AĞIRLIKLI PROJEKTİF UZAYLAR ÜZERİNDEKİ KODLAR VE ONLARIN CEBİRSEL DEĞİŞMEZLERİ

CODES ON WEIGHTED PROJECTIVE SPACES AND THEIR ALGEBRAIC INVARIANTS

YAĞMUR ÇAKIROĞLU

PROF. DR. MESUT ŞAHİN

Danışman

Hacettepe Üniversitesi

Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin

Matematik Anabilim Dalı için Öngördüğü

DOKTORA TEZİ olarak hazırlanmıştır

Ağustos 2024

Yeğenim Can Sarıkaya'ya ithafen.

ÖZET

AĞIRLIKLI PROJEKTİF UZAYLAR ÜZERİNDEKİ KODLAR VE ONLARIN CEBİRSEL DEĞİŞMEZLERİ

Yağmur Çakıroğlu
Doktora, Matematik Bölümü
Danışman: Prof. Dr. Mesut Şahin
Ağustos 2024, 125 sayfa

Ağırlıklı projektif uzay, projektif uzayın geometrik tanımını dikkate aldığımızda ve aşikâr olmayan ağırlıklara izin verdiğimizde ortaya çıkan geometrik ve cebirsel açıdan özgün yapılardır. Burada aşikâr olmayan ağırlık ile kasıt, tüm ağırlıkların 1 olmadığı durumdur. Tüm ağırlıkların 1 olduğu durum projektif uzaya karşılık geldiği için aslında ağırlıklı projektif uzaylar, klasik projektif uzayların doğal genellemeleridir. Ağırlıklı projektif uzaylar, sonlu cisimler üzerinde ilginç lineer kod sınıfları oluşturmak için uygun ortamlar olarak kabul edilir. Bu kodlar, **Ağırlıklı Projektif Reed-Muller kodları** olarak bilinir. Klasik projektif Reed-Muller kodları (PRM kodları) Reed-Muller kodlarının (RM kodları) bir genişlemesidir. RM kodları, dijital iletişim kanallarında bilgiyi güvenilir bir şekilde iletmek için önemli bir rol oynayan hata düzeltme kodlarıdır. Klasik PRM kodları da iyi çalışılmış olup, çeşitli gerçek hayat uygulamalarında kullanılmaktadır. Bu tez çalışmasında, PRM kodlarının bir genişlemesi olan Ağırlıklı projektif Reed-Muller kodları üzerine çalışmalar yapılmıştır.

Özel olarak, a, b pozitif ve aralarında asal tam sayılar olmak üzere $\mathbb{P}(1, a, b)$ biçimindeki ağırlıklı projektif uzaylar ailesi üzerindeki kodlar incelenmiş olup bu kodların parametreleri hesaplanmıştır. İlk olarak, $a = 1$ durumu göz önünde bulundurulup $\mathbb{F}_q$, q elemanlı sonlu bir cisim ve $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$, $X = \mathbb{P}(1, 1, b)$ ağırlıklı projektif uzayının $\mathbb{F}_q$-rasyonel noktalar kümesi olmak üzere, bu kümeye karşılık gelen $C_{d,Y}$ kodunun temel parametreleri verilmiştir. Bu temel parametrelerden biri olan kodun boyutu ile ilgili sonuçlar cebirsel

değişmezlerden Hilbert fonksiyonu vasıtasıyla elde edilmiştir. Bu sebepten dolayı, sırasıyla, bu uzaya karşılık gelen sıfırlayan ideal $I(Y)$'nin serbest çözülümü, Hilbert serisi ve Hilbert fonksiyonunun değerleri elde edilmiştir. Aşikâr (trivial) kodları eleyebilmek için önemli olan düzenlilik indeksi ve dolayısıyla düzenlilik kümesi de elde edilmiştir. Daha sonra, tüm bu sonuçlar ve yöntemlere ek olarak geometrik ve kombinatorik yöntemler de göz önüne alınarak $X = \mathbb{P}(1, a, b)$ uzayından elde edilen kodların temel parametreleri hesaplanmıştır. Bu uzaya karşılık gelen çokgenin kafes noktaları ile kodun boyutu arasındaki ilişkinin referans alınmasıyla birlikte kodun boyutunu hesaplamamızı sağlayan formüller verilmiştir. Ek olarak, literatürde ayakizi sınırı (footprint bound) olarak bilinen bir sınır vasıtasıyla, Gröbner baz teorisi de baz alınarak, bu uzaydan elde edilen kodun minimum uzaklığı için bir alt sınır verilmiştir. Bu uzaya karşılık gelen rasyonel noktalar kümesinin de düzenlilik kümesi verilmiş olup, düzenlilik indeksi elde edilmiştir. Dolayısıyla, en genelde $X = \mathbb{P}(1, a, b)$ ağırlıklı projektif uzayından elde edilen hesaplama kodlarının temel parametreleri ve ilişkili diğer geometrik ve cebirsel sonuçlar bu tez çalışması kapsamında elde edilmiştir.

Anahtar Kelimeler: Kodlama Teorisi, Lineer Kodlar, Hilbert Fonksiyonu, Hilbert Serisi, Serbest Çözülümler, Ağırlıklı Projektif Uzay, Sonlu Cisimler, Ağırlıklı Projektif Reed-Muller Kodlar.

ABSTRACT

CODES ON WEIGHTED PROJECTIVE SPACES AND THEIR ALGEBRAIC INVARIANTS

Yağmur Çakıroğlu
Doctor of Philosophy, Department of Mathematics
Supervisor: Prof. Dr. Mesut Şahin
August, 2024, 125 pages

Weighted projective spaces, when considered in light of the geometric definition for projective spaces and allowing non-trivial weights, exhibit unique structures both geometrically and algebraically. By non-trivial weights, we mean scenarios where not all the weights are equal to 1. When all the weights are 1, the structure corresponds to the classical projective space; thus, weighted projective spaces can be viewed as natural generalizations of classical projective spaces. These spaces are recognized as suitable environments for constructing interesting classes of linear codes over finite fields. Such codes are known as Weighted Projective Reed-Muller Codes. Classical Projective Reed-Muller (PRM) codes extend Reed-Muller (RM) codes, which play a crucial role in reliably transmitting information over digital communication channels. Classical PRM codes have been thoroughly studied and are used in various real-world applications. This thesis focuses on the study of **Weighted Projective Reed-Muller Codes** which are an extension of PRM codes.

Specifically, codes over the family of weighted projective spaces of the form $\mathbb{P}(1, a, b)$, where a and b are positive coprime integers, have been examined, and their parameters have been calculated. First, considering the case $a = 1$, let $\mathbb{F}_q$ be a finite field with q elements, $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-rational points of the weighted projective space $X = \mathbb{P}(1, 1, b)$. The basic parameters of the code $C_{d,Y}$ corresponding to this set have been provided. Results concerning the dimension of the code, one of these basic parameters, have been derived

through the Hilbert function which is one of the algebraic invariants. Consequently, the free resolution of the vanishing ideal $I(Y)$ corresponding to this space, its Hilbert series, and the values of its Hilbert function have been obtained. The regularity index and hence the regularity set, which are essential for eliminating trivial codes, have also been determined. Subsequently, in addition to these results and methods, the basic parameters of the codes obtained from the space $X = \mathbb{P}(1, a, b)$ have been calculated, considering both geometric and combinatorial methods. Formulas for calculating the code's dimension have been provided, referencing the relationship between the lattice points of the corresponding polygon and the dimension of the code. Additionally, using a bound known in the literature as the footprint bound, and also based on Gröbner basis theory, a lower bound for the minimum distance of the code obtained from this space has been provided. The regularity set and the regularity index of the set of rational points corresponding to this space have also been determined. Therefore, the main parameters of the codes obtained from the weighted projective space $X = \mathbb{P}(1, a, b)$ and other related geometric and algebraic results have been obtained within the scope of this thesis.

Keywords: Coding Theory, Linear Codes, Hilbert Function, Hilbert Series, Free Resolution, Weighted Projective spaces, Finite Fields, Weighted Projective Reed-Muller Codes

TEŞEKKÜR

Öncelikle, 2017 yılından bu yana hem yüksek lisans ve doktora tez çalışmalarımda hem de akademik hayatımın oluşmasında büyük katkı sağlayan, bana değerli tecrübeleriyle yol gösteren, bu tezdeki çalışmaların oluşmasında ve yazım aşamasında çok büyük katkı sağlayan, değerli görüş ve önerileri ile destekleyen, hem sabrı ve motivasyonu ile çalışmalarımda beni teşvik eden hem de bana inanmaktan vazgeçmeyen çok değerli danışman hocam Prof. Dr. Mesut Şahin'e teşekkürü bir borç bilirim.

Değerli görüş ve önerileri için tez izleme komitesi üyesi olan Prof. Dr. Derya Keskin Tütüncü ve Doç. Dr. Oğuz Yayla hocalarıma ve ayrıca tez savunma jürisinde bulunan çok değerli hocalarıma çok teşekkür ederim.

Hayatıma girdiği andan itibaren her koşulda yanımda olan, beni her zaman dinleyen ve anlayan, akademik hayattaki duruşu ve çalışmalarıyla kendisinden çok şey öğrendiğim çok kıymetli hocam Prof. Dr. Aslı Pekcan'a ne kadar teşekkür etsem az kalır.

Bir yaz okulu vasıtasıyla tanıştığım, çalışmaları, enerjisi ve duruşu ile hayranlık bırakan çok değerli hocam ve meslektaşım Dr. Jade Nardi'ye bana birlikte çalışma fırsatı sağladığı, bana inandığı ve nazik davetiyle hayatımın en güzel tecrübelerinden birini yaşamama vesile olduğu için çok ama çok teşekkür ederim. Ziyaret ettiğim süreçte bu ziyaretin maddi açıdan gerçekleşmesine destek olan CIMPA ve Rennes 1 Üniversitesi IRMAR laboratuvarına teşekkür ederim. (I am deeply grateful to my esteemed mentor and colleague, Dr. Jade Nardi, whom I had the privilege to meet through a summer school. Her work, energy, and demeanor have left me deeply impressed. I extend my heartfelt thanks to her for providing me with the opportunity to collaborate, for believing in me, and for graciously inviting me to experience one of the most beautiful moments of my life. During my visit, I would like to express my gratitude to CIMPA and the IRMAR at University of Rennes 1 for their support in making this visit possible financially.)

Bu yolu seçerken bir kez olsun sorgulamayan, kararlarımda yanımda olan, bana her koşulda inanan ve koşulsuz sevgileri ile şanslı olduğumu hissettiren annem Çiğlem Çakıroğlu, babam Mehmet Çakıroğlu ve ablam Merve Burcu Sarıkaya'ya, çok teşekkür ederim. Özellikle de (ek parantez açmam gerekirse) ne zaman bir fikre ihtiyacım olsa, derdimi paylaşmak istesem, beni sıkılmadan dinleyen sevgili anneme, bana anne-kız olmaktan ziyade bir arkadaş gibi

davrandığı için çok teşekkür ederim. Ailemize son yıllarda katılan, herkesin gönlünü çalan, hayatıma girdiği andan itibaren beni birçok şeyle barıştıran dünyalar tatlısı yeğenim Can Sarıkaya'ya da çokça teşekkür ederim. Bu tez çalışması o küçük kalbin hayatıma dokunuşu ile daha da anlamlandı, bu yüzden kendisine ithaf ediyorum. Ayrıca, şimdi aramızda olmayan sevgili anneannem Nimet Ören'in bana her zaman inandığını ve hayatta olsaydı inanmaktan vazgeçmeyeceğini bilerek, bu motivasyonla bu yolu yürümekten vazgeçmediğim için kendisine teşekkürü bir borç bilirim.

Bu süreçte yalnız olmadığımı hissettiren, sevincimi de üzüntümü de paylaşan, beni anlayan, dinleyen, birlikteyken hayata daha enerjik ve mutlu bakabildiğim ömürlük dostlarım Hazal Öznar, Özge Uçar'a;

Liseden bu yana yılda bir kez görüşme fırsatı bulmamıza rağmen asla kopmadığım arkadaşlarım Umut Deniz Göktepe, Ece Çağır Atıcı ve Tuğba Erdemir Yaldız'a ve yıllardır kopmadığım çocukluk arkadaşım Tezcan Yılmaz Kılıç'a;

Çok değerli arkadaşlarım ve meslektaşlarım olan, süreçte desteklerini eksik etmedikleri gibi, akademide de yalnız hissettirmeyen Ilgaz Çakar, Tansılu Altay, Hamide Kuru Suluyer ve Esma Baran Özkan'a, çok ama çok teşekkür ederim.

Varlıklarıyla bu sürece eşlik eden, yaklaşık 8 yıldır her anımda yanımda olan ve huzur veren kedilerim Mars ve Jaya'ya, çok ama çok teşekkür ederim. Siz olmasaydınız, olmazdı.

Son olarak yürütücülüğünü danışman hocam Prof. Dr. Mesut Şahin'in yaptığı ve Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) 1001 Programı tarafından desteklenen 119F177 numaralı proje kapsamında burs veren ve ayrıca Bilim İnsanı Destek Programları Başkanlığı (BİDEB) altında yürürlükte olan $2211/A$ Yurtiçi Doktora Burs Programı kapsamında burs veren TÜBİTAK'a;

sonsuz teşekkürler...

İçindekiler

Tablolar

Figürler

SİMGELER VE KISALTMALAR

$\mathbb{N}$	Doğal sayılar kümesi
$\subset$	Kesin olarak kapsama
$\mathbb{A}^r$	r boyutlu Afin Uzay
$X = \mathbb{P}(w_1, \ldots, w_r)$	Ağırlıklı Projektif Uzay
$\mathbf{w}$	Ağırlık
$\mathbb{P}^r$	Projektif Uzay
$V(S)$	Çeşitlem
$V_{\mathbb{P}}(S)$	Projektif Çeşitlem
$\mathbb{K}$	Cisim
$\mathbb{F}_q$	q elemanlı sonlu cisim
$X(\mathbb{F}_q)$	X uzayının $\mathbb{F}_q$-rasyonel noktalar kümesi
$\mathbb{K}[Y]$	Y'nin Koordinat Halkası
$\bigoplus$	Dik toplam
$H_Y(d)$	Y'nin d derecesindeki Hilbert Fonksiyonu
$HS_Y(t)$	Y'nin Hilbert Serisi
$C_{d,Y}$	Y kümesi üzerinde bir hesaplama kodu
$\mathrm{der}(x)$	x elemanının derecesi
$\dim(I)$	I idealinin boyutu
$d(\mathcal{C}_1, \mathcal{C}_2)$	$\mathcal{C}_1$ ve $\mathcal{C}_2$ kodlarının Hamming uzaklığı
N	Kodun uzunluğu
$d_{\min}$ ya da δ	Minimum uzaklık
$\dim_{\mathbb{F}_q}(C_{d,Y})$	$C_{d,Y}$ kodunun boyutu
P_D	Çokgen

1. GİRİŞ

1.1 Tezin Kapsamı

Bu tez çalışması, temel olarak Ağırlıklı projektif uzaylar üzerindeki kod ailelerinin yapısını anlamaya odaklanmıştır ve bu sebeple bu kodların cebirsel ve geometrik yapıları incelenmiştir. Bu kodların temel parametreleri ile ilgili sonuçlar vermek için çalışmalar yapılmıştır. Bu tez çalışmasının ilk hedeflerinden biri olan cebirsel değişmezler ile kodlama teorisi arasındaki ilişki, çalışılan kod ailesinin parametreleri üzerinden verilmiştir. Tez dönemi boyunca yapılan tüm çalışmalardan elde edilen sonuçlar hem yöntemlerin hem de alınan uzayın farklı olmasından dolayı iki bilimsel makale altında toplanmıştır. Bu sebepten dolayı bu tez çalışmasında da yapılan çalışmalar iki farklı kısım altında anlatılacaktır. Ağırlıklı projektif uzay ve kodlama teorisi her iki çalışmanın da temeli olduğu için ilk olarak bu iki konu ele alınacaktır.

Tezin ilk bölümünde, ilk olarak afin ve projektif çeşitlemler anlatılarak ön hazırlık oluşturulmuştur. Sonrasında ağırlıklı projektif uzaylar ele alınmış olup (bknz. Alt Kısım (2.3)), örnekler ve literatürdeki bazı sonuçlarla bu uzayların yapıları anlatılmıştır. Bir sonraki bölümde Kodlama Teorisi ele alınmıştır, genel bir bakış sağlamak amacıyla bu alandaki tanım ve kavramlar ele alınmıştır (bknz. Alt Kısım (2.4)).

Daha sonraki bölümler **Kısım I** ve **Kısım II** olarak ikiye ayrılmıştır. İlk olarak **Kısım I**'de, cebirsel değişmezler başlığı altında (bknz. Alt Kısım (3.1)) dereceli polinom halkaları, dereceli idealler, bu ideallerin serbest çözülümleri, Hilbert serisi ve Hilbert fonksiyonu incelenmiştir. Ayrıca kodlama teorisinde de önemli bir yer tutan ve cebirsel değişmezlerden biri olan düzenlilik kümesi de bu kısımda tanıtılmıştır. Burada anlatılan tüm kavramlar ve verilen bazı teoremler tez çalışmasının ilk amaçlarından biri olan cebirsel değişmezler ve ağırlıklı projektif uzaylar üzerindeki kodlar arasındaki ilişkiyi kurabilmek için gereklidir. Sonraki alt kısımda (bknz. Alt Kısım (3.2)) *Algebraic Invariants of Codes on Weighted Projective Planes* adlı [1] referansıyla verilmiş olan bilimsel makale altında toplanmış sonuçlar verilecektir. Buradaki çalışmalarda b pozitif bir tam sayı olmak üzere, $X = \mathbb{P}(1,1,b)$ ağırlıklı projektif uzayı göz önünde bulundurulmuş olup bu uzayın $\mathbb{F}_q$-rasyonel noktaları kümesinde d dereceli polinomların hesaplanmasıyla elde edilen kodlar çalışılmıştır. Bu çalışmalar kapsamında bu uzayın sıfırlayan idealinin serbest çözülümü (free resolution) elde edilmiş olup, buradan Hilbert serisine ve dolayısıyla da Hilbert fonksiyonuna geçilerek

literatürde de bilinen kodun boyutu ve Hilbert fonksiyonu arasındaki ilişki sayesinde kodun boyutu ile ilgili sonuçlar elde edilmiştir. Ayrıca, aşikâr kodların (trivial codes) elenmesinde rol oynayan, bu sebeple önemli bir cebirsel değişmez olan düzenlilik kümesi ile ilgili de sonuç verilmiş olup, düzenlilik indeksi elde edilmiştir. Tüm bunlara ek olarak, bu uzaya karşılık gelen kodların bir başka temel parametresi olan minimum uzaklıkla ilgili de sonuçlar verilerek bu kodların tüm parametrelerinin hesaplanmasını sağlayan formüller elde edilmiştir. Dolayısıyla, bu kısımda kodlama teorisinin cebir ile ilişkisi vurgulanmış ve bu kısımdaki sonuçlarla birlikte tezin temel hedefine ulaşılmıştır. Sonraki hedefler olarak planmış durumlar için çalışmaya devam edilmiştir ve bu çalışmaların sonuçları diğer kısımda anlatılmıştır.

