $z^{-1} \in \mathcal{O}$ dir [2].

2.1.5 Örnek: $K(x)\ /\ K$ bir rasyonel fonksiyon cismi olmak üzere, herhangi bir $p(x) \in K[x]$ monik indirgenemez polinomu verilsin. $\mathcal{O}_{p(x)} = \{\frac{f(x)}{g(x)} \mid f(x),\ g(x) \in K[x],\ p(x) \nmid g(x)\}$ kümesi tanımlansın. $\mathcal{O}_{p(x)} \subset K(x)$ olduğu açıktır. Her $\frac{f_1(x)}{g_1(x)},\ \frac{f_2(x)}{g_2(x)} \in \mathcal{O}_{p(x)}$ için $p(x) \nmid g_1(x)$ ve $p(x) \nmid g_2(x)$ olduğundan $p(x) \nmid g_1(x).g_2(x)$ olur. Böylece $\frac{f_1(x)}{g_1(x)} - \frac{f_2(x)}{g_2(x)} = \frac{f_1(x).g_2(x)-f_2(x).g_1(x)}{g_1(x).g_2(x)}$, $\frac{f_1(x)}{g_1(x)}.\frac{f_2(x)}{g_2(x)} = \frac{f_1(x).f_2(x)}{g_1(x).g_2(x)} \in \mathcal{O}_{p(x)}$ olur. Bu da $\mathcal{O}_{p(x)}$ in bir halka olduğunu gösterir. $\mathcal{O}_{p(x)}$ in $K(x)\ /\ K$ rasyonel fonksiyon cisminin bir değerlendirme halkası olduğu gösterilecektir. $x \notin K$ olduğundan $K \subsetneq \mathcal{O}_{p(x)}$ ve $\frac{1}{p(x)} \notin \mathcal{O}_{p(x)}$ olduğundan $\mathcal{O}_{p(x)} \subsetneq K(x)$ olur. Herhangi bir $\frac{f(x)}{g(x)} \in K(x)$ elemanı göz önüne alınsın. $(f(x), g(x)) = 1$ olduğu kabul edilebilir. $\frac{f(x)}{g(x)} \notin \mathcal{O}_{p(x)}$ olsun. Bu durumda $p(x) \mid g(x)$ olacağından en az bir $q(x) \in K[x]$ için $g(x) = p(x).q(x)$ olur. $(f(x), g(x)) = 1$ olduğundan $p(x) \nmid f(x)$ olur. Böylece $(\frac{f(x)}{g(x)})^{-1} = \frac{p(x).q(x)}{f(x)} \in \mathcal{O}_{p(x)}$ olacağından istenen elde edilir [2].

2.1.6 Önerme: $\mathcal{O}$, $F\ /\ K$ fonksiyon cisminin bir değerlendirme halkası olsun. O zaman aşağıdakiler sağlanır:

a) $\mathcal{O}$ bir yerel halkadır. Bu $\mathcal{O}$ değerlendirme halkasının teklikle belirli bir maksimal ideale sahip olması demektir. Gerçekten, $\mathcal{O}$ nun birimsel elemanlarının grubu $\mathcal{O}^x = \{\, z \in \mathcal{O} \mid$ en az bir $w \in \mathcal{O}$ elemanı için $z.w = 1\,\}$ olmak üzere $P = \mathcal{O} \setminus \mathcal{O}^{\times}$, $\mathcal{O}$ nun teklikle belirli maksimal idealidir.

b) Herhangi bir $x \in F$, $x \neq 0$ elemanı göz önüne alınsın. O zaman $x \in P$ olması için gerekli ve yeterli koşul $x^{-1} \notin \mathcal{O}$ olmasıdır.

c) $F\ /\ K$ fonksiyon cisminin sabitlerinin cismi $\widetilde{K}$ olmak üzere $\widetilde{K} \subseteq \mathcal{O}$ ve $\widetilde{K} \cap P = \{0\}$ dır [2].

2.1.7 Teorem: $\mathcal{O}$, $F\ /\ K$ fonksiyon cisminin herhangi bir değerlendirme halkası olsun ve P, $\mathcal{O}$ halkasının tek maksimal idealini göstersin. O zaman aşağıdakiler sağlanır:

a) P, $\mathcal{O}$ nun bir esas idealidir.

b) $P = t.\mathcal{O}$ olmak üzere herhangi bir $z \in F, z \neq 0$ elemanı en az bir $n \in \mathbb{Z}$ ve $u \in \mathcal{O}^{\times}$ için $z = t^n.u$ olacak şekilde teklikle belirli olarak yazılır.

c) $\mathcal{O}$ bir esas ideal bölgesidir. Daha açık olarak, eğer $P = t.\mathcal{O}$ ise herhangi bir $I \subseteq \mathcal{O}, I \neq \{0\}$ ideali için $I = t^n\mathcal{O}$ olacak şekilde en az bir $n \in \mathbb{N}$ elemanı vardır [2].

2.1.7 Teorem'deki özellikleri sağlayan bir halkaya ayrık değerlendirme halkası denir.

2.1.8 Tanım: $F\ /\ K$ fonksiyon cisminin herhangi bir $\mathcal{O}$ değerlendirme halkasının tek maksimal ideali P ye $F\ /\ K$ fonksiyon cisminin bir place'i denir. $F\ /\ K$ fonksiyon cisminin bütün placelerinin kümesi $\mathcal{P}_F$ ile gösterilecektir. $P = t.\mathcal{O}$ olacak şekildeki her $t \in P$ elemanına P place'i için bir asal eleman denir [2].

$\mathcal{O}$, $F\ /\ K$ fonksiyon cisminin herhangi bir değerlendirme halkası olsun ve P, $\mathcal{O}$ halkasının tek maksimal idealini göstersin. 2.1.6 Önerme b) gereğince $\mathcal{O} = \{\, z \in F \mid z^{-1} \notin P\}$ olduğundan $\mathcal{O}$, P tarafından teklikle belirlidir. Bu nedenle $F\ /\ K$ fonksiyon cisminin bir P place'i verildiğinde bu place'e karşılık gelen değerlendirme halkası $\mathcal{O}_P$ ile gösterilecektir.

2.1.9 Tanım: Aşağıdaki koşulları sağlayan bir $v: F \longrightarrow \mathbb{Z} \cup \{\infty\}$ fonksiyonuna $F\ /\ K$ fonksiyon cisminin bir ayrık değerlendirmesi denir [2].

(1) $v(x) = \infty \Leftrightarrow x = 0$

(2) Her $x, y \in F$ için $v(x.y) = v(x) + v(y)$

(3) Her $x, y \in F$ için $v(x + y) \geq min\{v(x), v(y)\}$

(4) En az bir $z \in F$ için $v(z) = 1$

(5) Her $a \in K, a \neq 0$ için $v(a) = 0$

Burada ∞ sembolü her $n, m \in \mathbb{Z}$ için $\infty + \infty = \infty + n = n + \infty = \infty$ ve $\infty > m$ olmak üzere $\mathbb{Z}$ de olmayan bir elemanı göstermektedir. (2) ve (4) ten v fonksiyonunun örten olduğu görülmektedir. (3) özelliğine üçgen eşitsizliği denir.

2.1.10 Lemma: v, $F\ /\ K$ fonksiyon cisminin herhangi bir ayrık değerlendirmesi olsun. O zaman herhangi $x, y \in F$ elemanları için $v(x) \neq v(y)$ ise $v(x+y) = \min\{v(x), v(y)\}$ olur [2].

2.1.11 Tanım: 2.1.7 Teorem b) den herhangi bir $P \in \mathcal{P}_F$ place'i için $P = t.\mathcal{O}_P$ olmak üzere, herhangi bir $z \in F$, $z \neq 0$ elemanının en az bir $n \in \mathbb{Z}$ ve $u \in {\mathcal{O}_P}^{\times}$ için $z = t^n.u$ şeklinde teklikle belirli olarak yazıldığı biliniyor. Böylece $F\ /\ K$ fonksiyon cisminin P place'ine karşılık $v_p: F \longrightarrow \mathbb{Z} \cup \{\infty\}$, $v_p(0) = \infty$, $z \neq 0$ olmak üzere $z \in F$ için $v_p(z) = n$ olacak şekilde bir fonksiyon tanımlıdır. Bu fonksiyon bir ayrık değerlendirmedir ve P place'ine karşılık gelen ayrık değerlendirme olarak isimlendirilecektir [2].

Bu fonksiyonun sadece P place'inin seçimine bağlı olduğu görülecektir. t', P place'i için başka bir asal eleman olsun. Böylece $P = t.\mathcal{O}_P = t'\mathcal{O}_P$ olur. O halde en az bir $w \in \mathcal{O}_P^{\times}$ elemanı için $t = t'.w$ olur. Bu nedenle $w^n.u \in \mathcal{O}_P^{\times}$ olmak üzere $z = t^n.u = (t'.w)^n.u = (t')^n.w^n.u$ olarak yazılabileceğinden istenen elde edilir.

2.1.12 Teorem: $F\ /\ K$ bir fonksiyon cismi olsun.

a) Herhangi bir $P \in \mathcal{P}_F$ place'i için $\mathcal{O}_P$, $\mathcal{O}_P^{\times}$, P aşağıdaki gibi yazılabilir:

$\mathcal{O}_P = \{\, z \in F \mid v_p(z) \geq 0\}$

$\mathcal{O}_P^{\times} = \{\, z \in F \mid v_p(z) = 0\}$

$P = \{\, z \in F \mid v_p(z) > 0\}$

b) Herhangi bir $x \in F$ elemanı göz önüne alınsın. x elemanının P place'inin bir asal elemanı olması için gerek ve yeter koşul $v_p(x) = 1$ olmasıdır.

c) v, $F\ /\ K$ fonksiyon cisminin bir ayrık değerlendirmesi olsun. O zaman $P = \{\, z \in F \mid v(z) > 0\,\}$ kümesi $F\ /\ K$ fonksiyon cisminin bir place'i dir ve $\mathcal{O}_P = \{\, z \in F \mid v(z) \geq 0\}$ olur.

d) $F\ /\ K$ fonksiyon cisminin her değerlendirme halkası $\mathcal{O}$, F nin öz maksimal alt halkasıdır [2].

P, $F\ /\ K$ fonksiyon cisminin bir place'i ve $\mathcal{O}_P$ bu place'e karşılık gelen değerlendirme halkası olsun. P maksimal ideal ve $\mathcal{O}_P$ değişmeli ve birimli bir halka olduğundan $\mathcal{O}_P\ /\ P$ kesir halkası bir cisimdir. Herhangi bir $x \in \mathcal{O}_P$ elemanı için x in modülo P ye göre kalan sınıfı $x(P)$ ile gösterilsin. 2.1.6 Önerme c) den $K \subsetneq \mathcal{O}$ ve $K \cap P = \{0\}$ olduğu biliniyor. $\varphi: K \longrightarrow \mathcal{O}_P\ /\ P$, $\varphi(x) = x(P)$ şeklinde bir dönüşüm tanımlansın. φ dönüşümü iyi tanımlı, kapalı ve bir homomorfizmadır.

φ dönüşümünün birebir olduğu gösterilecektir. Herhangi $x_1, x_2 \in K$ elemanları için $\varphi(x_1) = \varphi(x_2)$ olsun. Bu sebeple $x_1(P) = x_2(P)$ olacağından $x_1 - x_2 \in P$ dir. $x_1 - x_2 \in K$ olduğu da göz önünde bulundurulursa $K \cap P = \{0\}$ olduğundan $x_1 = x_2$ elde edilir. O halde φ dönüşümü birebirdir.

Sonuç olarak φ dönüşümünün bir doğal gömme dönüşümü olduğu görülür. Bu doğal gömme dönüşümü yardımıyla K, $\mathcal{O}_P\ /\ P$ cisminin bir alt cismi olarak düşünülecektir. Benzer şekilde $\widetilde{K}$ cismi de $\mathcal{O}_P\ /\ P$ cisminin bir alt cismi olarak düşünülebilir.

2.1.13 Tanım: Herhangi bir $P \in \mathcal{P}_F$ place'i göz önüne alınsın.

a) $F_P = \mathcal{O}_P\ /\ P$ cismine P place'inin rezüdü cismi denilir. $\varphi: F \longrightarrow F_P \cup \{\infty\}$, $x \in \mathcal{O}_P$ için $\varphi(x) = x(P)$ ve $x \in F \setminus \mathcal{O}_P$ için $\varphi(x) = \infty$ şeklinde tanımlı dönüşüme P place'ine göre rezüdü dönüşümü denir (Burada ∞ sembolü yine 2.1.9 Tanım'da olduğu gibi farklı bir anlamda kullanılmıştır). Herhangi bir $x \in \mathcal{O}_P$ elemanı için bazen $x + P = x(P)$ notasyonu kullanılacaktır.

b) $[F_P: K]$ genişlemesinin derecesine P place'inin derecesi denir ve $degP$ ile gösterilir. $F\ /\ K$ fonksiyon cisminin derecesi bir olan herhangi bir place'ine rasyonel place denir [2].

2.1.14 Önerme: P, $F\ /\ K$ fonksiyon cisminin herhangi bir place'i olsun. O zaman herhangi bir $x \in P$, $x \neq 0$ elemanı için $degP \leq [F: K(x)] < \infty$ olur [2].

2.1.15 Sonuç: $F\ /\ K$ fonksiyon cisminin sabitlerinin cismi $\widetilde{K}$, K cisminin sonlu bir cisim genişlemesidir [2].

2.1.16 Not: $F\ /\ K$ fonksiyon cisminin herhangi bir P rasyonel place'i göz önüne alınsın. Bu durumda $[F_P: K] = degP = 1$ olacağından P place'ine göre rezüdü dönüşümü F kümesinden $K \cup \{\infty\}$ kümesine tanımlanmış olur. $[F_P: K] < \infty$ olduğundan $F_P\ /\ K$ bir cebirsel cisim genişlemesidir. Bu sebeple K cebirsel olarak kapalı bir cisimse $F\ /\ K$ fonksiyon cisminin her place'i bir rasyonel placedir. Böylece herhangi bir $z \in F$ elemanı,

$$z: \mathcal{P}_F \to K \cup \{\infty\}, P \longmapsto z(P) \tag{2.1}$$

şeklinde bir fonksiyon olarak düşünülebilir. Bu nedenle $F\ /\ K$ fonksiyon cismi olarak isimlendirilir. K cisminin elemanları (2.1) anlamında sabit fonksiyon olduğundan K, F nin sabit cismi olarak isimlendirilir [2].

2.1.17 Tanım: Herhangi bir $z \in F$ elemanı ve $P \in \mathcal{P}_F$ place'i göz önüne alınsın. Eğer $v_p(z) > 0$ ise P place'ine z elemanının bir kökü, $v_p(z) < 0$ ise P place'ine z elemanının bir kutbu denir [2].

2.1.18 Teorem: $F\ /\ K$ bir fonksiyon cismi ve R, F cisminin $K \subseteq R \subseteq F$ olacak şekilde bir alt halkası olsun. $I \subsetneq R, I \neq \{0\}$ kümesinin R halkasının herhangi bir öz ideali olduğu varsayılsın. O zaman $I \subseteq P$ ve $R \subseteq \mathcal{O}_P$ olacak şekilde en az bir $P \in \mathcal{P}_F$ place'i vardır [2].

2.1.19 Sonuç: $F\ /\ K$ bir fonksiyon cismi ve $z \in F$, K cismi üzerinde transandant bir eleman olsun. O zaman $z \in F$ elemanı en az bir köke ve kutba sahiptir. Özel olarak $\mathcal{P}_F \neq \emptyset$ dır [2].

2.1.20 Sonuç sayesinde (2.1) anlamında $F\ /\ K$ fonksiyon cisminin sabit cismi $\widetilde{K}$ da olmayan her $z \in F$ elemanı sabit olmayan bir fonksiyon olarak yorumlanabilir.

2.1.20 Teorem (Zayıf Yaklaşım Teoremi): $F\ /\ K$ bir fonksiyon cismi ve $P_1, P_2 \ldots, P_n \in \mathcal{P}_F$, $F\ /\ K$ fonksiyon cisminin ikişer ikişer birbirinden farklı placeleri olsun. O zaman $x_1, x_2 \ldots, x_n \in F$ ve $r_1, r_2 \ldots, r_n \in \mathbb{Z}$ olmak üzere her $i \in \{1,2, \ldots, n\}$ için $v_{P_i}(x - x_i) = r_i$ olacak şekilde en az bir $x \in F$ elemanı vardır [2].

2.1.21 Sonuç: Her fonksiyon cismi sonsuz tane place'e sahiptir [2].

2.1.22 Sonuç: $F\ /\ K$ bir fonksiyon cismi olsun. O zaman her $x \in F$, $x \neq 0$ elemanı sonlu sayıda köke ve kutba sahiptir [2].

2.2 Rasyonel Fonksiyon Cismi

K üzerinde transandant olan herhangi bir $x \in F$ elemanı için $F = K(x)$ olmak üzere $F \,/\, K$ rasyonel fonksiyon cismi göz önüne alınsın. Bu kısımda fonksiyon cismi üzerinde tanımlanan kavramlar rasyonel fonksiyon cismi üzerinde incelenecektir.

Herhangi bir $p(x) \in K[x]$ monik indirgenemez polinomu için,

$$\mathcal{O}_{p(x)} = \{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \nmid g(x) \} \tag{2.2}$$

kümesi $F \,/\, K$ rasyonel fonksiyon cisminin bir değerlendirme halkasıdır. Bu değerlendirme halkasının tek maksimal ideali,

$$P_{p(x)} = \{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \nmid g(x) \} \tag{2.3}$$

kümesidir [2].

Herhangi bir $\alpha \in K$ elemanı için $p(x) = x - \alpha$ şeklinde ise $P_\alpha = P_{x-\alpha} \in \mathcal{P}_F$ notasyonu kullanılacaktır.

$F \,/\, K$ rasyonel fonksiyon cisminin diğer bir değerlendirme halkası,

$$\mathcal{O}_\infty = \{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) \leq deg g(x) \} \tag{2.4}$$

kümesidir. Bu değerlendirme halkasının tek maksimal ideali,

$$P_\infty = \{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], \deg f(x) < deg g(x) \} \tag{2.5}$$

kümesidir. Bu place'e $F \,/\, K$ rasyonel fonksiyon cisminin sonsuzdaki place'i denir [2].

2.2.1 Önerme: $K(x) \,/\, K$ bir rasyonel fonksiyon cismi olsun. Herhangi bir $p(x) \in K[x]$ monik indirgenemez polinomu için (2.3) de tanımlanan $P_{p(x)} \in \mathcal{P}_{K(x)}$ place'i göz önüne alınsın. O zaman $p(x)$ polinomu $P_{p(x)}$ place'inin bir asal elemanıdır. Böylece herhangi bir $z \in K(x) \setminus \{0\}$ elemanı en az $n \in \mathbb{Z}$, $f(x), g(x) \in K[x]$ elemanları için $p(x) \nmid f(x)$ ve $p(x) \nmid g(x)$ olmak üzere $z = p(x)^n . (f(x) \,/\, g(x))$ şeklinde yazılabilir ve $v_{P_{p(x)}}(z) = n$ olur. Üstelik $K(x)_{P_{p(x)}} = \mathcal{O}_{P_{p(x)}} \,/\, P_{p(x)}$ olmak üzere,

$$\phi : K[x] \,/\, (p(x)) \longrightarrow K(x)_{P_{p(x)}}, f(x) + (p(x)) \longmapsto f(x)(P_{p(x)}) \tag{2.6}$$

şeklinde tanımlı dönüşüm bir izomorfizmadır. Sonuç olarak $degP_{p(x)} = degp(x)$ olur [2].

2.2.2 Önerme: $K(x)\ /\ K$ bir rasyonel fonksiyon cismi olsun. Özel olarak en az bir $\alpha \in K$ elemanı için $p(x) = x - \alpha$ şeklinde ise $degP_{p(x)} = degp(x) = 1$ olur. O zaman $P_{p(x)}$ place'ine göre rezidü dönüşümü,

$$\varphi: K(x) \longrightarrow K \cup \{\infty\},\ z(x) \longmapsto z(\alpha) \tag{2.7}$$

şeklindedir. Burada $z(\alpha)$ şu şekilde tanımlıdır: $z(x) \in K(x)$ olduğundan $z(x) = \frac{f(x)}{g(x)}$ ve $(f(x), g(x)) = 1$ olacak şekilde en az $f(x),\ g(x) \in K[x]$ polinomları olduğu göz önünde bulundurulursa,

$$z(\alpha) = \begin{cases} \frac{f(\alpha)}{g(\alpha)} & , g(\alpha) \neq 0 \\ \infty & , g(\alpha) = 0 \end{cases} \tag{2.8}$$

şeklinde olur [2].

2.2.3 Önerme: $K(x)\ /\ K$ bir rasyonel fonksiyon cismi olmak üzere (2.5) da verilen P_∞ place'i göz önüne alınsın. $degP_\infty = 1$ dir. $t = \frac{1}{x} \in P_\infty$ elemanı P_∞ place'i için bir asal elemandır. P_∞ place'ine karşılık gelen ayrık değerlendirme $f(x),\ g(x) \in K[x]$ olmak üzere $v_{P_\infty}\left(\frac{f(x)}{g(x)}\right) = degg(x) - degf(x)$ şeklinde tanımlıdır. P_∞ place'ine göre rezüdü dönüşümü,

$$\varphi: K(x) \longrightarrow K \cup \{\infty\},\ z(x) \longmapsto z(x)(P_\infty) = z(\infty) \tag{2.9}$$

şeklindedir. Burada $z(\infty)$ şu şekilde tanımlıdır: $z(x) \in K(x)$ olduğundan en az $a_n,\ b_m \in K,\ a_n,\ b_m \neq 0$ elemanları için $z(x) = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0}$ şeklindedir. Bu durum göz önünde bulundurulursa,

$$z(\infty) = \begin{cases} \frac{a_n}{b_m} & , n = m \\ 0 & , n < m \\ \infty & , n > m \end{cases} \tag{2.10}$$

şeklinde olur [2].

2.2.4 Önerme: $K(x)\ /\ K$ bir rasyonel fonksiyon cismi olsun. K cismi, $K(x)\ /\ K$ rasyonel fonksiyon cisminin tam sabit cismidir [2].

2.2.5 Önerme: $K(x)\ /\ K$ rasyonel fonksiyon cisminin sırasıyla (2.3) ve (2.5) da tanımlanan $P_{p(x)}$ ve P_∞ place'inden başka bir place'i yoktur [2].

2.3 Riemann-Roch Teoremi

$F\ /\ K$ bir fonksiyon cismi olsun. 2.1.15 Sonuçtan $F\ /\ K$ fonksiyon cisminin sabitlerinin cismi $\widetilde{K}$, K cisminin sonlu bir cisim genişlemesidir. Bu nedenle F, $\widetilde{K}$ cismi üzerinde bir fonksiyon cismi olarak düşünülebilir. Böylece $F\ /\ K$ fonksiyon cisminin, sabitlerinin cismi K olan tek değişkenli bir fonksiyon cismi olarak kabul edilmesi teorik açıdan bir sorun teşkil etmeyecektir. Bu kısımdan itibaren bu varsayım kabul edilecektir.

2.3.1 Tanım: $F\ /\ K$ fonksiyon cisminin divizör grubu $F\ /\ K$ fonksiyon cisminin placeleri tarafından üretilen toplamsal olarak yazılmış serbest abelian grup olarak tanımlanır ve $Div(F)$ ile gösterilir. $Div(F)$ grubunun elemanlarına $F\ /\ K$ fonksiyon cisminin divizörleri denir. Herhangi bir $D \in Div(F)$ divizörü $n_P \in \mathbb{Z}$ ve hemen hemen her $n_P = 0$ olmak üzere $D = \sum_{P\in\mathcal{P}_F} n_P.P$ olarak tanımlanır. Herhangi bir $P \in \mathcal{P}_F$ place'i için $D = P$ şeklindeki bir divizöre asal divizör denir [2].

2.3.2 Tanım: Herhangi bir $D \in Div(F)$ divizörü için $suppD = \{\, P \in \mathcal{P}_F \mid n_P \neq 0 \,\}$ şeklinde tanımlanan kümeye D divizörünün support'u denir. Genelde D, $suppD \subseteq S$ olacak şekildeki sonlu bir alt küme $S \subseteq \mathcal{P}_F$ olmak üzere $D = \sum_{P\in S} n_P.P$ şeklinde gösterilecektir [2].

İki divizörün toplamı; $D_1 = \sum_{P\in\mathcal{P}_F} n_P.P$ ve $D_2 = \sum_{P\in\mathcal{P}_F} m_P.P$ olmak üzere $D_1 + D_2 = \sum_{P\in\mathcal{P}_F}(n_P + m_P).P$ şeklindedir.

$Div(F)$ divizör grubunun sıfır elemanı her $P \in \mathcal{P}_F$ için $r_P = 0$ olmak üzere $0 = \sum_{P\in\mathcal{P}_F} r_P.P$ şeklinde tanımlıdır.

Herhangi bir $Q \in \mathcal{P}_F$ place'i için $D = \sum_{P\in S} n_P.P \in Div(F)$ olmak üzere $v_Q : Div(F) \longrightarrow \mathbb{Z}$, $v_Q(D) = n_Q$ şeklinde tanımlı fonksiyon göz önüne alınsın. Böylece

$suppD = \{ P \in \mathcal{P}_F \mid v_P(D) \neq 0 \}$ ve $D = \sum_{P \in suppD} v_P(D).P \in Div(F)$ şeklinde yazılabilir.

$Div(F)$ kümesi üzerinde aşağıdaki gibi bir kısmi sıralama bağıntısı tanımlıdır:

$D_1 \leq D_2 \Leftrightarrow$ her $P \in \mathcal{P}_F$ place'i için $v_P(D_1) \leq v_P(D_2)$ (2.11)

$D_1 \leq D_2$ ve $D_1 \neq D_2$ olduğunda $D_1 < D_2$ yazılacaktır. $D \geq 0$ ise D divizörü pozitif veya efektif olarak isimlendirilir.

2.3.3 Tanım: Herhangi bir $D \in Div(F)$ divizörü göz önüne alınsın. $degD = \sum_{P \in \mathcal{P}_F} v_P(D).degP$ tam sayısına D divizörünün derecesi denir. Böylece $deg: Div(F) \longrightarrow \mathbb{Z}$, $D \mapsto degD$ şeklinde bir homomorfizma tanımlıdır [2].

F / K bir fonksiyon cismi olmak üzere herhangi bir $x \in F$, $x \neq 0$ elemanının 2.1.22 Sonuç gereğince sonlu sayıda köke ve kutba sahip olduğu biliniyor. Bu sebeple aşağıdaki tanım verilebilir.

2.3.4 Tanım: Herhangi bir $x \in F$, $x \neq 0$ elemanının köklerinin kümesi $\mathcal{Z}$ ve kutuplarının kümesi $\mathcal{N}$ olmak üzere,

$(x)_0 = \sum_{P \in \mathcal{Z}} v_P(x).P$, x elemanının kök divizörü (2.12)

$(x)_\infty = \sum_{P \in \mathcal{N}} (-v_P(x)).P$, x elemanının kutup divizörü (2.13)

$(x) = (x)_0 - (x)_\infty$, x elemanının esas divizörü (2.14)

olarak tanımlanır [2].