Kısım II adı altında toplanan tüm çalışmalar a, b pozitif ve aralarında asal tam sayılar olmak üzere, $X = \mathbb{P}(1, a, b)$ ağırlıklı projektif uzaylarındaki kodlar incelenmiştir. Bu kodların temel parametreleri ile ilgili olarak literatürde bilinmeyen boyut ve minimum uzaklıkla ilgili sonuçlar verilmiştir. Bu çalışmalarda bu uzaya karşılık gelen çokgenlerin integral noktaları (kafes noktaları), çalışılan halkanın bazını oluşturan monomlara karşılık geldiğinden, kodun boyutunu hesaplamak için bu kafes noktaları referans alınmıştır. Dolayısıyla buradaki yöntemler ilk kısımdaki yöntemlerden farklı olarak geometrik bakış açısına dayanmaktadır (bknz. Alt Kısım (4.2)). Bu çalışmalarda ayrıca bu uzayın rasyonel noktalar kümesinin sıfırlayan ideali ve düzenlilik kümesi ile ilgili sonuç verilmiştir. Ayrıca minimum uzaklık için verilecek olan alt sınır hesaplanırken, literatürde ayakizi sınırı (footprint bound) olarak da bilinen ve Gröbner baz teorisine dayanan sınır elde edilmiştir ve böylece minimum uzaklığa bir alt sınır verilmiştir. Bu çalışmalar da *Codes on Weighted Projective Planes* adlı, [2] referansıyla verilmiş olan bilimsel makale altında uluslararası bir dergide yayınlanmak üzere derlenmiştir.

1.2 Literatür

Reed-Muller kodları, literatürde, detaylı bir şekilde incelenmiş ve oldukça iyi anlaşılan doğrusal kodlar sınıfı oluşturur. Bu kodlar, ikili (binary) durumunda Muller [3] tarafından tanıtılmış ve 1954 yılında ise Reed [4] tarafından daha detaylı olarak incelenmiştir (detaylı tarihçesi ve daha fazla detaylı bilgi için bknz. [5]). Reed-Muller kodlarının q-ary durumuna genellemeleri, Kasami, Lin ve Peterson tarafından [6] ve Delsarte, Goethals ve MacWilliams [7] tarafından ele alınmış ve kapsamlı bir şekilde incelenmiştir. Berger ve Charpin [8] ve Heijnen ve Pellikaan [9] tarafından yapılan çalışmaların ve Reed ile Muller'in 1954 yılından

sonraki 10 yıl boyunca yapılan çalışmaların bir sonucu olarak, rastgele sıralı q-ary bir Reed-Muller kodları hakkında literatürde oldukça bilgi mevcuttur. Örneğin, uzunluk, boyut, minimum uzunluk, minimum ağırlıklı kod kelimelerinin analizi, genelleştirilmiş Hamming ağırlıkları gibi önemli olgular tamamen bilinmektedir.

Klasik genelleştirilmiş Reed-Muller kodlarının bir genişletilmesi olan, sonlu bir cisim üzerindeki Projektif Reed-Muller kodları literatürde ilk olarak Lachaud'un [10] makalesinde tanıtılmıştır. Bu kodlar, belirli bir projektif uzayın tüm $\mathbb{F}_q$-rasyonel noktalarında homojen polinomların hesaplanmasıyla elde edilir. Reed-Muller kodları, dijital iletişim kanallarında bilgiyi güvenilir bir şekilde iletmede önemli bir rol oynayan hata düzeltme kodlarıdır (error-correcting codes). Lachaud tarafından yine aynı makalede bu kodların uzunluğu ve boyutu ile minimum uzaklık için sınır elde edilmiştir. Ayrıca derece $d = 2$ ve $r \geq 2$ olmak üzere $q = 2^r$, olduğu durumda da minimum uzaklık tam olarak verilmiştir [10]. Tsfasman, belirli bir $d \leq q$ derecesindeki bir projektif hiperyüzeyin $\mathbb{F}_q$-rasyonel noktalarının sayısı için tam bir sınır vermiştir. Bu sınır, Serre [11] tarafından kanıtlanmış ve daha sonra Lachaud [12] tarafından, $d \leq q$ olduğu durumlar göz önüne alınarak ve Serre'nin eşitsizliği ile bağlantılı olarak projektif Reed-Muller kodlarının mimimum uzaklığına bir sınır verilmiştir. Sørensen [13] PRM kodlarının sadece $d \leq q$ durumunda değil, herhangi bir d derecesi için uzunluk, boyut ve minimum uzaklık için formül vermiştir. Çok yakın bir zamanda, Sørensen'in herhangi bir d derecesi için olan formülünün kanıtında bir hata görülmüş olup ve teoremin ifadesi doğru olduğu için [14] makalesinde Ghorpade ve Ludhani tarafından bu ispattaki eksiklikler giderilerek, Sørensen'in sonucuna alternatif bir kanıt verilmiştir. Dolayısıyla, Projektif Reed-Muller kodları da, gerçek yaşamda uygulamalarını gördüğümüz, literatürde oldukça çalışılmış, halen çalışılmakta olan kodlardır (bknz. [15, 13, 12, 10, 16, 17]).

Ağırlıklı projektif uzaylar, klasik projektif uzayların doğal genellemeleri olup, farklı cebirsel geometrik özellikler sergilerler. Literatürde, ağırlıklı projektif uzaylar, sonlu cisimler üzerinde lineer kodların farklı sınıflarını oluşturmak için uygun ortamlar olarak kabul edilir ve tez boyunca $C_{d,Y}$ ile göstereceğimiz ve tanıtacağımız **Ağırlıklı Projektif Reed-Muller kodları** ilk kez [18]'de incelenmiştir. Derecesi $d = k \cdot \operatorname{lcm}(a, b) \leq q$ olan ağırlıklı projektif düzlem $\mathbb{P}(1, a, b)$ üzerindeki kodun parametreleri, [18] makalesinde sunulmuştur. Sørensen tarafından [13]'de tanıtılan kodlar, bu kodlar ile aynı adı taşıyor olsa da her iki kod ailesi aslında birbirinden farklıdır, (bknz. [19]). İlgili bir kod ailesi olarak, Y kümesinin ağırlıklı projektif torusun $\mathbb{F}_q$-rasyonel noktalar kümesi olduğu durumda elde edilen kodlar Dias ve Neves [20] tarafından incelenmiştir. Dias ve Neves, Y'nin

sıfırlayan idealinin özel bir binomiyal ideal olduğunu ispatlamışlardır ve daha sonra Şahin tarafından daha genel bir simitli çeşitlemin torusunun $\mathbb{F}_q$-rasyonel noktalarının sıfırlayan idealine genelleştirilmiştir, (bknz. [21]). Nardi, Reed-Muller kodlarını projektif olanlara genişletmeye paralel olarak bir simitli kodun uzunluğunu, $\mathbb{F}_q$-rasyonel noktaların tam kümesinde değerlendirerek genişletmeyi önermiştir, bu yöntemler [22] makalesinde yer almaktadır. Hirzebruch yüzeylerinden gelen kodların parametreleri, kodların hesaplandığı küme tüm $\mathbb{F}_q$-rasyonel noktaların kümesi olduğunda, Nardi tarafından daha önce yayınlanan bir makalede hesaplanmıştır [23].

2. ÖN HAZIRLIKLAR

2.1 Afin Çeşitlemler (Affine Varieties)

Tanım 2.1.1. $\mathbb{K}$ bir cisim olmak üzere, bu cisim üzerinde n boyutlu **afin uzay**, bu cismin tüm n girdili elemanlarından oluşan kümedir. Bir başka deyişle,

$$\mathbb{A}^n = \{(a_0, \ldots, a_{n-1}) : \text{ Her } 0 \leq i \leq n-1 \text{ için } a_i \in \mathbb{K}\}.$$

Şimdi afin çeşitlem kavramının tanımını vereceğiz.

Tanım 2.1.2. $\mathbb{K}$ bir cisim olmak üzere $T \subseteq \mathbb{K}[x_0, \ldots, x_{n-1}]$ polinom kümesini alalım.

$$V(T) = \{P = (P_0, \ldots, P_{n-1}) \in \mathbb{A}^n : \text{ her } f \in T \text{ için } f(P) = 0\} \subset \mathbb{A}^n$$

şeklinde tanımlanan noktalar kümesine **afin çeşitlem** denir. Bir başka deyişle, eğer afin uzaydaki bir alt küme polinomların çözüm kümesi şeklinde yazılabiliyorsa yani $Y \subseteq \mathbb{A}^n$ olmak üzere $Y = V(T)$ olacak şekilde bir $T \subseteq \mathbb{K}[x_0, \ldots, x_{n-1}]$ polinom kümesi varsa bu Y kümesine afin çeşitlem (affine variety) denir.

Şimdi bazı afin çeşitlem örnekleri verelim.

Örnek 2.1.1. *(i) Afin uzayın kendisi de bir afin çeşitlemdir, bir başka deyişle,* $\mathbb{A}^n = V(0)$.

(ii) Boş küme bir afin çeşitlemdir, $\emptyset = V(1)$.

(iii) Afin uzaydaki herhangi bir nokta yine bir afin çeşitlem belirtir. Gerçekten, $(a_0, \ldots, a_{n-1}) = V(x_0 - a_0, \ldots, x_{n-1} - a_{n-1})$.

Şimdi ise afin uzaydaki bir alt kümenin idealinin tanımını vereceğiz.

Tanım 2.1.3. $Y \subset \mathbb{A}^n$ olmak üzere, Y'nin **ideali** veya **sıfırlayan ideali** aşağıdaki şekilde tanımlanır,

$$I(Y) = \{f \in \mathbb{K}[x_0, \ldots, x_{n-1}] : f(P) = 0, \, \forall P \in Y\}.$$

Şimdi sıfırlayan ideal (vanishing ideal) kavramı için örnekler vereceğiz.

Örnek 2.1.2. *(i) Boş kümenin ideali polinom halkasının kendisine eşittir. Yani,* $I(\emptyset) = (1) = \mathbb{K}[x_0, \ldots, x_{n-1}]$ *olur.*

(ii) $\mathbb{K}$ *cebirsel kapalı bir cisim olmak üzere afin uzayın ideali* $I(\mathbb{A}^n) = (0)$ *olur. Çünkü afin uzayın tüm noktalarında sıfır olan tek polinom* 0 *elemanı tarafından üretilir.*

2.2 Projektif Çeşitlemler (Projective Varieties)

Tanım 2.2.1. $\mathbb{K}$ bir cisim olmak üzere, n boyutlu projektif uzay $\mathbb{P}^n$, $\mathbb{K}^{n+1}$ vektör uzayının tüm bir boyutlu lineer alt uzaylarının kümesi olarak tanımlanır. Bir başka deyişle,

Her $\lambda \in \mathbb{K}^*$ için $(x_0, \ldots, x_n) \sim (\lambda x_0 \ldots, \lambda x_n)$ koşulu sağlanmak üzere **projektif uzayı**,

$$\mathbb{P}^n = (\mathbb{K}^{n+1} \setminus \{0\})/\mathbb{K}^*$$

şeklinde tanımlayabiliriz. Bir $(x_0, \ldots, x_n)$ noktasının denklik sınıfı $[x_0 : \cdots : x_n]$ ile gösterilir. Dolayısıyla, denklik sınıflarının bir kümesi olan projektif uzay aşağıdaki şekilde de gösterilir:

$$\mathbb{P}^n = \{[x_0 : \cdots : x_n] : (x_0, \ldots, x_n) \in \mathbb{K}^{n+1} \setminus \{0\}\}.$$

Projektif uzaydan aldığımız bir $P = [P_0 : \cdots : P_n] \in \mathbb{P}^n$ noktasının P_i girdilerinin tamamı sıfır değildir.

Tanım 2.2.2. [24] Bir $f \in \mathbb{K}[x_0, \ldots, x_n]$ polinomunun içinde sıfırdan farklı katsayılara sahip tüm monomların toplam derecesi aynı ise bu f polinomu, **homojen polinom** olarak adlandırılır.

Lemma 2.2.3. *[25, Definition 1, Theorem 2, Chap. 8]* $I \subset \mathbb{K}[x_0, \ldots, x_n]$ *bir ideal olmak üzere aşağıdaki ifadeler birbirine denktir.*

i I *ideali homojen polinomlar tarafından üretilir.*

ii Her $f \in I$ *için* f_d*,* d *dereceli homojen kısım olmak üzere* $f_d \in I$ *olur.*

Yukarıdaki koşulları sağlayan I *idealine* ***homojen ideal*** *denir.*

Kanıt. İspatı için Gathmann'ın [26] kaynağında verilen $2002/2003$ yıllarındaki ders notlarından derlenmiş kitapçığındaki Lemma $3.1.8$'in ispatına bakılabilir. Ayrıca, yazarın yüksek lisans tezindeki ispatına da bakılabilir, [27, Önerme 3.2.9, Sonuç 3.2.10]. □

Şimdi ise projektif uzaylar için projektif çeşitlem ve onun sıfırlayan idealinin tanımlarını vereceğiz.

Tanım 2.2.4. $I \subset \mathbb{K}[x_0, \ldots, x_n]$ homojen bir ideal veya homojen polinomların bir kümesi olmak üzere bu idealin (veya kümenin) **projektif çeşitlemi** aşağıdaki şekilde tanımlanır,

$$V(I) = \{P \in \mathbb{P}^n : \text{ her } f \in I \text{ için } f(P) = 0\}.$$

Tanım 2.2.5. $Y \subset \mathbb{P}^n$ olmak üzere, bu kümenin **sıfırlayan ideali** aşağıdaki şekilde tanımlanır,

$$I(Y) = \langle f \in \mathbb{K}[x_0, \ldots, x_n] \text{ homojen polinom } : f(P) = 0, P \in Y \rangle.$$

2.3 Ağırlıklı Projektif Uzay

Tezin bu bölümünde, bu tez çalışması boyunca üzerinde çalışılacak ve cebirsel ve geometrik açıdan zengin özelliklere sahip yapılar olan ağırlıklı projektif uzayları ele alacağız.

Her i için, her bir w_i pozitif tam sayı ve her i, j için w_i ve w_j tam sayıları aşikar en büyük ortak bölene sahip olsun. Bir başka deyişle, w_i ve w_j'lerin en büyük ortak bölenleri 1 olsun.

$\mathbb{K}^*$ grubunun $\mathbb{K}^{n+1} \setminus \{0\}$ kümesi üzerindeki etkisini her $\lambda \in \mathbb{K}^*$ için

$$(x_0, \ldots, x_n) \backsim (\lambda^{w_0} x_0, \ldots, \lambda^{w_n} x_n)$$

şeklinde tanımlayalım. Burada $\mathbf{w} = (w_0, \ldots, w_n)$'i **ağırlık** olarak adlandıracağız.

$$\mathbb{P}(w_0, \ldots, w_n) = (\mathbb{K}^{n+1} \setminus \{0\})/\mathbb{K}^*$$

şeklinde tanımlanan denklik sınıflarının bir kümesine **ağırlıklı projektif uzay** denir. Burada, $\mathbb{K}$, $\mathbb{F}_q$ cisminin cebirsel kapanışıdır (algebraic closure). Ağırlıklı projektif uzayın noktaları yukarıda tanımladığımız denklik sınıflarıdır. Ağırlıklı projektif uzayı tez boyunca $X = \mathbb{P}(w_0, \ldots, w_n)$ ile göstereceğiz. Ayrıca, tez boyunca X uzayının $\mathbb{F}_q$-rasyonel noktaları kümesini de $Y = X(\mathbb{F}_q)$ notasyonu ile göstereceğiz.

Eğer $w_0 = w_2 = \cdots = w_n = 1$ ise bu uzay **projektif uzay** olarak adlandırılır. Bir başka deyişle, $\mathbb{P}(1, 1, \ldots, 1) = \mathbb{P}^n$. Dolayısıyla ağırlıklı projektif uzaylar, projektif uzayların bir genellemesidir.

Ağırlıklı projektif uzaylar aşağıda verilen durumları sağlar. (Ayrıca bakınız, [28, Lemma 3A.3, Proposition 3C.5])

(i) $\mathbb{P}(w_0, \ldots, w_n) \sim \mathbb{P}(cw_0, \ldots, cw_n), \quad c \in \mathbb{N},$

(ii) Her $i = 1, \ldots, n$ için $c_i \in \mathbb{N}$ ve $c_i = \text{ekok}(\text{ebob}(w_0, \ldots, w_{i-1}, w_{i+1}, \ldots, w_n))$ olsun. Buradan,

$$\mathbb{P}(w_0, \ldots, w_n) \sim \mathbb{P}\left(\frac{w_0}{c_0}, \ldots, \frac{w_n}{c_n}\right).$$

Buna örnek olarak, aşağıdaki izomorflukları düşünebiliriz,

$$\mathbb{P}(4, 6, 15) \sim \mathbb{P}(4, 2, 5) \sim \mathbb{P}(2, 1, 5).$$

Bir ağırlıklı projektif polinom halkası, ağırlıklar $\mathbf{w} = (w_0 \ldots, w_n)$ ve her bir i için $\text{der}(x_i) = w_i$ olmak üzere, $S = \mathbb{K}[x_0, \ldots, x_n]$ şeklinde alınsın. Buradan, bu S halkasındaki bir monomun derecesini $\text{der}(\prod_{i=0}^{n} x_i^{c_i}) = \sum_{i=0}^{n} w_i c_i$ şeklinde düşünebiliriz. Böylece, bir ağırlıklı homojen polinomu da aşağıdaki şekilde tanımlayabiliriz.