Tanımları gereğince $(x)_0 \geq 0$, $(x)_\infty \geq 0$ ve $(x) = \sum_{P \in \mathcal{P}_F} v_P(x).P$ olur.

2.3.5 Teorem: F / K bir fonksiyon cismi olmak üzere herhangi bir $x \in F$, $x \neq 0$ elemanının K cisminin elemanı olması için gerekli ve yeterli koşul $(x) = 0$ olmasıdır [2].

2.3.6 Tanım: $Princ(F) = \{ (x) \mid x \in F$ ve $x \neq 0 \}$ kümesi F / K fonksiyon cisminin esas divizörlerinin grubu olarak isimlendirilir [2].

$1 \in F$ olduğundan $(1) \in Princ(F)$ olur. Böylece $Princ(F) \neq \emptyset$ dir. Herhangi (x), $(y) \in Princ(F)$ elemanları için $x.y^{-1} \in F$ olup $(x) - (y) = (x.y^{-1}) \in Princ(F)$ olur. Böylece $Princ(F)$, $Div(F)$ grubunun bir alt grubudur. $Div(F)$ bir abelyan grup

olduğundan her alt grubu normal alt gruptur. Böylece $Cl(F) = Div(F) \,/\, Princ(F)$ bölüm grubu tanımlıdır.

2.3.7 Tanım: $Cl(F)$ grubuna $F \,/\, K$ fonksiyon cisminin divizör sınıfları grubu denir. Herhangi bir $D \in Div(F)$ divizörüne $Cl(F)$ divizör sınıfları grubunda karşılık gelen elemana D nin divizör sınıfı denir ve ve $[D]$ ile gösterilir. Herhangi iki D_1, $D_2 \in Div(F)$ divizörü için $[D_1] = [D_2]$ oluyorsa bu divizörler denktir denir ve bu durum $D_1 \sim D_2$ ile gösterilir. Ayrıca bu bir denklik bağıntısıdır [2].

2.3.8 Tanım: Herhangi bir $A \in Div(F)$ divizörü için,

$$\mathcal{L}(A) = \{\, x \in F \mid (x) \geq -A \,\} \cup \{\, 0 \,\} \tag{2.15}$$

şeklinde tanımlanan kümeye A divizörünün Riemann-Roch uzayı denir [2].

Herhangi bir $x \in F$ verildiğinde $x \in \mathcal{L}(A)$ olması için gerekli ve yeterli koşulun her $P \in \mathcal{P}_F$ place'i için $v_P(x) \geq -v_P(A)$ olması olduğuna dikkat edilmelidir.

2.3.9 Teorem: Herhangi bir $A \in Div(F)$ divizörü göz önüne alınsın. $\mathcal{L}(A) \neq \{\, 0 \,\}$ olması için gerekli ve yeterli koşul $B \sim A$ ve $B \geq 0$ olacak şekilde en az bir $B \in Div(F)$ divizörünün var olmasıdır [2].

2.3.10 Lemma: Herhangi bir $A \in Div(F)$ divizörü göz önüne alınsın. O zaman,

a) $\mathcal{L}(A)$, K üzerinde bir vektör uzayıdır.

b) Herhangi bir $B \in Div(F)$ divizörü için $B \sim A$ ise $\mathcal{L}(B) \simeq \mathcal{L}(A)$ olur [2].

2.3.11 Lemma:

a) $\mathcal{L}(0) = K$ dır.

b) Herhangi bir $A \in Div(F)$ divizör için $A < 0$ ise $\mathcal{L}(A) = \{0\}$ olur [2].

V, K üzerinde herhangi bir vektör uzayı ise boyutu $dimV$ ile gösterilecektir. Şimdi herhangi bir $A \in Div(F)$ divizörü için $\mathcal{L}(A)$ nın K cismi üzerinde sonlu bir vektör uzayı olduğu gösterilecektir.

2.3.12 Lemma: A, $B \in Div(F)$, $F \,/\, K$ fonksiyon cisminin herhangi iki divizörü olsun. $A \leq B$ ise $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ ve $\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq degB - degA$ dır [2].

2.3.13 Önerme: Herhangi bir $A \in Div(F)$ divizörü için A_+ ve A_- pozitif divizörler olmak üzere $A = A_+ - A_-$ ise $dim\mathcal{L}(A) \leq degA_+ + 1$ olur. Böylece $\mathcal{L}(A)$, K cismi üzerinde sonlu boyutlu bir vektör uzayı olur [2].

2.3.14 Tanım: Herhangi bir $A \in Div(F)$ divizörü için $\ell(A) = dim\mathcal{L}(A)$ tam sayısına A divizörünün boyutu denir [2].

Cebirsel fonksiyon cismi teorisindeki en önemli problemlerden birisi bir divizörün boyutunun hesaplanmasıdır. Bu kısımdan sonra bu problemle ilgilenilecektir.

2.3.15 Önerme: Herhangi bir $F\ /\ K$ fonksiyon cismi göz önüne alınsın. Herhangi bir $x \in F \setminus K$ elemanı için $(x)_0$, x elemanının kök divizörü ve $(x)_\infty$, x elemanının kutup divizörü olmak üzere $deg(x)_0 = deg(x)_\infty = [F:K(x)]$ olur. Bu nedenle tüm esas divizörlerin derecesi sıfırdır [2].

2.3.15 Önerme gereğince herhangi bir $x \in F$, $x \neq 0$ elemanının kök ve kutup sayıları birbirine eşittir.

2.3.16 Sonuç: Herhangi iki A, $B \in Div(F)$ divizör için $A \sim B$ olsun. O zaman $\ell(A) = \ell(B)$ ve $degA = degB$ olur [2].

2.3.17 Sonuç: Herhangi bir $A \in Div(F)$ divizörü için $degA < 0$ ise $\ell(A) = 0$ dır [2].

2.3.18 Sonuç: Herhangi bir $A \in Div(F)$ divizörü için $degA = 0$ olsun. Bu durumda aşağıdaki ifadeler denktir [2].

(1) A esas divizördür.

(2) $\ell(A) \geq 1$

(3) $\ell(A) = 1$

Herhangi bir $F\ /\ K$ fonksiyon cismi göz önüne alınsın. $A \geq 0$ olacak şekildeki herhangi bir $A \in Div(F)$ divizörü için 2.3.13 Önerme gereğince $\ell(A) \leq degA + 1$ olduğu biliniyor. Şimdi bu eşitsizliğin derecesi sıfırdan büyük olan herhangi bir divizör için de gerçeklendiği gösterilecektir.

2.3.19 Önerme: Herhangi bir $A \in Div(F)$ divizörü için $degA \geq 0$ ise $\ell(A) \leq degA + 1$ dir [2].

Şimdi herhangi bir $A \in Div(F)$ divizörü verildiğinde $\ell(A)$ için bir alt sınırın var olduğu gösterilecektir.

2.3.20 Önerme: Herhangi bir $F\ /\ K$ fonksiyon cismi göz önüne alınsın. Her $A \in Div(F)$ divizörü için $degA - \ell(A) \leq \gamma$ olacak şekilde yalnızca $F\ /\ K$ fonksiyon cismine bağlı olan en az bir γ tam sayısı vardır [2].

Bu önerme sayesinde sıradaki tanım anlamlı olacaktır.

2.3.21 Önerme: Herhangi bir $F\ /\ K$ fonksiyon cismi göz önüne alınsın.

$$g = \max\{\, degA - \ell(A) + 1 \mid A \in Div(F) \,\} \tag{2.16}$$

tamsayısına $F\ /\ K$ fonksiyon cisminin cinsi denir. Cins bir fonksiyon cisminin en önemli değişmezidir [2].

2.3.22 Teorem: Herhangi bir $F\ /\ K$ fonksiyon cisminin cinsi $g \geq 0$ olacak şekilde bir tamsayıdır [2].

2.3.23 Teorem (Riemann Teoremi): $F\ /\ K$ bir fonksiyon cismi ve bu fonksiyon cisminin cinsi g olsun. O zaman,

a) Her $A \in Div(F)$ divizörü için $\ell(A) \geq degA + 1 - g$ dir.

b) Herhangi bir $A \in Div(F)$ divizörü için $degA \geq c$ olduğunda $\ell(A) = degA + 1 - g$ olacak şekilde yalnızca $F\ /\ K$ fonksiyon cismine bağlı bir c tamsayısı vardır [2].

2.3.24 Örnek: $K(x)\ /\ K$ rasyonel fonksiyon cisminin cinsinin sıfır olduğu gösterilecektir. x elemanının tek kutbu P_∞ place'i olduğundan,

$$(x)_\infty = -v_{P_\infty}(x).P_\infty = v_{P_\infty}\left(\frac{1}{x}\right).P_\infty = P_\infty \tag{2.17}$$

bulunur. Herhangi bir $r \geq 0$ tamsayısı için $\mathcal{L}(r.P_\infty)$ Riemann-Roch uzayı göz önüne alınsın. $\mathcal{L}(r.P_\infty)$ nın tanımından dolayı $1, x, x^2, \dots, x^r \in \mathcal{L}(r.P_\infty)$ olur. Bu elemanların K

cismi üzerinde lineer bağımsız olduğuna dikkat edilirse 2.3.23 Teorem b) gereğince yeteri kadar büyük bir $r \geq 0$ tamsayısı için,

$$r + 1 \leq \ell(r.P_\infty) = deg(r.P_\infty) + 1 - g = r + 1 - g \tag{2.18}$$

elde edilir. Böylece $g \leq 0$ bulunur. 2.3.22 Teorem gereğince $g \geq 0$ olduğundan $g = 0$ bulunur. Dolayısıyla istenilen elde edilmiş olur [2].

Genel olarak bir fonksiyon cisminin cinsini belirlemek zordur. Bu kısımda bu konu ile ilgilenilecektir.

2.3.25 Tanım: $F\ /\ K$ fonksiyon cisminin cinsi g olmak üzere herhangi bir $A \in Div(F)$ divizörü için $i(A) = \ell(A) - degA + g - 1$ tamsayısına A nın özellik indeksi denir [2].

2.3.23 Teorem a) gereğince $i(A)$ tamsayısı negatif değildir. Yine 2.3.23 Teorem b) gereğince $degA$ yeterince büyük olacak şekildeki bir $A \in Div(F)$ divizörü için $i(A) = 0$ dır.

Şimdiki bölümde belli vektör uzaylarının boyutu olarak $i(A)$ hakkında birkaç yorumda bulunulacaktır.

2.3.26 Tanım: $F\ /\ K$ herhangi bir fonksiyon cismi olsun. Hemen hemen her $P \in \mathcal{P}_F$ place'i için $\alpha_P \in \mathcal{O}_P$ olmak üzere $\alpha: \mathcal{P}_F \longrightarrow F$, $P \mapsto \alpha_P$ şeklindeki bir dönüşüme adele denir [2].

Bir adele $\prod_{P \in \mathcal{P}_F} F$ direk çarpımının bir elemanı olarak düşünülebilir. Bu nedenle $\alpha = (\alpha_P)_{P \in \mathcal{P}_F}$ notasyonu kullanılabilir veya daha kısa olarak $\alpha = (\alpha_P)$ yazılabilir.

2.3.27 Tanım: $\mathcal{A}_F = \{\, \alpha \mid \alpha,\ F/K$ fonksiyon cisminin bir adele'idir $\}$ kümesine F/K nın adele uzayı denir. $\mathcal{A}_F$, K üzerinde bir vektör uzayı olarak düşünülebilir [2].

F/K bir fonksiyon cismi olmak üzere herhangi bir $x \in F$ elemanının 2.1.22 Sonuç gereğince sonlu sayıda kutbu olduğundan sıradaki tanım anlamlıdır.

2.3.28 Tanım: F/K bir fonksiyon cismi olmak üzere herhangi bir $x \in F$ elemanı göz önüne alınsın. Tüm bileşenleri x elemanına eşit olan adele'e x elemanının esas adele'i denir [2].

2.3.28 Tanım yardımıyla $F \longrightarrow \mathcal{A}_F$ şeklinde bir gömme dönüşümü tanımlanabilir. Böylece F/K fonksiyon cisminin ayrık değerlendirmeleri herhangi bir $\alpha \in \mathcal{A}_F$ için $v_P(\alpha) = v_P(\alpha_P)$ alınarak $\mathcal{A}_F$ ye genişletilebilir. Burada α_P, α adele'inin P inci bileşenidir. α adele'inin tanımından dolayı sonlu sayıdaki eleman hariç her $P \in \mathcal{P}_F$ elemanı için $v_P(\alpha) \geq 0$ olur.

2.3.29 Tanım: Herhangi bir $A \in Div(F)$ divizörü göz önüne alınsın.

$$\mathcal{A}_F(A) = \{\, \alpha \in \mathcal{A}_F \mid \text{her } P \in \mathcal{P}_F \text{ elemanı için } v_P(\alpha) \geq -v_P(A) \,\} \tag{2.19}$$

şeklinde tanımlanır. $\mathcal{A}_F(A)$ kümesi $\mathcal{A}_F$ nin bir alt vektör uzayıdır [2].

2.3.30 Teorem: Herhangi bir $A \in Div(F)$ divizörü için $\mathcal{A}_F(A) \cap F = \mathcal{L}(A)$ dır [2].

2.3.31 Teorem: Herhangi bir $A \in Div(F)$ divizörü için,

$$i(A) = dim(\mathcal{A}_F \,/\, (\mathcal{A}_F(A) + F)) \tag{2.20}$$

dir [2].

Burada *dim* ile K-vektör uzayı olarak boyut kastedilmektedir. $\mathcal{A}_F$, $\mathcal{A}_F(A)$ ve F kümeleri K üzerinde sonsuz boyutlu vektör uzayları olmalarına rağmen bu teoremin $\mathcal{A}_F \,/\, (\mathcal{A}_F(A) + F)$ bölüm uzayının K üzerinde sonlu boyutlu bir vektör uzayı olduğunu belirttiğine dikkat edilmelidir.

Bu teorem her $A \in Div(F)$ divizörü için,

$$\ell(A) = degA + 1 - g + dim(\mathcal{A}_F \,/\, (\mathcal{A}_F(A) + F)) \tag{2.21}$$

şeklinde de ifade edilebilir.

Bu teorem sayesinde $F \,/\, K$ fonksiyon cisminin cinsi başka bir şekilde ifade edilebilecektir.

2.3.32 Sonuç: $F \,/\, K$ herhangi bir fonksiyon cismi olsun. $F \,/\, K$ fonksiyon cisminin cinsi g olmak üzere $g = dim(\mathcal{A}_F \,/\, (\mathcal{A}_F(0) + F))$ dir [2].

2.3.33 Tanım: En az bir $A \in Div(F)$ divizörü için $\omega: \mathcal{A}_F \longrightarrow K$, $\omega(\mathcal{A}_F(A) + F) = 0$ şeklindeki bir K-lineer dönüşüme $F \ / \ K$ fonksiyon cisminin bir Weil diferansiyeli denir [2].

2.3.34 Tanım: $F \ / \ K$ herhangi bir fonksiyon cismi olsun.

$$\Omega_F = \{\ \omega \mid \omega, F/K \text{ nın bir Weil diferansiyelidir } \} \tag{2.22}$$

kümesine $F \ / \ K$ fonksiyon cisminin Weil diferansiyellerinin modülü denir [2].

Ω_F, K cismi üzerinde bir vektör uzayıdır.

2.3.35 Tanım: Herhangi bir $A \in Div(F)$ divizörü göz önüne alınsın.

$$\Omega_F(A) = \{\ \omega \in \Omega_F \mid \omega(\mathcal{A}_F(A) + F) = 0\ \} \tag{2.23}$$

şeklinde tanımlanır. $\Omega_F(A)$, Ω_F nin bir alt vektör uzayıdır [2].

2.3.36 Lemma: Herhangi bir $A \in Div(F)$ divizörü göz önüne alınsın. K cismi üzerinde vektör uzayı olan $\Omega_F(A)$ ve $\mathcal{A}_F \ / \ (\mathcal{A}_F(A) + F)$ uzayları birbirine izomorftur [2].

2.3.37 Teorem: Herhangi bir $A \in Div(F)$ divizörü için $dim\Omega_F(A) = i(A)$ dir [2].

Yukarıdaki teoremin basit bir sonucu olarak $\Omega_F \neq 0$ olduğu gösterilecektir. $degA \leq -2$ olacak şekilde bir $A \in Div(F)$ divizörü seçilsin. $\ell(A) \geq 0$ ve $g \geq 0$ olduğuna dikkat edilirse $dim\Omega_F(A) = i(A) = \ell(A) - degA + g - 1 \geq 1$ olacağından $\Omega_F(A) \neq 0$ olur. Böylece $\Omega_F \neq 0$ olduğu görülmüş olur.

2.3.38 Tanım: Herhangi bir $x \in F$ ve $\omega \in \Omega_F$ için $x\omega: \mathcal{A}_F \longrightarrow K$ dönüşümü $(x\omega)(\alpha) = \omega(x\alpha)$ olarak tanımlanır [2].

2.3.39 Teorem: Herhangi bir $x \in F$ ve $\omega \in \Omega_F$ için $x\omega$, $F \ / \ K$ fonksiyon cisminin bir Weil diferansiyelidir [2].

Yukarıdaki teorem yardımıyla Ω_F, F cismi üzerinde bir vektör uzayı olarak düşünülebilecektir.

2.3.40 Önerme: Ω_F, F cismi üzerinde bir boyutlu bir vektör uzayıdır [2].

Şimdi her Weil diferansiyeli $\omega \neq 0$ bir divizör ile ilişkilendirilecektir. Bu amaçla,

$$M(\omega) = \{ A \in Div(F) \mid \omega(\mathcal{A}_F(A) + F) = 0 \} \quad (2.24)$$

şeklinde tanımlanan küme kullanılacaktır.

2.3.41 Lemma: Herhangi bir $\omega \in \Omega_F$, $\omega \neq 0$ Weil diferansiyeli göz önüne alınsın. O zaman her $A \in M(\omega)$ divizörü için $A \leq W$ olacak şekilde teklikle belirli bir $W \in M(\omega)$ divizörü vardır [2].

Yukarıdaki lemma sayesinde şimdi yapılacak olan tanımlar anlamlıdır.

2.3.42 Tanım:

a) Bir Weil diferansiyelinin $\omega \neq 0$, (ω) divizörü aşağıdaki koşulları sağlayan, $F\ /\ K$ fonksiyon cisminin teklikle belirli bir divizörüdür.

(1) $\omega(\mathcal{A}_F((\omega)) + F) = 0$

(2) Herhangi bir $A \in Div(F)$ divizörü için $\omega(\mathcal{A}_F(A) + F) = 0$ ise $A \leq (\omega)$ dır.

b) Herhangi bir $\omega \in \Omega_F$, $\omega \neq 0$ Weil diferansiyeli göz önüne alınsın. Her $P \in \mathcal{P}_F$ place'i için $v_P(\omega) = v_P((\omega))$ olarak tanımlanır.

c) Herhangi bir $P \in \mathcal{P}_F$ place'i göz önüne alınsın. $v_P(\omega) > 0$ ise P place'ine ω nin bir kökü denir. $v_P(\omega) < 0$ ise P place'ine ω nin bir kutbu denir. $v_P(\omega) \geq 0$ ise ω Weil diferansiyeli P place'inde düzenli denir. ω Weil diferansiyeli her $P \in \mathcal{P}_F$ place'inde düzenli ise ω ye düzenli (ya da holomorfik) denir.

d) Herhangi bir $W \in Div(F)$ divizörü için $W = (\omega)$ olacak şekilde en az bir $\omega \in \Omega_F$ Weil diferansiyeli var ise W bir doğal divizördür denir [2].

2.3.43 Not: Yukarıda belirtilen tanımlardan dolayı,

$$\Omega_F(A) = \{ \omega \in \Omega_F \mid \omega = 0 \text{ veya } (\omega) \geq A \} \quad (2.25)$$

ve

$$\Omega_F(0) = \{ \omega \in \Omega_F \mid \omega \text{ düzenlidir} \} \quad (2.26)$$

şeklinde yazılabilir.

Ayrıca 2.3.37 Teorem ve 2.3.25 Tanım gereğince $dim\Omega_F(0) = i(0) = g$ elde edilir [2].

2.3.44 Önerme: Herhangi bir $x \in F,\ x \neq 0$ ve $\omega \in \Omega_F,\ \omega \neq 0$ elemanı için $(x\omega) = (x) + (\omega)$ dir [2].

2.3.45 Önerme: $F\ /\ K$ fonksiyon cisminin herhangi iki doğal divizörü denktir [2].

2.3.46 Tanım: 2.3.45 Önerme $F\ /\ K$ fonksiyon cisminin doğal divizörlerinin, $Cl(F)$ divizör sınıf grubunda bir sınıf oluşturduğunu gösterir. Bu divizör sınıfına $F\ /\ K$ fonksiyon cisminin doğal sınıfı denir [2].

Sıradaki teorem Riemann-Roch Teoreminin kanıtı için önemli olduğundan kanıtıyla birlikte verilmiştir.

2.3.47 Teorem: A, $F\ /\ K$ nın herhangi bir divizörü ve $W = (\omega)$, $F\ /\ K$ nın herhangi bir doğal divizörü olsun. O zaman,

$$\varphi: \mathcal{L}(W - A) \longrightarrow \Omega_F(A),\ x \mapsto x\omega \tag{2.27}$$

dönüşümü K-vektör uzaylarının bir izomorfizmasıdır. Özel olarak $i(A) = \ell(W - A)$ olur [2].

Kanıt:

φ dönüşümü iyi tanımlı, K-lineer ve birebirdir.

Önce φ dönüşümünün kapalı olduğu gösterilecektir. Herhangi bir $x \in \mathcal{L}(W - A)$ elemanı göz önüne alınsın. $\mathcal{L}(W - A)$ nın tanımı gereğince $(x) \geq -W + A$ olur. Ayrıca 2.3.44 Önerme gereğince $(x\omega) = (x) + (\omega)$ olur. Bu sebeple $(x\omega) = (x) + (\omega) \geq -W + A + (\omega) = -W + A + W = A$ elde edilir. 2.3.43 Not gereğince $x\omega \in \Omega_F(A)$ olur. Böylece φ dönüşümünün kapalı olduğu görülmüş olur.

Şimdi φ dönüşümünün örten olduğu gösterilecektir. Herhangi bir $\omega_1 \in \Omega_F(A)$ Weil diferansiyeli göz önüne alınsın. $\omega_1 = 0$ ise $0 \in \mathcal{L}(W - A)$ için $\varphi(0) = \omega_1$

olacağından $\omega_1 \neq 0$ olduğu varsayılabilir. 2.3.43 Not gereğince $(\omega_1) \geq A$ olur. 2.3.40 Önerme gereğince $\omega_1 = x\omega$ olacak şekilde en az bir $x \in F, x \neq 0$ elemanı vardır. 2.3.44 Önerme gereğince $(\omega_1) = (x\omega) = (x) + (\omega) = (x) + W \geq A$ olur. Böylece $(x) \geq -(W - A)$ elde edileceğinden $x \in \mathcal{L}(W - A)$ olur. $\varphi(x) = x\omega$ olacağından istenilen elde edilir.

Sonuç olarak φ dönüşümünün K-vektör uzaylarının bir izomorfizması olduğu görülmüş olur. Böylece 2.3.37 Teorem gereğince $i(A) = \ell(W - A)$ olduğu da görülmüş olur [2].

Bu bölümde elde edilen sonuçlar kullanılarak Riemann-Roch Teoremi kanıtlanacaktır. Bu teorem cebirsel fonksiyon cismi teorisindeki açık ara en önemli teoremdir. Bu nedenle kanıtıyla birlikte verilmiştir.

2.3.48 Teorem (Riemann-Roch Teoremi): W, $F\ /\ K$ fonksiyon cisminin herhangi bir doğal divizörü olsun. O zaman her $A \in Div(F)$ divizörü için,

$$\ell(A) = degA + 1 - g + \ell(W - A) \tag{2.28}$$

olur [2].

Kanıt:

Herhangi bir $A \in Div(F)$ divizörü ve $F\ /\ K$ fonksiyon cisminin herhangi bir doğal divizörü W için 2.3.47 Teorem gereğince $i(A) = \ell(W - A)$ olduğu biliniyor. 2.3.25 Tanım gereğince $i(A) = \ell(A) - degA + g - 1$ olduğuna dikkat edilirse $\ell(A) = degA + 1 - g + \ell(W - A)$ elde edilir. Böylece teorem kanıtlanmış olur [2].

2.3.49 Sonuç: $F\ /\ K$ fonksiyon cisminin herhangi bir doğal divizörü W için $degW = 2g - 2$ ve $\ell(W) = g$ dir [2].

Kanıt:

$0 \in Div(F)$ divizörü için 2.3.48 Teorem gereğince $\ell(0) = deg0 + 1 - g + \ell(W)$ olur. Böylece $\ell(W) = g$ elde edilir.

$W \in Div(F)$ divizörü için 2.3.48 Teorem gereğince $\ell(W) = degW + 1 - g + \ell(0)$ olur. Böylece $degW = 2g - 2$ elde edilir.

Sonuç olarak kanıt tamamlanmış olur.

Herhangi bir $A \in Div(F)$ divizörü için 2.3.23 Teorem b) gereğince $degA \geq c$ olduğunda $i(A) = 0$ olacak şekilde yalnızca F / K fonksiyon cismine bağlı bir c tamsayısının olduğu biliniyor. Şimdi bu sabitin nasıl seçilebileceğine dair daha kesin bir yöntem verilecektir.

2.3.50 Teorem: Herhangi bir $A \in Div(F)$ divizörü için $degA \geq 2g - 1$ ise $\ell(A) = degA + 1 - g$ dir [2].

Herhangi bir W doğal divizörü için 2.3.49 Sonuç gereğince $degW = 2g - 2$ ve $\ell(W) > degW + 1 - g$ olduğundan yukarıdaki teoremdeki $2g - 1$ sınırı mümkün olan en iyi sınırdır.

Şimdi Riemann-Roch teoreminin F / K fonksiyon cisminin doğal sınıfının yanında cinsini de karakterize ettiği gösterilecektir. Sıradaki önerme kanıtıyla birlikte verilmiştir.

2.3.51 Önerme: $g_0 \in \mathbb{Z}$ ve $W_0 \in Div(F)$ olmak üzere her $A \in Div(F)$ divizörü için $\ell(A) = degA + 1 - g_0 + \ell(W_0 - A)$ olsun. O zaman $g_0 = g$ ve W_0 bir doğal divizör olur [2].

Kanıt:

$0 \in Div(F)$ divizörü için hipotez gereğince $\ell(0) = deg0 + 1 - g_0 + \ell(W_0)$ olur. Böylece $\ell(W_0) = g_0$ elde edilir.

$W_0 \in Div(F)$ divizörü için hipotez gereğince $\ell(W_0) = degW_0 + 1 - g_0 + \ell(0)$ olur. Böylece $degW_0 = 2g_0 - 2$ elde edilir.

$degA > max\{2g - 2,\ 2g_0 - 2\}$ olacak şekilde bir $A \in Div(F)$ divizörü göz önüne alınsın. $degA \geq 2g - 1$ olacağından 2.3.50 Teorem gereğince $\ell(A) = degA + 1 - g$ elde edilir. Ayrıca $deg(W_0 - A) < 0$ olduğundan 2.3.17 Sonuç gereğince

$\ell(W_0 - A) = 0$ bulunur. Hipotez gereğince $\ell(A) = degA + 1 - g_0$ olur. Böylece $g = g_0$ elde edilir.

W, $F\ /\ K$ fonksiyon cisminin herhangi bir doğal divizörü olmak üzere hipotez gereğince $\ell(W) = degW + 1 - g + \ell(W_0 - W)$ elde edilir. W doğal bir divizör olduğundan 2.3.49 Sonuç gereğince $degW = 2g - 2$ ve $\ell(W) = g$ dir. Böylece $\ell(W_0 - W) = 1$ olur. Ayrıca $g = g_0$ olduğundan dolayı $deg(W_0 - W) = 0$ olduğuna dikkat edilirse 2.3.18 Sonuç gereğince $W_0 - W$ bir esas divizördür. Bu sebeple en az bir $x \in F$, $x \neq 0$ için $W_0 = W + (x)$ olur. Bu durumda 2.3.44 Önerme gereğince W_0 bir doğal divizördür [2].

Sonuç olarak kanıt tamamlanmış olur.

Herhangi bir $F\ /\ K$ fonksiyon cismi göz önüne alınsın. Herhangi bir $A \in Div(F)$ divizörü için $degA < 0$ ise 2.3.17 Sonuç gereğince $\ell(A) = 0$ olduğu biliniyor. $degA \geq 2g - 1$ ise 2.3.50 Teorem gereğince $\ell(A) = degA + 1 - g$ olduğu biliniyor. Yani bu durumlarda A divizörünün boyutu $degA$ ya bağlıdır.

Şimdi $0 \leq degA \leq 2g - 2$ olması durumunda A divizörünün boyutu araştırılacaktır.

2.3.52 Lemma: Herhangi iki $A, B \in Div(F)$ divizör için $\ell(A) > 0$ ve $\ell(B) > 0$ ise $\ell(A) + \ell(B) \leq 1 + \ell(A + B)$ dir [2].

Sıradaki teorem kanıtıyla birlikte verilmiştir.

2.3.53 Teorem (Clifford Teoremi): Herhangi bir $A \in Div(F)$ divizörü için $0 \leq degA \leq 2g - 2$ ise $\ell(A) \leq 1 + \frac{1}{2} degA$ dır [2].

Kanıt:

$\ell(A) = 0$ olduğu varsayılsın. Bu durumda $\ell(A) \leq 1 + \frac{1}{2} degA$ eşitsizliği sağlanır.

Şimdi herhangi bir $W \in Div(F)$ doğal divizörü için $\ell(W - A) = 0$ olduğu kabul edilsin. Bu sebeple 2.3.48 Teorem gereğince $\ell(A) = degA + 1 - g + \ell(W - A) =$

$degA + 1 - g = 1 + \frac{1}{2}degA + \frac{1}{2}(degA - 2g)$ elde edilir. $degA \leq 2g - 2$ olduğundan $\ell(A) < 1 + \frac{1}{2}degA$ olur. Böylece istenilen elde edilir.

Son olarak $\ell(A) > 0$ ve $\ell(W - A) > 0$ olduğunda eşitsizliğin sağlandığı gösterilecektir. 2.3.52 Lemma gereğince $\ell(A) + \ell(W - A) \leq 1 + \ell(W)$ olur. 2.3.49 Sonuç gereğince $\ell(W) = g$ olduğuna dikkat edilirse $\ell(W - A) \leq 1 + g - \ell(A)$ elde edilir. Ayrıca 2.3.48 Teorem gereğince $\ell(A) = degA + 1 - g + \ell(W - A)$ olduğundan $\ell(A) \leq degA + 1 - g + 1 + g - \ell(A)$ bulunur. Böylece $\ell(A) \leq 1 + \frac{1}{2}degA$ eşitsizliği sağlandığından kanıt tamamlanmış olur [2].

2.4 Weil Diferansiyellerinin Yerel Bileşenleri

2.4.1 Tanım: Herhangi bir $P \in \mathcal{P}_F$ place'i göz önüne alınsın. Herhangi bir $x \in F$ için $\iota_P(x) \in \mathcal{A}_F$, P inci bileşeni x, diğer bileşenleri $0 \in F$ olan adele olarak tanımlanır [2].

2.4.2 Tanım: Herhangi bir $P \in \mathcal{P}_F$ place'i ve $\omega \in \Omega_F$ Weil diferansiyeli göz önüne alınsın. $\omega_P : F \longrightarrow K$, $\omega_P(x) = \omega(\iota_P(x))$ şeklinde tanımlanan dönüşüme ω Weil diferansiyelinin yerel bileşeni denir [2].

ω_P bir K-lineer dönüşümdür.

2.4.3 Önerme: Herhangi bir $\omega \in \Omega_F$ Weil diferansiyeli ve $\alpha = (\alpha_P) \in \mathcal{A}_F$ adele'i göz önüne alınsın. O zaman en fazla sonlu sayıda $P \in \mathcal{P}_F$ place'i için $\omega_P(\alpha_P) \neq 0$ dır ve $\omega(\alpha) = \sum_{P \in \mathcal{P}_F} \omega_P(\alpha_P)$ olur. Özel olarak $1 \in F$ için $\sum_{P \in \mathcal{P}_F} \omega_P(1) = 0$ dır [2].

Şimdi bir Weil diferansiyelinin, yerel bileşenlerinin her biri tarafından teklikle belirli olduğu gösterilecektir.

2.4.4 Önerme: Herhangi bir $P \in \mathcal{P}_F$ place'i ve $\omega \in \Omega_F$, $\omega \neq 0$ Weil diferansiyeli göz önüne alınsın. O zaman,

$v_P(\omega) = max\{\, r \in \mathbb{Z} \mid v_P(x) \geq -r$ olacak şekildeki her $x \in F$ için $\omega_P(x) = 0$ dır $\}$

olur. Özel olarak $\omega_P \neq 0$ dır [2].

2.4.4 Önerme gereğince $r \in \mathbb{Z}$ olmak üzere,

$v_P(\omega) \geq r \Leftrightarrow v_P(x) \geq -r$ olacak şekildeki her $x \in F$ için $\omega_P(x) = 0$ (2.29)

yazılabilir.

2.4.5 Önerme: $K(x) \,/\, K$ bir rasyonel fonksiyon cismi olsun.

a) $-2P_\infty$ bir doğal divizördür.

b) $(\eta) = -2P_\infty$ ve $\eta_{P_\infty}(x^{-1}) = -1$ olacak şekilde teklikle belirli bir $\eta \in \Omega_F$ Weil diferansiyeli vardır.

c) Yukarıdaki η Weil diferansiyelinin yerel bileşenleri η_{P_∞} ve $a \in K$ için η_{P_a} olmak üzere,

$$\eta_{P_\infty}((x-a)^n) = \begin{cases} 0 & ,n \neq -1 \\ -1 & ,n = -1 \end{cases} \quad (2.30)$$

ve

$$\eta_{P_a}((x-a)^n) = \begin{cases} 0 & ,n \neq -1 \\ 1 & ,n = -1 \end{cases} \quad (2.31)$$

olur [2].

BÖLÜM 3

CEBİRSEL GEOMETRİK KODLAR

Bu bölümde cebirsel fonksiyon cisimleri kullanılarak Goppa'nın hata-düzeltici kodlarının yapısı ifade edilecektir.

3.1 Kodlar

$\mathbb{F}_q$, q elemanlı herhangi bir sonlu cisim olsun. Herhangi bir elemanı, $a_i \in \mathbb{F}_q$ olmak üzere $a = (a_1, a_2, \dots, a_n)$ şeklinde olan $\mathbb{F}_q$ üzerinde n-boyutlu bir vektör uzayı ${\mathbb{F}_q}^n$ göz önüne alınsın.

3.1.1 Tanım: Herhangi iki $a = (a_1, a_2, \dots, a_n)$, $b = (b_1, b_2, \dots, b_n) \in {\mathbb{F}_q}^n$ elemanı için $d(a,b) = |\{\, i \mid a_i \neq b_i \,\}|$ şeklinde tanımlı d fonksiyonuna ${\mathbb{F}_q}^n$ üzerinde Hamming uzaklığı denir [2].

Hamming uzaklığı ${\mathbb{F}_q}^n$ üzerinde bir metriktir.

3.1.2 Tanım: Herhangi bir $a \in {\mathbb{F}_q}^n$ elemanı için $wt(a) = d(a,0) = |\{\, i \mid a_i \neq 0 \,\}|$ değerine a nın ağırlığı denir [2].

3.1.3 Tanım: ${\mathbb{F}_q}^n$ vektör uzayının herhangi bir alt vektör uzayına C kod denir. C kodunun herhangi bir elemanına kod sözcüğü denir. Bu durumda C kodunun uzunluğu n olarak tanımlanır. C kodunun $\mathbb{F}_q$-vektör uzayı olarak boyutu $dimC$ ile gösterilir [2].

Uzunluğu n ve boyutu k olan bir kod $[n,k]$ ile gösterilecektir.

3.1.4 Tanım: Herhangi bir $C \neq 0$ kodu göz önüne alınsın.

$$d(C) = min\{\, d(a,b) \mid a,b \in C \text{ ve } a \neq b \,\} = min\{\, wt(c) \mid c \in C, c \neq 0 \,\} \qquad (3.1)$$

değerine C kodunun minimum uzaklığı denir [2].

Minimum uzaklığı d olan bir $[n, k]$ kodu $[n, k, d]$ ile gösterilecektir.

3.1.5 Tanım: Herhangi bir $C \neq 0$ kodunun minimum uzaklığı d olmak üzere $t = [(d-1) / 2]$ olsun. O zaman C bir t-hata düzeltici koddur denir [2].

Herhangi bir C kodunu açık bir şekilde ifade etmenin basit bir yolu $\mathbb{F}_q$ üzerindeki tabanını göz önüne almaktır.

3.1.6 Tanım: C, $\mathbb{F}_q$ üzerinde bir $[n, k]$ kod olsun. Satırları C kodunun tabanı olan $k \times n$ lik matrise C nin bir üreteç matrisi denir [2].

3.1.7 Tanım: Herhangi iki $a = (a_1, a_2, \dots, a_n)$, $b = (b_1, b_2, \dots, b_n) \in {\mathbb{F}_q}^n$ elemanı göz önüne alınsın. ${\mathbb{F}_q}^n$ üzerinde $< a, b >= \sum_{i=1}^{n} a_i \,.\, b_i$ şeklinde tanımlı iç çarpıma doğal iç çarpım denir [2].

3.1.8 Tanım: $C \subseteq {\mathbb{F}_q}^n$ herhangi bir kod olmak üzere,

$$C^{\perp} = \{\, u \in {\mathbb{F}_q}^n \mid \text{her } c \in C \text{ için} < u, c >= 0 \,\} \tag{3.2}$$

kümesi C nin duali olarak isimlendirilir. $(C^{\perp})^{\perp} = C$ dir [2].

$C = C^{\perp}$ ise C kodu self-dual olarak adlandırılır. $C \subseteq C^{\perp}$ ise C kodu self-ortogonal olarak adlandırılır.

Herhangi bir $[n, k]$ kodunun duali $[n, n-k]$ kodudur. Özel olarak n uzunluğundaki bir self-dual kodun boyutu $n / 2$ dir.

3.1.9 Tanım: Herhangi bir C kodu göz önüne alınsın. H, $C^{\perp}$ kodunun bir üreteç matrisi olsun. Bu durumda H, C kodunun bir parity check matrisi olarak isimlendirilir [2].

Herhangi bir $[n, k]$ kodunun parity check matrisi, rankı $n-k$ olan $(n-k) \times n$ lik bir matristir. Ayrıca herhangi bir $u \in {\mathbb{F}_q}^n$ vektörünün transpozu u^t ile gösterilmek üzere $C = \{\, u \in {\mathbb{F}_q}^n \mid H.u^t = 0 \,\}$ şeklinde yazılabilir. Böylece bir parity check

matrisinin, herhangi bir $u \in \mathbb{F}_q{}^n$ vektörünün kod sözcüğü olup olmadığını kontrol etmek için kullanılabileceği gösterilmiş olur.

Olabildiğince fazla hata düzeltebilmek için uzunluğu ve boyutu verilen bir kodun minimum uzaklığının olabildiğince büyük olması istenir. Benzer şekilde olabildiğince fazla veri gönderebilmek için uzunluğu ve minimum uzaklığı verilen bir kodun boyutunun olabildiğince büyük olması istenir. Bu nedenle cebirsel kod teorisindeki temel problemlerden biri sonlu bir $\mathbb{F}_q$ cismi üzerinde boyutu ve minimum uzaklığı, uzunluğu ile karşılaştırıldığında büyük olan kodlar inşa edebilmektir. Ancak bu bazı kısıtlamaları beraberinde getirir. Kabaca ifade edilecek olursa, bir kodun boyutu uzunluğuna kıyasla büyükse minimum uzaklığı küçük olur. Şimdi en basit sınır verilecektir.

3.1.10 Önerme (Singleton Sınırı): Herhangi bir $[n, k, d]$ kodu göz önüne alınsın. O zaman $k + d \leq n + 1$ olur [2].

Singleton sınırının $\mathbb{F}_q$ cisminin eleman sayısından bağımsız olduğuna dikkat edilmelidir.

3.1.11 Önerme: $k + d = n + 1$ özelliğini sağlayan herhangi bir koda, maksimum uzaklık ayrılabilir (MDS) kod denir [2].

Genel olarak bir kod veya kodların bir sınıfı verildiğinde minimum uzaklık için alt sınırlar elde etmek çok daha zor bir problemdir. Sonraki kısımda tanımlanacak olan cebirsel geometrik kodlarla ilgilenilmesinin nedenlerinden biri bu kodların minimum uzaklığı için iyi bir alt sınırın elde edilmiş olmasıdır.

3.2 Cebirsel Geometrik Kodlar

Cebirsel geometrik kodlar (AG kodlar), V.D. Goppa tarafından tanıtılmıştır. Bu nedenle bazen geometrik Goppa kodları olarak da isimlendirilirler. Bu kodların yapısının daha iyi anlaşılabilmesi için öncelikle $\mathbb{F}_q$ üzerinde tanımlanan Reed-Solomon kodları üzerinde durulacaktır. Kodların bu önemli sınıfı, kod teorisinde uzun süredir bilinmektedir. Cebirsel geometrik kodlar, Reed-Solomon kodlarının doğal bir genelleştirilmesidir.

$n = q - 1$ ve $\beta \in \mathbb{F}_q$ elemanı, çarpımsal $\mathbb{F}_q^{\times}$ grubunun ilkel bir elemanı olsun. $1 \leq k \leq n$ olmak üzere herhangi bir k tamsayısı için k-boyutlu,

$$\mathcal{L}_k = \{ f \in \mathbb{F}_q[x] \mid degf \leq k - 1 \} \tag{3.3}$$

vektör uzayı ve

$$\varphi: \mathcal{L}_k \longrightarrow {\mathbb{F}_q}^n, f \mapsto (f(\beta), f(\beta^2), \dots, f(\beta^n)) \tag{3.4}$$

dönüşümü göz önüne alınsın.

φ dönüşümü iyi tanımlı ve kapalıdır. φ nin bir $\mathbb{F}_q$-lineer dönüşüm olduğu gösterilecektir. Herhangi $f,\ g \in \mathcal{L}_k$ ve $k \in K$ elemanları göz önüne alınsın. $\varphi(f + k.g) = ((f + k.g)(\beta), (f + k.g)(\beta^2), \dots, (f + k.g)(\beta^n)) = (f(\beta), f(\beta^2), \dots, f(\beta^n)) + k.(g(\beta), g(\beta^2), \dots, g(\beta^n)) = \varphi(f) + k.\varphi(g)$ olduğundan istenilen elde edilir.

φ dönüşümünün birebir olduğu görülecektir. Bunun için $ker\varphi = \{0\}$ olduğunu göstermek yeterlidir. $0 \in \mathcal{L}_k$ için $\varphi(0) = (0,0, \dots,0) \in {\mathbb{F}_q}^n$ olduğundan $\{0\} \subseteq ker\varphi$ olur. Diğer taraftan herhangi bir $f \in ker\varphi$ elemanı göz önüne alınsın ve $f \neq 0$ olduğu kabul edilsin. $f \in ker\varphi$ olduğundan $\varphi(f) = (f(\beta), f(\beta^2), \dots, f(\beta^n)) = (0,0, \dots,0)$ olur. $\beta, \beta^2, \dots, \beta^n$ elemanları ikişerli olarak farklı olduğundan $degf \geq n$ bulunur. Ancak $degf < k$ olduğundan $degf < n$ dir. Böylece bir çelişki elde edilmiş olur. O halde $f = 0$ dır ve $ker\varphi \subseteq \{0\}$ elde edilir. Bu durumda $ker\varphi = \{0\}$ olacağından φ dönüşümünün birebir olduğu görülmüş olur.

φ dönüşümünün tanımı gereğince $C_k = \{ (f(\beta), f(\beta^2), \dots, f(\beta^n)) \mid f \in \mathcal{L}_k \}$ kümesi $\mathbb{F}_q$ üzerinde bir $[n, k]$ koddur.

3.2.1 Tanım: $n = q - 1$ ve $\beta \in \mathbb{F}_q$ elemanı, çarpımsal $\mathbb{F}_q^{\times}$ grubunun ilkel bir elemanı olsun. $\mathbb{F}_q$ üzerinde $C_k = \{ (f(\beta), f(\beta^2), \dots, f(\beta^n)) \mid f \in \mathcal{L}_k \}$ şeklinde tanımlı koda bir Reed-Solomon kodu denir [2].

Reed-Solomon kodunun, herhangi bir $c = \varphi(f) \in C_k,\ c \neq 0$ kod sözcüğünün ağırlığı,

$$wt(c) = n - |\{\, i \in \{1, \dots, n\} \mid f(\beta^i) = 0 \,\}| \tag{3.5}$$

şeklinde tanımlanabilir.

$degf \geq |\{\, i \in \{1, \dots, n\} \mid f(\beta^i) = 0 \,\}|$ ve $degf \leq k - 1$ olduğuna dikkat edilirse $wt(c) \geq n - degf \geq n - (k - 1)$ elde edilir. Böylece C_k kodunun minimum uzaklığı $d \geq n - (k - 1)$ eşitsizliğini sağlar. Diğer yandan 3.1.10 Önerme gereğince $d \leq n + 1 - k$ olduğundan $d + k = n + 1$ eşitliği elde edilir. Bu nedenle Reed-Solomon kodları, $\mathbb{F}_q$ üzerinde MDS kodlarıdır. Ancak $n = q - 1$ olduğundan Reed-Solomon kodlarının uzunluğunun, $\mathbb{F}_q$ cisminin eleman sayısına kıyasla küçük olduğuna dikkat edilmelidir.

Uyarı: Sıradaki ifadeler bölüm boyunca geçerli olacaktır. $F \,/\, \mathbb{F}_q$ cinsi g olan bir fonksiyon cismidir. $P_1, P_2, \dots, P_n \in \mathcal{P}_F$ ikişer ikişer ayrık rasyonel placeler olmak üzere $D = P_1 + P_2 + \cdots + P_n$ şeklinde tanımlanır. G, $F \,/\, \mathbb{F}_q$ fonksiyon cisminin $suppG \cap suppD = \emptyset$ olacak şekilde bir divizörüdür.

$\varphi_D : \mathcal{L}(G) \longrightarrow {\mathbb{F}_q}^n$, $\varphi_D(x) = (x(P_1), x(P_2), \dots, x(P_n))$ şeklinde tanımlı dönüşüm göz önüne alınsın. φ_D dönüşümü iyi tanımlıdır. φ_D dönüşümünün kapalı olduğu gösterilecektir. Herhangi bir $x \in \mathcal{L}(G)$ elemanı göz önüne alınsın. $suppG \cap suppD = \emptyset$ olduğundan her $i \in \{1,2, \dots, n\}$ için $v_{P_i}(x) \geq 0$ dır. Böylece $x(P_i) \in F_{P_i}$ olur. 2.1.13 Tanım b) gereğince $[F_{P_i} : \mathbb{F}_q] = degP_i = 1$ olduğundan $x(P_i) \in \mathbb{F}_q$ olur. Bu sebeple $(x(P_1), x(P_2), \dots, x(P_n)) \in {\mathbb{F}_q}^n$ olacağından, φ_D dönüşümünün kapalı olduğu görülmüş olur.

φ_D dönüşümünün bir $\mathbb{F}_q$-lineer dönüşüm olduğunun gösterilmesi için herhangi $x, y \in \mathcal{L}(G)$ ve $k \in \mathbb{F}_q$ elemanları göz önüne alınsın. $\varphi_D(x + k.y) = ((x + k.y)(P_1), (x + k.y)(P_2), \dots, (x + k.y)(P_n)) = (x(P_1), x(P_2), \dots, x(P_n)) + (k(P_1).y(P_1), k(P_2).y(P_2), \dots, k(P_n).y(P_n))$ bulunur. Her $i \in \{1,2, \dots, n\}$ için $\mathbb{F}_q$, F_{P_i} cisminin bir alt cismi olarak düşünülebileceğinden $k(P_1) = k(P_2) = \cdots = k(P_n) = k$ olacağına dikkat edilirse $(k(P_1).y(P_1), k(P_2).y(P_2), \dots, k(P_n).y(P_n)) = k.(y(P_1), y(P_2), \dots, y(P_n))$ elde edilir. Böylece $\varphi_D(x + k.y) = \varphi_D(x) + k.\varphi_D(y)$ olacağından φ_D nin bir $\mathbb{F}_q$-lineer dönüşüm olduğu görülmüş olur.

φ_D dönüşümü gereğince $Im\varphi_D = \{ (x(P_1), x(P_2), \dots, x(P_n)) \mid x \in \mathcal{L}(G) \} \subseteq {\mathbb{F}_q}^n$ kümesi $\mathbb{F}_q$ üzerinde bir kod olacağından sıradaki tanım anlamlıdır:

3.2.2 Tanım: $\mathbb{F}_q$ üzerinde $C_{\mathcal{L}}(D, G) = \{ (x(P_1), x(P_2), \dots, x(P_n)) \mid x \in \mathcal{L}(G) \} \subseteq {\mathbb{F}_q}^n$ şeklinde tanımlı koda, D ve G divizörleri ile ilişkili bir fonksiyonel cebirsel geometrik kod denir [2].

Cebirsel geometrik kodlar ve Reed-Solomon kodlarının tanımlanış biçimlerinin benzerliği açıktır. Üstelik, $F \,/\, \mathbb{F}_q$ fonksiyon cismi ile birlikte D ve G divizörleri uygun bir şekilde seçilirse Reed-Solomon kodlarının, cebirsel geometrik kodların özel bir durumu olduğu görülebilir.

Cebirsel geometrik kodların en önemli özelliklerinden biri, bu koda ait n, k ve d parametreleri hakkında 2.3.48 Teorem (Riemann-Roch Teoremi) yardımıyla yorumda bulunulabilmesidir. Ayrıca bu kodların minimum uzaklıkları için aşikar olmayan bir alt sınır mevcuttur. Sıradaki teorem ve sonucu kod yapısının daha iyi anlaşılabilmesi için kanıtıyla birlikte verilmiştir.

3.2.3 Teorem: $C_{\mathcal{L}}(D, G)$, $k = \ell(G) - \ell(G - D)$ ve $d \geq n - degG$ olmak üzere bir $[n, k, d]$ koddur [2].

Kanıt:

Öncelikle $k = \ell(G) - \ell(G - D)$ olduğu gösterilecektir. $\varphi_D : \mathcal{L}(G) \longrightarrow C_{\mathcal{L}}(D, G)$, $\varphi_D(x) = (x(P_1), x(P_2), \dots, x(P_n))$ şeklinde tanımlı dönüşümün iyi tanımlı, kapalı, $\mathbb{F}_q$-lineer ve örten olduğu biliniyor.

$Ker\varphi_D = \mathcal{L}(G - D)$ olduğu gösterilecektir. Herhangi bir $x \in Ker\varphi_D$ elemanı göz önüne alınsın. O halde $\varphi_D(x) = (x(P_1), x(P_2), \dots, x(P_n)) = ((P_1), (P_2), \dots, (P_n))$ olacağından her $i \in \{1,2, \dots, n\}$ için $v_{P_i}(x) \geq 1$ bulunur. Böylece, $suppG \cap suppD = \emptyset$ olduğuna dikkat edilirse $\mathcal{L}(G - D)$ nin tanımı gereğince $x \in \mathcal{L}(G - D)$ elde edilir. Diğer taraftan herhangi bir $x \in \mathcal{L}(G - D)$ elemanı göz önüne alınsın. $\mathcal{L}(G - D)$ nin tanımı gereğince $i \in \{1,2, \dots, n\}$ için $v_{P_i}(x) \geq 1$ olacağından $(x(P_1), x(P_2), \dots, x(P_n)) = ((P_1), (P_2), \dots, (P_n))$ elde edilir. Bu sebeple $x \in Ker\varphi_D$ olacağından istenilen elde edilir.

Böylece $k = dim C_{\mathcal{L}}(D,G) = \ell(G) - \ell(G-D)$ olduğu gösterilmiş olur.

Şimdi $d \geq n - degG$ olduğu gösterilecektir. Bu eşitsizliğin anlamlı olabilmesi için $C_{\mathcal{L}}(D,G) \neq 0$ olduğu varsayılacaktır. $wt(\varphi_D(x)) = d$ olacak şekilde bir $x \in \mathcal{L}(G)$ elemanı göz önüne alınsın. Böylece x elemanının kökü olacak şekilde $n-d$ tane $P_{i_1}, P_{i_2}, \dots, P_{i_{n-d}} \in suppD$ place vardır. Böylece $x \in \mathcal{L}(G - (P_{i_1} + P_{i_2} + \cdots + P_{i_{n-d}}))$ olur. $x \neq 0$ olduğundan 2.3.17 Sonuç gereğince $deg(G - (P_{i_1} + P_{i_2} + \cdots + P_{i_{n-d}})) \geq 0$ olur. Böylece $deg(G - (P_{i_1} + P_{i_2} + \cdots + P_{i_{n-d}})) = degG - (n-d)$ olduğuna dikkat edilirse $d \geq n - degG$ eşitsizliğinin sağlandığı görülmüş olur [2].

3.2.4 Sonuç: $degG < n$ olsun. O zaman,

a) $k = \ell(G) \geq degG + 1 - g$ ve $d \geq n - degG$ olmak üzere $C_{\mathcal{L}}(D,G)$ bir $[n,k,d]$ koddur. Böylece $k + d \geq n + 1 - g$ olur.

b) Özel olarak, $2g - 2 < degG < n$ ise $k = degG + 1 - g$ dır.

c) $\{x_1, x_2, \dots, x_k\}$ kümesi, $\mathcal{L}(G)$ Riemann-Roch uzayının bir tabanı olmak üzere,

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \cdots & x_1(P_n) \\ \vdots & \vdots & & \vdots \\ x_k(P_1) & x_k(P_2) & \cdots & x_k(P_n) \end{pmatrix} \tag{3.6}$$

matrisi $C_{\mathcal{L}}(D,G)$ kodu için bir üreteç matrisidir [2].