Tanım 2.3.1. [29, Definition 3.0.3] $\mathbf{w} = (w_0, \ldots, w_n)$ bir ağırlık olmak üzere her i için $\text{der}(x_i) = w_i$ derecelendirmesiyle birlikte $f \in \mathbb{K}[x_0, \ldots, x_n]$ polinomunu alalım. f polinomu, derecesi d olan bir **ağırlıklı homojen polinomdur** gerek ve yeter şart

$$f = \sum_{i=1}^{m} c_i \left(\prod_{j=0}^{n} x_j^{d_j^{(i)}} \right)$$

olacak şekilde $c_i \in \mathbb{K}$ ile bir $m \in \mathbb{N}$ sayıları vardır ki $0 \leq i \leq n$ için $d = \sum_{j=0}^{n} w_j d_j^{(i)}$'dir.

Buradan yola çıkarak, bir ağırlıklı homojen idealin, ağırlıklı homojen elemanlar tarafından üretildiğini söyleyebiliriz. Şimdi ağırlık projektif çeşitlemlerin ve onların ideallerinin tanımını vereceğiz.

Tanım 2.3.2. $I \subset \mathbb{K}[x_0, \ldots, x_n]$, bir ağırlıklı homojen ideal olsun. Burada bu idealle ilişkili olan ağırlıklı projektif çeşitlem aşağıdaki şekilde tanımlanır,

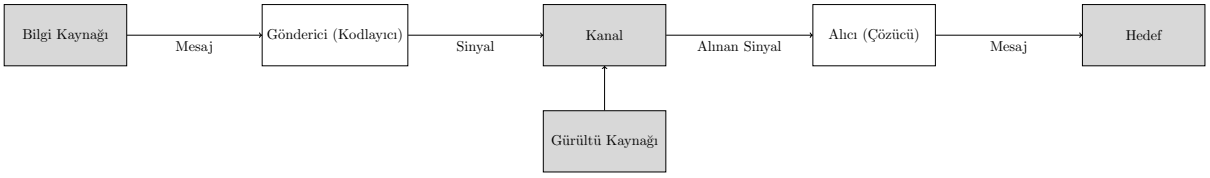
$$V(I) = \{P \in \mathbb{P}(w_0, \ldots, w_n) : \text{ her } f \in I \text{ için } f(P) = 0\}.$$

Ayrıca, $Y \subset \mathbb{P}(w_0, \ldots, w_n)$ ağırlıklı projektif uzayının bir altkümesi olsun. Y'nin ideali, aşağıdaki şekilde tanımlanır,

$$I(Y) = \langle f \in \mathbb{K}[x_0, \ldots, x_n], \text{ w} - \text{ağırlıklı homojen polinom} : \forall P \in Y \text{ için } f(P) = 0 \rangle.$$

2.4 Kodlama Teorisine Giriş

Kodlama teorisinin başlangıcı genellikle literatürde Claude Shannon ile ilişkilendirilir. Çünkü, Shannon tarafından yazılan ve 1948 yılında Bell System Technical Journal'da yayımlanan "A Mathematical Theory of Communication" [30] adlı çalışması kodlama üzerine matematiksel bir bakış açısı ve bir temel sunmuştur. Elbette, kodlama teorisinin çıkışının Shannon'un bu çalışması ile ilişkilendirilmesi doğrultusunda, daha öncesinde kodlama kavramı ve kodlama teorisi ile ilgili çalışmalar olmadığı anlamını çıkaramayız. Fakat Shannon'un bu çalışması iletişimi nasıl modelleyeceğimize dair matematiksel bir temel sağlamıştır. Bu çalışma ile birlikte popülerleşmeye başlayan kodlama teorisinin en temel problemlerinden birkaçı iletilen bir mesajda mesajın sağlıklı iletilmemesini sağlayan hatalar, bu hatalara sebebiyet veren güvenilmez bir kanal üzerinden yapılan iletişim ve bu hataların oluşması, düzeltilmesi için gereken durumlardır.



Şekil 2.1 Shannon'ın iletişim kanalı modeli (Shannon, 1948)

Kodlama teorisine ilk başlarda katkıda bulunan isimler arasında Marcel Golay (Golay kodları), Richard Hamming (Hamming uzaklığı ve Hamming kodları) ile Irving S. Reed ve Gustave Solomon (Reed-Solomon kodları, Reed-Muller kodları) bulunmaktadır. Bu tez çalışmasında da Reed-Muller tipindeki kod ailelerinden biri olan Ağırlıklı Projektif Reed-Muller kodları çalışılacaktır.

Veriler bir kanal üzerinden iletildiğinde, hataların meydana gelmesi muhtemeldir. Kodlama teorisinin amacı, bu hataların tespit edilmesini, hatta düzeltilmesini sağlayacak verimli kodlama yolları bulmaktır. Geleneksel olarak bakıldığında, kodlama teorisinde kullanılan ana metodlar kombinatorik ve grup teorisi gibi matematiksel alanlara dayanmaktadır. İlk olarak, 1977'de Goppa, cebirsel geometrik kodlar olarak da anılan Goppa kodlarını tanımlamıştır [31] ve böylece cebirsel geometriye ait geniş bir yelpazedeki tekniklerin kodlama teorisinde de uygulanmasına Goppa sayesinde olanak tanınmıştır. Goppa'nın orijinal makalesinden kısa bir süre sonra, Tsfasman, Vladut ve Zink [32] modüler eğriler kullanarak önceki kodlardan daha iyi asimptotik parametrelere sahip bir dizi kod ailesi elde etmişlerdir. Bir kodu matematiksel olarak tanımlamadan önce günlük hayatta karşımıza çıkan kod örneklerinden bahsetmek gerekirse, en sık karşılaşılan kod, Uluslararası Standart Kitap Numarası, ISBN, (International Standard Book Number) Kodu'dur. Bu kodun nasıl çalıştığını kısaca anlatmak istersek, öncelikle her kitaba bir ISBN kodu atanır ve bu ISBN kodu genellikle kitabın arka kapağında gösterilir. ISBN kodları ait oldukları kitap hakkında bilgi vermektedir. Örneğin, Hartshorne'nun cebirsel geometride önemli bir yeri olan "Algebraic Geometry" adlı kitabının ISBN kodu $0-387-90244-9$ olarak verilmiştir. Burada, kodun sonunda yer alan rakam 9, bir kontrol rakamıdır ve asıl olarak ilk dokuz rakam baz alınır. Yani, genel olarak baktığımızda eğer bir ISBN kodunu $a_1 - a_2a_3a_4 - a_5a_6a_7a_8a_9 - a_{10}$ şeklinde düşünürsek, kontrol rakamı olan a_{10}'u belirlemek için $a_{10}^{'} = a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9$ eşitliğini kullanmamız gereklidir. Eğer $a_{10}^{'} \equiv i, \mod 11$ denkliği göz önünde bulundurulursa $0 \leq i \leq 9$ arasındaki bazı i değerleri için, $a_{10} = i$ eşitliği elde edilir. Buradan açıkça görülür ki 9 rakamı bu kitap için kontrol rakamıdır. Eğer $a_{10}^{'} \equiv 10, \mod 11$ olarak elde edilirse, bu durumda a_{10} değeri, x sembolü ile gösterilir. Bunun anlamı, her kitabın kontrol rakamını seçmek için aynı sistem kullanılarak bir ISBN kodu atanmasıdır. Ve örneğin, herhangi bir kütüphanede yeni kitapları kataloglarken bu kodun yazılışında bir hata yaparsanız, bilgisayar hatanızı yakalayacak şekilde programlanabilir olması gereklidir. ISBN kodları da bu durumlar göz önünde bulundurulacak şekilde oluşturulmaktadır.

ISBN kodlarına ek olarak tekrarlama kodları da (Repetition Codes) sıklıkla karşılaştığımız kod örnekleri arasındadır. Tekrarlama kodlarına örnek olarak her olası veri parçasına dört bitlik bir dizi (uzunluğu dört olan 0 ve 1'lerden oluşan dizi) atandığını varsayalım ve veriyi yalnızca iletmek yerine her veri parçasını üç kez ilettiğimizi varsayalım. Yani, eğer uzunluğu dört bit olan bir dizi olarak 1011 veri dizisini alırsak, her veri parçasını üç kez ilettiğimizde bu veri dizisi $1011 - 1011 - 1011$ olarak iletilir. Bir hata olursa, bu hata üç bloktan birinde olacaktır. Dolayısıyla bu durum diğer iki bloğun hala uyumlu

olacağı ve hatayı tespit edip düzeltebileceğimiz anlamına gelmektedir. Bir başka örnek, eğer iki hatayı düzeltebilmek istiyorsak, her veri parçasını beş kez iletmemiz gerekmektedir ve dolayısıyla genel olarak, t tane hata düzeltmek için veriyi $2t + 1$ kez iletmemiz gerekmektedir. Tekrarlama Kodları, sadece hataları tespit etmek yerine hatayı düzeltebilme avantajına da sahiptir. Ancak, yalnızca bir hatayı düzeltebilmek istiyorsak, her bilgi sembolü için toplam üç sembol iletmemiz gerektiğinden verimli bir yöntem olduğu söylenemez. Tüm bunlardan yola çıkarak şunu söyleyebiliriz ki; Kodlama teorisinin **temel problemi**, güvenilmez bir kanal üzerinden iletişimde gönderilen mesajda hataların oluşması muhtemel olduğundan, bu iletişimdeki hataları tespit etmek ve düzeltebilmek üzerine dayanır. Tüm iletişim kanallarının hatalara sahip olduğunu söyleyebiliriz ve bu sebeple kodlar özellikle de teknolojik gelişmelerin gün geçtikçe hızlanması ile birlikte yaygın olarak kullanılmaktadır. Aslında, kodlar sadece ağ iletişimi, USB kanalları, uydu iletişimi gibi alanlarda değil, aynı zamanda hatalara eğilimli olan diskler ve diğer fiziksel medyalarda da kullanılır. Bahsettiğimiz bu tür pratikteki uygulamalarının yanı sıra, kodlama teorisinin bilgisayar bilimi teorisinde de birçok uygulaması vardır. Bu nedenle, hem günlük hayata uygulamaları üzerine çalışanların, hem de teorisi üzerine çalışanların yani özellikle matematikçilerin ilgisini çeken bir konu ve alandır.

2.4.1 Lineer Kodlar

Verilen $\mathcal{A}$ kümesi sonlu bir küme olsun ve bu küme **alfabe** olarak adlandırılsın. Set $\mathcal{A}$'nın elemanlarından oluşan herhangi bir N-uzunluğundaki diziye **N-uzunluklu kelime** denir. Diğer bir deyişle, $\mathcal{A}^N := \mathcal{A} \times \cdots \times \mathcal{A}$ (N kez) kümesinin bir elemanına N-uzunluklu kelime denir. $\mathcal{A}^N$ kümesinin bir alt kümesine **kod** denir. Kodu $\mathcal{C}$ harfi ile gösterelim. Eğer kodun elemanlarına $C = (c_1, \ldots, c_N)$ dersek, bu elemanlara **kod kelimeleri** denir. $\mathcal{A}_q(N, \delta)$ ifadesi, N uzunluğunda ve minimum uzaklığı δ olan bir q-ary blok kodunda mümkün olan maksimum kod kelimesi sayısını temsil eder. Bir başka deyişle, $\mathcal{A}_q(N, \delta)$ ifadesi, uzunluğu N olan ve minimum Hamming uzaklığı δ olan bir q-ary (yani q elemanlı bir alfabeden oluşan) blok kodunda mümkün olan maksimum kod kelimesi sayısını temsil eder. Burada,

q: Kod kelimelerinin oluşturulduğu alfabenin (veya cismin) büyüklüğü,

N: Her bir kod kelimesinin uzunluğu,

δ: Kod içindeki herhangi iki farklı kod kelimesi arasındaki minimum Hamming uzaklığıdır.

Bir blok kodunda, her kod kelimesi genellikle q tane sembol (genellikle $\mathbb{F}_q$ gibi sonlu bir cisimden elemanlar) üzerinde N-uzunluklu bir kelime olarak tanımlanır.

Kodlama teorisindeki amaç, $\mathcal{A}_q(N, \delta)$ değerini maksimize etmektir çünkü bu, kodun verimliliğini ve güvenilirliğini belirler. Daha büyük $\mathcal{A}_q(N, \delta)$ değerleri, daha fazla kod kelimesi demektir ve böylece bu durum daha fazla bilgi kodlanabilir anlamına gelirken, daha büyük minimum uzaklık δ daha iyi hata tespiti ve düzeltme kapasitesi sağlar.

Dolayısıyla, $\mathcal{A}_q(N, \delta)$, uzunluğu N ve minimum uzaklığı δ olan bir kodun potansiyel boyutunu ifade eder. Tüm bunlara ilaveten $\mathcal{C}$ bir kod olmak üzere bu kodun minimum uzaklığı, farklı kod kelimeleri arasındaki en küçük uzaklık olduğundan dolayı kodun hata düzeltme yeteneğini belirlemede önemlidir; minimum uzaklık ne kadar yüksekse, kod o kadar fazla hatayı düzeltebilir.

Tanım 2.4.1. (Lineer Kod) Eğer verilen $\mathcal{A}$ alfabe kümesi bir cisim ise ve $C \subset \mathcal{A}^n$ oluyorsa bir başka deyişle $\mathcal{C}$, $\mathcal{A}^n$'nin bir vektör alt uzayı ise $\mathcal{C}$'ye bir **lineer kod** denir.

Bir lineer kodun 3 temel $[N, K, \delta]$ parametresi vardır.

Tanım 2.4.2. N, yani kodun **uzunluğu (length)** $|Y|$ eleman sayısı ile tanımlanır. $\mathcal{C}$ kodunun **boyutu** ise $K = \dim_{\mathbb{F}_q}(C)$ ile gösterilir. Bir başka deyişle, $\mathcal{C}$ bir lineer kod olduğundan dolayı kodun boyutu $\mathcal{A}$ cismi üzerindeki $\mathcal{C}$ vektör alt uzayının boyutu ile tanımlıdır.

Şimdi minimum uzaklık kavramını en genelde tanımlayabilmek için önce **Hamming uzaklığı** kavramını tanımlayacağız.

Hamming uzaklığı, $c_i = (c_{i1}, \ldots, c_{in})$, $c_j = (c_{j1}, \ldots, c_{jn}) \in \mathcal{A}^n$ olmak üzere,

$$d(c_i, c_j) = \#\{k : c_{ik} \neq c_{jk}\}$$

şeklinde tanımlanır.

Dolayısıyla **minimum uzaklık** aşağıdaki şekilde tanımlanır,

$$\delta = d_{\min}(\mathcal{C}) = \min\{d(c_i, c_j) : c_i, c_j \in \mathcal{C} \text{ ve } c_i \neq c_j\}.$$

$c \in \mathcal{C}$'nin sıfırdan farklı girdi sayısına onun **ağırlığı** denir ve eğer $\mathcal{C}$ lineer bir kod ise $\mathcal{C}$ kodunun **minimum uzaklığı** $c \in C\backslash\{0\}$ kod kelimeleri arasında en küçük ağırlıktır. Yani

kod lineer iken minimum uzaklık ve minimum ağırlık aynıdır. Bir başka deyişle, ağırlık

$$w(c) = \#\{i \in \{1, \ldots, N\} : c_i \neq 0\},$$

şeklinde tanımlı olduğundan $\mathcal{C}$ kodu lineer bir kod ise $\mathcal{C}$ kodunun minimum uzaklığı, her $c \in \mathcal{C}$ için $\delta = \min(w(c))$ şeklinde tanımlanır.

Örnek 2.4.1. *$\mathcal{C} = \{(1,0,0,1), (0,0,0,1), (1,0,0,0), (0,0,0,0)\}$ kodu $\mathbb{F}_2$ cismi üzerinde tanımlansın. Buradan,*

$$N = 4, \dim(C) = K = \log_2(4) = 2$$

olur. Minimum uzaklık için ise, öncelikle tüm kod kelimeleri için uzaklıklara bakacağız. Buradan,

$$\begin{aligned} &d((1,0,0,1),(0,0,0,1)) = 1, \quad d((0,0,0,1),(1,0,0,0)) = 2, \\ &d((1,0,0,1),(1,0,0,0)) = 1, \quad d((0,0,0,1),(0,0,0,0)) = 1, \\ &d((1,0,0,1),(0,0,0,0)) = 2, \quad d((1,0,0,0),(0,0,0,0)) = 1. \end{aligned}$$

olduğundan dolayı yukarıda tanımlı olan uzaklıkların minimumu 1 elde edileceğinden $\delta = 1$ olur.

Literatürde bilinen, temel parametrelerin aralarında ilişki kurabilmek ve kodların özelliklerini detaylandırabilmek için verilmiş bir çok sınır vardır. Bunlardan en çok bilinen aşağıda tanımını vereceğimiz Singleton Sınırıdır.

Tanım 2.4.3. $\mathcal{C}$, temel parametreleri sırasıyla N,K ve δ olan bir kod olmak üzere

$$\delta \leq N - K + 1$$

şeklinde tanımlı sınıra **Singleton Sınırı** denir. Eğer $K + \delta = N + 1$ ise bu $\mathcal{C}$ koduna **MDS kod** denir.