Kanıt:

a) 3.2.3 Teorem gereğince $d \geq n - degG$ olduğu bilinmektedir. $degG < n$ olduğundan $deg(G-D) = degG - n < 0$ olur. 2.3.17 Sonuç gereğince $\ell(G-D) = 0$ elde edilir. 3.2.3 Teorem gereğince $k = \ell(G) - \ell(G-D)$ olduğundan $k = \ell(G)$ bulunur. Ayrıca 2.3.23 Teorem a) gereğince $\ell(G) \geq degG + 1 - g$ olduğuna dikkat edilirse istenilen elde edilir.

b) a) gereğince $k = \ell(G)$ olduğu biliniyor. $2g - 2 < degG$ olduğundan 2.3.50 Teorem gereğince $\ell(G) = degG + 1 - g$ olur. Böylece $k = \ell(G) = degG + 1 - g$ olacağından istenilen elde edilmiş olur.

c) Herhangi bir $(x(P_1), x(P_2), \dots, x(P_n)) \in C_{\mathcal{L}}(D,G)$ elemanı göz önüne alınsın. Burada $x \in \mathcal{L}(G)$ dir. $\{x_1, x_2, \dots, x_k\}$ kümesi, $\mathcal{L}(G)$ Riemann-Roch uzayının bir tabanı olduğundan $x = c_1.x_1 + c_2.x_2 + \cdots + c_k.x_k,\ c_i \in \mathbb{F}_q$ yazılabilir. Böylece $(x(P_1),\ x(P_2), \dots, x(P_n)) = c_1.(x_1(P_1), x_1(P_2), \dots, x_1(P_n)) + c_2.(x_2(P_1), x_2(P_2), \dots, x_2(P_n)) + \cdots + c_k.(x_k(P_1), x_k(P_2), \dots, x_k(P_n))$ yazılabilir. Bu sebeple $\{(x_1(P_1), x_1(P_2), \dots, x_1(P_n)),\ (x_2(P_1), x_2(P_2), \dots, x_2(P_n)),\ \dots,\ (x_k(P_1), x_k(P_2), \dots, x_k(P_n))\}$ kümesi $C_{\mathcal{L}}(D,G)$ vektör uzayını üretmektedir. Ayrıca bu kümenin elemanlarının lineer bağımsız olduğuna dikkat edilirse, $C_{\mathcal{L}}(D,G)$ vektör uzayının bir tabanını oluşturacaklarından istenilen elde edilir [2].

Böylece 3.2.4 Sonuç kanıtlanmış olur.

Herhangi bir $C_{\mathcal{L}}(D,G)$ kodu göz önüne alınsın ve $degG < n$ olsun. 3.1.10 Önerme gereğince $k + d \leq n + 1$ olduğu biliniyor. Diğer taraftan 3.2.4 Sonuç gereğince $k + d \geq n + 1 - g$ olur. Bu nedenle $F\ /\ K$ fonksiyon cisminin cinsi sıfır ise $k + d = n + 1$ elde edilir. Böylece $degG < n$ olmak üzere $\mathbb{F}_q(z)\ /\ \mathbb{F}_q$ rasyonel fonksiyon cismi anlamında oluşturulan cebirsel geometrik kodlar daima MDS kodları olacaktır.

3.2.3 Teorem gereğince herhangi bir $C_{\mathcal{L}}(D,G)$ kodunun minimum uzaklığı için $d \geq n - degG$ eşitsizliği sağlanır. Bu nedenle $C_{\mathcal{L}}(D,G)$ kodunun minimum uzaklığının anlamlı bir alt sınırını elde edebilmek için genellikle $degG < n$ olduğu varsayılacaktır.

3.2.5 Tanım: $d^* = n - degG$ tamsayısına $C_{\mathcal{L}}(D,G)$ kodunun tasarlanmış uzaklığı denir [2].

3.2.3 Teorem gereğince bir cebirsel geometrik kodun minimum uzaklığı onun tasarlanmış uzaklığından daha küçük olamaz. Şimdi $d^* = d$ veya $d^* < d$ olma durumları incelenecektir.

Şimdi Weil diferansiyellerinin yerel bileşenleri kullanılarak, G ve D divizörleri ile ilişkili diğer bir kod tanımlanacaktır. Bu nedenle Weil diferansiyelleri ile ilgili birkaç hatırlatma yapılacaktır. Herhangi bir $A \in Div(F)$ divizörü için $\Omega_F(A)$, $(\omega) \geq A$ olacak şekildeki Weil diferansiyellerinin uzayıdır. 2.3.37 Teorem gereğince $\Omega_F(A)$, $\mathbb{F}_q$ üzerinde boyutu $i(A)$ olan sonlu boyutlu bir vektör uzayıdır. Herhangi bir $\omega \in \Omega_F$ Weil

diferansiyeli ve $P \in \mathcal{P}_F$ place'i için $\omega_P: F \longrightarrow \mathbb{F}_q$ dönüşümü ω nin, P place'indeki yerel bileşenini gösterir.

3.2.6 Tanım: $\mathbb{F}_q$ üzerinde $C_\Omega(D,G) = \{ (\omega_{P_1}(1), \omega_{P_2}(1), \dots, \omega_{P_n}(1)) \mid \omega \in \Omega_F(G-D) \} \subseteq {\mathbb{F}_q}^n$ şeklinde tanımlı koda, D ve G divizörleri ile ilişkili bir rezidü cebirsel geometrik kod denir [2].

Sıradaki teorem kod yapısının daha iyi anlaşılabilmesi için kanıtı ile birlikte verilmiştir.

3.2.7 Teorem: $C_\Omega(D,G)$, $k' = i(G-D) - i(G)$ ve $d' \geq degG - (2g-2)$ olmak üzere bir $[n, k', d']$ koddur. Özel olarak $degG > 2g-2$ ise $k' = i(G-D) \geq n + g - 1 - degG$ olur. Ayrıca $2g-2 < degG < n$ ise $k' = n + g - 1 - degG$ dir [2].

Kanıt:

Öncelikle herhangi bir $\omega \in \Omega_F, \omega \neq 0$ Weil diferansiyeli ve birinci dereceden $P \in \mathcal{P}_F$ place'i için $v_P(\omega) \geq -1$ ise,

$$\omega_P(1) = 0 \Leftrightarrow v_P(\omega) \geq 0 \tag{3.7}$$

olduğu gösterilecektir.

$\Longrightarrow$: $\omega_P(1) = 0$ olsun. $v_P(x) \geq 0$ olacak şekildeki herhangi bir $x \in F$ elemanı göz önüne alınsın. 2.1.13 Tanım b) gereğince $[F_P: \mathbb{F}_q] = degP = 1$ olduğundan $x = a + y$ olacak şekilde en az bir $a \in \mathbb{F}_q$ ve $y \in P$ elemanı vardır. ω_P, bir $\mathbb{F}_q$ lineer dönüşüm olduğundan $\omega_P(a) = a.\omega_P(1) = 0$ bulunur. Ayrıca $v_P(\omega) \geq -1$ ve $v_P(y) \geq 1$ olduğundan (2.29) gereğince $\omega_P(y) = 0$ olacağından $\omega_P(x) = \omega_P(a) + \omega_P(y) = 0 + 0 = 0$ elde edilir. Böylece (2.29) gereğince $v_P(\omega) \geq 0$ elde edilir.

$\Longleftarrow$: $v_P(\omega) \geq 0$ olsun. $v_P(1) = 0$ olduğundan (2.29) gereğince $\omega_P(1) = 0$ olur.

Şimdi teorem kanıtlanacaktır.

$$\varphi_D: \Omega_F(G-D) \longrightarrow C_\Omega(D,G), \omega \mapsto (\omega_{P_1}(1), \omega_{P_2}(1), \dots, \omega_{P_n}(1)) \tag{3.8}$$

şeklinde tanımlanan dönüşüm göz önüne alınsın. φ_D iyi tanımlı, kapalı, $\mathbb{F}_q$-lineer ve örten bir dönüşümdür.

$Ker\varphi_D = \Omega_F(G)$ olduğunun gösterilmesi için herhangi bir $\omega \in Ker\varphi_D$ elemanı göz önüne alınsın. $\omega \neq 0$ olduğu kabul edilebilir. $\omega \in \Omega_F(G-D)$ olduğundan her $i \in \{1, \dots, n\}$ için $v_{P_i}(\omega) \geq -1$ dir. $\omega \in Ker\varphi_D$ olduğundan her $i \in \{1, \dots, n\}$ için $\omega_{P_i}(1) = 0$ dir. Böylece (3.7) gereğince $v_{P_i}(\omega) \geq 0$ olur. $suppG \cap suppD = \emptyset$ olduğundan $(\omega) \geq G$ elde edilir. Bu nedenle $\omega \in \Omega_F(G)$ olur. Diğer taraftan herhangi bir $\omega \in \Omega_F(G)$ Weil diferansiyeli göz önüne alınsın. $\omega \neq 0$ olduğu kabul edilebilir. $(\omega) \geq G$ olacağından her $i \in \{1, \dots, n\}$ için $v_{P_i}(\omega) \geq 0$ olur. (3.7) gereğince $\omega_{P_i}(1) = 0$ olur. Böylece $\varphi_D(\omega) = (\omega_{P_1}(1), \omega_{P_2}(1), \dots, \omega_{P_n}(1)) = (0,0, \dots,0)$ olacağından $\omega \in Ker\varphi_D$ olur. Sonuç olarak $Ker\varphi_D = \Omega_F(G)$ olduğu gösterilmiş olur.

φ_D dönüşümünün tanımı gereğince $k' = dim\Omega_F(G-D) - dim\Omega_F(G) = i(G-D) - i(G)$ elde edilir.

Şimdi $d' \geq degG - (2g-2)$ olduğu gösterilecektir. Bu eşitsizliğin anlamlı olabilmesi için $C_\Omega(D,G) \neq 0$ olduğu varsayılacaktır. Ağırlığı $m > 0$ olan herhangi bir kod sözcüğü $\varphi_D(\omega) \in C_\Omega(D,G)$ göz önüne alınsın. O zaman belli $i = i_1, i_2, \dots, i_{n-m}$ indisleri için $\omega_{P_i}(1) = 0$ olur. Böylece $(\omega) \geq G - D + \sum_{j=1}^{n-m} P_{i_j}$ olduğundan $\omega \in \Omega_F(G - D + \sum_{j=1}^{n-m} P_{i_j})$ elde edilir. $\omega \neq 0$ olduğundan $dim\Omega_F(G - D + \sum_{j=1}^{n-m} P_{i_j}) = i(G - D + \sum_{j=1}^{n-m} P_{i_j}) \neq 0$ olur. $i(G - D + \sum_{j=1}^{n-m} P_{i_j})$ nın tanımı gereğince $i(G - D + \sum_{j=1}^{n-m} P_{i_j}) \neq 0$ olduğundan $\ell(G - D + \sum_{j=1}^{n-m} P_{i_j}) \neq deg(G - D + \sum_{j=1}^{n-m} P_{i_j}) + 1 - g$ olur. Bu nedenle 2.3.50 Teorem gereğince $deg(G - D + \sum_{j=1}^{n-m} P_{i_j}) \leq 2g - 2$ elde edilir. $deg(G - D + \sum_{j=1}^{n-m} P_{i_j}) = degG - n + n - m$ olduğundan istenilen elde edilir.

Özel olarak $degG > 2g - 2$ ise $k' = i(G-D) \geq n + g - 1 - degG$ olduğu gösterilecektir. $degG > 2g - 2$ olduğundan 2.3.50 Teorem gereğince $\ell(G) = degG + 1 - g$ olur. Böylece $i(G) = \ell(G) - degG + g - 1 = 0$ olacağından $k' = i(G-D) - i(G) = i(G-D)$ olur. $\ell(G-D) \geq 0$ ve $k' = i(G-D) = \ell(G-D) - degG + n + g - 1$ olduğuna dikkat edilirse $k' = i(G-D) \geq n + g - 1 - degG$ olacağından istenilen elde edilir.

Son olarak $2g-2<degG<n$ olduğunda $k'=n+g-1-degG$ olacağı gösterilecektir. $2g-2<degG$ ise $k'=i(G-D)$ olduğu biliniyor. Ayrıca $degG<n$ olduğundan $deg(G-D)=degG-n<0$ olur. Böylece 2.3.17 Sonuç gereğince $\ell(G-D)=0$ olur. $k'=i(G-D)=\ell(G-D)-degG+n+g-1$ olduğuna dikkat edilirse $k'=n+g-1-degG$ olacağından istenilen elde edilir.

Sonuç olarak teorem kanıtlanmış olur [2].

3.2.8 Tanım: $d^*=degG-(2g-2)$ tamsayısına $C_\Omega(D,G)$ kodunun tasarlanmış uzaklığı denir [2].

Şimdi $C_\mathcal{L}(D,G)$ ve $C_\Omega(D,G)$ kodları arasında yakın bir ilişki olduğu gösterilecektir.

3.2.9 Teorem: $C_\mathcal{L}(D,G)$ ve $C_\Omega(D,G)$ kodları birbirinin dualidir. Yani $C_\Omega(D,G)=C_\mathcal{L}(D,G)^\perp$ dir [2].

Şimdi uygun bir $H\in Div(F)$ divizörü ile $C_\Omega(D,G)$ kodunun $C_\mathcal{L}(D,H)$ şeklinde temsil edilebileceği gösterilecektir.

3.2.10 Lemma: $i=1,\dots,n$ için $v_{P_i}(\eta)=-1$ ve $\eta_{P_i}(1)=1$ olacak şekilde bir $\eta\in\Omega_F$ Weil diferansiyeli vardır [2].

3.2.11 Önerme: $i=1,\dots,n$ için $v_{P_i}(\eta)=-1$ ve $\eta_{P_i}(1)=1$ olacak şekildeki $\eta\in\Omega_F$ Weil diferansiyeli göz önüne alınsın. O zaman $H=D-G+(\eta)$ olmak üzere $C_\Omega(D,G)=C_\mathcal{L}(D,H)$ dır [2].

3.2.12 Not: 3.2.11 Önerme kullanılarak 3.2.7 Teorem, 3.2.3 Teorem şeklinde ifade edilebilir. Böylece 3.2.7 Teorem farklı bir şekilde kanıtlanmış olur. Bu nedenle herhangi bir cebirsel geometrik kodun minimum uzaklığı için belirlenen alt sınırlar, kodun temsil seçiminden bağımsızdır [2].

3.3 Rasyonel Cebirsel Geometrik Kodlar

Bu kısımda rasyonel fonksiyon cisminin divizörleri ile ilişkili cebirsel geometrik kodlar incelenecektir. Kod teorisinde kodların bu sınıfı, genelleştirilmiş Reed-Solomon kodları olarak bilinir. Pratikte kullanılan en önemli kodlardan bazıları (BCH ve Goppa kodları gibi) genelleştirilmiş Reed-Solomon kodlarının alt cisim alt kodları olarak temsil edilebilir.

3.3.1 Tanım: $\mathbb{F}_q(z) \,/\, \mathbb{F}_q$ rasyonel fonksiyon cisminin G ve D divizörleri ile ilişkili bir cebirsel geometrik koda $C_{\mathcal{L}}(D,G)$, rasyonel kod denir. Burada G ve D divizörleri Bölüm 3.2 de olduğu gibi tanımlanmaktadır [2].

3.3.2 Teorem: $C_{\mathcal{L}}(D,G)$, $\mathbb{F}_q$ üzerinde parametreleri n, k ve d olan bir rasyonel cebirsel geometrik kod olsun. O zaman aşağıdakiler sağlanır.

a) $n \leq q+1$

b) $k = 0 \Leftrightarrow degG < 0$

c) $k = n \Leftrightarrow degG > n-2$

d) $0 \leq degG \leq n-2$ ise $k = 1 + degG$ ve $d = n - degG$ dır [2].

Şimdi rasyonel cebirsel geometrik kodların üreteç matrisleri incelenecektir. Burada $degG < n$ olduğu varsayılacaktır. Sıradaki teorem kanıtıyla birlikte verilmiştir.

3.3.3 Teorem: $C = C_{\mathcal{L}}(D,G)$, $\mathbb{F}_q$ üzerinde parametreleri n, k ve d olan bir rasyonel cebirsel geometrik kod olsun. O zaman aşağıdakiler sağlanır.

a) $n \leq q$ ise,

$$C = \{\, (v_1.f(\alpha_1), v_2.f(\alpha_2), \dots, v_n.f(\alpha_n)) \mid f \in \mathbb{F}_q[z] \text{ ve } degf \leq k-1 \,\} \qquad (3.9)$$

olacak şekilde ikişer ikişer farklı $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ ve $v_1, v_2, \dots, v_n \in \mathbb{F}_q^{\times}$ (farklı olmaları gerekmez) elemanları vardır. Ayrıca,

$$M = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_n v_n \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \cdots & \alpha_n^2 v_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \cdots & \alpha_n^{k-1} v_n \end{pmatrix} \tag{3.10}$$

matrisi C kodu için bir üreteç matrisidir.

b) $n = q + 1$ ise $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_{n-1}\}$ ve $v_1, v_2, \dots, v_{n-1} \in \mathbb{F}_q^{\times}$ olmak üzere,

$$M = \begin{pmatrix} v_1 & v_2 & \cdots & v_{n-1} & 0 \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_{n-1} v_{n-1} & 0 \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \cdots & \alpha_{n-1}^2 v_{n-1} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \cdots & \alpha_{n-1}^{k-1} v_{n-1} & 1 \end{pmatrix} \tag{3.11}$$

matrisi C kodu için bir üreteç matrisidir [2].

Kanıt:

a) $D = P_1 + P_2 + \cdots + P_n$ olsun. 2.2.1 Önerme ve 2.2.5 Önerme gereğince rasyonel fonksiyon cisminin $q + 1$ tane birinci dereceden place'i olduğuna dikkat edilirse, $P \notin suppD$ olacak şekilde birinci dereceden en az bir P place'i vardır.

Herhangi bir $Q \in \{P_1, P_2, \dots, P_n\}$ place'i göz önüne alınsın. $deg(Q - P) = 0 \geq -1$ olduğundan 2.3.50 Teorem gereğince $\ell(Q - P) = deg(Q - P) + 1 - g$ olur. Rasyonel fonksiyon cisminin cinsi sıfır olduğundan $\ell(Q - P) = deg(Q - P) + 1 = 1$ elde edilir. Böylece 2.3.18 Sonuç gereğince $Q - P$ esas divizördür.

O halde en az bir $z \in F$, $z \neq 0$ elemanı için $Q - P = (z)$ olur. $v_P(z) = -1$, $v_Q(z) = 1$ ve her $i \in \{1, \dots, n\}$ için $P_i \neq Q$ olmak üzere $v_{P_i}(z) = 0$ olduğundan $z \in F$ elemanı, rasyonel fonksiyon cisminin $\mathbb{F}_q$ üzerinde bir üretecidir. Burada P, $z \in F$ elemanının kutup divizörü olduğundan $P = P_\infty$ yazılacaktır.

Şimdi $degG = k - 1 \geq 0$ olduğunun varsayılabileceği gösterilecektir. $k = 0$ olduğunda teoremin kanıtı aşikar olacağından $k > 0$ olduğu varsayılacaktır. Bu nedenle 3.3.2 Teorem b) gereğince $degG \geq 0$ olur. $degG < n$ olduğu biliniyor. $0 \leq degG \leq n - 2$ ise 3.3.2 Teorem d) gereğince $degG = k - 1 \geq 0$ olur. $degG = n - 1$ olduğu durumda

ise 3.3.2 Teorem c) gereğince $k = n$ olacağından yine $degG = k - 1 \geq 0$ elde edilir. Bu nedenle $degG = k - 1 \geq 0$ olduğunun varsayılabileceği gösterilmiş olur.

Böylece $deg((k-1).P_\infty - G) = 0$ olur. $deg((k-1).P_\infty - G) \geq -1$ olduğundan 2.3.50 Teorem gereğince $\ell((k-1).P_\infty - G) = deg((k-1).P_\infty - G) + 1 - g$ olur. Rasyonel fonksiyon cisminin cinsi sıfır olduğundan $\ell((k-1).P_\infty - G) = deg((k-1).P_\infty - G) + 1 = 1$ elde edilir. Böylece 2.3.18 Sonuç gereğince $(k-1).P_\infty - G$ esas divizördür. O halde $(k-1).P_\infty - G = (u)$ olacak şekilde en az bir $u \in F, u \neq 0$ elemanı vardır.

$\mathcal{L}(G)$ nin tanımı gereğince $u, z.u, \dots, z^{k-1}.u \in \mathcal{L}(G)$ olur. Ayrıca $u, z.u, \dots, z^{k-1}.u$ elemanları $\mathbb{F}_q$ üzerinde lineer bağımsızdır.

$degG = k - 1 \geq 0$ olduğundan 2.3.50 Teorem gereğince $\ell(G) = degG + 1 - g$ elde edilir. $\mathbb{F}_q(z) / \mathbb{F}_q$ rasyonel fonksiyon cisminin cinsinin sıfır olduğuna dikkat edilirse $\ell(G) = degG + 1 = k - 1 + 1 = k$ olur. Böylece $\{u, z.u, \dots, z^{k-1}.u\}$ kümesi, $\mathcal{L}(G)$ Riemann-Roch uzayının $\mathbb{F}_q$ üzerinde bir tabanıdır. Bu sebeple $\mathcal{L}(G) = \{ u.f(z) \mid f \in \mathbb{F}_q[z] \text{ ve } degf \leq k-1 \}$ olur.

$i = 1, \dots, n$ için $\alpha_i = z(P_i)$ ve $v_i = u(P_i)$ denilsin. $z \in F$ elemanı, rasyonel fonksiyon cisminin $\mathbb{F}_q$ üzerinde bir üreteç elemanı olduğundan $\alpha_1, \alpha_2, \dots, \alpha_n$ elemanları ikili olarak farklıdır. Ayrıca her $i \in \{1, \dots, n\}$ için $v_{P_i}(u) = 0$ olduğundan $v_i \in \mathbb{F}_q^\times$ olur.

Böylece $(u.f(z))(P_i) = u(P_i).f(z(P_i)) = v_i.f(\alpha_i)$ olacağından $C_{\mathcal{L}}(D, G) = \{ (v_1.f(\alpha_1), v_2.f(\alpha_2), \dots, v_n.f(\alpha_n)) \mid f \in \mathbb{F}_q[z] \text{ ve } degf \leq k-1 \}$ olur.

Ayrıca herhangi bir $j \in \{1, \dots, k-1\}$ için $z^j.u \in \mathcal{L}(G)$ elemanına karşılık gelen kod sözcüğü $(\alpha_1^j.v_1, \alpha_2^j.v_2, \dots, \alpha_n^j.v_n)$ olduğundan, (3.10) deki matris C kodu için bir üreteç matrisidir.

Sonuç olarak a) kanıtlanmış olur.

b) $D = P_1 + P_2 + \cdots + P_n$ olsun. $n = q + 1$ olduğundan kutbu $P_n = P_\infty$ olacak şekilde en az bir $z \in F$, $z \neq 0$ elemanı seçilebilir. a) da yapıldığı gibi $degG = k - 1 \geq 0$ olduğu varsayılabilir.

O halde $(k-1).P_\infty - G = (u)$ olacak şekilde en az bir $u \in F$, $u \neq 0$ elemanı vardır.

$\mathcal{L}(G)$ nin tanımı gereğince $u, z.u, \dots, z^{k-1}.u \in \mathcal{L}(G)$ olur. Ayrıca $u, z.u, \dots, z^{k-1}.u$ elemanları $\mathbb{F}_q$ üzerinde lineer bağımsızdır.

$degG = k - 1 \geq 0$ olduğundan 2.3.50 Teorem gereğince $\ell(G) = degG + 1 - g$ elde edilir. $\mathbb{F}_q(z) / \mathbb{F}_q$ rasyonel fonksiyon cisminin cinsinin sıfır olduğuna dikkat edilirse $\ell(G) = degG + 1 = k - 1 + 1 = k$ olur. Böylece $\{u, z.u, \dots, z^{k-1}.u\}$ kümesi, $\mathcal{L}(G)$ Riemann-Roch uzayının $\mathbb{F}_q$ üzerinde bir tabanıdır.

Her $1 \leq i \leq n - 1 = q$ için $\alpha_i = z(P_i)$ ve $v_i = u(P_i)$ denilsin. $z \in F$ elemanı, rasyonel fonksiyon cisminin $\mathbb{F}_q$ üzerinde bir üreteç elemanı olduğundan $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ elemanları ikişer ikişer farklıdır. Bu sebeple $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_{n-1}\}$ olur. Ayrıca her $i \in \{1, \dots, n-1\}$ için $v_{P_i}(u) = 0$ olduğundan $v_i \in \mathbb{F}_q^\times$ olur.

$0 \leq j \leq k - 2$ için $v_{P_\infty}(z^j.u) = j.v_{P_\infty}(z) + v_{P_\infty}(u) = j.(-1) + (k-1) = k - j - 1 > 0$ olduğundan $z^j.u \in \mathcal{L}(G)$ elemanına karşılık gelen kod sözcüğü $(\alpha_1^j.v_1, \alpha_2^j.v_2, \dots, \alpha_{n-1}^j.v_{n-1}, 0)$ olur. $j = k - 1$ için $v_{P_\infty}(z^j.u) = j.v_{P_\infty}(z) + v_{P_\infty}(u) = j.(-1) + (k-1) = 0$ olduğundan en az bir $\gamma \in \mathbb{F}_q$, $\gamma \neq 0$ elemanı için $(z^j.u)(P_\infty) = \gamma$ olur. Teoremin kanıtında $u \in F$ elemanı yerine $\gamma^{-1}.u \in F$ elemanı alınırsa $(z^j.\gamma^{-1}.u)(P_\infty) = \gamma^{-1}(P_\infty).(z^j.u)(P_\infty) = \gamma^{-1}.\gamma = 1$ olacağından $z^j.u \in \mathcal{L}(G)$ elemanına karşılık gelen kod sözcüğü $(\alpha_1^{k-1}.v_1, \alpha_2^{k-1}.v_2, \dots, \alpha_{n-1}^{k-1}.v_{n-1}, 1)$ olur. Böylece C kodunun üreteç matrisi, (3.11) deki gibi olur [2].

Bu durumda teoremin kanıtı tamamlanmış olur.

3.3.4 Tanım: $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ ikişer ikişer farklı elemanlar olmak üzere $\alpha = \{\alpha_1, \dots, \alpha_n\}$ ve $v_1, v_2, \dots, v_n \in \mathbb{F}_q^\times$ olmak üzere (farklı olmaları gerekmez) $v = \{v_1, \dots, v_n\}$ olarak tanımlansın. Herhangi bir $0 \leq k \leq n$ tamsayısı için, $\mathbb{F}_q$ üzerinde

$GRS_k(\alpha, v) = \{ (v_1.f(\alpha_1), v_2.f(\alpha_2), \dots, v_n.f(\alpha_n)) \mid f(z) \in \mathbb{F}_q[z]$ ve $degf \leq k-1 \}$ şeklinde tanımlı koda bir genelleştirilmiş Reed-Solomon kodu denir [2].

$GRS_k(\alpha, v)$ bir $[n, k]$ koddur.

$n = q-1$ ve $\beta \in \mathbb{F}_q$ elemanı, çarpımsal $\mathbb{F}_q^{\times}$ grubunun ilkel bir elemanı olmak üzere, $\alpha = \{\beta, \beta^2, \dots, \beta^n\}$ ve $v = \{1, \dots, 1\}$ olması durumunda ise $GRS_k(\alpha, v)$, bir Reed-Solomon kodudur.

3.3.3 Teorem a) gereğince $\mathbb{F}_q$ üzerinde, uzunluğu $n \leq q$ olacak şekildeki her rasyonel cebirsel geometrik kod bir genelleştirilmiş Reed-Solomon kodudur. Şimdi her genelleştirilmiş Reed-Solomon kodunun bir rasyonel cebirsel geometrik kod olduğu gösterilecektir.

3.3.5 Teorem: Her genelleştirilmiş Reed-Solomon kodu $GRS_k(\alpha, v)$, bir rasyonel cebirsel geometrik kod olarak temsil edilebilir [2].

Kanıt:

Herhangi bir genelleştirilmiş Reed-Solomon kodu $GRS_k(\alpha, v)$ ve $\mathbb{F}_q(z) \,/\, \mathbb{F}_q$ rasyonel fonksiyon cismi göz önüne alınsın. $z \in \mathbb{F}_q(z)$ elemanının kutbu P_∞ ve $i = 1, \dots, n$ için $z - \alpha_i \in \mathbb{F}_q(z)$ elemanının kökü P_i ile gösterilsin.

Zayıf yaklaşım teoremi (2.1.20 Teorem) gereğince $i = 1, \dots, n$ için $u(P_i) = v_i$ olacak şekilde en az bir $u \in F$ elemanı vardır.

$D = P_1 + P_2 + \cdots + P_n$ ve $G = (k-1).P_\infty - (u)$ denilsin. 3.3.3 Teorem a) nın kanıtı gereğince $C_{\mathcal{L}}(D, G) = GRS_k(\alpha, v)$ olacağından istenilen elde edilir [2].

Benzer şekilde, $\mathbb{F}_q$ üzerinde uzunluğu $n = q+1$ ve üreteç matrisi (3.11) şeklinde olan bir kodun da, rasyonel cebirsel geometrik kod olarak temsil edilebileceği gösterilebilir.

Bundan sonraki kısımda BCH ve Goppa kodlarının, rasyonel cebirsel geometrik kodlar tarafından temsil edilebileceği gösterilecektir. Bunun için önce aşağıdaki tanım verilecektir.

3.3.6 Tanım: $\mathbb{F}_q$ cisminin bir cisim genişlemesi $\mathbb{F}_{q^m}$ ve $\mathbb{F}_{q^m}$ üzerinde uzunluğu n olan bir C kodu göz önüne alınsın. O zaman $C|_{\mathbb{F}_q} = C \cap {\mathbb{F}_q}^n$ kümesi $\mathbb{F}_q$ üzerinde bir koddur. Bu koda, C kodunun alt cisim alt kodu veya C kodunun $\mathbb{F}_q$ ya kısıtlanışı denir [2].

$dimC|_{\mathbb{F}_q} \leq dimC$ olduğuna dikkat edilmelidir.

3.3.7 Tanım: $n|(q^m - 1)$ ve $\beta \in \mathbb{F}_{q^m}$ elemanı, birimin n inci ilkel kökü olsun. $l \in \mathbb{Z}$ ve $\delta \in \mathbb{Z}$, $\delta \geq 2$ olmak üzere $\mathbb{F}_{q^m}$ üzerinde üreteç matrisi,

$$H = \begin{pmatrix} 1 & \beta^{l} & \beta^{2l} & \dots & \beta^{(n-1)l} \\ 1 & \beta^{l+1} & \beta^{2(l+1)} & \dots & \beta^{(n-1)(l+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{l+\delta-2} & \beta^{2(l+\delta-2)} & \dots & \beta^{(n-1)(l+\delta-2)} \end{pmatrix} \tag{3.12}$$

olan bir $C(n, l, \delta)$ kodu tanımlansın. $C = C(n, l, \delta)^{\perp}|_{\mathbb{F}_q}$ koduna tasarlanmış uzaklığı δ olan bir BCH kodu denir [2].

Ayrıca herhangi bir $c \in {\mathbb{F}_q}^n$ vektörünün transpozu c^t ile gösterilmek üzere $C = \{ c \in {\mathbb{F}_q}^n \mid H.c^t = 0 \}$ şeklinde yazılabilir.

3.3.8 Lemma: $\mathbb{F}_q(z) \,/\, \mathbb{F}_q$ rasyonel fonksiyon cismi ve n farklı $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ elemanı göz önüne alınsın. $i = 1, \dots, n$ için $z - \alpha_i \in \mathbb{F}_q(z)$ elemanının kökü $P_i \in \mathcal{P}_{\mathbb{F}_q(z)}$ place'i ile gösterilsin ve $h(z) = \prod_{i=1}^{n}(z - \alpha_i)$ olsun. Herhangi bir $y \in \mathbb{F}_q(z)$ elemanı $i = 1, \dots, n$ için $y(P_i) = 1$ özelliğini sağlasın. O zaman $\mathbb{F}_q(z) \,/\, \mathbb{F}_q$ rasyonel fonksiyon cisminin $i = 1, \dots, n$ için $v_{P_i}(\omega) = -1$, $\omega_{P_i}(1) = 1$ ve $(\omega) = (y) + (h'(z)) - (h(z)) - 2.P_\infty$ özelliğine sahip bir Weil diferansiyeli vardır. Burada $h'(z) \in \mathbb{F}_q[z]$ polinomu $h(z)$ polinomunun türevini ifade etmektedir [2].

Sıradaki önerme kanıtıyla birlikte verilmiştir.

3.3.9 Önerme: $n|(q^m - 1)$ ve $\beta \in \mathbb{F}_{q^m}$ elemanı, birimin n inci ilkel kökü olsun ve $\mathbb{F}_{q^m}(z) \,/\, \mathbb{F}_{q^m}$ rasyonel fonksiyon cismi göz önüne alınsın. $z \in \mathbb{F}_{q^m}(z)$ elemanının kutbu P_∞, kökü P_0 ile gösterilsin. $i = 1, \dots, n$ için $z - \beta^{i-1} \in \mathbb{F}_{q^m}(z)$ elemanının kökü P_i

ile gösterilsin ve $D_\beta = P_1 + P_2 + \cdots + P_n$ olsun. Herhangi iki $a, b \in \mathbb{Z}$ tamsayısı için $0 \leq a + b \leq n - 2$ özelliği sağlansın.

a) $l = -a$ ve $\delta = a + b + 2$ olmak üzere $C_{\mathcal{L}}(D_\beta, a.P_0 + b.P_\infty) = C(n, l, \delta)$ olur.

b) $r = -(a + 1)$ ve $s = n - b - 1$ olmak üzere,

$$C_{\mathcal{L}}(D_\beta, a.P_0 + b.P_\infty)^\perp = C_{\mathcal{L}}(D_\beta, r.P_0 + s.P_\infty) \tag{3.13}$$

olur. Böylece $C(n, l, \delta)^\perp|_{\mathbb{F}_q}$ BCH kodu, $r = l - 1$ ve $s = n + 1 - \delta - l$ olmak üzere $C_{\mathcal{L}}(D_\beta, r.P_0 + s.P_\infty)$ kodunun $\mathbb{F}_q$ ya bir kısıtlanışıdır [2].

Kanıt:

a) $0 \leq a + b \leq n - 2$ olmak üzere $C_{\mathcal{L}}(D_\beta, a.P_0 + b.P_\infty)$ kodu göz önüne alınsın. $\mathcal{L}(a.P_0 + b.P_\infty)$ nin tanımı gereğince, $0 \leq j \leq a + b$ olmak üzere $z^{-a}.z^j \in \mathcal{L}(a.P_0 + b.P_\infty)$ olur. Ayrıca $0 \leq j \leq a + b$ olmak üzere $z^{-a}.z^j \in \mathcal{L}(a.P_0 + b.P_\infty)$ elemanları $\mathbb{F}_{q^m}$ üzerinde lineer bağımsızdır.

$deg(a.P_0 + b.P_\infty) = a + b \geq 0$ olduğundan 2.3.50 Teorem gereğince $\ell(a.P_0 + b.P_\infty) = deg(a.P_0 + b.P_\infty) + 1 - g$ elde edilir. $\mathbb{F}_{q^m}(z) / \mathbb{F}_{q^m}$ rasyonel fonksiyon cisminin cinsinin sıfır olduğuna dikkat edilirse $\ell(a.P_0 + b.P_\infty) = deg(a.P_0 + b.P_\infty) + 1 = a + b + 1$ olur. Böylece $0 \leq j \leq a + b$ olmak üzere $z^{-a}.z^j$ elemanları, $\mathcal{L}(a.P_0 + b.P_\infty)$ Riemann-Roch uzayının $\mathbb{F}_{q^m}$ üzerinde bir tabanıdır.

Böylece $C_{\mathcal{L}}(D_\beta, a.P_0 + b.P_\infty)$ rasyonel cebirsel geometrik kodunun üreteç matrisi,

$$H = \begin{pmatrix} z^{-a}(P_1) & z^{-a}(P_2) & z^{-a}(P_3) & \cdots & z^{-a}(P_n) \\ z^{-a+1}(P_1) & z^{-a+1}(P_2) & z^{-a+1}(P_3) & \cdots & z^{-a+1}(P_n) \\ \vdots & \vdots & \vdots & & \vdots \\ z^{b}(P_1) & z^{b}(P_2) & z^{b}(P_3) & \cdots & z^{b}(P_n) \end{pmatrix} \tag{3.14}$$

şeklinde olur.

Böylece (3.14) de verilen matris,

$$H = \begin{pmatrix} 1 & \beta^{-a} & \beta^{2.(-a)} & \dots & \beta^{(n-1).(-a)} \\ 1 & \beta^{-a+1} & \beta^{2.(-a+1)} & \dots & \beta^{(n-1).(-a+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{b} & \beta^{2.b} & \dots & \beta^{(n-1).b} \end{pmatrix} \tag{3.15}$$

şeklinde yazılabilir. Gerekli düzenlemeler yapılırsa,

$$H = \begin{pmatrix} 1 & \beta^{-a} & \beta^{-2a} & \dots & (\beta^{(n-1)})^{-a} \\ 1 & \beta^{-a+1} & \beta^{-2a+2} & \dots & (\beta^{(n-1)})^{-a+1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{-a+(a+b)} & \beta^{-2a+2(a+b)} & \dots & (\beta^{(n-1)})^{-a+(a+b)} \end{pmatrix} \tag{3.16}$$

elde edilir. $l = -a$ ve $\delta = a + b + 2$ alınırsa, (3.12) da verilen matris elde edileceğinden $C_{\mathcal{L}}(D_\beta, a.P_0 + b.P_\infty) = C(n, l, \delta)$ olur.

Böylece a) kanıtlanmış olur.

b) $y = z^{-n}$ ve $h(z) = \prod_{i=1}^{n}(z - \beta^{i-1}) = z^n - 1$ olsun. 3.3.8 Lemma da verilen $(\omega) = (y) + (h'(z)) - (h(z)) - 2.P_\infty$ özelliğine sahip Weil diferansiyeli göz önüne alınsın.

3.3.8 Lemma gereğince $i = 1, \dots, n$ için $v_{P_i}(\omega) = -1$ ve $\omega_{P_i}(1) = 1$ olduğu biliniyor. Bu nedenle $H = D_\beta - (a.P_0 + b.P_\infty) + (\omega)$ olmak üzere, 3.2.11 Önerme ve 3.2.9 Teorem gereğince $C_{\mathcal{L}}(D_\beta, a.P_0 + b.P_\infty)^{\perp} = C_{\mathcal{L}}(D_\beta, H)$ yazılabilir.

$H = D_\beta - (a.P_0 + b.P_\infty) + (\omega) = D_\beta - (a.P_0 + b.P_\infty) + (z^{-n}) + (h'(z)) - (h(z)) - 2.P_\infty = D_\beta - (a.P_0 + b.P_\infty) + n.(P_\infty - P_0) + (n-1).(P_0 - P_\infty) - (D_\beta - n.P_\infty) - 2.P_\infty = (-a-1).P_0 + (n-b-1).P_\infty$ olacağından, $r = -(a+1)$ ve $s = n - b - 1$ olmak üzere $C_{\mathcal{L}}(D_\beta, a.P_0 + b.P_\infty)^{\perp} = C_{\mathcal{L}}(D_\beta, r.P_0 + s.P_\infty)$ olur.

Ayrıca a) gereğince $l = -a$ ve $\delta = a + b + 2$ olduğuna dikkat edilirse, $C(n, l, \delta)^{\perp}|_{\mathbb{F}_q}$ BCH kodunun, $r = l - 1$ ve $s = n + 1 - \delta - l$ olmak üzere $C_{\mathcal{L}}(D_\beta, r.P_0 + s.P_\infty)$ kodunun $\mathbb{F}_q$ ya bir kısıtlanışı olduğu görülmüş olur.

Böylece 3.3.9 Önerme kanıtlanmış olur [2].

Şimdi Goppa kodları tanıtılacaktır.

3.3.10 Tanım: $L = \{\alpha_1, \dots, \alpha_n\} \in \mathbb{F}_{q^m}$ olsun. $1 \leq t \leq n-1$ olmak üzere derecesi t ve her $\alpha_i \in L$ için $g(\alpha_i) \neq 0$ olacak şekilde bir $g(z) \in \mathbb{F}_{q^m}[z]$ polinomu göz önüne alınsın. $\mathbb{F}_{q^m}$ üzerinde üreteç matrisi,

$$H = \begin{pmatrix} g(\alpha_1)^{-1} & g(\alpha_2)^{-1} & \cdots & g(\alpha_n)^{-1} \\ \alpha_1 . g(\alpha_1)^{-1} & \alpha_2 . g(\alpha_2)^{-1} & \cdots & \alpha_n . g(\alpha_n)^{-1} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{t-1} . g(\alpha_1)^{-1} & \alpha_2^{t-1} . g(\alpha_2)^{-1} & \cdots & \alpha_n^{t-1} . g(\alpha_n)^{-1} \end{pmatrix} \tag{3.17}$$

olan bir $C(L, g(z))$ kodu tanımlansın. $\Gamma(L, g(z)) = C(L, g(z))^{\perp}|_{\mathbb{F}_q}$ koduna, Goppa polinomu $g(z)$ olan bir Goppa kodu denir [2].

Ayrıca herhangi bir $c \in \mathbb{F}_q{}^n$ vektörünün transpozu c^t ile gösterilmek üzere $\Gamma(L, g(z)) = \{\, c \in \mathbb{F}_q{}^n \mid H . c^t = 0 \,\}$ şeklinde yazılabilir.

Şimdi Goppa kodlarının, rasyonel cebirsel geometrik kodlarla ilişkisi incelenecektir. Bu ilişkinin daha iyi anlaşılabilmesi için sıradaki önerme kanıtı ile birlikte verilmiştir.

3.3.11 Önerme: $\mathbb{F}_{q^m}(z) \,/\, \mathbb{F}_{q^m}$ rasyonel fonksiyon cismi göz önüne alınsın. $z \in \mathbb{F}_{q^m}(z)$ elemanının kutbu P_∞ ile gösterilsin. $i = 1, \dots, n$ için $\alpha_i \in L$ olmak üzere, $z - \alpha_i \in \mathbb{F}_{q^m}(z)$ elemanının kökü P_i ile gösterilsin ve $D_L = P_1 + P_2 + \cdots + P_n$ olsun. $g(z) \in \mathbb{F}_{q^m}(z)$ elemanının kök divizörü G_0 ile gösterilsin. O zaman $h(z) = \prod_{\alpha_i \in L}(z - \alpha_i)$ ve $A = (h'(z)) + (n-1).P_\infty$ olmak üzere,

$$C(L, g(z)) = C_{\mathcal{L}}(D_L, G_0 - P_\infty) = C_{\mathcal{L}}(D_L, A - G_0)^{\perp} \tag{3.18}$$

ve

$$\Gamma(L, g(z)) = C_{\mathcal{L}}(D_L, G_0 - P_\infty)^{\perp}|_{\mathbb{F}_q} = C_{\mathcal{L}}(D_L, A - G_0)|_{\mathbb{F}_q} \tag{3.19}$$

olur [2].

Kanıt:

Sadece $C(L, g(z)) = C_{\mathcal{L}}(D_L, G_0 - P_\infty) = C_{\mathcal{L}}(D_L, A - G_0)^{\perp}$ olduğunu göstermek yeterli olacaktır.

Her $j \in \{0, \dots, t-1\}$ için $(z^j.g(z)^{-1}) = j.(P_0 - P_\infty) - (G_0 - t.P_\infty) \geq -G_0 + P_\infty$ olduğundan, $\mathcal{L}(G_0 - P_\infty)$ nin tanımı gereğince $z^j.g(z)^{-1} \in \mathcal{L}(G_0 - P_\infty)$ olur. Ayrıca $0 \leq j \leq t-1$ olmak üzere $z^j.g(z)^{-1} \in \mathcal{L}(G_0 - P_\infty)$ elemanları $\mathbb{F}_{q^m}$ üzerinde lineer bağımsızdır.

$g(z) \in \mathbb{F}_{q^m}(z)$ elemanı $\mathbb{F}_{q^m}$ üzerinde transandant olduğundan 2.1.19 Sonuç gereğince en az bir köke ve kutba sahiptir. Böylece $degG_0 > 0$ olacağından $deg(G_0 - P_\infty) \geq 0$ olur. 2.3.50 Teorem gereğince $\ell(G_0 - P_\infty) = deg(G_0 - P_\infty) + 1 - g$ elde edilir. $\mathbb{F}_{q^m}(z) \,/\, \mathbb{F}_{q^m}$ rasyonel fonksiyon cisminin cinsinin sıfır olduğuna dikkat edilirse $\ell(G_0 - P_\infty) = deg(G_0 - P_\infty) + 1 = degG_0$ olur.

2.3.15 Önerme gereğince $g(z) \in \mathbb{F}_{q^m}(z)$ elemanının esas divizörünün derecesi sıfır olduğundan $deg(G_0 - t.P_\infty) = 0$ dır. Bu sebeple $degG_0 = t$ olacağından $\ell(G_0 - P_\infty) = t$ bulunur.

Böylece $0 \leq j \leq t-1$ olmak üzere $z^j.g(z)^{-1}$ elemanları, $\mathcal{L}(G_0 - P_\infty)$ Riemann-Roch uzayının $\mathbb{F}_{q^m}$ üzerinde bir tabanıdır. Bu sebeple (3.17) de verilen matris, $C_{\mathcal{L}}(D_L, G_0 - P_\infty)$ kodunun üreteç matrisi olacağından $C(L, g(z)) = C_{\mathcal{L}}(D_L, G_0 - P_\infty)$ elde edilir.

Şimdi $C_{\mathcal{L}}(D_L, G_0 - P_\infty) = C_{\mathcal{L}}(D_L, A - G_0)^\perp$ olduğu gösterilecektir. 3.3.8 Lemma da verilen $(\omega) = (h'(z)) - (h(z)) - 2.P_\infty$ özelliğine sahip Weil diferansiyeli göz önüne alınsın. Burada $i = 1, \dots, n$ için $y(P_i) = 1$ özelliğini sağlayan $y \in \mathbb{F}_{q^m}(z)$ elemanı $y = 1$ olarak alınmıştır.

3.3.8 Lemma gereğince $i = 1, \dots, n$ için $v_{P_i}(\omega) = -1$ ve $\omega_{P_i}(1) = 1$ olduğu biliniyor. Bu nedenle $H = D_L - (G_0 - P_\infty) + (\omega)$ olmak üzere, 3.2.11 Önerme ve 3.2.9 Teorem gereğince $C_{\mathcal{L}}(D_L, G_0 - P_\infty)^\perp = C_{\mathcal{L}}(D_L, H)$ yazılabilir.

$H = D_L - (G_0 - P_\infty) + (\omega) = D_L - (G_0 - P_\infty) + (h'(z)) - (h(z)) - 2.P_\infty = D_L - G_0 + P_\infty + A - (n-1).P_\infty - (D_L - n.P_\infty) - 2.P_\infty = A - G_0$ olduğundan kanıt tamamlanmış olur [2].

3.3.9 Önerme ve 3.3.11 Önerme yardımıyla, rasyonel cebirsel geometrik kodların minimum uzaklığı için elde edilen sonuçlar, BCH ve Goppa kodlarının minimum uzaklığı için kullanılabilir. Sıradaki sonuç kanıtı ile birlikte verilmiştir.

3.3.12 Sonuç:

a) (BCH sınırı) Tasarlanmış uzaklığı δ olan bir BCH kodunun minimum uzaklığı en az δ dır.

b) (Goppa Sınırı) Bir Goppa kodunun $\Gamma(L, g(z))$ minimum uzaklığı en az $1 + degg(z)$ dir [2].

Kanıt:

a) 3.3.9 Önerme de verilen notasyon göz önüne alınsın. $r = l - 1$ ve $s = n + 1 - \delta - l$ olmak üzere herhangi bir $C_{\mathcal{L}}(D_\beta, r.P_0 + s.P_\infty)|_{\mathbb{F}_q}$ BCH kodu verilsin.

$C_{\mathcal{L}}(D_\beta, r.P_0 + s.P_\infty)$ kodunun minimum uzaklığı bulunacaktır. $deg(r.P_0 + s.P_\infty) = r + s = l - 1 + n + 1 - \delta - l = n - \delta$ olur. 3.3.2 Teorem b) gereğince $k = 0 \Leftrightarrow deg(r.P_0 + s.P_\infty) < 0$ olduğundan $deg(r.P_0 + s.P_\infty) \geq 0$ olduğu varsayılabilir. 3.3.7 Tanım gereğince $\delta \in \mathbb{Z}$, $\delta \geq 2$ olduğundan $0 \leq n - \delta \leq n - 2$ olur. Böylece 3.3.2 Teorem d) gereğince $d = n - deg(r.P_0 + s.P_\infty) = n - n + \delta = \delta$ olur.

Bu durumda $C_{\mathcal{L}}(D_\beta, r.P_0 + s.P_\infty)|_{\mathbb{F}_q}$ kodunun minimum uzaklığı δ değerinden küçük olamayacağından istenilen elde edilir.

b) 3.3.11 Önerme de verilen notasyon göz önüne alınsın. $h(z) = \prod_{\alpha_i \in L}(z - \alpha_i)$ ve $A = (h'(z)) + (n-1).P_\infty$ olmak üzere herhangi bir $C_{\mathcal{L}}(D_L, A - G_0)|_{\mathbb{F}_q}$ Goppa kodu verilsin.

$C_{\mathcal{L}}(D_L, A - G_0)$ kodunun minimum uzaklığı bulunacaktır. $deg(A - G_0) = (n-1) - t = (n-1) - degg(z)$ dir. 3.3.2 Teorem b) gereğince $k = 0 \Leftrightarrow deg(A - G_0) < 0$ olduğundan $deg(A - G_0) \geq 0$ olduğu varsayılabilir. $1 \leq degg(z)$ olduğundan olduğundan $0 \leq (n-1) - degg(z) \leq n - 2$ olur. Böylece 3.3.2 Teorem d) gereğince $d = n - deg(A - G_0) = n - ((n-1) - degg(z)) = 1 + degg(z)$ olur.

Bu durumda $C_{\mathcal{L}}(D_L, A - G_0)|_{\mathbb{F}_q}$ kodunun minimum uzaklığı $1 + degg(z)$ değerinden küçük olamayacağından istenilen elde edilir [2].

3.3.13 Not: Cebirsel açıdan rasyonel fonksiyon cismi, bir cebirsel fonksiyon cisminin en açık örneğidir. Buna rağmen bu kısımda, rasyonel fonksiyon cisminin divizörleri ile ilişkili rasyonel cebirsel geometrik kodların, halihazırda bilininen ve yaygın olarak kullanılan kodları temsil edebildiği görülmüştür. Bu da rasyonel olmayan fonksiyon cisimlerinin divizörleri ile ilişkili kodların araştırılmasını cazip kılmaktadır [2].

3.4 Tsfasman-Vladut-Zink Teoremi

3.4.1 Tanım: C, $\mathbb{F}_q$ üzerinde bir $[n, k, d]$ kod olsun. $R = R(C) = k \,/\, n$ sayısına C kodunun haberleşme oranı denir. $\delta = \delta(C) = d \,/\, n$ sayısına da C kodunun göreceli minimum uzaklığı denir [2].

$V_q = \{\, (\delta(C), R(C)) \in [0,1]^2 \mid C, \mathbb{F}_q$ üzerinde bir koddur $\}$ kümesi tanımlansın. V_q kümesinin limit noktalarının kümesi $U_q \subseteq [0,1]^2$ ile gösterilsin.

3.4.2 Önerme: $U_q = \{\, (\delta, R) \in [0,1]^2 \mid 0 \leq \delta \leq 1$ ve $0 \leq R \leq \alpha_q(\delta)\,\}$ olacak şekilde sürekli bir $\alpha_q : [0,1] \longrightarrow [0,1]$ fonksiyon vardır. $\alpha_q(0) = 1,\ 1 - q^{-1} \leq \delta \leq 1$ olmak üzere $\alpha_q(\delta) = 0$ dır. Ayrıca α_q fonksiyonu $[0, 1 - q^{-1}]$ aralığında artmayandır [2, 7].

$0 < \delta < 1 - q^{-1}$ için $\alpha_q(\delta)$ nin değeri tam olarak bilinmemektedir. Ancak birkaç üst ve alt sınır mevcuttur. Bu kısımda, bu sınırlardan birkaçı verilecektir.

3.4.3 Tanım: $H_q : [0, 1 - q^{-1}] \longrightarrow \mathbb{R}$, $H_q(0) = 0$ ve $0 < x \leq 1 - q^{-1}$ için $H_q(x) = x.\log_q(q-1) - x.\log_q(x) - (1-x).\log_q(1-x)$ şeklinde tanımlanan fonksiyona q-entropi fonksiyonu denir [2].

3.4.4 Önerme: $\alpha_q(\delta)$ için aşağıdaki üst sınırlar sağlanır:

a) (Plotkin Sınırı) $0 \leq \delta \leq 1 - q^{-1}$ için $\alpha_q(\delta) \leq 1 - q.(q-1)^{-1}.\delta$ dır.

b) (Hamming Sınırı) $0 \leq \delta \leq 1$ için $\alpha_q(\delta) \leq 1 - H_q(\delta \,/\, 2)$ dır.

c) (Bassalygo-Elias Sınırı) $0 \leq \delta \leq \theta = 1 - q^{-1}$ için $\alpha_q(\delta) \leq 1 - H_q\left(\theta - \sqrt{\theta.(\theta - \delta)}\right)$ [2].