2.4.2 Hesaplama Kodları ve Literatürde Bilinenler

Tanım 2.4.4. $S = \mathbb{F}_q[x_0, \ldots, x_n]$ bir polinom halkası olsun. $Y = \{P_1, \ldots, P_N\} \subseteq \mathbb{P}(w_0, \ldots, w_n)(\mathbb{F}_q)$ kümesini ele alalım.

$$ev_Y\colon \begin{cases} S_d \to \mathbb{F}_q^N \\ f \mapsto \Big(f(P_1), \ldots, f(P_N)\Big) \end{cases}$$

Yukarıda tanımlanan dönüşüm **hesaplama dönüşümü** olarak adlandırılır. $C_{d,Y}$, $\mathbb{F}_q^N$ uzayının bir alt uzayı olmak üzere, d dereceli homojen polinomların Y kümesindeki noktalarda hesaplanmasıyla elde edilir ve **hesaplama kodu** olarak adlandırılır. Dolayısıyla hesaplama dönüşümünün görüntüsü hesaplama kodu adını alır.

$I(Y)$, Y'nin her noktasında sıfırlanan S halkası üzerindeki homojen polinomlar tarafından üretilen homojen bir ideal olmak üzere (sıfırlayan ideal), bu sıfırlayan ideal ile ilişkili kodların boyutu ile idealin Hilbert serisi arasında cebirsel bir ilişki vardır. Yukarıdaki Tanım 2.4.4'da tanımladığımız hesaplama dönüşümünün çekirdeği d dereceli $I_d(Y)$ homojen kısma eşit olduğundan dolayı $S_d/I_d(Y) \cong C_{d,Y}$ izomorfizmasını elde ederiz. Dolayısıyla, $C_{d,Y}$ kodunun boyutu dereceli Hilbert fonksiyonu ile elde edilir. Yani,

$$\dim_{\mathbb{F}_q} C_{d,Y} = \dim_{F_q}(S_d) - \dim_{\mathbb{F}_q}(I_d(Y)) = H_Y(d) \tag{1}$$

Ve ayrıca [18] makalesinde $C_{d,Y}$ kodunun uzunluğu N, aşağıdaki eşitlikle verilmiştir.

$$N = q^{r-1} + q^{r-2} + \cdots + q + 1.$$

Minimum uzaklık olarak adlandırılan bir diğer parametrenin, lineer kodlar ile ilgili kavramlardan bahsettiğimiz (2.4.1) bölümünde ele alınan ağırlık kavramıyla ilişkili olduğunu biliyoruz. Bir başka deyişle, lineer kodlarda minimum uzaklık ve minimum ağırlık kavramları birbirine denktir. Şimdi ise bu bilgiler doğrultusunda hesaplama kodlarının minimum uzaklığını ele alalım. Hesaplama dönüşümü altında dönüşümün görüntüsünden elde edilen kodu $\big(f(P_1), \ldots, f(P_N)\big) = \mathcal{C}$ olarak alalım. $c \in \mathcal{C}$ bir kod kelimesi olmak

üzere, her bir kod kelimesinin ağırlığı $w(c)$ aşağıdaki gibi tanımlıdır:

$$\begin{aligned} w(c) &= \#\{i \in \{1,\ldots,N\} : c_i \neq 0\} \\ &= N - \#\{i : c_i = 0\} \\ &= N - \#\{P_i \in X : f(P_i) = 0\} \\ &= N - |V_X(f)| \end{aligned}$$

Dolayısıyla minimum uzaklığın, (kod lineerse) minimum ağırlık olmasından dolayı kodun minimum uzaklığı olan δ'yı aşağıdaki şekilde de elde edebiliriz:

$$\begin{aligned} \delta &= \min\{w(c) : c \in \mathcal{C} \text{ ve } \mathcal{C} \in ev_Y(S_d)\} \\ &= N - \max\{|V_X(f)| : f \in S_d\} \end{aligned} \tag{2}$$

Bir başka deyişle, hesaplama dönüşümünün tanımını göz önünde bulundurduğumuzda ve hesaplama kodu olarak adlandırılan $C_{d,Y}$ kodunun, hesaplama dönüşümünün görüntüsü olduğuna da dikkat edersek, bu doğrultuda $f \in S_d$ olmak üzere bu polinomların $Y = \{P_1,\ldots,P_N\}$ noktalarında 0 değeri aldıkları yerler bize f polinomlarının kök sayısını vereceğinden minimum uzaklığı hesaplama problemi aslında maksimum kök sayısına ulaşma hedefi ile ilişkilidir.

Şimdi literatürde çok defa çalışılan ve bilinen kod ailelerinden olan Reed-Solomon ve Reed-Muller kod ailelerinin tanımlarını vereceğiz. Bu tez çalışmasında kod ailesi olarak Ağırlıklı Projektif Reed-Muller kod aileleri göz önünde bulundurulacaktır ve bu kod ailesinin temel parametreleri üzerine elde edilen sonuçlar verilecektir.

Tanım 2.4.5. (Reed-Solomon Kodları) $\alpha_1,\ldots,\alpha_{q-1}$, $\mathbb{F}_q$ sonlu cisminin $q-1$ tane sıfırdan farklı elemanı olsun ve $1 \leq K \leq q-1$ olmak üzere $K \in \mathbb{Z}$ tamsayısını alalım. Reed-Solomon Kod (RS(K,q)) aşağıdaki şekilde tanımlanır.

$$\text{RS}(K,q) = \{(f(\alpha_1),\ldots,f(\alpha_{q-1})) : f \in \mathcal{L}_{K-1}\}$$

Burada, $\mathcal{L}_{K-1}$ ile gösterilmek istenen derecesi K tam sayısından kesin küçük olan sonlu cisim üzerindeki polinomların kümesidir. Bir başka deyişle, $\mathcal{L}_{K-1} = \{f \in \mathbb{F}_q[x] : \text{der}(f) \leq K-1\}$ şeklinde tanımlanır.

Tanım 2.4.6. (Genelleştirilmiş (Afin) Reed-Muller Kodları) [33] $\mathbb{A}^n$, $\mathbb{F}_q$ sonlu cismi üzerindeki n boyutlu afin uzay olmak üzere ve $S = \mathbb{K}[x_0,\ldots,x_{n-1}]$ polinom halkası olmak

üzere $1 \leq d \leq n(q-1)-1$ koşulunu sağlayan bir pozitif d tam sayısı için S halkasındaki derecesi d'den küçük olan polinomların kümesini,

$$S_{\leq d} = \mathbb{K}[x_0, \ldots, x_{n-1}]_{\leq d} = \{f \in S : \operatorname{der}(f) \leq d\}$$

ile gösterelim. Buradan, afin uzayın noktalarındaki hesaplama dönüşümü aşağıdaki şekilde tanımlanır,

$$\text{ev}: S_{\leq d} \to \mathbb{F}_q^N, \quad \text{ev}(f) = (f(P_1), \ldots, f(P_N)).$$

Bu dönüşümlerin görüntüleri **Genelleştirilmiş Reed-Muller Kodları** olarak adlandırılır.

Şimdi bu tez çalışmasının odak noktası olan **Ağırlıklı Projektif Reed-Muller** ve **Projektif Reed-Muller** kodların tanımını vereceğiz. Hatırlatmak gerekirse, literatürde Projektif Reed-Muller kodları ilk olarak Lachaud tarafından [10] makalesinde tanıtılmıştır. (ayrıca bknz. [34, 35, 13, 36])

Tanım 2.4.7. $X = \mathbb{P}^n$ projektif uzay olsun. Ve Tanım 2.4.4'daki gibi tanımlanan hesaplama dönüşümü göz önünde bulundurulsun. Bu dönüşümdeki Y kümesi, $Y = \{P_1, \ldots, P_N\} \subseteq X(\mathbb{F}_q)$ ve $S = \mathbb{F}_q[x_0, \ldots, x_n]$ standart dereceli polinom halkası olmak üzere, bu şekilde tanımlı hesaplama dönüşümünün görüntüsü **Projektif Reed-Muller** tipindeki kod olarak adlandırılır.

Uyarı 2.4.8. Bu tez çalışması boyunca üzerinde çalışacağımız kod olan **Ağırlıklı Projektif Reed-Muller** tipindeki kod ise Tanım 2.4.4'da verildiği gibi $S = \mathbb{F}_q[x_0, \ldots, x_n]$ **w** derecelendirmeli bir polinom halkası ve $Y = \{P_1, \ldots, P_N\} \subseteq \mathbb{P}(w_0, \ldots, w_n)(\mathbb{F}_q)$ olduğu durumdaki hesaplama dönüşümünün görüntüsü olarak tanımlanır.

2.4.3 Hata Düzeltme Kodları

Hata düzeltme kodları, veri iletimi veya depolama sırasında oluşabilecek hataları tespit etmek ve düzeltmek amacıyla kullanılan yöntemlerdir. Bu kodlar, özellikle dijital iletişim ve bilgi depolama sistemlerinde önemli bir rol oynar. Hata düzeltme kodları (çoğunlukla) veri iletimi veya veri depolama sırasında meydana gelen bağımsız, rastgele hataları düzeltmek için kullanılır.

Tanım 2.4.9. Hata düzeltme kodu, bir sayı dizisini öyle bir şekilde ifade etmeyi sağlayan bir algoritmadır ki, bu dizide meydana gelen herhangi bir hata, kalan sayılar temelinde (bazı sınırlamalarla birlikte) tespit edilip düzeltilebilir.

Şimdi en bilinen hata düzeltme kodlarından biri olan Reed-Solomon kodlarını ele alarak hata düzeltme kodlarına örnek vereceğiz. Bu kodları daha hesaplama kodlarını anlatırken de ele almıştık çünkü bu kodlar tanımları gereği aynı zamanda bir hesaplama kodudur, (bknz. Tanım 2.4.5). Burada biraz daha detaylı ele alıp hata düzeltme kodu olduğunu vurgulamaya çalışacağız.

Örnek 2.4.2. ***(Reed-Solomon Kodları)*** *Reed–Solomon kodları, Irving S. Reed ve Gustave Solomon tarafından* 1960 *yılında tanıtılan bir hata düzeltme kodudur. Reed-Solomon kodları, dijital iletişim ve depolamada geniş bir uygulama alanına sahip blok tabanlı hata düzeltme kodlarıdır. Aşağıdaki şekilde tanımlanan örten dönüşüm de* (27) *ile tanımlanan dönüşüm gibi bir hesaplama dönüşümüdür. Ve bu dönüşümün görüntüsü bize bir kod verir. Burada, dikkat edilirse iki dönüşüm arasındaki fark* f *polinomlarının derecesi* K *değerinden kesin küçüktür.*

Öncelikle, $K < N \leq q$ *olsun. Ve* $\mathbb{F}_q$*'nin elemanlarını* $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ *olarak alalım ve tüm* i, j *için* $\alpha_i \neq \alpha_j$ *olduğunu varsayalım.*

$$ev_{RS} : = \mathbb{F}_q[x]_{<K} \to \mathbb{F}_q^N, \qquad f \mapsto \big(f(\alpha_1), \ldots, f(\alpha_N)\big) \tag{3}$$

Reed-Solomon kodu yukarıdaki dönüşümün görüntüsü olarak elde edilir. Bir başka deyişle, K *boyutlu ve* α *noktası üzerinde tanımlı Reed-Solomon Kodu* $RS_K(\alpha) = ev_\alpha(\mathbb{F}_q[x]_{<K})$ *olan bir lineer koddur.*

Lineer kodlar bölümünde ele aldığımız Singleton sınırının (bknz. Tanım 2.4.3) $d \leq N - K + 1$ *olduğunu biliyoruz. Genel olarak, lineer (doğrusal) kodlar Singleton Sınırını sağlar. Reed-Solomon Kodu,* $[N, K, N - K + 1]$ *temel parametrelerine sahiptir ve dolayısıyla Singleton sınırına ulaşır ve Singleton sınırını sağlayan kodlara MDS kodu (maximum distance seperable ya da türkçe olarak maksimum uzaklığa ayrıştırılabilir kodlar) denir. Bu nedenle* $RS_K(\alpha)$ *bir MDS kodudur.*

Daha önce bahsettiğimiz gibi Reed-Solomon kodları ***hata düzeltme kodlarıdır*** *ve birden fazla sembol hatasını tespit edip düzeltebilirler. Veriye* $T = N - K$ *kontrol sembolü*

ekleyerek, bir Reed-Solomon kodu herhangi bir kombinasyonda T hatalı sembolü tespit edebilir (düzeltemez) veya bilinmeyen konumlarda $\left\lfloor \frac{t}{2} \right\rfloor$ hatalı sembolü bulup düzeltebilir.

Başka bir deyişle, bir Reed-Solomon kodu S-bit sembollerle belirlenir. Bu, kodlayıcının her biri S bit olan K veri sembolünü alıp bir N sembol kod sözcüğü oluşturmak için parite sembolleri eklediği anlamına gelir. Her biri S bit olan $N - K$ parite sembolü vardır. Bir Reed-Solomon kod çözücüsü, hatalar içeren bir kod sözcüğünde T sembole kadar düzeltebilir, burada $2T = N - K$ ile verilir.

Öncelikle $\mathbf{m} = (m_0, \ldots, m_r)$ bir mesaj olsun. $\mathbf{c} = (c_0, \ldots, c_n)$ ise bilgi kaynağından gelen mesajın kodlayıcıdan geçtikten sonraki hali olan kodumuz olsun. Eğer $\mathbf{c}$ kanala girerse ve $\mathbf{y}$ kanaldan çıkarsa, $\mathbf{y} - \mathbf{c}$ ile gösterilen fark aslında **hata (error)** olarak adlandırdığımız $\mathbf{e}$ olur. Bu durum, Shannon tarafından verilen iletişim kanalı modelinde (bkz. Şekil 2.1), en kısa ve kolay biçimde görselleştirilerek açıklanmaya çalışılmıştır.

Uyarı 2.4.10. Hata düzeltme kodlarının geniş kapsamlı araştırmaları için [37, 38] kaynaklarına bakılabilir.

Bu tez çalışmasında ele alınan Ağırlıklı Projektif Reed-Muller kodlar dahil olmak üzere hesaplama kodları hata düzeltme kodlarıdır.

KISIM I

3. AĞIRLIKLI PROJEKTİF UZAYLAR ÜZERİNDEKİ KODLAR VE CEBİRSEL DEĞİŞMEZLERİ

Tezin bu bölümünde ele alınacak kavramların daha detaylı anlatımı yüksek lisans tezinde mevcut olduğu için bu bölümde daha çok tanımlar ve örnekler üzerinden gidilecektir. Yüksek lisans tezine ulaşmak için [27] kaynağına bakılabilir. Bu bölümde verilen tanım ve kavramlar, bu tez çalışmasının (3.2) kısmında verilen tüm sonuçlar için hazırlık niteliğindedir.

3.1 Cebirsel Değişmezler

3.1.1 Dereceli Polinom Halkaları ve İdealler

Bu bölümde standart derecelendirme, homojen polinomlar ve dereceli bir polinom halkasının homojen elemanları ele alınacaktır. Bu bölüm, aynı zamanda yazarın yüksek lisans tezinde detaylı bir şekilde ele alınmıştır. Bu sebeple, bu bölümle ilgili olarak türkçe kaynak için ayrıca [27] tezine bakılabilir. Ek olarak, ingilizce kaynak için [39] kitabına da bakılabilir.

$S = \mathbb{K}[x_0, \ldots, x_n]$ bir polinom halkası olmak üzere, bu polinom halkası üzerinde her i için x_i'lerin derecesi 1 olsun. $x_0^{c_0} + \cdots + x_n^{c_n}$ monomunun derecesi bu derecelendirme ile $c_0 + \cdots + c_n$ değerine eşittir. Bu derecelendirmeye **standart derecelendirme** denir. Her bir $i \in \mathbb{N}$ için, derecesi i olan monomlar tarafından gerilen (üretilen) $\mathbb{K}$-vektör uzayını S_i ile gösterelim. S halkası eğer dereceli bir polinom halkası ise S_i vektör uzayı i dereceli **homojen eleman** olarak adlandırılır. Örneğin, $i = 0$ için $S_0 = \mathbb{K}$ olur.

$P \in S$ bir polinom olmak üzere eğer herhangi bir i için $P \in S_i$ durumu sağlanıyorsa P polinomuna **homojen** denir. Burada P polinomunun derecesi i'dir.

Her $f \in S$ polinomu, sıfırdan farklı $f_i \in S_i$ elemanlarının sonlu bir toplamı olarak tek bir şekilde yazılabilir, bir başka deyişle, f polinomu $\sum_i f_i$ toplamı şeklinde tek bir biçimde yazılabilir. Bu durumda f_i elemanı, f'in derecesi i olan **homojen bileşeni** olarak adlandırılır. Ek olarak, her $i, j \in \mathbb{N}$ için $S_i S_j \subseteq S_{i+j}$ koşulu sağlanmak üzere, S polinom halkasını

S_i'lerin dik toplamı (direct sum) şeklinde yani $\bigoplus_{i\in\mathbb{N}} S_i$ biçiminde yazabiliriz. Buradan, S halkasına **standart dereceli halka** denir.

$J \subseteq S$ öz alt ideal olmak üzere, eğer J ideali aşağıdaki denk koşulları sağlıyorsa bu ideale **dereceli** ya da **homojen ideal** denir.

(i) $f \in J$ olmak üzere f'in her bir homojen bileşeni de J'dedir.

(ii) $J_i = S_i \cap J$ olmak üzere $J = \bigoplus_{i\in\mathbb{N}} J_i$ olarak yazılır.

(iii) Eğer $J^{'}$ ideali J'nin tüm homojen elemanları tarafından üretiliyorsa $J = J^{'}$ olur.

Burada, J_i'ler J'nin homojen bileşenleridir.

Bu tez çalışmasında, ağırlıklı projektif uzay üzerinde çalışılacağından şimdi standart derecelendirme dışındaki derecelendirme ile verilen homojen koordinat halkasının tanımını vereceğiz.