Verilen bu üç sınırdan, Bassalygo-Elias Sınırı daima en iyisidir.

$\alpha_q(\delta)$ için aşikar olmayan her alt sınır, $\mathbb{F}_q$ cismi üzerinde iyi parametrelere sahip kodların varlığını garantilemektedir. Bu nedenle $\alpha_q(\delta)$ için, üst sınırlara oranla alt sınırlar daha fazla önem arz etmektedir.

3.4.5 Önerme (Gilbert-Varshamov Sınırı): $0 \leq \delta \leq 1 - q^{-1}$ için $\alpha_q(\delta) \geq 1 - H_q(\delta)$ dır [2].

Gilbert-Varshamov Sınırı, $\alpha_q(\delta)$ için en iyi alt sınırdır.

Şekil 3.1 de $q = 2$ için bu sınırlar verilmiştir.

Bu kısımdaki amaç, Gilbert-Varshamov Sınırını geliştirmek olacaktır. Bunun için büyük uzunluğa sahip cebirsel geometrik kodlar göz önüne alınacaktır.

Herhangi bir $F\ /\ \mathbb{F}_q$ fonksiyon cismi göz önüne alınsın. Bu fonksiyon cisminin birinci dereceden place'lerinin sayısı $N = N(F)$ ile gösterilsin. $F\ /\ \mathbb{F}_q$ fonksiyon cisminin D ve G divizörleri ile ilişkili, herhangi bir cebirsel geometrik kod $C_{\mathcal{L}}(D, G)$ (sırasıyla $C_{\Omega}(D, G)$) olsun.

3.4.6 Lemma: $F\ /\ \mathbb{F}_q$ fonksiyon cisminin ikişer ikişer birbirinden farklı, birinci dereceden $P_1, \dots, P_n$ placeleri göz önüne alınsın. O zaman her $r \geq 0$ tamsayısı için $degG = r$ ve $P_i \notin suppG$ ($i = 1, \dots, n$) olacak şekilde bir G divizörü vardır [2].

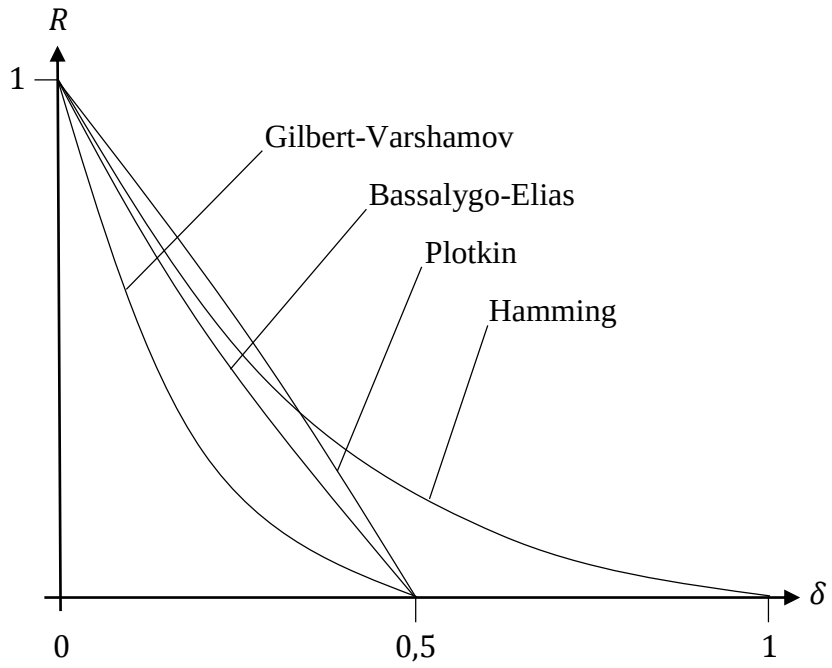
3.4.6 Lemma $C_{\mathcal{L}}(D, G)$ (sırasıyla $C_{\Omega}(D, G)$) kodunun uzunluğu üzerindeki tek kısıtlamanın, N kümesinin eleman sayısı olduğunu göstermektedir.

3.4.7 Tanım: Herhangi bir $g \geq 0$ tamsayısı için,

$N_q(g) = max\{\, N(F) \mid F/\mathbb{F}_q$ cinsi g olan bir fonksiyon cismidir $\}$ (3.20)

olarak tanımlansın.

$$A(q) = \lim_{g \to \infty} sup \frac{N_q(g)}{g} \tag{3.21}$$



Şekil 3.1 $q = 2$ için sınırlar [2].

reel sayısına Ihara sabiti denir [2].

Sıradaki önerme kanıtı ile birlikte verilmiştir.

3.4.8 Önerme: $A(q) > 1$ olduğu varsayılsın. O zaman $0 \leq \delta \leq 1 - A(q)^{-1}$ için $\alpha_q(\delta) \geq 1 - A(q)^{-1} - \delta$ dır [2].

Kanıt:

Herhangi bir $\delta \in [0,1 - A(q)^{-1}]$ sayısı göz önüne alınsın. $i \to \infty$ için,

$$g_i \to \infty \text{ ve } \frac{N(F_i)}{g_i} \to A(q) \tag{3.22}$$

özelliğine sahip fonksiyon cisimlerinin bir dizisi $F_i/\mathbb{F}_q$ olsun.

$$\frac{r_i}{N(F_i)} \to 1 - \delta \tag{3.23}$$

olacak şekilde bir $\{r_i\} \subseteq \mathbb{R}^+$ dizisi seçilsin. $i \to \infty$ için $N(F_i) \to \infty$ olduğundan böyle bir dizinin seçilebileceğine dikkat edilmelidir. $F_i/\mathbb{F}_q$ fonksiyon cisminin birinci dereceden tüm placelerinin toplamı D_i ile gösterilsin. Bu durumda $degD_i = N(F_i)$ olur.

3.4.6 Lemma gereğince her $i \geq 1$ için, $F_i/\mathbb{F}_q$ fonksiyon cisminin $degG_i = r_i$ ve $suppG_i \cap suppD_i = \emptyset$ olacak şekilde bir G_i divizörü vardır. Böylece her $i \geq 1$ için $C_i = C_{\mathcal{L}}(D_i, G_i)$ kodu tanımlıdır. Her $i \geq 1$ için C_i kodunun uzunluğu $degD_i = N(F_i)$ dir. Her $i \geq 1$ için C_i kodunun boyutu k_i, minimum uzaklığı d_i ile gösterilsin. 3.2.4 Sonuç gereğince C_i kodunun parametreleri,

$$k_i \geq degG_i + 1 - g_i = r_i + 1 - g_i \tag{3.24}$$

ve

$$d_i \geq N(F_i) - degG_i = N(F_i) - r_i \tag{3.25}$$

eşitsizliklerini sağlar. Böylece,

$$R_i = R(C_i) \geq \frac{r_i+1}{N(F_i)} - \frac{g_i}{N(F_i)} \text{ve } \delta_i = \delta(C_i) \geq 1 - \frac{r_i}{N(F_i)} \tag{3.26}$$

elde edilir. Genelleştirme kaybına uğramaksızın $(R_i)_{i\geq 1}$ ve $(C_i)_{i\geq 1}$ dizilerinin yakınsak olduğu varsayılabilir. Diğer durumda uygun bir alt dizi seçilir. $R_i \to R$ ve $\delta_i \to \tilde{\delta}$ olduğu kabul edilsin. (3.26) de verilen eşitsizliklerde $i \to \infty$ için limite geçilirse, (3.22) ve (3.23) gereğince $R \geq 1 - \delta - A(q)^{-1}$ ve $\tilde{\delta} \geq \delta$ elde edilir.

Her $i \geq 1$ için $\delta_i \leq 1$ olduğundan $\tilde{\delta} \leq 1$ dir. Böylece α_q fonksiyonunun tanımı gereğince $\alpha_q(\tilde{\delta}) \geq R \geq 1 - \delta - A(q)^{-1}$ olur. 3.4.2 Önerme gereğince α_q fonksiyonu artmayan olduğundan $\alpha_q(\delta) \geq \alpha_q(\tilde{\delta}) \geq 1 - \delta - A(q)^{-1}$ bulunur. Böylece 3.4.8 Önerme kanıtlanmış olur [2].

3.4.9 Lemma: En az bir $l > 0$ tamsayısı için $q = l^2$ ise $A(q) = q^{1/2} - 1$ dir [2].

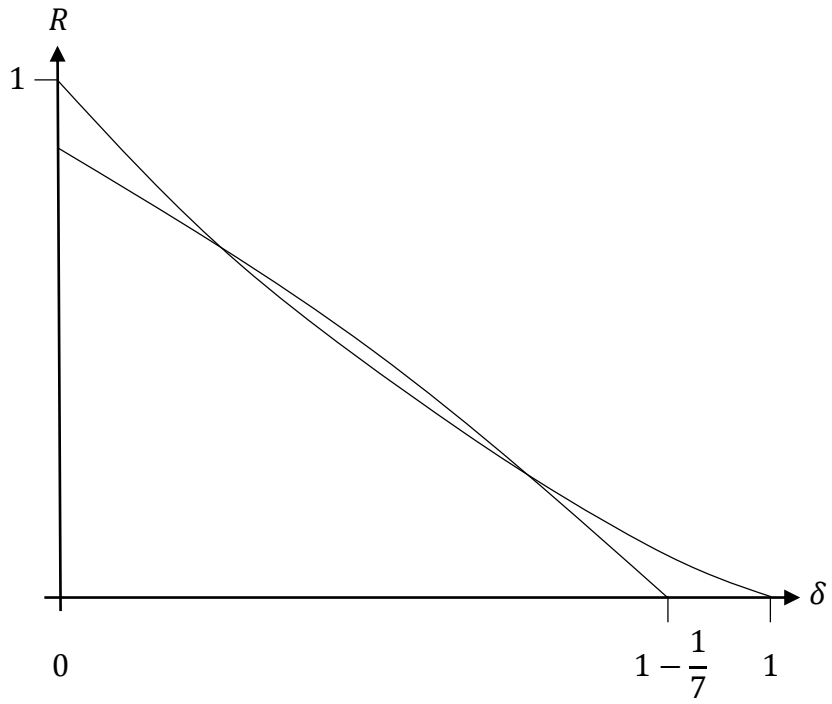
Sıradaki teorem kanıtıyla birlikte verilmiştir.

3.4.10 Teorem (Tsfasman-Vladut-Zink Sınırı): En az bir $l > 0$ tamsayısı için $q = l^2$ olsun. O zaman $0 \leq \delta \leq 1 - (q^{1/2} - 1)^{-1}$ için $\alpha_q(\delta) \geq 1 - \left(q^{1/2} - 1\right)^{-1} - \delta$ dır [2,6].

Kanıt:

En az bir $l > 0$ tamsayısı için $q = l^2$ olduğundan 3.4.9 Lemma gereğince $A(q) = q^{1/2} - 1$ dır. Bu durumda $q > 2$ olacağından $A(q) > 1$ dır. Böylece 3.4.8 Önerme gereğince $0 \leq \delta \leq 1 - (q^{1/2} - 1)^{-1}$ için $\alpha_q(\delta) \geq 1 - \left(q^{1/2} - 1\right)^{-1} - \delta$ elde edileceğinden kanıt tamamlanır.

$q = l^2 \geq 49$ olacak şekildeki her $l > 0$ tamsayısı için Tsfasman-Vladut-Zink Sınırı, Gilbert-Varshamov Sınırını belli bir aralıkta geliştirmektedir. Şekil 3.2 de $q = 64$ için bu sınırlar gösterilmiştir [2].



Şekil 3.2 $q = 64$ için sınırlar [2].

3.5 Cebirsel Geometrik Kodların Minimum Uzaklığı için Taban Sınırları

Cebirsel geometrik kodların, tasarlanmış uzaklığını geliştirmek için çeşitli metodlar kullanılmıştır. Bu metodlar iki ana kategoriye ayrılabilir. Bunlardan ilki mertebe sınırıdır. Mertebe sınırının temeli, Feng ve Rao'nun ünlü [8] makalesine dayanmaktadır.

Kullanılan diğer metod ise taban sınırıdır. Bir kaçı hariç, cebirsel geometrik kodların minimum uzaklığı için bilinen tüm alt sınırlar bu iki metodun özel hali olarak ifade edilebilir. Bu kısımda taban sınırı incelenecektir.

Bir divizörün "tabanı" ilk olarak Maharaj ve Matthews tarafından [9] de tanımlanmıştır. Daha sonra bu tanım yardımıyla cebirsel geometrik kodların tasarlanmış uzaklığı üzerinde bir dizi gelişme elde edilmiştir. Bu nedenle bu sınırlar literatürde taban sınırları olarak bilinmektedir.

3.5.1 Tanım: $F\ /\ \mathbb{F}_q$ fonksiyon cisminin herhangi iki $A, B \in Div(F)$ divizörü göz önüne alınsın. $gcd(A,B) = \sum_{P\in\mathcal{P}_F} min\{v_P(A), v_P(B)\}.P$ divizörüne, A ve B nin en büyük ortak divizörü denir [10].

3.5.2 Önerme: $F\ /\ \mathbb{F}_q$ fonksiyon cisminin $\ell(G) > 0$ özelliğine sahip herhangi bir $G \in Div(F)$ divizörü göz önüne alınsın. $F\ /\ \mathbb{F}_q$ fonksiyon cisminin $\mathcal{L}(G) = \mathcal{L}(G')$ olacak şekildeki, minimum dereceye sahip divizörü $G' \in Div(F)$ olsun. O zaman $G \geq G'$ dir. Üstelik, bu özelliklere sahip olan $G' \in Div(F)$ divizörü tek şekilde belirlidir [10].

3.5.3 Tanım: $F\ /\ \mathbb{F}_q$ fonksiyon cisminin $\ell(G) > 0$ özelliğine sahip herhangi bir $G \in Div(F)$ divizörü göz önüne alınsın. $F\ /\ \mathbb{F}_q$ fonksiyon cisminin $\mathcal{L}(G) = \mathcal{L}(G')$ olacak şekildeki, minimum dereceye sahip ve teklikle belirli $G' \in Div(F)$ divizörüne, G divizörünün tabanı denir ve $G \in Div(F)$ divizörünün tabanı $\lfloor G \rfloor$ ile gösterilir [10].

Şimdi verilen bir divizörün tabanını bulmaya yardımcı olabilecek birkaç sonuç verilecektir.

3.5.4 Önerme: $F\ /\ \mathbb{F}_q$ fonksiyon cisminin $\ell(G) > 0$ özelliğine sahip herhangi bir $G \in Div(F)$ divizörü göz önüne alınsın. $E = gcd(G + (x) \mid x \in \mathcal{L}(G) \setminus \{0\})$ efektif divizörü tanımlansın. O zaman $\lfloor G \rfloor = G - E$ dir [10].

Taban kavramının daha iyi anlaşılabilmesi için sıradaki teorem kanıtıyla birlikte verilmiştir.

3.5.5 Teorem: $F\ /\ \mathbb{F}_q$ fonksiyon cisminin efektif bir $G \in Div(F)$ divizörü göz önüne alınsın. O zaman $\lfloor G \rfloor$ divizörü de efektiftir. Ayrıca $supp\lfloor G \rfloor \subseteq suppG$ dir [10].

Kanıt:

$E = gcd(G + (x) \mid x \in \mathcal{L}(G) \setminus \{0\})$ efektif divizörü göz önüne alınsın. Herhangi bir $P \in \mathcal{P}_F$ place'i için $\min\limits_{x\in\mathcal{L}(G)\setminus\{0\}} v_p(x) = -v_p(G - E)$ olduğu biliniyor. 3.5.4 Önerme gereğince $\lfloor G \rfloor = G - E$ olduğundan $\min\limits_{x\in\mathcal{L}(G)\setminus\{0\}} v_p(x) = -v_p(\lfloor G \rfloor)$ olur.

$G \geq 0$ olduğundan, Riemann-Roch uzayının tanımından $\mathbb{F}_q \subseteq \mathcal{L}(G)$ olur. Bu sebeple $\min\limits_{x\in\mathcal{L}(G)\setminus\{0\}} v_p(x) \leq 0$ dır.

Böylece her $P \in \mathcal{P}_F$ place'i için $v_p(G) \geq v_p(\lfloor G \rfloor) = -\min_{x \in \mathcal{L}(G)\setminus\{0\}} v_p(x) \geq 0$ olacağından kanıt tamamlanmış olur [10].

Bir divizörün tabanı kavramı üzerinde çalışılmasının temel amacı, bir cebirsel geometrik kodun minimum uzaklığı üzerinde gelişme elde edebilmektedir. Şimdi bu kavram kullanılarak elde edilebilecek en basit gelişme verilecektir.

$C_{\mathcal{L}}(D,G)$ kodunun minimum uzaklığının anlamlı bir alt sınırını elde edebilmek için $degG < n$ olduğu varsayılacaktır. Böylece $C_{\mathcal{L}}(D,G) \neq 0$ olacağından $\ell(G) > 0$ dır.

3.5.6 Teorem: $k \geq degG - g + 1$ ve $d \geq n - deg\lfloor G \rfloor$ olmak üzere $C_{\mathcal{L}}(D,G)$ bir $[n,k,d]$ koddur [10].

Şimdi bir divizörün tabanı kavramı kullanılarak elde edilen ilk önemli sonuç verilecektir.

$C_{\Omega}(D,G)$ kodunun minimum uzaklığının anlamlı bir alt sınırını elde edebilmek için bundan sonraki kısımda $degG > 2g - 2$ olduğu varsayılacaktır. Böylece $C_{\Omega}(D,G) \neq 0$ dir. Sıradaki teorem kanıtıyla birlikte verilmiştir.

3.5.7 Teorem (Maharaj-Matthews-Pirsic Sınırı): Her $i \in \{1,\dots,n\}$ için $P_i \notin suppH$ olacak şekilde efektif bir $H \in Div(F)$ divizörü göz önüne alınsın ve $G = H + \lfloor H \rfloor$ ve $E_H = H - \lfloor H \rfloor$ divizörleri tanımlansın. O zaman $C_{\Omega}(D,G)$, $k \geq n - degG + g - 1$ ve $d \geq degG - (2g-2) + degE_H = 2.degH - (2g-2)$ olmak üzere bir $[n,k,d]$ koddur [10].

Kanıt:

$degG > 2g - 2$ olduğundan 3.2.7 Teorem gereğince $k \geq n - degG + g - 1$ olur.

Şimdi $d \geq 2degH - (2g-2)$ olduğu gösterilecektir. $C_{\Omega}(D,G) \neq 0$ olduğundan en az bir $\omega \in \Omega_F(G-D)$, $\omega \neq 0$ Weil diferansiyeli için, minimum ağırlığa sahip olacak şekilde en az bir $(\omega_{P_1}(1), \omega_{P_2}(1), \dots, \omega_{P_n}(1))$ kod sözcüğü vardır. Bu kod sözcüğünün ağırlığı $d > 0$ olsun. $(\omega_{P_1}(1), \omega_{P_2}(1), \dots, \omega_{P_n}(1))$ kod sözcüğünün ilk d bileşeninin sıfırdan farklı ve diğerlerinin sıfır olduğu varsayılabilir.

$D' = \sum_{i=1}^{d} P_i$ divizörü göz önüne alınsın. $(\omega) \geq G - D'$ olduğu gösterilecektir. $\omega \in \Omega_F(G - D)$, $\omega \neq 0$ olduğundan 2.3.43 Not gereğince $(\omega) \geq G - D$ olur. Böylece $i = i_{d+1}, i_{d+2}, \dots, i_n$ için $v_{P_i}(\omega) \geq -1$ bulunur. Ayrıca $i = i_{d+1}, i_{d+2}, \dots, i_n$ için $\omega_{P_i}(1) = 0$ olduğundan (3.7) gereğince $v_{P_i}(\omega) \geq 0$ olur. Bu sebeple $(\omega) \geq G - D'$ olduğu görülmüş olur.

Şimdi $i = i_1, i_2, \dots, i_d$ için $v_{P_i}(\omega) = -1$ olduğu gösterilecektir. $(\omega) \geq G - D$ olduğundan $v_{P_i}(\omega) \geq -1$ olur. Ayrıca $i = i_1, i_2, \dots, i_d$ için $\omega_{P_i}(1) \neq 0$ olduğundan (3.7) gereğince $v_{P_i}(\omega) \leq -1$ olur. Bu sebeple $i = i_1, i_2, \dots, i_d$ için $v_{P_i}(\omega) = -1$ olduğu görülmüş olur.

Böylece $i = i_1, i_2, \dots, i_d$ için $P_i \notin suppA$ olmak üzere, $(\omega) = G - D' + A$ olacak şekilde en az bir $A \in Div(F)$, $A \geq 0$ divizörü vardır. Bir doğal divizörün derecesinin $2g - 2$ olacağı göz önünde bulundurulursa, $d = degG - (2g - 2) + degA$ elde edilir.

İstenilen eşitsizliğin sağlandığını göstermek için $degA \geq degE_H$ olduğunu göstermek yeterlidir. $H + A \geq H$ olduğundan 2.3.12 Lemma gereğince $degA \geq \ell(H + A) - \ell(H)$ elde edilir. $\ell(H) = \ell(\lfloor H \rfloor)$ olduğundan $degA \geq \ell(H + A) - \ell(\lfloor H \rfloor)$ olur. $A + \lfloor H \rfloor \geq \lfloor H \rfloor$ olduğundan 2.3.12 Lemma gereğince $\mathcal{L}(\lfloor H \rfloor) \subseteq \mathcal{L}(A + \lfloor H \rfloor)$ olacağından $\ell(\lfloor H \rfloor) \leq \ell(A + \lfloor H \rfloor)$ olur. Böylece $degA \geq \ell(H + A) - \ell(A + \lfloor H \rfloor)$ elde edilir.

Son olarak $degE_H = \ell(H + A) - \ell(A + \lfloor H \rfloor)$ olduğu gösterilecektir. (ω) bir doğal divizör olduğundan Riemann-Roch Teoremi (2.3.48 Teorem) gereğince,

$$\ell(H + A) = deg(H + A) + 1 - g + \ell((\omega) - H - A) \tag{3.27}$$

ve

$$\ell(A + \lfloor H \rfloor) = deg(A + \lfloor H \rfloor) + 1 - g + \ell((\omega) - A - \lfloor H \rfloor) \tag{3.28}$$

olur. (3.27) ve (3.28) gereğince $\ell(H + A) - \ell(A + \lfloor H \rfloor) = degE_H + \ell((\omega) - H - A) - \ell((\omega) - A - \lfloor H \rfloor) = degE_H + \ell(\lfloor H \rfloor - D') - \ell(H - D')$ bulunur.

Bu nedenle $degE_H = \ell(H + A) - \ell(A + \lfloor H \rfloor)$ olduğunu göstermek için $\ell(\lfloor H \rfloor - D') = \ell(H - D')$ olduğunu göstermek yeterli olacaktır. $H - D' \leq H$ olduğundan 2.3.12 Lemma gereğince $\mathcal{L}(H - D') \subseteq \mathcal{L}(H) = \mathcal{L}(\lfloor H \rfloor)$ olur. Böylece $\mathcal{L}(H - D') = \mathcal{L}(H - D') \cap \mathcal{L}(\lfloor H \rfloor) = \mathcal{L}(gcd(H - D', \lfloor H \rfloor))$ olur.

$H \geq 0$ olduğundan 3.5.5 Teorem gereğince $supp\lfloor H \rfloor \subseteq suppH$ dir. Ayrıca 2.3.2 Önerme gereğince $H \geq \lfloor H \rfloor$ ve hipotez gereğince $suppH \cap suppD = \emptyset$ olduğundan $gcd(H - D', \lfloor H \rfloor) = \lfloor H \rfloor - D'$ olur.

Böylece $\mathcal{L}(H - D') = \mathcal{L}(\lfloor H \rfloor - D')$ olacağından 3.5.7 Teorem kanıtlanmış olur [10].

Şimdi Maharaj-Matthews-Pirsic sınırının sonuçları üzerinde durulacaktır. Bu amaçla sıradaki önerme verilecektir.

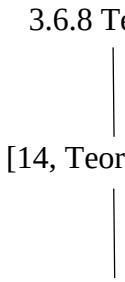
3.5.8 Önerme: $n_1, \dots, n_m \geq 0$ tam sayıları ve $F \,/\, \mathbb{F}_q$ fonksiyon cisminin ikişer ikişer farklı $Q_1, \dots, Q_m$ rasyonel placeleri göz önüne alınsın. $(n_1, \dots, n_m)$ elemanının, $(Q_1, \dots, Q_m)$ placelerinin Weierstrass boşluk kümesinin bir elemanı olması için gerekli ve yeterli koşul $\ell(\sum_{i=1}^{m} n_i . Q_i) = \ell((n_j - 1) . Q_j + \sum_{i=1, i \neq j}^{m} n_i . Q_i)$ olacak şekilde bir $j \in \{1, \dots, m\}$ elemanının var olmasıdır [10].

Herhangi bir place'in Weierstrass boşluk kümesi klasik olarak çalışılan bir konu olmakla beraber, iki farklı place'in Weierstrass boşluk kümesi [11] de ve iki veya daha fazla farklı place'in Weierstrass boşluk kümesi [12] de tanımlanmıştır.

Weierstrass boşluk kümeleri kullanılarak, cebirsel geometrik kodların minimum uzaklığı üzerinde gelişmeler elde edilmiştir [13, Teorem 3.3, 14, Teorem 3.4]. [13, Teorem 3.3] ve [14, Teorem 3.4], 3.6.8 Teoreminin özel durumlarıdır [10]. Şekil 3.3 de bu gelişmeler verilmiştir.

Şimdi bir örnek verilecektir.

3.5.9 Örnek: $y^8 - y = x^{10} - x^3$ eşitliği ile tanımlanan $\mathbb{F}_8(x, y) \,/\, \mathbb{F}_8$ fonksiyon cismi göz önüne alınsın. Bu fonksiyon cismi bazen $\mathbb{F}_8$ üzerinde Suzuki fonksiyon cismi



Şekil 3.3

olarak da isimlendirilir ve cinsi $g = 14$ tür. $\mathbb{F}_8(x,y)\ /\ \mathbb{F}_8$ fonksiyon cisminin $\alpha, \beta \in \mathbb{F}_8$ için $P_{\alpha,\beta}$ ve P_∞ olmak üzere 65 tane rasyonel place'i vardır [10].

$G = 27.P_\infty + 22.P_{0,0}$ olsun. $\mathbb{F}_8(x,y)\ /\ \mathbb{F}_8$ fonksiyon cisminin, P_∞ ve $P_{0,0}$ dan farklı rasyonel placelerinin toplamı $D = P_1 + \cdots + P_{63}$ olmak üzere $C_\Omega(D,G)$ cebirsel geometrik kodu göz önüne alınsın.

3.5.7 Teoreminin kullanılabilmesi için, $G = H + \lfloor H \rfloor$ olacak şekilde bir $H \in Div(\mathbb{F}_8(x,y))$ divizörünün bulunması gerekmektedir. $H = 14.P_\infty + 11.P_{0,0}$ divizörü için $\lfloor H \rfloor = 13.P_\infty + 11.P_{0,0}$ dir [10]. Böylece 3.5.7 Teorem gereğince $d \geq 2.degH - (2g-2) = 2.25 - (2.14 - 2) = 24$ olur.