Tanım 3.1.1. $S = \mathbb{K}[x_0, \ldots, x_n]$, her $i = 1, \ldots, n$ için $\deg x_i = w_i$ derecelendirmesi ile birlikte $\mathbb{K}$ cismi üzerinde bir polinom halkası olsun. Böylece, S_d, derecesi $d = m_0w_0 + \cdots + m_nw_n$ olan $x_0^{m_0} \cdots x_n^{m_n}$ monomları tarafından gerilen vektör uzayı olmak üzere,

$$S = \bigoplus_{d\in\langle w_0,\ldots,w_n\rangle} S_d$$

şeklinde yazabiliriz. Ve bu halkaya **homojen koordinat halkası** denir.

Tanım 3.1.2. $I(Y)$, Y kümesi üzerinde sıfırlanan homojen polinomlar tarafından üretilen, $S = \mathbb{F}_q[x_1, \ldots, x_r]$ halkasının (homojen) idealidir. Böylece

$$I(Y) = \bigoplus_{d\in\mathbb{N}W} I_d(Y),$$

şeklinde tanımlanır ve burada $I_d(Y)$, d dereceli homojen kısımdır. Ayrıca, $\mathbb{N}W$, ağırlıklar tarafından üretilen $\mathbb{N}$'nin bir alt yarıgrubunu (numerical semigroup) ifade eder.

Y kümesinin, $I(Y)$ sıfırlayan idealinin minimal serbest çözülümü (free resolution) aracılığı ile bu kümenin, rasyonel bir fonksiyon olan Hilbert serisi elde edilir. Hilbert serisi de tanımı gereği Hilbert fonksiyonu ile ilişkili olduğundan (bknz. Tanım 3.1.6) Hilbert serisinin

açılımı kullanılarak Hilbert fonksiyonu elde edilir. Kodun boyutu ve Hilbert fonksiyonu arasındaki ilişkiyi de göz önünde bulundurduğumuzda cebirsel değişmezlerden biri olan serbest çözülüm ile ilgili olan sonuçlar, tez çalışmasında önemli bir yer tutmaktadır. Şimdi serbest çözülümün (free resolutions) tanımını vereceğiz.

3.1.2 Serbest Çözülümler

Tanım 3.1.3. S bir R-modül olsun. Aşağıda verilen dizi eğer

(i) Her bir i için F_i'ler serbest modül (free module) ise ve

(ii) Her $i > 0$ için $H_i(\mathcal{Z}) = 0$ ve $H_0(\mathcal{Z}) = S$ ise, (Yani, dizi tamdır.)

bu zincire S'nin **serbest çözülümü** denir.

$$\mathcal{Z} : \cdots \to F_{i+1} \xrightarrow{\lambda_{i+1}} F_i \xrightarrow{\lambda_i} F_{i-1} \to \cdots \to F_1 \xrightarrow{\lambda_1} F_0 \to S \to 0$$

Burada eğer en az bir j tamsayısı varsa ve her $i > j$ için $F_i = 0$ iken $F_j \neq 0$ durumu sağlanıyor ise bu çözülüm sonludur denir. Ve j uzunluklu serbest çözülüm olarak adlandırılır.

Örnek 3.1.1. *$X = \mathbb{P}(1,1,2)$ ağırlıklı projektif uzay ve $Y = \mathbb{P}(1,1,2)(\mathbb{F}_q)$ $\mathbb{F}_q$-rasyonel noktalar kümesi olmak üzere, bu kümenin sıfırlayan idealinin minimal üreteçleri,*

$$I(Y) = \langle x_1^9 x_2 - x_1 x_2^9, x_0^9 x_2 - x_0 x_2^9, x_0^5 x_1 - x_0 x_1^5 \rangle$$

şeklinde elde edilir. Burada, idealin minimal üreteçlerini $f_0 = x_1^9 x_2 - x_1 x_2^9$, $f_1 = x_0^9 x_2 - x_0 x_2^9$ ve $f_2 = x_0^5 x_1 - x_0 x_1^5$ şeklinde adlandırırsak, bu idealin serbest çözülümü aşağıdaki şekilde elde edilir:

$$0 \to R^2 \xrightarrow{\begin{bmatrix} x_1 & -x_1^5 - x_1 x_2^4 \\ -x_2 & 0 \\ x_1^4 x_3 + x^4 x_3 & x_2^8 x_3 - x_3^5 \end{bmatrix}} R^3 \xrightarrow{\begin{bmatrix} f_0 & f_1 & f_2 \end{bmatrix}} R \to R/I \to 0.$$

Şimdi ise dereceli serbest çözülümü ile ilgili gerekli tanım ve kavramları vererek bir örnek üzerinden anlatmaya çalışacağız. Bunun için öncesinde dereceli modül kavramı ve

modüllerin derece üzerinden kaydırılması kavramı üzerinde kısaca duracağız. Dereceli R-modül tanımı için [27, Tanım 3.3.3]'e bakılabilir. Aşağıdaki tanım belli bir a dereceli modülleri tanımlamak için verilecektir.

Tanım 3.1.4. M bir dereceli R-modül ve a bir tam sayı olsun. $M(a)_d = M_{a+d}$ şeklinde tanımlı olmak üzere

$$M(a) = \bigoplus_{d\in\mathbb{Z}} M(a)_d$$

eşitliğini sağlayan $M(a)$, bir dereceli R-modüldür. Burada, $M(a)$ dereceli modülüne M'nin a **derecesi kadar kaydırılması** denir.

Örnek 3.1.2. $\mathbf{w} = (1,2,3)$ *ve* $R = \mathbb{K}[x_0, x_1, x_2]$ *olup, her* $i = 0,1,2$ *için* $\deg(x_i) = w_i$ *olacak şekilde derecelendirildiğini varsayalım.* $f_0 = x_0^4 - x_1^2$ *ve* $f_1 = x_2^3$ *olmak üzere* $I = \langle f_1, f_2\rangle$ *olsun.*

$$0 \to R(-13) \xrightarrow{\begin{bmatrix} -f_1 \\ f_0 \end{bmatrix}} R(-4) \oplus R(-9) \xrightarrow{\begin{bmatrix} f_0 & f_1 \end{bmatrix}} R \to R/I = M \to 0$$

Yukarıda verilmiş olan dizi, R/I*'nın dereceli serbest çözülümüdür. Burada,* $\begin{bmatrix} f_0 & f_1 \end{bmatrix}$ *çarpma dönüşümünü* ϕ_0*, ve* $\begin{bmatrix} -f_1 \\ f_0 \end{bmatrix}$ *matrisi ile çarpma dönüşümünü* ϕ_1 *ile adlandıralım:*

$$\begin{array}{lll} \phi_1: & R^2 \to R & \\ & (a,b) \to (af_0 + bf_1) & \end{array} \qquad \begin{array}{lll} \phi_2: & R \to R^2 & \\ & c \to (-f_1 c, f_0 c) & \end{array}$$

Burada, $\deg_R(af_0) = \deg(a) + \deg(f_0) = \deg(a) + 4 = 0$ *ve* $\deg_R(bf_1) = \deg b + \deg f_1 = \deg(b) + 9 = 0$ *olur. Böylece* $\deg_R(a) = -4$ *ve* $\deg_R(b) = -9$ *olarak yani,* $a \in R(-4)_0$ *ve* $b \in R(-9)_0$ *elde edilir. Benzer şekilde,* ϕ_1 *için de derecenin korunması gerektiğinden,* $\deg_R(-f_1 c) = \deg(c) + 4 = -9$ *ve* $\deg_R(f_0 c) = \deg(c) + 9 = -4$ *olur ve* $c \in R(-13)_0$ *olarak elde edilir.*

3.1.3 Hilbert Fonksiyonu ve Serisi

Tanım 3.1.5. S_d, $d = m_0 w_0 + \cdots + m_n w_n$ dereceli $x_0^{m_0} \cdots x_n^{m_n}$ monomları tarafından gerilen vektör uzayını ve $I_d(Y)$, Y üzerinde sıfırlanan d dereceli homojen polinomların

vektör uzayını bir başka deyişle $I(Y)$ sıfırlayan idealinin d dereceli kısmını temsil etsin. Y'nin (ağırlıklı) Hilbert fonksiyonu şu şekilde tanımlanır:

$$H_Y(d) = \dim_{\mathbb{F}_q} S_d - \dim_{\mathbb{F}_q} I_d(Y).$$

Tanım 3.1.6. Y'nin dereceli Hilbert serisi şu şekilde tanımlanır:

$$HS_Y(d) = \sum_{d \in \mathbb{N}W} H_Y(d)t^d.$$

Teorem 3.1.7. *[24, Chapter 6, Theorem 4.4] $R = \mathbb{K}[x_0 \ldots, x_n]$ ve S, dereceli bir R-modül olmak üzere, S modülünün herhangi bir dereceli serbest çözülümü aşağıdaki şekilde verilsin.*

$$0 \to F_k \to F_{k-1} \to \cdots \to F_1 \to F_0 \to S \to 0$$

S'nin Hilbert fonksiyonu aşağıdaki şekilde verilir.

$$H_S(d) = \dim_{\mathbb{K}} S_d = \sum_{j=0}^{k} (-1)^j \dim_{\mathbb{K}} (F_j)_d = \sum_{j=0}^{k} (-1)^j H_{F_j}(d)$$

Yukarıdaki teoremin bir sonucu olarak, Hilbert serisi de $HS(S,t) = \sum_{j=0}^{k} (-1)^j HS(F_j, t)$, şeklinde verilir. Dolayısıyla buradan söyleyebiliriz ki serbest çözülümü bilinen bir R-modülün Hilbert fonksiyonu ve serisi de hesaplanabilirdir.

Örnek 3.1.3. *Öncelikle, Örnek 3.1.2'de ele alınan dereceli serbest çözülümü düşünelim. Teorem 3.1.7 kullanılarak M'nin Hilbert serisini aşağıdaki şekilde elde ederiz.*

$$HS(M,t) = HS(R,t) - HS(R(-4),t) - HS(R(-9),t) + HS(R(-13),t)$$

$HS(R(-a),t) = t^a HS(R,t)$ olduğundan (bknz. [40, Section 4.1]), aşağıdaki denklemi elde ederiz.

$$HS(M,t) = HS(R,t) - t^4 HS(R,t) - t^9 HS(R,t) + t^{13} HS(R,t).$$

$HS(R,t) = \frac{1}{(1-t)(1-t^2)(1-t^3)}$ denklemini düşünürsek, $M = R/I$'nin Hilbert serisini aşağıdaki gibi elde ederiz:

$$HS(R/I,t) = \frac{1 - t^4 - t^9 + t^{13}}{(1-t)(1-t^2)(1-t^3)}.$$

3.1.4 Düzenlilik Kümesi

Şimdi bir başka cebirsel değişmez olan ve aşikâr (trivial) kodları elemek için kullanılan düzenlilik kümesinin (regularity set) tanımını vereceğiz.

Tanım 3.1.8. Y'nin düzenlilik kümesi aşağıdaki şekilde tanımlanır:

$$\mathrm{reg}(Y) = \{d \in \mathbb{N}W : H_Y(d) = |Y|\}.$$

Düzenlilik kümesinin tanımından da anlaşılacağı üzere, bu küme, Y kümesinin Hilbert fonksiyonunun maksimum değere ulaştığı d derecelerinin kümesidir. Kodun boyutu da Hilbert fonksiyonu ile ilişkili olduğundan bu kümedeki d değerlerine bakıldığında bu derecelerde kodun aşikâr (trivial) kod olduğu görülür. Dolayısıyla tanımdan önce de belirttiğimiz gibi bu küme aşikâr kodları eleyebilmemizi sağlayan önemli bir kümedir. Ayrıca Hilbert fonksiyonunun maksimum değere ulaştığı ilk d derecesine **düzenlilik indeksi** denir.

3.1.5 Cebirsel Değişmezlerle ilgili Literatürdeki bazı Sonuçlar

Sıfırlayan idealin minimal serbest çözülümü ile ilgili bir sonraki bölümde vereceğimiz sonucu kanıtlamak için (bir başka deyişle çözülümün tamlığını göstermek için) aşağıdaki Lemma ile verilen önemli kriterleri kullanacağız.

Lemma 3.1.9. *[41, Corollary 2] S Noetherian halkası üzerinde serbest modüllerin bir dizisi aşağıdaki şekilde verilsin.*

$$0 \to F_n \xrightarrow{\phi_n} F_{n-1} \xrightarrow{\phi_{n-1}} \cdots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0$$

ϕ_i'yi tanımlayan matristeki sıfır olmayan en büyük minörün büyüklüğünü $\mathrm{rank}(\phi_i)$ ile ve en büyük ranka sahip matrisin minörleri tarafından üretilen ideali ise $I(\phi_i)$ ile gösterelim. Eğer tüm $1 \leq i \leq n$ için,

(i) $\mathrm{rank}(\phi_{i+1}) + \mathrm{rank}(\phi_i) = \mathrm{rank}(F_i)$,

(ii) *$I(\phi_i)$, i uzunluğunda bir S-dizisini içerir,*

*yukarıdaki koşullar sağlanıyorsa bu diziye **tam dizi** (exact sequence) denir.*

Şimdi aşağıdaki tam zinciri göz önünde bulundurursak,

$$0 \to F_n \xrightarrow{\phi_n} F_{n-1} \xrightarrow{\phi_{n-1}} \cdots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0$$

Bu tam zincirde ϕ_1'in eşçekirdeği (cokernel) olan M modülü, dereceli bir modül olduğunda, serbest modüller şu şekilde olur:

$$F_i = \bigoplus_{j=1}^{\operatorname{rank} F_i} S(-d_{ij}).$$

Burada, $d_{ij} = d \in \mathbb{N}W$ olan j indekslerinin sayısına M'nin dereceli i**-Betti sayısı** denir ve $\beta_{i,d}(M)$ ile gösterilir. $d \in \mathbb{N}W$ olan neredeyse sonlu sayıdaki elemanlar, $\beta_{i,d}(M) = 0$ olan aşikâr (trivial) dereceli Betti sayısına karşılık gelir.

Y'nin Hilbert serisini, $I(Y)$'nin minimal serbest çözülümünü kullanarak, bir rasyonel fonksiyon olarak vermek için aşağıdaki sonucu kullanıyoruz.

Teorem 3.1.10. *[42, Theorem 8.20, Proposition 8.23] $S = \mathbb{F}_q[x_0, \ldots, x_n]$ polinom halkası $\mathbb{N}W$ nümerik yarıgrubu ile derecelendirilmiş pozitif dereceli bir polinom halkası olmak üzere, S üzerinde sonlu üreteçli dereceli bir M modülünün Hilbert serisi bir rasyonel fonksiyon olarak aşağıdaki şekilde verilir:*

$$HS_M(t) = \frac{\mathcal{K}_M(t)}{\prod_{i=0}^{n}(1 - t^{w_i})},$$

burada $\mathcal{K}_M(t)$ ile gösterilen, $\mathcal{K}_M(t) = \sum_{i=0}^{m} \sum_{d \in \mathbb{N}W} (-1)^i \beta_{i,d}(M) t^d$ polinomudur.

3.2 SONUÇLAR VE YÖNTEMLER-I

Bu bölümde [1] referansı ile verilen **"Algebraic Invariants of Codes on Weighted Projective Planes"** adlı makalesindeki yöntem ve sonuçlar ele alınacaktır.

3.2.1 Cebirsel Değişmezler ile İlgili Sonuçlar

Tanım 3.2.1. $S = \mathbb{F}_q[x_0, \ldots, x_n]$, her $i = 1, \ldots, r$ için $\deg x_i = w_i$ derecelendirmesi ile birlikte $\mathbb{F}_q$ cismi üzerinde bir polinom halkası olsun. Böylece, S_d, derecesi $d = m_0w_0 + \cdots + m_nw_n$ olan $x_0^{m_0} \cdots x_n^{m_n}$ monomları tarafından gerilen vektör uzayı olmak üzere,

$$S = \bigoplus_{d \in \langle w_0, \ldots, w_n \rangle} S_d$$

şeklinde yazabiliriz. Ve bu halkaya **homojen koordinat halkası** denir.

Belirtmek gerekirse, burada $\langle w_0, \ldots, w_n \rangle$, $\mathbb{N}$'nin ağırlıklar tarafından üretilen alt yarıgrubudur.

$X = \mathbb{P}(w_0, \ldots, w_n)$ **ağırlıklı projektif uzayını** ve $Y = X(\mathbb{F}_q)$ $\mathbb{F}_q$**-rasyonel noktalarının kümesini** ele alalım. İlk olarak Y'nin cebirsel değişmezlerinin tanımını vereceğiz. Ve daha sonra X uzayı üzerindeki kodların parametrelerinin tanımlarını ve bilinen bazı sonuçları vereceğiz.

Uyarı 3.2.2. Bu tez çalışması boyunca $X = \mathbb{P}(w_0, \ldots, w_n)$ ifadesi ile ağırlıklı projektif uzay ve $Y = X(\mathbb{F}_q)$ ifadesi ile ise $\mathbb{K} = \overline{\mathbb{F}}_q$ cebirsel kapalı cismi üzerindeki X ağırlıklı projektif uzayının $\mathbb{F}_q$-rasyonel noktalarının kümesi belirtilecektir.

Teorem 3.2.3. *[43] a, b pozitif tamsayılar ve $X = \mathbb{P}(1, a, b)$, sonlu bir cisim üzerindeki ağırlıklı projektif uzay olsun. $Y = X(\mathbb{F}_q)$ olmak üzere, Y'nin ideali aşağıdaki şekilde elde edilir.*

$$I(Y) = \langle f_1, f_2, f_3 \rangle = \langle x_2^{(q-1)b+1}x_3 - x_2x_3^{(q-1)a+1}, x_1^{(q-1)b+1}x_3 - x_1x_3^q, x_1^{(q-1)a+1}x_2 - x_1x_2^q \rangle$$

Sonuç 3.2.4. *[43] $X = \mathbb{P}(1, 1, b)$, $\mathbb{F}_q$ sonlu cismi üzerinde bir ağırlıklı projektif uzay olsun. $Y = X(\mathbb{F}_q)$ olmak üzere, Y'in sıfırlayan ideali aşağıdaki şekilde verilir.*

$$I(Y) = \langle f_1, f_2, f_3 \rangle = \langle x_2^{(q-1)b+1}x_3 - x_2x_3^q, x_1^{(q-1)b+1}x_3 - x_1x_3^q, x_1^qx_2 - x_1x_2^q \rangle$$

Teorem 3.2.5. *$X = \mathbb{P}(1,a,b)$ ve $Y = X(\mathbb{F}_q)$ olmak üzere Y'nin ideali Teorem 3.2.3'in ifadesindeki gibi tanımlansın. İdealin minimal dereceli serbest çözülümü aşağıdaki gibi elde edilir.*

$$0 \to \bigoplus_{j=1}^{2} S(-\sigma_j) \xrightarrow{\begin{bmatrix} x_1 & 0 \\ A_1 & f_3/x_1 \\ A_2 & -f_2/x_1 \end{bmatrix}} \bigoplus_{j=1}^{3} S(-\lambda_j) \xrightarrow{\begin{bmatrix} f_1 & f_2 & f_3 \end{bmatrix}} S \to S/I \to 0$$

Burada, $\lambda_1 = (q-1)ab + a + b, \quad \lambda_2 = qb + 1, \quad \lambda_3 = qa + 1,$

$$A_1 = -\sum_{i=1}^{a} x_1^{(i-1)(q-1)b} x_2 x_3^{(q-1)a-iq+i}, \quad A_2 = \sum_{i=1}^{b} x_1^{(i-1)(q-1)a} x_2^{(q-1)b-iq+i} x_3,$$
$$\sigma_1 = (q-1)ab + a + b + 1, \qquad \sigma_2 = qb + qa + 1.$$

Kanıt. $\phi_1 = \begin{bmatrix} f_1 & f_2 & f_3 \end{bmatrix}$ ve $\phi_2 = \begin{bmatrix} x_1 & 0 \\ A_1 & f_3/x_1 \\ A_2 & -f_2/x_1 \end{bmatrix}$ olarak tanımlayalım. Aşağıdaki dereceli modüller dizisinin tam bir dizi olduğunu göstermek için Lemma 3.1.9'yi kullanacağız.

$$0 \to F_2 \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} S \to S/I \to 0, \tag{4}$$

Burada $F_2 = S(-\sigma_1) \oplus S(-\sigma_2)$, $F_1 = S(-\lambda_1) \oplus S(-\lambda_2) \oplus S(-\lambda_3)$. rank$(\phi_2) = 2$, rank$(\phi_1) = 1$ ve rank$(S^3) = 3$ olduğu kolayca görülmektedir. Böylece, aşağıdaki sonucu elde ederiz:

$$\text{rank}(S^3) = \text{rank}(\phi_2) + \text{rank}(\phi_1).$$

Şimdi, Lemma 3.1.9'deki ikinci maddenin sağlandığını göstereceğiz. $I(\phi_1)$ ideali, $I = \langle f_1, f_2, f_3 \rangle$ idealidir ve bu ideal S üzerinde sıfır bölen olmayan bir polinom içerir. ϕ_2'nin minörleri şunlardır:

$$\begin{vmatrix} A_1 & f_3/x_1 \\ A_2 & -f_2/x_1 \end{vmatrix} = -f_1 \neq 0, \begin{vmatrix} x_1 & 0 \\ A_2 & -f_2/x_1 \end{vmatrix} = -f_2 \neq 0 \text{ ve } \begin{vmatrix} x_1 & 0 \\ A_1 & f_3/x_1 \end{vmatrix} = f_3 \neq 0.$$

Bu nedenle, $I(\phi_2)$ yine $I = \langle f_1, f_2, f_3 \rangle$ idealidir ve düzenli dizi (regular sequence) $\{f_1 + f_2, f_2 + f_3\}$ içerir. Bu iddia doğrudur çünkü eğer $f_2 + f_3$, $S/\langle f_1 + f_2 \rangle$'da sıfır bölen olsaydı,

o zaman $(f_2 + f_3)g \in \langle f_1 + f_2 \rangle$ olacak şekilde S'de $\langle f_1 + f_2 \rangle$ dışında bir g bulunurdu, bu da $h(f_1 + f_2) = g(f_2 + f_3)$ olacak şekilde bir h bulunduğu anlamına gelirdi, fakat bu durum mümkün değildir. Böylece, Lemma 3.1.9'e göre (4)'te verilen dizi tam dizidir.

Şimdi bu çözülümün dereceli olduğunu, yani ϕ_1 ve ϕ_2 dönüşümlerinin dereceleri koruduğunu kanıtlayalım. $\phi\colon M = \bigoplus M_d \to N = \bigoplus N_d$ dönüşümünün dereceli (veya dereceyi koruyan) olduğunu, tüm $d \in \mathbb{N}W$ için $\phi(M_d) \subseteq N_d$ olduğu durumda söyleriz. (bknz. [42, Definition 8.12, Page 153])

Öncelikle, $\phi_1((F_1)_d) \subseteq (F_0)_d$ olduğunu göstermemiz gerekiyor. Dolayısıyla, eğer $d \in \mathbb{N}W$ için (m_1, m_2, m_3), $(F_1)_d = S_{d-\lambda_1} \oplus S_{d-\lambda_2} \oplus S_{d-\lambda_3}$'nin bir elemanıysa, o zaman şunu elde ederiz:

$$\operatorname{der}(m_j f_j) = (d - \lambda_j) + \operatorname{der}(f_j) = d, \text{ çünkü } \lambda_j = \operatorname{der}(f_j) \text{ olur, tüm } j = 1, 2, 3 \text{ için.}$$

Bu nedenle, $\phi_1(m_1, m_2, m_3) = m_1 f_1 + m_2 f_2 + m_3 f_3$ derecelidir.

$\phi_2((F_2)_d) \subseteq (F_1)_d$ olduğunu göstermek için $(m_1, m_2) \in (F_2)_d = S_{d-\sigma_1} \oplus S_{d-\sigma_2}$'yi alalım. $\phi_2(m_1, m_2) = (x_1 m_1 + 0 m_2, A_1 m_1 + m_2 f_3/x_1, A_2 m_1 - m_2 f_2/x_1)$ olduğundan, şu durumları elde ederiz:

$$\begin{aligned}
\operatorname{der}(x_1 m_1) &= \operatorname{der}(x_1) + \operatorname{der}(m_1) = 1 + d - ((q-1)ab + q + b + 1) = d - \lambda_1. \\
\operatorname{der}(A_1 m_1) &= \operatorname{der}(m_2 f_3/x_1) = qa + d - (qb + qa + 1) = d - (qb + 1) = d - \lambda_2. \\
\operatorname{der}(A_2 m_1) &= \operatorname{der}(-m_2 f_2/x_1) = qb + d - (qa + qb + 1) = d - (qa + 1) = d - \lambda_3.
\end{aligned}$$

Bunlar, ϕ_2'nin dereceli olduğunu kanıtlar ve kanıt bu şekilde tamamlanır. □

Sonuç 3.2.6. *$X = \mathbb{P}(1, 1, b)$ bir ağırlıklı projektif uzay ve $Y = X(\mathbb{F}_q)$ olmak üzere Y'nin ideali Teorem 3.2.4'in ifadesindeki gibi tanımlansın. İdealin minimal dereceli serbest çözülümü aşağıdaki gibi elde edilir.*

$$0 \to \bigoplus_{j=1}^{2} S(-\sigma_j) \xrightarrow{\begin{bmatrix} x_1 & 0 \\ -x_2 x_3^{q-1} & f_3/x_1 \\ A & -f_2/x_1 \end{bmatrix}} \bigoplus_{j=1}^{3} S(-\lambda_j) \xrightarrow{\begin{bmatrix} f_1 & f_2 & f_3 \end{bmatrix}} S \to S/I \to 0$$

Burada,

$$A = \sum_{i=1}^{b} x_1^{(i-1)(q-1)} x_2^{(q-1)b-iq+i} x_3, \qquad \sigma_1 = qb+2, \qquad \sigma_2 = qb+q+1,$$
$$\lambda_1 = qb+1, \qquad \lambda_2 = qb+1, \qquad \lambda_3 = q+1.$$

Kanıt. Yukarıdaki teoremin ispatındaki yöntem ve argümanlar kullanılarak benzer şekilde ispatlanır. Ana fikir, Lemma 3.1.9'deki argümanların gösterilmesiyle birlikte dizinin tam olduğunu ve dereceli olduğunu göstermektir. □

Teorem 3.2.7. $\mathbb{P}(1,a,b)$ *uzayının Hilbert serisinin formülü aşağıdaki gibi elde edilir.*

$$\frac{1-t^{qa+1}-t^{qb+1}+t^{qa+qb+1}-t^{(q-1)ab+a+b}+t^{(q-1)ab+a+b+1}}{(1-t)(1-t^a)(1-t^b)}.$$

Kanıt. Teorem 3.2.5'de verilen dereceli serbest çözülümünü göz önünde bulundurursak ve Teorem 3.1.10'de verilen fikri de dikkate aldığımızda aşağıdaki eşitliği elde ederiz:

$$\mathcal{K}_M(t) = \sum_{d\in\mathbb{N}W} (-1)^0 \beta_{0,d}(M) t^d + \sum_{d\in\mathbb{N}W} (-1)^1 \beta_{1,d}(M) t^d + \sum_{d\in\mathbb{N}W} (-1)^2 \beta_{2,d}(M) t^d.$$

Burada, $\beta_{0,0}(F_0) = 1$, $\beta_{1,\lambda_1}(F_1) = 1$, $\beta_{1,\lambda_2}(F_1) = 1$, $\beta_{1,\lambda_3}(F_1) = 1$ ve $\beta_{2,\sigma_1}(F_2) = 1$, $\beta_{2,\sigma_2}(F_2) = 1$ şeklindedir. Bu nedenle, düzenlediğimizde, aşağıdaki eşitliği elde ederiz:

$$\mathcal{K}_M(t) = 1 - t^{qa+1} - t^{qb+1} - t^{(q-1)ab+a+b} + t^{qa+qb+1} + t^{(q-1)ab+a+b+1}.$$

Böylece, Teorem 3.1.10'in sonucunu göz önünde bulundurduğumuzda aşağıdaki rasyonel fonksiyonu elde ederiz.

$$HS_M(t) = \frac{1-t^{qa+1}-t^{qb+1}-t^{(q-1)ab+a+b}+t^{qa+qb+1}+t^{(q-1)ab+a+b+1}}{(1-t)(1-t^a)(1-t^b)}. \tag{5}$$

ve bu da kanıtı tamamlar. □

Yukarıdaki teoremin ifadesinde $a = 1$ alındığında aşağıdaki sonuç doğrudan elde edilir.

Sonuç 3.2.8. $\mathbb{P}(1,1,b)$*'nın Hilbert serisinin formülü aşağıdaki gibi verilir.*

$$HS(\mathbb{P}(1,1,b),t) = \frac{1-t^{q+1}-2t^{qb+1}+t^{qb+2}+t^{qb+q+1}}{(1-t)(1-t)(1-t^b)}. \tag{6}$$

3.2.2 Kodun Boyutu ve Cebirsel Değişmez İlişkisi

Bu bölümde kodların temel parametreleri ve cebirsel değişmezler arasındaki ilişki vurgulanarak bu durum üzerinen elde edilen sonuçlar paylaşılacaktır. Bir hesaplama dönüşünümün çekirdeği, $I_d(Y)$ ile gösterilen $I(Y)$ idealinin d dereceli homojen kısmına eşit olduğundan ve hem dönüşümün tanımı hem de Birinci İzomorfizma Teoremi göz önünde bulundurulduğunda kodun boyutu, Hilbert fonksiyonu vasıtasıyla elde edilir. (bknz. Eşitlik (1))

Hilbert fonksiyonunun değerlerini elde etmek için ise bu tez çalışmasında Y kümesinin sıfırlayan idealinden bu idealin minimal dereceli serbest çözülümüne, bu çözülümden ise Hilbert serisine geçiş şeklinde bir yol izlenmiştir.

Şimdi, eşitlik (6) ile verilen seriyi göz önünde bulunduralım. Bu seri açılırsa, bir başka deyişle $1 - t^{q+1} - 2t^{qb+1} + t^{qb+2} + t^{qb+q+1}$ ifadesini, $1/(1-t)$ ile iki kez çarparsak aşağıdaki $p(t)$ polinomunu elde ederiz:

$$1 + 2t + \cdots + qt^{q-1} + (q+1)t^q + \cdots + (q+1)t^{qb} + (q-1)t^{qb+1} + \cdots + 2t^{qb+q-2} + t^{qb+q-1}.$$

Bu toplamı $1/(1-t^b)$ ile çarparsak aşağıda verilen Hilbert serisi $HS_M(t)$'yi elde ederiz.

$$HS_M(t) = \sum_{d \in \mathbb{N}W} H_Y(d)t^d = \sum_{i=0}^{\infty} t^{ib} p(t). \tag{7}$$

Böylece, $H_Y(d)$ Hilbert fonksiyonunun değeri, $p(t)$ polinomundaki t^{d-ib} teriminin katsayısı olan $C_i(d)$'dir. Bu polinom aşağıdaki şekilde tanımlanır:

$$p(t) = \sum_{j=0}^{q}(j+1)t^j + \sum_{k=q+1}^{qb}(q+1)t^k + \sum_{s=1}^{q-1}(q-s)t^{qb+s}.$$

Burada dikkat edilirse, $qb+1 \leq j \leq qb+q-1$ eşitsizliğindeki j için $p(t)$ polinomundaki t^j teriminin katsayısının $qb+q-j$ olduğu görülür. En genelde, bu terimlerin katsayıları bize Hilbert fonksiyonunun değerlerini verir. Dolayısıyla kodun boyutunu da veren aşağıdaki sonuçlar elde edilir.

Teorem 3.2.9. *$0 \leq r_0 < b$ olmak üzere $d = d_0 b + r_0$ olsun. $q \leq b$ pozitif bir tamsayı, $X = \mathbb{P}(1,1,b)$ ve $Y = X(\mathbb{F}_q)$ olmak üzere, Y'nin Hilbert fonksiyonlarının değerleri aşağıdaki*

gibidir. Ve kodun boyutu da bu değerlerle verilir.

$$H_Y(d) = \dim_{\mathbb{F}_q}(C_{d,Y}) = \begin{cases} d_0(q+1) + r_0 + 1, & \textit{eğer } 0 \leq d_0 \leq q-1 \textit{ ve } 0 \leq r_0 \leq q-1 \\ (d_0+1)(q+1), & \textit{eğer } 0 \leq d_0 \leq q-1 \textit{ ve } q \leq r_0 < b \\ q(q+1), & \textit{eğer } d_0 \geq q \textit{ ve } 0 < r_0 < b \\ q(q+1)+1, & \textit{eğer } d_0 \geq q \textit{ ve } r_0 = 0 \end{cases}$$

Kanıt. $H_Y(d)$'nin, (7) 'de verilen sonsuz toplamda t^d 'nin katsayısı olduğunu hatırlarsak, polinomda t^{d-ib}'nin katsayısı $C_i(d)$ üzerine yoğunlaşmamız gerektiği açıktır. Buradan, $0 \leq i \leq d_0$ için,

$$p(t) = \sum_{j=0}^{q}(j+1)t^j + \sum_{k=q+1}^{qb}(q+1)t^k + \sum_{s=1}^{q-1}(q-s)t^{qb+s} = \sum_{i=0}^{d_0} C_i(d)t^{d-ib} \tag{8}$$

olur ve böylece $H_Y(d) = \sum_{i=0}^{d_0} C_i(d)$ eşitliği elde edilir. Burada, hatırlatmak gerekirse $d - ib = (d_0 - i)b + r_0$ eşitliği vardır.

Durum I: $0 \leq d_0 \leq q-1$ olsun.

$i = d_0$ için, $d - ib = r_0$ olur ve t^{r_0}'nin $p(t)$'deki katsayısını elde ederiz:

$$C_i(d) = \begin{cases} r_0 + 1, & \text{eğer } 0 \leq r_0 \leq q-1 \\ q+1, & \text{eğer } q \leq r_0 < b. \end{cases} \tag{9}$$

$0 \leq i \leq d_0 - 1$ olduğu her durumda, $q \leq b \leq (d_0 - i)b + r_0 \leq (d_0+1)b \leq qb$ olur. Dolayısıyla, $d - ib = (d_0 - i)b + r_0$, q ile qb arasında olup, bu nedenle, tüm $0 \leq i \leq d_0 - 1$ için (8)'e göre $C_i(d) = q + 1$ olur. Bu nedenle,

$$H_Y(d) = \sum_{i=0}^{d_0} C_i(d) = d_0(q+1) + \begin{cases} r_0 + 1, & \text{eğer } 0 \leq r_0 \leq q-1 \\ q+1, & \text{eğer } q \leq r_0 < b. \end{cases} \tag{10}$$

Durum II: $d_0 = q$ olsun. Dolayısıyla, $d = qb + r_0$ ve $d - ib = (q - i)b + r_0$ olur.
Öncelikle, $i = 0$ durumunu ele alalım. O zaman şu formülleri elde ederiz:

$$C_i(d) = \begin{cases} q+1 & \text{eğer } r_0 = 0, \\ q - r_0 & \text{eğer } 0 < r_0 \leq q-1, \\ 0 & \text{eğer } q \leq r_0 < b. \end{cases} \tag{11}$$

Şimdi $1 \leq i \leq q-1$ olan durumları ele alalım. O zaman,

$$q \leq b \leq (q-i)b \leq (q-1)b \Rightarrow q \leq (q-i)b + r_0 \leq (q-1)b + r_0 < qb \Rightarrow C_i(d) = q+1.$$

$i = q$ durumu için, şu formülleri elde ederiz:

$$C_i(d) = \begin{cases} 1 & \text{eğer } r_0 = 0, \\ r_0 + 1 & \text{eğer } 0 < r_0 \leq q-1, \\ q+1 & \text{eğer } q \leq r_0 < b. \end{cases} \tag{12}$$

Böylece, tüm bu durumları düzenlersek, aşağıdaki formülleri elde ederiz:

$$H_Y(d) = \begin{cases} q(q+1)+1 & \text{eğer } r_0 = 0, \\ q(q+1) & \text{eğer } 0 < r_0 \leq q-1, \\ q(q+1) & \text{eğer } q \leq r_0 < b. \end{cases} \tag{13}$$

Durum III: $d_0 > q$ olduğunu varsayalım. Bu durumda, $d_0 - q > 0$ olur.