Ayrıca $2g - 2 = 26 < degG = 49 < n = 63$ olduğundan 3.2.7 Teorem gereğince $k = n + g - 1 - degG = 63 + 14 - 1 - 49 = 27$ olur.

Böylece uzunluğu 63 olan $C_\Omega(D,G)$ cebirsel geometrik kodunun boyutu 27, minimum uzaklığı en az 24 tür. $C_\Omega(D,G)$ kodu, $\mathbb{F}_8$ üzerinde uzunluğu 63 ve boyutu 27 olan kodlar arasında bilinen en iyi koddur [10]. Ayrıca [13, Teorem 3.3] ve [14, Teorem 3.4] bu koda uygulanamamaktadır.

Maharaj-Matthews-Pirsic sınırı, B. Lundell ve J. McCullough tarafından geliştirilmiştir [15]. Sıradaki teorem kanıtıyla birlikte verilmiştir.

3.5.10 Teorem (Lundell-McCullough Sınırı): $Z \geq 0$, $\mathcal{L}(A) = \mathcal{L}(A - Z)$, $\mathcal{L}(B) = \mathcal{L}(B + Z)$ koşullarını sağlayan $A, B, Z \in Div(F)$ divizörleri göz önüne alınsın. $(suppA \cup suppB \cup suppZ) \cap suppD = \emptyset$ olsun. O zaman $G = A + B$ olmak üzere, $d(C_\Omega(D, G)) \geq degG - (2.g - 2) + degZ$ dir [15].

Kanıt:

$C_\Omega(D, G) \neq 0$ olduğundan en az bir $\omega \in \Omega_F(G - D)$, $\omega \neq 0$ Weil diferansiyeli için, minimum ağırlığa sahip olacak şekilde en az bir $(\omega_{P_1}(1), \omega_{P_2}(1), \dots, \omega_{P_n}(1))$ kod sözcüğü vardır. Bu kod sözcüğünün ağırlığı $d > 0$ olsun. $(\omega_{P_1}(1), \omega_{P_2}(1), \dots, \omega_{P_n}(1))$ kod sözcüğünün ilk d bileşeninin sıfırdan farklı ve diğerlerinin sıfır olduğu varsayılabilir.

$D' = \sum_{i=1}^{d} P_i$ divizörü göz önüne alınsın. 3.5.7 Teoremde de olduğu gibi $i = i_1, i_2, \dots, i_d$ için $P_i \notin suppE$ olmak üzere, $(\omega) = G - D' + E$ olacak şekilde en az bir $E \in Div(F)$, $E \geq 0$ divizörü vardır. Bir doğal divizörün derecesinin $2g - 2$ olacağı göz önünde bulundurulursa, $d = degG - (2.g - 2) + degE$ elde edilir.

İstenilen eşitsizliğin sağlandığını göstermek için $degE \geq degZ$ olduğunu göstermek yeterlidir. $A + E \geq A$ olduğundan 2.3.12 Lemma gereğince $degE \geq \ell(A + E) - \ell(A)$ olur. $\ell(A) = \ell(A - Z)$ olduğundan $degE \geq \ell(A + E) - \ell(A - Z)$ bulunur. $A + E - Z \geq A - Z$ olduğundan 2.3.12 Lemma gereğince $\mathcal{L}(A - Z) \subseteq \mathcal{L}(A + E - Z)$ olacağından $\ell(A - Z) \leq \ell(A + E - Z)$ olur. Böylece $degE \geq \ell(A + E) - \ell(A + E - Z)$ olur.

Son olarak $degZ = \ell(A + E) - \ell(A + E - Z)$ olduğu gösterilecektir. (ω) bir doğal divizör olduğundan Riemann-Roch Teoremi (2.3.48 Teorem) gereğince,

$$\ell(A + E) = deg(A + E) + 1 - g + \ell((\omega) - A - E) \tag{3.29}$$

ve

$$\ell(A + E - Z) = deg(A + E - Z) + 1 - g + \ell((\omega) - A - E + Z) \tag{3.30}$$

olur. (3.29) ve (3.30) eşitlikleri gereğince $\ell(A+E)-\ell(A+E-Z)=degZ+\ell((\omega)-A-E)-\ell((\omega)-A-E+Z)=degZ+\ell(B-D')-\ell(B+Z-D')$ bulunur.

Bu nedenle $degZ=\ell(A+E)-\ell(A+E-Z)$ olduğunu göstermek için $\ell(B-D')=\ell(B+Z-D')$ olduğunu göstermek yeterli olacaktır. $B+Z-D'\leq B+Z$ olduğundan 2.3.12 Lemma gereğince $\mathcal{L}(B+Z-D')\subseteq\mathcal{L}(B+Z)=\mathcal{L}(B)$ olur. Böylece $\mathcal{L}(B+Z-D')=\mathcal{L}(B+Z-D')\cap\mathcal{L}(B)=\mathcal{L}(gcd(B+Z-D',B))$ bulunur.

$(suppB\cup suppZ)\cap suppD=\emptyset$ ve $Z\geq 0$ olduğundan $gcd(B+Z-D',B)=B-D'$ dır.

Böylece $\mathcal{L}(B+Z-D')=\mathcal{L}(B-D')$ olacağından $\ell(B-D')=\ell(B+Z-D')$ olur. Dolayısıyla 3.5.10 Teorem kanıtlanmış olur [15].

Şimdi Lundell-McCullough sınırının sonuçları üzerinde durulacaktır.

3.5.11 Sonuç: Maharaj-Matthews-Pirsic sınırı, Lundell-McCullough sınırının özel bir durumudur [15].

Kanıt:

$A=H$, $B=\lfloor H\rfloor$ ve $Z=H-\lfloor H\rfloor$ divizörleri göz önüne alınsın. 3.5.2 Önerme gereğince $H\geq\lfloor H\rfloor$ olduğundan $Z\geq 0$ dır. Ayrıca $\mathcal{L}(A)=\mathcal{L}(A-Z)$, $\mathcal{L}(B)=\mathcal{L}(B+Z)$ dir.

$H\geq 0$ olduğundan 3.5.5 Teorem gereğince $supp\lfloor H\rfloor\subseteq suppH$ dir. Her $i\in\{1,\dots,n\}$ için $P_i\notin suppH$ olduğundan $(suppA\cup suppB\cup suppZ)\cap suppD=\emptyset$ dir. Böylece 3.5.10 Teoreminin ön koşulları sağlanmış olur.

3.5.10 Teorem gereğince $G=A+B$ olmak üzere, $d(C_\Omega(D,G))\geq degG-(2g-2)+degZ=2.degH-(2g-2)$ olduğundan istenilen elde edilir.

Sonuç olarak 3.5.11 Sonuç kanıtlanmış olur.

Herhangi bir $G\in Div(F)$ divizörü verildiğinde, $G=H+\lfloor H\rfloor$ olacak şekilde bir $H\in Div(F)$, $H\geq 0$ divizörü bulunamayabilir. Bu nedenle Maharaj-Matthews-Pirsic

sınırının kullanılamayacağı durumlar vardır. Ancak $A = G$ ve $B = Z = 0$ olarak alınırsa, Lundell-McCullough sınırı daima kullanılabilir.

C. Kirfel ve R. Pellikaan, bir $P \in \mathcal{P}_F$ place'inin Weierstrass boşluk dizisini kullanarak, cebirsel geometrik kodların minimum uzaklığı üzerinde gelişme elde etmişlerdir [16].

3.5.12 Tanım: Herhangi bir $P \in \mathcal{P}_F$ place'i ve $A \in Div(F)$ divizörü göz önüne alınsın. $\mathcal{L}(A + \alpha.P) = \mathcal{L}(A + (\alpha - 1).P)$ olacak şekildeki bir $\alpha \in \mathbb{Z}$ tamsayısına, P place'inde bir A-boşluk denir [15].

3.5.13 Teorem (Kirfel-Pellikaan Sınırı): Her $i \in \{1, \dots, n\}$ için $P \neq P_i$ olacak şekilde bir $P \in \mathcal{P}_F$ place'i ve $(suppF \cup suppG) \cap suppD = \emptyset$ koşulunu sağlayan $F, G \in Div(F)$ divizörleri göz önüne alınsın. $\alpha, \alpha + 1, \dots, \alpha + t \in \mathbb{Z}$ tamsayılarının her biri, P place'inde bir F-boşluk ve $\beta - t, \beta - t + 1, \dots, \beta \in \mathbb{Z}$ tamsayılarının her biri, P place'inde bir G-boşluk olsun. O zaman $H = F + G + (\alpha + \beta - 1).P$ olmak üzere, $d(C_\Omega(D, G)) \geq degH - (2g - 2) + (t + 1)$ dır [15].

Sıradaki sonuç kanıtıyla birlikte verilmiştir.

3.5.14 Sonuç: Kirfel-Pellikaan sınırı, Lundell-McCullough sınırının özel bir durumudur [15].

Kanıt:

$A = F + (\alpha + t).P$, $B = G + (\beta - t - 1).P$ ve $Z = (t + 1).P$ divizörleri göz önüne alınsın. $Z \geq 0$ dır. Ayrıca $(suppA \cup suppB \cup suppZ) \cap suppD = \emptyset$ dır.

$\alpha, \alpha + 1, \dots, \alpha + t \in \mathbb{Z}$ tamsayılarının her biri, P place'inde bir F-boşluk olduğundan $\mathcal{L}(F + (\alpha + t).P) = \mathcal{L}(A + (\alpha + t - 1).P) = \cdots = \mathcal{L}(F + (\alpha - 1).P)$ olur. Böylece $\mathcal{L}(A) = \mathcal{L}(A - Z)$ elde edilir.

$\beta - t, \beta - t + 1, \dots, \beta \in \mathbb{Z}$ tamsayılarının her biri, P place'inde bir G-boşluk olduğundan $\mathcal{L}(G + \beta.P) = \mathcal{L}(G + (\beta - 1).P) = \cdots = \mathcal{L}(G + (\beta - t - 1).P)$ olur. Böylece $\mathcal{L}(B) = \mathcal{L}(B + Z)$ elde edilir.

O zaman 3.5.10 Teorem gereğince $G = A + B$ olmak üzere, $d(C_\Omega(D,G)) \geq degG - (2g-2) + degZ = deg(F + G + (\alpha+\beta-1).P) - (2g-2) + (t+1)$ olur.

Böylece 3.5.14 Sonuç kanıtlanmış olur [15].

Bunlara ek olarak [17, Teorem 2.1],[13, Teorem 3.4] ve [14, Teorem 3.3], 3.5.10 Teoreminin özel durumlarıdır [18]. Şekil 3.4 de bu gelişmeler verilmiştir.

Şimdi Lundell-McCullough sınırının, kodlara nasıl uygulanacağına dair örnekler verilecektir. Bu amaçla önce sıradaki tanım verilecektir.

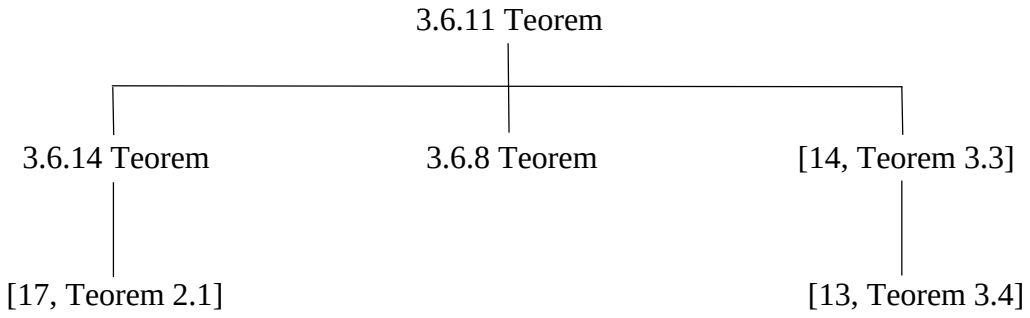
3.5.15 Tanım: $y^q + y = x^{q+1}$ eşitliği ile tanımlanan $\mathbb{F}_{q^2}(x,y) \,/\, \mathbb{F}_{q^2}$ fonksiyon cismine Hermitian fonksiyon cismi denir ve cinsi $g = q.(q-1)\,/\,2$ dir [10].

Her $\alpha \in \mathbb{F}_{q^2}$ elemanı için, $\beta^q + \beta = \alpha^{q+1}$ eşitliğini sağlayan tam olarak q tane $\beta \in \mathbb{F}_{q^2}$ elemanı vardır. $\mathbb{F}_{q^2}(x,y) \,/\, \mathbb{F}_{q^2}$ Hermitian fonksiyon cisminin bu şekildeki α, $\beta \in \mathbb{F}_{q^2}$ elemanlarına karşılık bir $P_{\alpha,\beta}$ rasyonel place'i vardır. Böylece $\mathbb{F}_{q^2}(x,y) \,/\, \mathbb{F}_{q^2}$ Hermitian fonksiyon cisminin, x ve y elemanlarının ortak kutbu P_∞ da dahil olmak üzere toplam $q^3 + 1$ tane rasyonel place'i vardır.

3.5.16 Örnek: $y^4 + y = x^5$ eşitliği ile tanımlanan $\mathbb{F}_{16}(x,y) \,/\, \mathbb{F}_{16}$ Hermitian fonksiyon cismi göz önüne alınsın. Bu fonksiyon cisminin cinsi 6 dır ve 65 tane rasyonel place'i vardır. Ayrıca $\mathcal{L}(11.P_\infty) = \mathcal{L}(10.P_\infty)$ ve $\mathcal{L}(7.P_\infty) = \mathcal{L}(6.P_\infty)$ dır.

$A = 11.P_\infty$, $B = 6.P_\infty$ ve $Z = P_\infty$ olsun. $\mathbb{F}_{16}(x,y) \,/\, \mathbb{F}_{16}$ fonksiyon cisminin, P_∞ dan farklı rasyonel placelerinin toplamı $D = P_1 + \cdots + P_{64}$ ile gösterilsin. O zaman $G = A + B$ olmak üzere 3.5.10 Teorem gereğince $d(C_\Omega(D,G)) \geq degG - (2g-2) + degZ = 17 - (2.6-2) + 1 = 8$ olur.

$C_\Omega(D,G)$ kodunun tasarlanmış uzaklığı $degG - (2g-2) = 17 - (2.6-2) = 7$ dır. Böylece Lundell-McCullough sınırı kullanılarak, tasarlanmış uzaklık üzerinde 1 birim gelişme elde edildiği gösterilmiş olur. Bu gelişme Kirfel-Pellikaan sınırı kullanılarak da elde edilebilir. Ancak $G = H + \lfloor H \rfloor$ olacak şekilde bir $H \in Div(\mathbb{F}_{16}(x,y))$ divizörü olmadığından, Maharaj-Matthews-Pirsic sınırı bu koda uygulanamamaktadır.



Şekil 3.4

[19] gereğince $C_\Omega(D,G)$ kodunun minimum uzaklığı 8 dir. Böylece Lundell-McCullough ve Kirfel-Pellikaan sınırı minimum uzaklığı karşılamaktadır [15].

3.5.17 Örnek: 3.6.17 Örnekte verilen $\mathbb{F}_{16}(x,y)\ /\ \mathbb{F}_{16}$ fonksiyon cismi göz önüne alınsın. $\mathbb{F}_{16}(x,y)\ /\ \mathbb{F}_{16}$ fonksiyon cisminin, $P_{0,0}$ ve P_∞ dan farklı rasyonel placelerinin toplamı $D = P_1 + \cdots + P_{63}$ ile gösterilsin. $G = 2.P_{0,0} + 8.P_\infty$ olmak üzere $C_\Omega(D,G)$ kodu göz önüne alınsın.

$\mathcal{L}(2.P_{0,0} + 6.P_\infty) = \mathcal{L}(5.P_\infty)$ ve $\mathcal{L}(2.P_{0,0} + 3.P_\infty) = \mathcal{L}(2.P_\infty)$ dır. $A = 2.P_{0,0} + 6.P_\infty$, $B = 2.P_\infty$ ve $Z = 2.P_{0,0} + P_\infty$ olmak üzere 3.6.11 Teorem gereğince $d(C_\Omega(D,G)) \geq degG - (2g-2) + degZ = 10 - (2.6-2) + 3 = 3$ elde edilir.

$C_\Omega(D,G)$ kodunun tasarlanmış uzaklığı $degG - (2g-2) = 10 - (2.6-2) = 0$ dır. Böylece Lundell-McCullough sınırı kullanılarak, tasarlanmış uzaklık üzerinde 3 birim gelişme elde edildiği gösterilmiş olur [15].

Efektif divizörlerin kullanılması durumunda, Maharaj-Matthews-Pirsic sınırı ve Kirfel-Pellikaan sınırı bu gelişmeyi sağlayamamaktadır. $G = H + \lfloor H \rfloor$ olacak şekildeki en iyi $H \in Div(\mathbb{F}_{16}(x,y))$ divizörünün seçimi, $H = 2.P_{0,0} + 4.P_\infty$ dır. Bu durumda Maharaj-Matthews-Pirsic sınırı gereğince $d \geq 2.degH - (2g-2) = 2.6 - (2.6-2) = 2$ elde edilir. Benzer şekilde Kirfel-Pellikaan sınırı için en ideal seçimler

yapıldığında $F = G = 2.P_{0,0} + 4.P_{\infty}$, $P = P_{0,0}$, $\alpha = 1$, $\beta = 1$ ve $t = 1$ olmak üzere $C_{\Omega}(D, G)$ kodunun minimum uzaklığı için $d \geq 2$ elde edilir [15].

A ve B divizörlerinin efektif olduğu durumlarda Lundell-McCullough sınırı, tasarlanmış uzaklık üzerinde genellikle iyi sonuçlar vermektedir. Şimdi A veya B divizörlerinin efektif olmadığı durumlarda Lundell-McCullough sınırının daha iyi sonuçlar verebileceği gösterilecektir.

3.5.18 Örnek: 3.5.9 Örnekte verilen $\mathbb{F}_8(x, y)$ / $\mathbb{F}_8$ Suzuki fonksiyon cismi göz önüne alınsın. P_{∞} dan farklı rasyonel placelerinin toplamı $D = P_1 + \cdots + P_{64}$ ile gösterilsin. $G = 32.P_{\infty}$ olmak üzere $C_{\Omega}(D, G)$ kodu göz önüne alınsın.

$\mathcal{L}(-5.P_{0,0} + 17.P_{\infty}) = \mathcal{L}(-5.P_{0,0} + 15.P_{\infty})$ ve $\mathcal{L}(5.P_{0,0} + 15.P_{\infty}) = \mathcal{L}(5.P_{0,0} + 13.P_{\infty})$ dır. Böylece $A = 5.P_{0,0} + 15.P_{\infty}$, $B = -5.P_{0,0} + 17.P_{\infty}$ve $Z = 2.P_{\infty}$ olmak üzere 3.5.10 Teorem gereğince $d(C_{\Omega}(D, G)) \geq degG - (2g - 2) + degZ = 32 - (2.14 - 2) + 2 = 8$ elde edilir.

A ve B divizörleri efektif olacak şekilde en ideal seçimler yapıldığında, $C_{\Omega}(D, G)$ kodunun minimum uzaklığı için $d \geq 7$ elde edilir [15].

Lundell-McCullough sınırı C. Güneri, H. Stichtenoth ve İ. Taşkın tarafından geliştirilmiştir [18].

Sıradaki lemma kanıtıyla birlikte verilmiştir.

3.5.19 Lemma: $\mathcal{L}(A) \subseteq \mathcal{L}(B)$, $H \geq 0$ ve her $P \in suppH$ place'i için $v_P(A) = v_P(B)$ olacak şekildeki A, B ve $H \in Div(F)$ divizörleri göz önüne alınsın. O zaman $\mathcal{L}(A - H) \subseteq \mathcal{L}(B - H)$ dır [18].

Kanıt:

Herhangi bir $x \in \mathcal{L}(A - H)$, $x \neq 0$ elemanı göz önüne alınsın. $\mathcal{L}(A - H)$ Riemann-Roch uzayının tanımı gereğince $(x) \geq -A + H$ dır.

Herhangi bir $P \in suppH$ place'i için $v_P(A) = v_P(B)$ olduğundan $v_P(x) \geq -v_P(A) + v_P(H) = -v_P(B) + v_P(H)$ olur. Böylece $x \in \mathcal{L}(B - H)$ olur.

Şimdi herhangi bir $P \notin suppH$ place'i göz önüne alınsın. $H \geq 0$ olduğundan $A - H \leq A$ dır. 2.3.12 Lemma gereğince $\mathcal{L}(A-H) \subseteq \mathcal{L}(A) \subseteq \mathcal{L}(B)$ elde edilir. Böylece $x \in \mathcal{L}(B)$ dir. $P \notin suppH$ olduğundan $v_P(H) = 0$ olacağına dikkat edilirse $v_P(x) \geq -v_P(B) = -v_P(B) + v_P(H)$ bulunur. Böylece $x \in \mathcal{L}(B-H)$ olur.

Sonuç olarak $\mathcal{L}(A-H) \subseteq \mathcal{L}(B-H)$ olduğu görülmüş olur [18].

3.5.20 Sonuç: $\mathcal{L}(A) = \mathcal{L}(B)$, $H \geq 0$ ve her $P \in suppH$ place'i için $v_P(A) = v_P(B)$ olacak şekildeki A, B ve $H \in Div(F)$ divizörleri göz önüne alınsın. O zaman $\mathcal{L}(A-H) = \mathcal{L}(B-H)$ dır [18].

3.5.21 Not: $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ ve $H \geq 0$ olacak şekildeki A, B ve $H \in Div(F)$ divizörleri göz önüne alınsın. En az bir $P \in suppH$ place'i için $v_P(A) \neq v_P(B)$ olsun. Bu durumda 3.5.19 Lemmanın gerçeklenemeyebileceği gösterilecektir.

$A = P$ ve $\ell(A) = 1$ olacak şekilde bir $P \in \mathcal{P}_F$ place'i göz önüne alınsın. $B = 0$ ve $H = P$ olsun. $\ell(A) = 1$ olduğundan $\mathcal{L}(A) = \mathbb{F}_q$ dır. Ayrıca $B = 0$ olduğundan 2.3.11 Lemma a) gereğince $\mathcal{L}(B) = \mathbb{F}_q$ dır. Bu durumda $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ olur.

Ancak $\mathcal{L}(A-H) = \mathcal{L}(0) = \mathbb{F}_q$ ve 2.3.11 Lemma b) gereğince $\mathcal{L}(B-H) = \mathcal{L}(-P) = \{0\}$ olduğundan $\mathcal{L}(A-H) \nsubseteq \mathcal{L}(B-H)$ dır [18].

Sıradaki teorem kanıtıyla birlikte verilmiştir.

3.5.22 Teorem (Güneri-Stichtenoth-Taşkın Sınırı): $(suppA \cup suppB \cup suppC \cup suppZ) \cap suppD = \emptyset$, $\mathcal{L}(A) = \mathcal{L}(A-Z)$, $\mathcal{L}(B) = \mathcal{L}(B+Z)$ ve $\mathcal{L}(C) = \mathcal{L}(B)$ olacak şekildeki A, B, C ve $Z \in Div(F)$ divizörleri göz önüne alınsın. O zaman $G = A + B$ olmak üzere $d(C_\Omega(D,G)) \geq degG - (2.g-2) + degZ + (i(A) - i(G-C))$ dır [18].

Kanıt:

$C_\Omega(D,G) \neq 0$ olduğundan en az bir $\omega \in \Omega_F(G-D)$, $\omega \neq 0$ Weil diferansiyeli için, minimum ağırlığa sahip olacak şekilde en az bir $(\omega_{P_1}(1), \omega_{P_2}(1), \dots, \omega_{P_n}(1))$ kod sözcüğü vardır. Bu kod sözcüğünün ağırlığı $d > 0$ olsun. $(\omega_{P_1}(1), \omega_{P_2}(1), \dots, \omega_{P_n}(1))$ kod sözcüğünün ilk d bileşeninin sıfırdan farklı ve diğerlerinin sıfır olduğu varsayılabilir.

$D' = \sum_{i=1}^{d} P_i$ divizörü göz önüne alınsın. 3.5.7 Teoremde de olduğu gibi $i = i_1, i_2, \dots, i_d$ için $P_i \notin suppE$ olmak üzere, $(\omega) = G - D' + E$ olacak şekilde en az bir $E \in Div(F)$, $E \geq 0$ divizörü vardır. Bir doğal divizörün derecesinin $2g - 2$ olacağı göz önünde bulundurulursa, $d = degG - (2.g - 2) + degE$ elde edilir.

$degE \geq degZ + (i(A) - i(G - C))$ olduğu gösterilecektir. 2.3.25 Tanım gereğince $i(A) = \ell(A) - degA + g - 1$ ve $i(A + E) = \ell(A + E) - deg(A + E) + g - 1$ dir. Böylece $degE = (\ell(A + E) - \ell(A)) + (i(A) - i(A + E))$ dir.

Şimdi $\ell(A + E) - \ell(A) \geq degZ$ olduğu gösterilecektir. $\ell(A) = \ell(A - Z)$ olduğundan $\ell(A + E) - \ell(A) = \ell(A + E) - \ell(A - Z)$ olur. $E \geq 0$ olduğundan 2.3.12 Lemma gereğince $\ell(A + E) - \ell(A - Z) \geq \ell(A + E) - \ell((A - Z) + E)$ elde edilir. Riemann-Roch Teoremi (2.3.48 Teorem) gereğince,

$$\ell(A + E) = deg(A + E) + 1 - g + \ell((\omega) - A - E) \tag{3.31}$$

ve

$$\ell((A - Z) + E) = deg((A - Z) + E) + 1 - g + \ell((\omega) - (A - Z) - E) \tag{3.32}$$

olduğundan $\ell(A + E) - \ell((A - Z) + E) = degZ + \ell((\omega) - A - E) - \ell((\omega) - (A - Z) - E)$ olur. $(\omega) = G - D' + E$ olduğundan $degZ + \ell((\omega) - A - E) - \ell((\omega) - (A - Z) - E) = degZ + \ell(B - D') - \ell((B + Z) - D')$ olur.

$\mathcal{L}(B) = \mathcal{L}(B + Z)$ ve her $P \in suppD'$ place'i için $v_P(B) = v_P(B + Z)$ olduğundan 3.5.20 Sonuç gereğince $\ell(B - D') = \ell((B + Z) - D')$ olur. Böylece $\ell(A + E) - \ell(A) \geq degZ$ olduğu görülmüş olur.