$0 \leq i < d_0 - q$ olmak üzere, bu durumda , $C_i(d) = 0$ olur, çünkü aşağıdaki durum sağlanır:

$$q+1 \leq d_0 - i \Rightarrow (q+1)b \leq (d_0 - i)b \Rightarrow qb + (q-1) < qb + b \leq (d_0 - i)b \leq d - ib.$$

$d_0 - q \leq i < d_0$ olan durumlarda ise, aşağıdaki durum sağlanır:

$$0 < d_0 - i \leq q \Rightarrow q \leq b \leq (d_0 - i)b \leq qb.$$

Bu yüzden, $d - ib = (d_0 - i)b + r_0$ olur ve bu durum r_0'a bağlıdır.

Eğer $r_0 = 0$ ise, $C_i(d) = q + 1$ olur, çünkü $d_0 - q \leq i \leq d_0 - 1$ için, $d - ib = (d_0 - i)b$, geçerlidir.

Eğer $r_0 > 0$ ve $i = d_0 - q$ ise, $d - ib = qb + r_0$ olur ve bu yüzden,

$$C_i(d) = \begin{cases} q - r_0 & \text{eğer } 1 \leq r_0 \leq q - 1, \\ 0 & \text{eğer } q \leq r_0 < b, \end{cases} \tag{14}$$

elde edilir. Eğer $r_0 > 0$ ve $i > d_0 - q$ ise, $d_0 - i < q \Rightarrow d_0 - i \leq q - 1$ olur ve bu yüzden aşağıdaki durum geçerlidir:

$$d - ib = (d_0 - i)b + r_0 \leq (q - 1)b + r_0 = qb - b + r_0 < qb.$$

Bu durumda, $d_0 - (q - 1) \leq i \leq d_0 - 1$ için $C_i(d) = q + 1$ olur. Son olarak, $i = d_0$ durumu için, $d - ib = r_0$ olur ve bu yüzden aşağıdaki durum elde edilir:

$$C_i(d) = \begin{cases} r_0 + 1 & \text{eğer } 0 \leq r_0 \leq q - 1, \\ q + 1 & \text{eğer } q \leq r_0 < b. \end{cases} \tag{15}$$

Özetlemek gerekirse, $d_0 - (q - 1) \leq i \leq d_0 - 1$ için $C_i(d) = q + 1$ olur ve

$$C_{d_0-q}(d) + C_{d_0}(d) = \begin{cases} (q + 1) + 1 & \text{eğer } r_0 = 0, \\ q + 1 & \text{eğer } 0 < r_0 < b. \end{cases} \tag{16}$$

Bu nedenle,

$$H_Y(d) = \begin{cases} q(q + 1) + 1 & \text{eğer } r_0 = 0, \\ q(q + 1) & \text{eğer } 0 < r_0 < b, \end{cases} \tag{17}$$

olur ve böylece ispat tamamlanır. □

Teorem 3.2.10. *$0 \leq r_0 < b$ olmak üzere $d = d_0b + r_0$ ve $0 \leq r < b$ olmak üzere $d = q + kb + r$ olsun. $q > b$ ise Hilbert fonksiyonunun değerlerini ve dolayısıyla kodun boyutunu aşağıdaki*

gibi elde ederiz.

$$\dim_{\mathbb{F}_q}(C_{d,Y}) = \begin{cases} d+1 & \textit{eğer } 0 \leq d \leq b-1, \\ (d_0+1)(d+1-bd_0/2) & \textit{eğer } b \leq d \leq q, \\ (d_0-k)(d-(d_0+k+1)b/2)+q(k+1)+1 & \textit{eğer } q+1 \leq d \leq qb \\ (k+q)(k-q+1)b/2+q(k+d+1)-dk-bd_0+\kappa & \textit{eğer } d > qb \textit{ ve } k \geq q, \end{cases}$$

$$\kappa = \begin{cases} q-r_0, & \textit{eğer } 0 < r_0 < q, \\ q+1 & \textit{eğer } r_0 = 0. \end{cases}$$

Kanıt. $d = d_0 b + r_0$ için $0 \leq r_0 < b < q$ olduğunu varsayalım. (7) eşitliğinde verilen Hilbert serisi, $\sum_{i=0}^{\infty} t^{ib} p(t)$ olarak verilmişti. $C_i(d)$, önceki ispatta olduğu gibi $0 \leq i \leq d_0$ için $p(t)$ polinomunda t^{d-ib} teriminin katsayısıdır. (8) eşitliği ile verilen $p(t)$ polinomunda $j = d - ib$ değerini yerine koyarsak aşağıdaki durumları elde ederiz:

$$C_i(d) = \begin{cases} d-ib+1 & \text{eğer } 0 \leq d-ib \leq q, \\ q+1 & \text{eğer } q+1 \leq d-ib \leq qb, \\ q+(qb-d+ib) & \text{eğer } qb+1 \leq d-ib \leq qb+q-1. \end{cases} \tag{18}$$

Durum I: $0 \leq d \leq b-1$ olduğunu varsayalım. Bu durumda, $d_0 = 0$ olur. Böylece $i = 0$ olur. Dolayısıyla, $H_Y(d) = d+1$ olur.

Durum II: $b \leq d \leq q$ olduğunu varsayalım. Açıkça, $d_0 > 0$ olur. O zaman, $d - ib \leq q$ olur. Böylece, $C_i = d - ib + 1$ olur. Dolayısıyla, aşağıdaki eşitlik elde edilir:

$$H_Y(d) = \sum_{i=0}^{d_0}(d-ib+1) = (d_0+1)(d+1) - b\sum_{i=0}^{d_0} i = (d_0+1)(d+1) - b\left(\frac{d_0(d_0+1)}{2}\right).$$

Durum III: $q+1 \leq d < qb$ ve ayrıca $d = q + kb + r$ ve $0 \leq r < b$ olduğunu varsayalım. $d > q$ olduğundan, $d-q = kb+r$ olur. Öncelikle, $k = 0$ ise, $i = 0$ için $C_i = q+1$ olur. $i > 0$ için, $d - d_0 b < \cdots < d - 2b < d - b < q$ olur. Buradan, $i = 1, 2, \ldots, d_0$ için $C_i = d - ib + 1$ olur. Dolayısıyla, $H_Y(d) = q + 1 + \sum_{i=1}^{d_0}(d - ib + 1)$ olur.

$i = 0$ için, $C_i = q + 1$ olur. $1 \leq i \leq k$ için, $q \leq d - b < (q-1)a$ açıktır. Dolayısıyla, $q \leq d - kb \leq d - ib \leq d \leq qb$ olur. O zaman, $1 \leq i \leq k$ için $C_i = q + 1$ olur. $k+1 \leq i \leq d_0$ için, $-i \leq -k-1$ olduğundan $d-ib \leq d-kb-b$ olur. Ayrıca, $d = q+kb+r$ olduğundan ve $r < b$ olduğundan, $d - ib \leq d - kb - b \leq q + r - b < q$ olur. Böylece, $H_Y(d) = (k+1)(q+1) + \sum_{i=k+1}^{d_0} (d - ib + 1)$ olur. Eşitliği düzenlersek,

$$H_Y(d) = (k+1)(q+1) + (d_0 - k)(d+1) - b\left(\frac{d_0(d_0+1)}{2} - \frac{k(k+1)}{2}\right)$$

olduğunu elde ederiz.

Durum IV: $qb < d$ ve $k < q$ olduğunu varsayalım. $d = d_0 b + r_0$ olduğundan, $d_0 \geq q$ olur.

$0 \leq i < d_0 - q$ olduğunda, $i < d_0 - q$ için $d - ib > qb$ olur. Böylece, $C_i = q + qb - d + ib$ olur.

$d_0 - q < i \leq d_0 - k$ olduğunda, ilk olarak $d_0 - q < i$ olduğunu düşünürsek, V. Durum'da olduğu gibi $d - ib < qb$ olur. Ayrıca, $i \leq d_0 - k$ olduğunda, $d - ib \geq d - d_0 b + kb = r_0 + kb > kb = d - q - r > qb - q - r > qb - 2q = q(b-2)$ olur.Ve $b \geq 2$ olduğundan $d - ib > q(b-2) \geq q$ olur. O zaman, $C_i = q + 1$ olur.

$d_0 - k < i \leq k$ olduğunda, $d - ib \leq d - d_0 b + kb - b = r_0 - b + kb < qb + r_0 - b$ olur. $r_0 < b$ olduğundan, $d - ib < qb$ olur. Böylece, $C_i = q + 1$ olur.

$k + 1 \leq i \leq d_0$ olduğunda, IV. Durum'daki argümanı kullanarak $C_i = d - ib + 1$ olur. $i = d_0 - q$ olduğunda, $d - d_0 b + qb = r_0 + qb$ olur. $0 < r_0 < q$ olduğundan, $qb < d - ib \leq qb + q - 1$ olur. Böylece, $C_i = q - r_0$ elde edilir. Ayrıca, $r_0 = 0$ olduğunda, $d - ib = d - d_0 b + qb = r_0 + qb = qb$ olur. Böylece, $C_i = q + 1$ elde edilir. Dolayısıyla, aşağıdaki durumların elde edildiğini söyleyebiliriz:

$$\sum_{i=0}^{d_0-q-1} (q+qb-d+ib) + (q+k-d_0)(q+1) + \sum_{i=k+1}^{d_0} (d+1-ib) + \kappa = \begin{cases} q - r_0 & \text{eğer } 0 < r_0 < q, \\ q + 1 & \text{eğer } r_0 = 0. \end{cases}$$

Tüm eşitlikleri $d > qb$ ve $k < q$ için düzenlersek,

$$\begin{aligned} H_Y(d) &= (d_0 - q)(q + qb - d) + \frac{b}{2}\big((d_0 - q - 1)(d_0 - q)\big) + (q + k - d_0)(q + 1) \\ &\quad + (d + 1)(d_0 - k) - \frac{b}{2}\big(d_0(d_0 + 1) - k(k + 1)\big) + \kappa. \\ &= qd - \frac{q^2 b}{2} - bd_0 + \frac{bq}{2} + q + kq - dk + \frac{bk^2}{2} + \frac{bk}{2} + \kappa \\ &= \frac{b}{2}\big((k + q)(k - q + 1)\big) + q(d + 1 + k) - bd_0 - kd + \kappa = \begin{cases} q - r_0 & \text{eğer } r_0 < q, \\ q + 1 & \text{eğer } r_0 = 0. \end{cases} \end{aligned}$$

durumlarını elde ederiz.

Durum V: $qb < d$ ve $k \geq q$ olduğunu varsayalım. $d = d_0 b + r_0$ olduğunu hatırlayalım ve $d_0 \geq q$ olduğunu kabul edelim.

$0 \leq i \leq k - q$ olduğunda, $d - ib \geq d - kb + qb = q + r + qb \geq qb + q > qb + q - 1$ olur. $d - ib > qb + q - 1$ olduğundan, $C_i = 0$ olarak elde edilir.

Ayrıca, $k - q < i < d_0 - q$ olduğunda, $i < d_0 - q$ olduğunu düşünürsek, $-i > q - d_0 \Rightarrow d - ib > d + qb - d_0 b = r_0 + qb > qb$ olur. İlaveten, $i > k - q$ olduğunu düşünürsek, $-i \leq -k + q - 1 \Rightarrow d - ib \leq d - kb + qb - b$ olur. $d = q + kb + r$ olduğundan ve $r < b$ olduğundan, $d - ib \leq d - kb + qb - b \leq q + r + qb - b \leq qb + q - 1$ olur. Böylece, $qb < d - ib \leq qb + q - 1$ ve $C_i = q + qb - d + ib$ olarak elde edilir.

$d_0 - q < i \leq k$ olduğunda, $d = kb + q + r$ eşitliğini de dikkate alırsak, $d - ib \geq d - kb = q + r \geq q$ olur. Ayrıca, $i \geq d_0 - q + 1 \Rightarrow -i \leq q - 1 - d_0 \Rightarrow d - ib \leq d + qb - b - d_0 b = qb + r_0 - b$ eşitsizliklerini de elde ederiz. $r_0 < b$ olduğundan, $d - ib < qb$ olur ve böylece, $C_i = q + 1$ olur.

$k + 1 \leq i \leq d_0$ olduğunda, IV. Durum'daki argümanı kullanarak $C_i = d - ib + 1$ olduğunu elde ederiz.

$i = d_0 - q$ olduğunda, $d - d_0 b + qb = r_0 + qb$ olur. $0 < r_0 < q$ olduğundan, $qb < d - ib \leq qb + q - 1$ elde edilir. Böylece, $C_i = q - r_0$ olur. Ayrıca, $r_0 = 0$ olduğunda, $d - ib = d - d_0 b + qb = r_0 + qb = qb$ olur ve böylece, istenildiği gibi $C_i = q + 1$ eşitliği elde edilir.

Dolayısıyla, tüm eşitlikleri $d > qb$ ve $k \geq q$ için düzenlersek, teoremin iddiasındaki tüm durumları elde ederiz. □

3.2.3 Kodun Boyutu ile İlgili Diğer Sonuçlar

Tüm bunlara ek olarak [33, Lemma 9] makalesindeki yöntemler incelenerek bu metodların çalıştığımız uzaya modifiye edilmesi ile birlikte aşağıdaki sonuçlar elde edilmiştir. Öncelikle, $X = \mathbb{P}(1, a, b)$ ve $Y = X(\mathbb{F}_q)$ olmak üzere, $I(Y)$ sıfırlayan idealinin üreteçleri Teorem 3.2.3'da verildiği gibi alınsın. Buradaki f_1, f_2, f_3 üreteçleri $x_1 > x_2 > x_3$ sıralamasına göre bir Gröbner bazdır. Bilhassa, $S/I(Y)$ ve $S/\mathrm{LT}(I(Y))$ koordinat halkaları aynı Hilbert fonksiyonuna sahiptir. Burada, *LT* ile kast edilen baş terim'dir (leading term). $C_{d,Y}$ kodunun boyutu bu bilgiler doğrultusunda aşağıdaki şekilde elde edilmiştir.

Teorem 3.2.11. *V_1, V_2 ve V_3 kümeleri aşağıdaki gibi tanımlansın.*

$$V_1 = \mathrm{span}\{x_1^{a_1}x_2^{a_2} : a_1 + aa_2 = d, 0 \leq a_1 \leq \min(d, (q-1)a), a_2 > 0\} \cup \{x_1^d\},$$
$$V_2 = \mathrm{span}\{x_1^{a_1}x_3^{a_3} : a_1 + ba_3 = d, 0 \leq a_1 \leq \min(d, (q-1)b), a_3 > 0\},$$
$$V_3 = \mathrm{span}\{x_1^{a_1}x_2^{a_2}x_3^{a_3} : a_3 > 0, 0 < a_2 \leq (q-1)b \text{ ve } 0 \leq a_1 = d - aa_2 - ba_3 \leq (q-1)b\}.$$

$S_d/I_d(Y)$ vektör uzayının boyutu aşağıdaki şekilde verilir:

$$\dim_{\mathbb{F}_q}(S_d/I_d(Y)) = \dim_{\mathbb{F}_q}(V_1) + \dim_{\mathbb{F}_q}(V_2) + \dim_{\mathbb{F}_q}(V_3) \tag{19}$$

Burada,

$$\dim_{\mathbb{F}_q}(V_1) = \begin{cases} \lfloor \frac{d}{a} \rfloor + 1 & \text{eğer } d < qa, \\ q+1 & \text{eğer } d \geq qa \text{ ve } a \mid d, \\ q & \text{eğer } d > qa \text{ ve } a \nmid d. \end{cases} \quad \dim_{\mathbb{F}_q}(V_2) = \begin{cases} \left\lfloor \frac{d}{b} \right\rfloor & \text{eğer } d < qb, \\ q & \text{eğer } d \geq qb \text{ ve } b \mid d, \\ q-1 & \text{eğer } d > qb \text{ ve } b \nmid d \end{cases}$$

$$\dim_{\mathbb{F}_q}(V_3) = \begin{cases} s_1 + s_2 + s_3 & \text{eğer } \eta_1 \geq 1 \text{ ve } \eta_2 \geq 1, \\ s_2 + s_3 & \text{eğer } \eta_1 = 0 \text{ ve } \eta_2 \geq 1 \\ s_3 & \text{eğer } \eta_1 = 0 \text{ ve } \eta_2 = 0, \end{cases}$$

Burada,

$$s_1 = \eta_1((q-1)b+q) - \sum_{a_3=1}^{\eta_1} \left\lceil \frac{d-ba_3}{a} \right\rceil \quad s_2 = (\eta_2 - \eta_1)q, \text{ ve} \quad s_3 = \sum_{a_3=\eta_2+1}^{\left\lfloor \frac{d}{b} \right\rfloor} \left\lfloor \frac{d-ba_3}{a} \right\rfloor,$$

$$\eta_1 = \max\left(0, \left\lfloor \frac{d}{b} \right\rfloor - (q-1)a\right) \text{ ve } \eta_2 = \max\left(0, \left\lfloor \frac{d-qa}{b} \right\rfloor\right).$$

Kanıt. [33]'de verilen Lemma 9'un ifadesindeki ve ispatındaki fikirlerden ilham alınarak, $S_d/\text{LT}(I_d(Y))$ vektör uzayı için bir baz elde edilecektir. $x_1^{a_1}x_2^{a_2}x_3^{a_3}$ monomu, $a_1+aa_2+ba_3 = d$'dir ve $\{x_2^{(q-1)b+1}x_3, x_1^{(q-1)b+1}x_3, x_1^{(q-1)a+1}x_2\}$ üreteçleri tarafından bölünmüyordur ancak ve ancak o zaman bu monom bir baz elemanıdır. Bu tür monomların kümesinin, $a_3 = 0$ olduğunda V_1, $a_2 = 0 < a_3$ olduğunda V_2 ve hem a_2 hem de a_3 pozitif olduğunda V_3'ü kapsadığı açıktır. Böylece, (19)'deki formülü elde ederiz.

$$S_d/I_d \cong x_3\mathbb{F}_q[x_1,x_2,x_3]_{d-b}/x_3J_{d-b} \oplus \mathbb{F}_q[x_1,x_2]_d/J'_d,$$

burada $J = J' + \langle x_1^{(q-1)b+1}x_3, x_2^{(q-1)b+1}x_3\rangle$ ve $J' = \langle x_1^{(q-1)a+1}x_2\rangle$'dır. O zaman,

$$V_2 = \mathbb{F}_q[x_1,x_3]_{d-b}/J_{d-b} \text{ ve } V_1 = \mathbb{F}_q[x_1,x_2]_d/J'_d.$$

olduğunu söyleyebiliriz.