Şimdi $i(G - C) \geq i(A + E)$ olduğu gösterilecektir. 2.3.47 Teorem gereğince $i(G - C) = \ell((\omega) - G + C)$ dır. $(\omega) = G - D' + E$ olduğu göz önünde bulundurulursa $\ell((\omega) - G + C) = \ell(C - D' + E)$ elde edilir. $E \geq 0$ olduğundan 2.3.12 Lemma gereğince $\ell(C - D' + E) \geq \ell(C - D')$ olur. $\mathcal{L}(C) = \mathcal{L}(B)$ ve her $P \in suppD'$ place'i için $v_P(C) = v_P(B)$ olduğundan 3.5.20 Sonuç gereğince $\ell(C - D') = \ell(B - D')$ dir. $(\omega) = G - D' + E$ olduğu göz önünde bulundurulursa $\ell(B - D') = \ell((\omega) - A - E)$

olur. 2.3.47 Teorem gereğince $i(A+E)=\ell((\omega)-A-E)$ olduğundan $i(G-C)\geq i(A+E)$ olduğu görülmüş olur.

Sonuç olarak $\ell(A+E)-\ell(A)\geq degZ$ ve $i(G-C)\geq i(A+E)$ olduğundan $degE\geq degZ+(i(A)-i(G-C))$ olduğu görülmüş olur. Böylece 3.5.22 Teorem kanıtlanmış olur [18].

3.5.23 Not: 3.5.22 Teorem göz önüne alınsın. $C=B$ olduğu varsayılsın. $G=A+B$ olduğundan $i(A)-i(G-C)=i(A)-i(A)=0$ olur. Böylece $i(A)-i(G-C)\geq 0$ olduğu varsayılabilir [18].

3.5.24 Sonuç: Lundell-McCullough sınırı, Güneri-Stichtenoth-Taşkın sınırının özel bir durumudur [18].

Kanıt:

$Z\geq 0$, $\mathcal{L}(A)=\mathcal{L}(A-Z)$, $\mathcal{L}(B)=\mathcal{L}(B+Z)$ olacak şekildeki $A, B, Z\in Div(F)$ divizörleri göz önüne alınsın. $(suppA\cup suppB\cup suppZ)\cap suppD=\emptyset$ ve $G=A+B$ olsun. $C=B$ olarak tanımlanırsa 3.5.22 Teoreminin ön koşulları sağlanmış olur.

Böylece 3.5.22 Teorem gereğince $d(C_\Omega(D,G))\geq degG-(2.g-2)+degZ+(i(A)-i(G-C))$ olur. $C=B$ olduğundan $i(A)-i(G-C)=i(A)-i(A)=0$ dır. Bu durumda $d(C_\Omega(D,G))\geq degG-(2.g-2)+degZ$ olacağından istenilen elde edilir.

3.5.25 Örnek: 3.5.9 Örnekte verilen $\mathbb{F}_8(x,y)$ / $\mathbb{F}_8$ fonksiyon cismi göz önüne alınsın.

$G=17.P_\infty+11.P_{0,0}$ olsun. $\mathbb{F}_8(x,y)$ / $\mathbb{F}_8$ fonksiyon cisminin, P_∞ ve $P_{0,0}$ dan farklı rasyonel placelerinin toplamı $D=P_1+\cdots+P_{63}$ olmak üzere $C_\Omega(D,G)$ cebirsel geometrik kodu göz önüne alınsın.

$\mathcal{L}(13.P_\infty+3.P_{0,0})=\mathcal{L}(15.P_\infty+3.P_{0,0})$ ve $\mathcal{L}(8.P_{0,0})=\mathcal{L}(2.P_\infty+8.P_{0,0})=\mathcal{L}(4.P_\infty+8.P_{0,0})$ dır. Bu nedenle $A=15.P_\infty+3.P_{0,0}$, $B=2.P_\infty+8.P_{0,0}$, $C=8.P_{0,0}$ ve $Z=2.P_\infty$ olarak tanımlanırsa 3.5.22 Teoreminin ön koşulları sağlanmış olur. Böylece 3.5.22 Teorem gereğince $d(C_\Omega(D,G))\geq degG-(2.g-2)+degZ+(i(A)-i(G-C))=28-(2.14-2)+2+1=5$ elde edilir.

Lundell-McCullough sınırı bu gelişmeyi sağlayamamaktadır. Lundell-McCullough sınırı gereğince, $C_\Omega(D,G)$ kodunun minimum uzaklığı için $d \geq 4$ elde edilir [18].

3.5.26 Not: 3.5.22 Teorem göz önüne alınsın. $\mathcal{L}(A) = \mathcal{L}(A-Z)$ olduğundan 2.3.25 Tanım gereğince $i(A-Z) - i(A) = \ell(A-Z) - deg(A-Z) + g - 1 - \ell(A) + degA - g + 1 = degZ$ olur.

Böylece $degZ + i(A) - i(G-C) = i(A-Z) - i(G-C)$ elde edilir. 2.3.23 Teorem a) gereğince $i(G-C) \geq 0$ olduğundan $degZ + i(A) - i(G-C) \leq i(A-Z)$ bulunur. Bu nedenle Güneri-Stichtenoth-Taşkın sınırı kullanılarak bir cebirsel geometrik kodun tasarlanmış uzaklığı üzerinde elde edilebilecek gelişme $i(A-Z)$ sayısı ile sınırlıdır [18].

Güneri-Stichtenoth-Taşkın sınırı, I. Duursma ve S. Park tarafından geliştirilmiştir [20].

Sıradaki lemma kanıtıyla birlikte verilmiştir.

3.5.27 Lemma: D', $E \geq 0$ ve $suppE \cap suppD' = \emptyset$ olmak üzere, $(\omega) = G - D' + E$ olacak şekilde bir $\omega \in \Omega_F$, $\omega \neq 0$ Weil diferansiyeli göz önüne alınsın. $Z \geq 0$ ve $suppZ \cap suppD' = \emptyset$ olmak üzere, $G = A + B + Z$ olsun. O zaman $degD' \geq \ell(A) - \ell(A-D') + \ell(B) - \ell(B-D')$ dır [20].

Kanıt:

$\varphi_1 : \mathcal{L}(A) \,/\, \mathcal{L}(A-D') \longrightarrow \mathcal{L}(A+E) \,/\, \mathcal{L}(A+E-D')$, $x + \mathcal{L}(A-D') \mapsto x + \mathcal{L}(A+E-D')$ şeklinde tanımlı dönüşüm göz önüne alınsın. φ_1 dönüşümü iyi tanımlı, kapalı ve $\mathbb{F}_q$-lineerdir.

$Ker\varphi_1 = \{\mathcal{L}(A-D')\}$ olduğu gösterilecektir. $\varphi_1(\mathcal{L}(A-D')) = \mathcal{L}(A+E-D')$ olduğundan $\mathcal{L}(A-D') \in Ker\varphi_1$ dır. Diğer taraftan herhangi bir $x + \mathcal{L}(A-D') \in Ker\varphi_1$ elemanı göz önüne alınsın ve $x \notin \mathcal{L}(A-D')$ olduğu kabul edilsin.

$x \in \mathcal{L}(A)$ olduğundan en az bir $P \in suppD'$ place'i için $v_P(x) < -v_P(A-D')$ dir. Ayrıca $x + \mathcal{L}(A-D') \in Ker\varphi_1$ olduğundan $x \in \mathcal{L}(A+E-D')$ dır. Böylece

$v_P(x) \geq -v_P(A+E-D')$ elde edilir. $suppE \cap suppD' = \emptyset$ olduğundan $v_P(E) = 0$ dır. Bu sebeple $v_P(x) \geq -v_P(A-D')$ elde edilir. Ancak bu $v_P(x) < -v_P(A-D')$ olması ile çelişir. Bu nedenle $x \in \mathcal{L}(A-D')$ dir. Böylece $x + \mathcal{L}(A-D') \in \{\mathcal{L}(A-D')\}$ olacağından istenilen elde edilir.

$Ker\varphi_1 = \{\mathcal{L}(A-D')\}$ olduğundan φ_1 dönüşümü birebirdir.

$\varphi_2 : \mathcal{L}(B) \,/\, \mathcal{L}(B-D') \longrightarrow \mathcal{L}(B+Z) \,/\, \mathcal{L}(B+Z-D')$, $x + \mathcal{L}(B-D') \mapsto x + \mathcal{L}(B+Z-D')$ şeklinde tanımlı dönüşüm göz önüne alınsın. φ_2 dönüşümü iyi tanımlı, kapalı ve $\mathbb{F}_q$-lineerdir. φ_2 dönüşümünün birebir olduğu benzer şekilde gösterilebilir.

2.3.25 Tanım gereğince $i(A+E) = \ell(A+E) - deg(A+E) + g - 1$ ve $i(A+E-D') = \ell(A+E-D') - deg(A+E-D') + g - 1$ dir. Böylece $degD' = \ell(A+E) - \ell(A+E-D') + i(A+E-D') - i(A+E)$ elde edilir.

2.3.47 Teorem gereğince $i(A+E-D') = \ell((\omega) - A - E + D')$ ve $i(A+E) = \ell((\omega) - A - E)$ dir. $(\omega) = G - D' + E$ olduğu göz önünde bulundurulursa $degD' = \ell(A+E) - \ell(A+E-D') + \ell(B+Z) - \ell(B+Z-D')$ olur.

φ_1 ve φ_2 dönüşümleri birebir olduğundan sırasıyla,

$$\ell(A+E) - \ell(A+E-D') \geq \ell(A) - \ell(A-D') \tag{3.33}$$

ve

$$\ell(B+Z) - \ell(B+Z-D') \geq \ell(B) - \ell(B-D') \tag{3.34}$$

olur. Böylece $degD' \geq \ell(A) - \ell(A-D') + \ell(B) - \ell(B-D')$ olacağından kanıt tamamlanmış olur [20].

3.5.28 Not: 3.5.27 Lemma göz önüne alınsın. $Z \geq 0$ şartı daha zayıf olan $\mathcal{L}(B) \subseteq \mathcal{L}(B+Z)$ şartı ile değiştirilebilir. Ancak bu $degD'$ için daha iyi bir alt sınırın elde edilmesini sağlamaz.

$\mathcal{L}(B) \subseteq \mathcal{L}(B+Z)$ ve $suppZ \cap suppD' = \emptyset$ olmak üzere, $G = A + B + Z$ olsun. $Z^+, Z^- \geq 0$ ve $suppZ^+ \cap suppZ^- = \emptyset$ olmak üzere $Z = Z^+ - Z^-$ yazılabilir. Böylece Riemann-Roch uzayı tanımı gereğince $\mathcal{L}(B) = \mathcal{L}(B) \cap \mathcal{L}(B+Z) = \mathcal{L}(B-Z^-)$ olur.

Ayrıca $suppZ \cap suppD' = \emptyset$ olduğundan her $P \in suppD'$ place'i için $v_P(B) = v_P(B - Z^-)$ dir. Böylece 3.5.20 Sonuç gereğince $\mathcal{L}(B - D') = \mathcal{L}(B - Z^- - D')$ dir.

$Z^+ \geq 0$ ve $suppZ^+ \cap suppD' = \emptyset$ olmak üzere $G = A + (B - Z^-) + Z^+$ şeklinde yazılabileceğinden 3.5.27 Lemma gereğince $degD' \geq \ell(A) - \ell(A - D') + \ell(B - Z^-) - \ell(B - Z^- - D') = \ell(A) - \ell(A - D') + \ell(B) - \ell(B - D')$ olur [20].

Sıradaki teorem kanıtıyla birlikte verilmiştir.

3.5.29 Teorem (ABZ Sınırı): $Z \geq 0$ ve $(suppA \cup suppB \cup suppZ) \cap suppD = \emptyset$ olmak üzere, $G = A + B + Z$ olsun. O zaman $W \in Div(F)$ bir doğal divizör ve $C = G - W$ olmak üzere,

$$d(C_\Omega(D, G)) \geq \ell(A) - \ell(A - C) + \ell(B) - \ell(B - C) \tag{3.35}$$

dır [20].

Kanıt:

$C_\Omega(D, G) \neq 0$ olduğundan en az bir $\omega \in \Omega_F(G - D)$, $\omega \neq 0$ Weil diferansiyeli için, minimum ağırlığa sahip olacak şekilde en az bir $(\omega_{P_1}(1), \omega_{P_2}(1), \dots, \omega_{P_n}(1))$ kod sözcüğü vardır. Bu kod sözcüğünün ağırlığı $d > 0$ olsun. $(\omega_{P_1}(1), \omega_{P_2}(1), \dots, \omega_{P_n}(1))$ kod sözcüğünün ilk d bileşeninin sıfırdan farklı ve diğerlerinin sıfır olduğu varsayılabilir.

$D' = \sum_{i=1}^{d} P_i$ divizörü göz önüne alınsın. 3.5.7 Teoremde de olduğu gibi $\omega \in \Omega_F(G - D')$ dir ve $i = i_1, i_2, \dots, i_d$ için $P_i \notin suppE$ olmak üzere, $(\omega) = G - D' + E$ olacak şekilde en az bir $E \in Div(F)$, $E \geq 0$ divizörü vardır.

Ayrıca $Z \geq 0$, $suppZ \cap suppD = \emptyset$ ve $G = A + B + Z$ olduğundan 3.5.27 Lemma gereğince $degD' \geq \ell(A) - \ell(A - D') + \ell(B) - \ell(B - D')$ olur.

Şimdi $C = G - (\omega)$ olmak üzere $degD' \geq \ell(A) - \ell(A - C) + \ell(B) - \ell(B - C)$ olduğu gösterilecektir. 2.3.47 Teorem gereğince $\Omega_F(G - D') \simeq \mathcal{L}((\omega) - G + D')$ olur. $(\omega) - G + D' = D' - C$ dir. Ayrıca $\omega \in \Omega_F(G - D')$, $\omega \neq 0$ olduğundan $\mathcal{L}(D' - C) \neq \{ 0 \}$ dır. 2.3.9 Teorem gereğince $H \sim D' - C$ ve $H \geq 0$ olacak şekilde en az bir $H \in Div(F)$ divizörü vardır. Bu durumda $A - C \sim A - D' + H$ olacağından 2.3.10 Lemma b)

gereğince $\ell(A-C)=\ell(A-D'+H)$ olur. $H\geq 0$ olduğundan 2.3.12 Lemma gereğince $\ell(A-C)\geq\ell(A-D')$ olur. Benzer şekilde $\ell(B-C)\geq\ell(B-D')$ olduğu da gösterilebilir. Sonuç olarak $degD'\geq\ell(A)-\ell(A-C)+\ell(B)-\ell(B-C)$ olduğu görülmüş olur.

$d(C_\Omega(D,G))=degD'$ olduğundan 3.5.29 Teorem kanıtlanmış olur [20].

3.5.30 Not: 3.5.29 Teorem göz önüne alınsın. ABZ sınırı kullanılarak bir cebirsel geometrik kodun minimum uzaklığı üzerinde elde edilebilecek gelişmenin $degC+degZ$ sayısı ile sınırlı olacağı gösterilecektir.

2.3.25 Tanım gereğince $i(A)=\ell(A)-degA+g-1$ ve $i(A-C)=\ell(A-C)-deg(A-C)+g-1$ dir. Böylece $\ell(A)-\ell(A-C)+\ell(B)-\ell(B-C)=degC+i(A)-i(A-C)+\ell(B)-\ell(B-C)$ olur. 2.3.47 Teorem gereğince $i(A)=\ell(W-A)$ ve $i(A-C)=\ell(W-A+C)$ dir. $W=G-C$ olduğu da göz önünde bulundurulursa $\ell(A)-\ell(A-C)+\ell(B)-\ell(B-C)=degC+\ell(B+Z-C)-\ell(B+Z)+\ell(B)-\ell(B-C)$ bulunur. Yine 2.3.25 Tanım gereğince $i(B+Z-C)=\ell(B+Z-C)-deg(B+Z-C)+g-1$ ve $i(B-C)=\ell(B-C)-deg(B-C)+g-1$ olduğundan $\ell(A)-\ell(A-C)+\ell(B)-\ell(B-C)=degC+degZ+i(B+Z-C)-\ell(B+Z)+\ell(B)-i(B-C)$ olur. 2.3.47 Teorem gereğince $i(B+Z-C)=\ell(W-B-Z+C)$ ve $i(B-C)=\ell(W-B+C)$ dir. Yine $W=G-C$ olduğu göz önünde bulundurulursa $\ell(A)-\ell(A-C)+\ell(B)-\ell(B-C)=degC+degZ+\ell(A)-\ell(A+Z)+\ell(B)-\ell(B+Z)$ elde edilir.

$Z\geq 0$ olduğundan 2.3.12 Lemma gereğince $\ell(A+Z)\geq\ell(A)$ ve $\ell(B+Z)\geq\ell(B)$ olur. Böylece istenilen elde edilir [20].

3.5.31 Sonuç: Güneri-Stichtenoth-Taşkın sınırı, ABZ sınırının özel bir durumudur [20].

Kanıt:

$(suppA\cup suppB\cup suppC\cup suppZ)\cap suppD=\emptyset$, $\mathcal{L}(A)=\mathcal{L}(A-Z)$, $\mathcal{L}(B)=\mathcal{L}(B+Z)$ ve $\mathcal{L}(C)=\mathcal{L}(B)$ olacak şekilde A, B, C ve $Z\in Div(F)$ divizörleri göz önüne alınsın ve $G=A+B$ olsun.

Eğer gerekli ise C divizörü, $gcd(C, B+Z)$ divizörüyle değiştirilerek $C \leq B+Z$ olduğu varsayılabilir. Böylece en az bir $H \in Div(F)$, $H \geq 0$ divizörü için $C+H = B+Z$ olur. Bu durumda $G = (A-Z)+C+H$ şeklinde yazılabilir. Ayrıca $H \geq 0$ ve $(supp(A-Z) \cup suppC \cup suppH) \cap suppD = \emptyset$ olduğundan 3.5.29 Teoreminin ön koşulları sağlanmış olur. O zaman $W \in Div(F)$ bir doğal divizör ve $T = G - W$ olmak üzere 3.5.29 Teorem gereğince $d(C_\Omega(D,G)) \geq \ell(A-Z) - \ell(A-Z-T) + \ell(C) - \ell(C-T)$ olur. 3.5.30 Nottakine benzer bir şekilde $\ell(A-Z) - \ell(A-Z-T) + \ell(C) - \ell(C-T) = degT + degH + \ell(A-Z) - \ell(A-Z+H) + \ell(C) - \ell(C+H)$ olduğu gösterilebilir.

$H = B+Z-C$, $\mathcal{L}(B) = \mathcal{L}(B+Z)$ ve $\mathcal{L}(C) = \mathcal{L}(B)$ olduğu göz önünde bulundurulursa $\ell(C) - \ell(C+H) = 0$ olur.

$\mathcal{L}(A) = \mathcal{L}(A-Z)$ ve $G = (A-Z)+C+H$ olduğundan $\ell(A-Z) - \ell(A-Z+H) = \ell(A) - \ell(G-C)$ olur. 2.3.25 Tanım gereğince $i(A) = \ell(A) - degA + g - 1$ ve $i(G-C) = \ell(G-C) - deg(G-C) + g - 1$ olduğundan $\ell(A) - \ell(G-C) = i(A) - i(G-C) + degZ - degH$ elde edilir.

Ayrıca $T = G - W$ ve 2.3.49 Sonuç gereğince $degW = 2g-2$ olduğundan $degT = degG - 2g + 2$ dir.

Sonuç olarak $d(C_\Omega(D,G)) \geq degG - 2g + 2 + degZ + i(A) - i(G-C)$ elde edileceğinden kanıt tamamlanır [20].

3.5.9 Örnekte verilen $\mathbb{F}_8(x,y)$ / $\mathbb{F}_8$ fonksiyon cismi göz önüne alınsın. $\mathbb{F}_8(x,y)$ / $\mathbb{F}_8$ fonksiyon cisminin, P_∞ ve $P_{0,0}$ dan farklı rasyonel placelerinin toplamı $D = P_1 + \cdots + P_{63}$ ile gösterilsin. Lundell-McCullough, Güneri-Stichtenoth-Taşkın ve ABZ sınırı için en uygun seçimler yapılarak elde edilen gelişmeler sırasıyla d_{LM}, d_{GST} ve d_{ABZ} ile gösterilmek üzere Tablo 3.1 de bu gelişmeler verilmiştir. d_{GOP} ile bu geometrik cebirsel kodların tasarlanmış uzaklıkları gösterilmektedir.

Kod	d_{GOP}	d_{LM}	d_{GST}	d_{ABZ}
$C_\Omega(D, G = 22.P_\infty + 4.P_{0,0})$	0	3	4	4
$C_\Omega(D, G = 21.P_\infty + 5.P_{0,0})$	0	3	4	4
$C_\Omega(D, G = 20.P_\infty + 6.P_{0,0})$	0	4	5	5
$C_\Omega(D, G = 20.P_\infty + 7.P_{0,0})$	1	4	5	5
$C_\Omega(D, G = 23.P_\infty + 4.P_{0,0})$	1	4	5	5
$C_\Omega(D, G = 21.P_\infty + 6.P_{0,0})$	1	4	5	5
$C_\Omega(D, G = 22.P_\infty + 6.P_{0,0})$	2	5	6	6
$C_\Omega(D, G = 24.P_\infty + 4.P_{0,0})$	2	4	5	5
$C_\Omega(D, G = 24.P_\infty + 5.P_{0,0})$	3	5	6	6
$C_\Omega(D, G = 24.P_\infty + 6.P_{0,0})$	4	6	7	7
$C_\Omega(D, G = 26.P_\infty + 4.P_{0,0})$	4	6	7	7
$C_\Omega(D, G = 24.P_\infty + 3.P_{0,0})$	1	3	3	3
$C_\Omega(D, G = 27.P_\infty)$	1	2	2	2
$C_\Omega(D, G = 30.P_\infty + 1.P_{0,0})$	5	7	7	8
$C_\Omega(D, G = 32.P_\infty + 1.P_{0,0})$	7	9	9	10
$C_\Omega(D, G = 40.P_\infty)$	14	15	15	15

Tablo 3.1 [20].

BÖLÜM 4

SONUÇLAR VE TARTIŞMA

Bu çalışmada, fonksiyon cismi teorisi ile kodlama teorisi arasındaki literatürde verilen ilişki incelenmiştir. Cebirsel geometrik kodların parametreleri hakkında, fonksiyon cismi teorisinin en önemli teoremi olan Riemann-Roch teoremi yardımıyla yorumda bulunulabilir ve böylece iyi parametrelere sahip kodlar elde edilebilir. Reed-Solomon, BCH ve "klasik" Goppa kodları gibi pratikte kullanılan en önemli kodlardan bazıları cebirsel geometrik kodlar olarak temsil edilebilir. Belli cebirsel geometrik kodlar, asimptotik Gilbert-Varshamov Sınırını geçmektedir. Ayrıca bir divisorün tabanı kavramı yardımıyla cebirsel geometrik kodların tasarlanmış uzaklığı üzerinde bir dizi gelişme elde edilebilmektedir.

KAYNAKLAR

[1] R. Dedekind, H. Weber, ***Theorie der algebraischen Funktionen einer Veränderlichen***, Journ. für Math., 92, 181-290, (1882)

[2] Henning Stichtenoth, ***Algebraic Function Fields and Codes*** (Springer-Verlag, Berlin, 2009)

[3] C. Chevalley, ***Introduction to the Theory of Algebraic Functions of One Variable*** (American Mathematical Society, Rhode Island, 1951)

[4] M. Deuring, ***Lectures on the theory of algebraic functions of one variable***, (Springer-Verlag, Berlin, 1973)

[5] V. D. Goppa, ***Codes on algebraic curves***, Soviet Math. Dokl. 24, No. 1, 170-172, (1981)

[6] M. A. Tsfasman, S. G. Vladut, T. Zink, ***Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound***, Math. Nachrichten, 109, 21-28, (1982)

[7] Y. I. Manin, ***What is the maximum number of points on a curve over*** $\mathbb{F}_2$ ***?***, J. Fac. Sci. Univ. Tokyo Sect. IA Math, 28, 715-720, (1981)

[8] Gui Liang Feng, T.R.N. Rao, ***Decoding algebraic-geometric codes up to the designed minimum distance***, IEEE Trans. Inform. Theory, 39 (1), 37-45, (1993)

[9] Hiren Maharaj, Gretchen L. Matthews, ***On the floor and the ceiling of a divisor***, Finite Fields Appl., 12 (1), 38-55, (2006)

[10] Hiren Maharaj, Gretchen L. Matthews, Gottlieb Pirsic, ***Riemann-Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences***, Journal of Pure and Applied Algebra, 195, 261-280, (2005)

[11] E. Arbello, M. Cornalba, P. Griffiths, J. Harris, ***Geometry of Algebraic Curves*** (Springer, Berlin, 1985)

[12] E. Ballico, S.J. Kim, ***Weierstrass multiple loci of n-pointed algebraic curves***, J. Algebra, 199, 455-471, (1998)

[13] M. Homma, J. Kim, ***Goppa codes with Weierstrass pairs***, Journal of Pure and Applied Algebra, 162, 273-290, (2001)

[14] C. Carvalho, F. Torres, ***On Goppa codes and Weierstrass gaps at several points***, Des. Codes Cryptogr., 35 (2), 211-225, (2005)

[15] B. Lundell, J. McCullough, ***A generalized floor bound for the minimum distance of geometric Goppa codes***, Journal of Pure and Applied Algebra, 207, 155-164, (2006)

[16] C. Kirfel, R. Pellikaan, ***The minimum distance of codes in an array coming from telescopic semigroups***, IEEE Transactions on Information Theory, 41 (6), Birinci kısım, (1995)

[17] A. Garcia, R. F. Lax, ***Goppa codes and Weierstrass gaps***, in: Lecture Notes in Math., vol. 1518, 33-42, (1992)

[18] Cem Güneri, Henning Stichtenoth, İhsan Taşkın, ***Further Improvements on the designed minimum distance of algebraic geometry codes***, Journal of Pure and Applied Algebra, 213, 87-97, (2009)

[19] K. Yang, P. V. Kumar, H. Stichtenoth, ***On the weight hierarchy of geometric Goppa codes***, IEEE Transactions on Information Theory, IT-40, (1994)

[20] I. Duursma, R. Kirov, S. Park, ***Distance bounds for algebraic geometric codes***, Journal of Pure and Applied Algebra, 215, 1863-1878, (2011)

ÖZGEÇMİŞ

28.11.1989 tarihinde İstanbul'da doğdum. İlkokul ve ortaokul öğretimimi Bağcılar Malazgirt İlköğretim Okulu'nda, lise öğretimimi de Akşemsettin Lisesi'nde 2006 yılında tamamladım. 2006 yılında kayıt olduğum Çanakkale Onsekiz Mart Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü'nden 2011 yılında mezun oldum. Bir yıl özel bir dershanede ve altı ay Milli Eğitim Bakanlığı'nda matematik öğretmeni olarak çalıştıktan sonra 2015 yılında Trakya Üniversitesi Fen Fakültesi Matematik Bölümü Cebir ve Sayılar Teorisi Anabilim Dalı'na Araştırma Görevlisi olarak atandım ve görevimi halen sürdürmekteyim.

BİLİMSEL FAALİYETLER

Katıldığı Kongre	: Trakya Üniversiteler Birliği II. Lisansüstü Öğrenci Kongresi, 15-16 Mayıs 2017
Bildiri Adı	: Cebirsel Geometrik Kodlar
Düzenleyen Kuruluş	: Trakya Üniversitesi