Öncelikle, $\dim_{\mathbb{F}_q}(V_1)$ için olan iddiamızı kanıtlayacağız.

$d \leq qa$ durumunda, tüm $i \geq 2$ için $d-a \leq (q-1)a \Rightarrow d-ia < d-a \leq (q-1)a$ $1 \leq a_2 \leq \left\lfloor \frac{d}{a} \right\rfloor$ olduğunda ise, $a_1 = d-a_2a \leq d-a \leq (q-1)a$ durumu elde edilir. Ayrıca V_1, x_1^d elemanını içerdiğinden kümede bir eleman daha vardır. Böylece, $\dim(V_1) = \left\lfloor \frac{d}{a} \right\rfloor + 1$ olarak elde edilir. $d > qa$ durumunda, V_1 kümesinin tanımından $a_1 \leq (q-1)a$ olduğu sonucunu elde ederiz. O zaman,

$$\begin{aligned} a_1 = d - aa_2 \leq (q-1)a &\iff d-(q-1)a \leq aa_2 \\ &\iff \frac{d-(q-1)a}{a} \leq a_2 \Rightarrow \left\lfloor \frac{d}{a} \right\rfloor - (q-1) \leq a_2. \end{aligned}$$

olur ve böylece, $a_2 = \left\lfloor \frac{d}{a} \right\rfloor - (q-1) + i$ yazarsak, $0 \leq i \leq q-1$ için $a_1 = d - aa_2 = d - a\left\lfloor \frac{d}{a} \right\rfloor + (q-1)a - ia$ olarak elde ederiz.

Buradan, $i \geq 1$ ise $a_1 = (q-1)a + r_a - ia \leq (q-1)a$ olur, çünkü $0 \leq d - \left\lfloor \frac{d}{a} \right\rfloor a = r_a < a$. Ayrıca, $i = 0$ ise $a_2 = \left\lfloor \frac{d}{a} \right\rfloor - (q-1)$ ve $a_1 = (q-1) + r_a \leq (q-1)a$ sadece $r_a = 0$ olduğunda olur. Bu nedenle, $d > qa$ ve $a \mid d$ olduğunda (yani $r_a = 0$), $\left\lfloor \frac{d}{a} \right\rfloor - (q-1) \leq a_2 \leq \left\lfloor \frac{d}{a} \right\rfloor$ ile ilişkili olarak q tane baz elemanımız olur. Ayrıca, bazda x_1^d elemanı bulunduğundan, $\dim_{\mathbb{F}_q}(V_1) = q+1$ olur. Ancak, $d > qa$ ve $a \nmid d$ olduğunda, $\dim_{\mathbb{F}_q}(V_1) = q$ olur.

$\dim_{\mathbb{F}_q}(V_1)$'in ispatını taklit ederek, Teorem'de verilen $\dim_{\mathbb{F}_q}(V_2)$ formülünü de elde ederiz.

Şimdi, $\dim_{\mathbb{F}_q}(V_3)$ iddiamızı kanıtlayacağız. $1 \leq a_3 \leq \lfloor \frac{d}{b} \rfloor$, $1 \leq a_2 \leq (q-1)b$ ve $0 \leq a_1 = d - aa_2 - ba_3 \leq (q-1)a$ olması gerektiğini göstereceğiz. Öncelikle, $0 \leq a_1 = d - aa_2 - ba_3 \iff a_2 \leq \frac{d-ba_3}{a} \iff a_2 \leq \left\lfloor \frac{d-ba_3}{a} \right\rfloor$. Böylece, $a_2 \leq \min\left((q-1)b, \left\lfloor \frac{d-ba_3}{a} \right\rfloor\right)$. Benzer şekilde, $a_1 = d - aa_2 - ba_3 \leq (q-1)a \iff \frac{d-ba_3}{a} - (q-1) \leq a_2$. Sonuç olarak, $\max\left(1, \left\lceil \frac{d-ba_3}{a} \right\rceil - (q-1)\right) \leq a_2$. Bu ifadeler aşağıdaki formülü verir:

$$\dim_{\mathbb{F}_q}(V_3) = \sum_{a_3=1}^{\lfloor \frac{d}{b} \rfloor} \sum_{a_2=\max\left(1, \left\lceil \frac{d-ba_3}{a} \right\rceil - (q-1)\right)}^{\min\left((q-1)b, \left\lfloor \frac{d-ba_3}{a} \right\rfloor\right)} 1.$$

Farklı a_3 değerleri için $\max\left(1, \left\lceil \frac{d-ba_3}{a} \right\rceil - (q-1)\right)$ ve $\min\left((q-1)b, \left\lfloor \frac{d-ba_3}{a} \right\rfloor\right)$ değerlerini belirlememiz gereklidir. $(q-1)b \leq \left\lfloor \frac{d-ba_3}{a} \right\rfloor \iff (q-1)b \leq \frac{d-ba_3}{a} \iff a_3 \leq \frac{d}{b} - (q-1)a$ olduğunu göz önünde bulundurduğumuzda, $\eta_1 = \lfloor \frac{d}{b} \rfloor - (q-1)a > 0$ ve $a_3 \leq \eta_1$ durumunda $\min\left((q-1)b, \left\lfloor \frac{d-ba_3}{a} \right\rfloor\right) = (q-1)b$ olur. Başka bir deyişle, $\eta_1 = 0$ ise, $\min\left((q-1)b, \left\lfloor \frac{d-ba_3}{a} \right\rfloor\right) = \left\lfloor \frac{d-ba_3}{a} \right\rfloor$ olur.

$\frac{d-ba_3}{a} - (q-1) \geq 1 \iff d - ba_3 \geq qa \iff \frac{d-qa}{b} \geq a_3$ olduğunu hatırlatmak gerekirse ve $\eta_2 = 0$, veya $a_3 > \frac{d-qa}{b} > 0$ ise, $1 > \frac{d-qa}{b}$ veya $1 \leq a_3 \leq \frac{d-qa}{b}$ durumları elde edilir. Bu durumlar, aşağıdaki şekilde yeniden yazılabilir:

$$\max\left(1, \left\lceil \frac{d-ba_3}{a} \right\rceil - (q-1)\right) = \begin{cases} \left\lceil \frac{d-ba_3}{a} \right\rceil - (q-1) & \text{eğer } 1 \leq a_3 \leq \eta_2, \\ 1 & \text{eğer } \eta_2 = 0 \text{ veya } \eta_2 < a_3 \leq \lfloor \frac{d}{b} \rfloor. \end{cases}$$

Şimdi, $\eta_1 \geq 1$ ise $\eta_1 \leq \eta_2$ olduğunu göstereceğiz. Eğer $b > 1$ ise, $\left\lfloor \frac{d-qa}{b} \right\rfloor \geq \lfloor \frac{d}{b} \rfloor - (q-1)a$ olur, çünkü $qa = (q-1)a + a \leq (q-1)a + (q-1)a(b-1) = (q-1)ab$. Böylece, $\eta_1 \leq \eta_2$ olur. $\eta_3 := \left\lceil \frac{d-ba_3}{a} \right\rceil - (q-1)$ olarak tanımlayalım. Eğer $\eta_1 \geq 1$ ve $\eta_2 \geq 1$ ise, şu sonucu elde ederiz:

$$\dim_{\mathbb{F}_q}(V_3) = s_1 + s_2 + s_3,$$

burada, $s_1 = \sum_{a_3=1}^{\eta_1} \sum_{a_2=\eta_3}^{(q-1)b} 1$, $s_2 = \sum_{a_3=\eta_1+1}^{\eta_2} \sum_{a_2=\eta_3}^{\left\lfloor \frac{d-ba_3}{a} \right\rfloor} 1$ ve $s_3 = \sum_{a_3=\eta_2+1}^{\lfloor \frac{d}{b} \rfloor} \sum_{a_2=1}^{\left\lfloor \frac{d-ba_3}{a} \right\rfloor} 1$ şeklindedir. İspatın geri kalan kısmı benzer şekilde yapılır ve ispat tamamlanır. □

Buradan, yukarıdaki teorem bize $X = \mathbb{P}(1, a, b)$ ve $Y = X(\mathbb{F}_q)$ iken $C_{d,Y}$ kodunun boyutunu verir. Ve eğer bu teoremde $a = 1$ olarak alırsak, Teorem 3.2.9 ve Teorem 3.2.10 ile aynı sonuçları elde ederiz.

Sonuç 3.2.12. *$X = \mathbb{P}(1, 1, b)$ ve $Y = X(\mathbb{F}_q)$ olsun. $d = d_0 b + r_0$ ile $0 \leq r_0 < b$ olacak şekilde tanımlayalım. $d > q$ olduğunda, ayrıca $d = q + kb + r$ ile $0 \leq r < b$ olacak şekilde tanımlayalım. Eğer $q \leq b$ ise*

$$\dim_{\mathbb{F}_q}(S_d/I_d) = \begin{cases} d_0(q+1) + r_0 + 1, & \text{eğer } 0 \leq d_0 \leq q-1 \text{ ve } 0 \leq r_0 \leq q-1 \text{ ise} \\ (d_0+1)(q+1), & \text{eğer } 0 \leq d_0 \leq q-1 \text{ ve } q \leq r_0 < b \text{ ise} \\ q(q+1), & \text{eğer } d_0 = q \text{ ve } r_0 = q \text{ ya da } 0 < r_0 < b \text{ ise} \\ q(q+1) + 1, & \text{eğer } d_0 = q \text{ ve } r_0 = 0 \text{ ise.} \end{cases} \tag{20}$$

Ayrıca, eğer $q > b$ ise $\dim_{\mathbb{F}_q}(S_d/I_d)$'yi aşağıdaki gibi elde ederiz.

$$\begin{cases} d+1 & \text{eğer } 0 \leq d \leq b-1, \\ (d_0+1)(d+1-bd_0/2) & \text{eğer } b \leq d \leq q, \\ (d_0-k)(d-(d_0+k+1)b/2) + q(k+1) + 1 & \text{eğer } q+1 \leq d \leq qb, \\ (k+q)(k-q+1)b/2 + q(k+d+1) - dk - bd_0 + \kappa & \text{eğer } d > qb \text{ ve } k < q \text{ ise}, \\ q^2 + r_0 + \kappa & \text{eğer } d > qb \text{ ve } k \geq q \text{ ise.} \end{cases} \tag{21}$$

Burada,

$$\kappa = \begin{cases} q - r_0, & \textit{eğer } 0 < r_0 < q \textit{ ise}, \\ q + 1 & \textit{eğer } r_0 = 0 \textit{ ise}. \end{cases}$$

Kanıt. Aşağıdaki şekilde tanımlanan V_1, V_2 ve V_3 kümelerini ele alalım.

$$V_1 = \operatorname{span}\{x_1^{a_1}x_2^{a_2} : a_1 + a_2 = d, 0 \leq a_1 \leq \min(d, (q-1)), a_2 > 0\} \cup \{x_1^d\},$$
$$V_2 = \operatorname{span}\{x_1^{a_1}x_3^{a_3} : a_1 + ba_3 = d, 0 \leq a_1 \leq \min(d, (q-1)b), a_3 > 0\},$$
$$V_3 = \operatorname{span}\{x_1^{a_1}x_2^{a_2}x_3^{a_3} : a_1 + a_2 + ba_3 = d, a_2 > 0, a_3 > 0, a_1 \leq (q-1) \text{ ve } a_2 \leq (q-1)b\}.$$

Bu durumda,

$$\dim_{\mathbb{F}_q}(S_d/I_d(Y)) = \dim_{\mathbb{F}_q}(V_1) + \dim_{\mathbb{F}_q}(V_2) + \dim_{\mathbb{F}_q}(V_3)$$

olur, burada

$$\dim_{\mathbb{F}_q}(V_1) = \begin{cases} d+1 & \text{eğer } d < q, \\ q+1 & \text{eğer } d \geq q. \end{cases} \quad \dim_{\mathbb{F}_q}(V_2) = \begin{cases} d_0 & \text{eğer } d < qb, \\ q & \text{eğer } d \geq qb \text{ ve } b \mid d, \\ q-1 & \text{eğer } d > qb \text{ ve } b \nmid d. \end{cases}$$

$$\dim_{\mathbb{F}_q}(V_3) = \begin{cases} s_1 + s_2 + s_3 & \text{eğer } \eta_1 \geq 1 \text{ ve } \eta_2 \geq 1, \\ s_2 + s_3 & \text{eğer } \eta_1 \leq 0 \text{ ve } \eta_2 \geq 1 \\ s_3 & \text{eğer } \eta_1 \leq 0 \text{ ve } \eta_2 \leq 0, \end{cases}$$

burada

$$s_1 = \eta_1((q-1)b + q) - \sum_{a_3=1}^{\eta_1}(d - ba_3) \quad s_2 = (\eta_2 - \eta_1)q \quad s_3 = \sum_{a_3=\eta_2+1}^{d_0}(d - ba_3)$$

ve

$$\eta_1 = \max\left(0, \left\lfloor \frac{d}{b} \right\rfloor - (q-1)\right) = \max(0, d_0 - q + 1) \text{ ve } \eta_2 = \max\left(0, \left\lfloor \frac{d-q}{b} \right\rfloor\right) = \max(1, k).$$

Bu durumda, s_1, s_2 ve s_3 toplamlarını duruma göre düzenlersek,

$$s_1 = (d_0 - q + 1)(qb - d + q - b) + \frac{b}{2}((d_0 - q)^2 + 3(d_0 - q) + 2) \text{ eğer } \eta_1 \geq 0,$$
$$s_2 = q(k-1) - q(d_0 - q) \text{ eğer } \eta_1 \geq 0 \text{ ve } \eta_2 \geq 0,$$
$$s_3 = d(d_0 - k) - \frac{b}{2}((d_0 - k)(d_0 + k + 1)).$$

Durum I: $q \leq b$ olsun.

$0 \leq d_0 \leq q-1$ ve $0 \leq r_0 \leq q-1$ olduğunu varsayalım. $d > q$ olduğundan, $\dim_{\mathbb{F}_q}(V_1) = q+1$ ve $d < qb$ olduğundan $\dim_{\mathbb{F}_q}(V_2) = d_0$ olduğunu görüyoruz. Bu durumda $d_0 - 1 = k$ olurken $d_0 \geq 1$ olur. Ayrıca, $s_1 = 0$'dır. $\mu_1 = 0$ olduğundan $s_2 = kq$ olur. Ve $d_0 - 1 = k$ olduğundan $s_3 = r_0$ olur. Bu nedenle, boyut $d_0(q+1)+r_0+1$ olarak elde edilir. Ayrıca, $d_0 = 0$ olduğunda $\dim_{\mathbb{F}_q}(V_3) = 0 = \dim_{\mathbb{F}_q}(V_2)$ ve $\dim_{\mathbb{F}_q}(V_1) = d + 1$ olur. Böylece, $r_0 + 1$ elde ederiz.

$0 \leq d_0 \leq q - 1$ ve $q \leq r_0 \leq b$ olduğunu varsayalım. Benzer şekilde, $d > q$ olduğundan $\dim_{\mathbb{F}_q}(V_1) = q+1$ ve $d < qb$ olduğundan $\dim_{\mathbb{F}_q}(V_2) = d_0$ olduğunu görüyoruz. Bu durumda $k = d_0$ olur. Böylece, $s_1 = 0$, $s_2 = qd_0$ ve $s_3 = 0$ olur. Sonuç olarak $(d_0 + 1)(q + 1)$ elde ederiz.

$d_0 = q$ ve $0 < r_0 < b$ olduğunu varsayalım. Bu durumda $\dim_{\mathbb{F}_q}(V_1) = q+1$ ve $\dim_{\mathbb{F}_q}(V_2) = q-1$ olduğunu görüyoruz. Bu durumda $d_0 - 1 = k$ olur, bu nedenle $s_1 = q - r_0$, $s_2 = q^2 - 2q$ ve $s_3 = r_0$ olur. Bu nedenle, $q + 1 + q - 1 + q - r_0 + q^2 - 2q + r_0 = q(q + 1)$ elde ederiz.

$d_0 = q$ ve $r_0 = 0$ olduğunu varsayalım. Bu durumda $\dim_{\mathbb{F}_q}(V_1) = q + 1$ ve $\dim_{\mathbb{F}_q}(V_2) = q$ olur. $d_0 = q$ ve $r_0 = 0$ olduğunda $s_1 = q - r_0 = q$ elde ederiz. Ve $s_2 = q^2 - 2q$ olur. Ayrıca, $d_0 - 1 = k$ ve $r_0 = 0$ olduğunda $s_3 = r_0 = 0$ olur. Böylece $q(q + 1) + 1$ elde ederiz.

Durum II: $q > b$ olduğunu varsayalım.

Öncelikle $0 \leq d \leq b - 1$ olduğunu varsayalım. Bu durumda $d_0 = 0$ olur. Dolayısıyla, $\dim_{\mathbb{F}_q}(V_2) = \dim_{\mathbb{F}_q}(V_3) = 0$ elde edilir ve ayrıca $d < q$ olduğundan $\dim_{\mathbb{F}_q}(V_1) = d+1$ olur.

d değerinin $b \leq d \leq q$ arasında olduğunu varsayalım. $d < q$ olduğundan $\dim_{\mathbb{F}_q}(V_1) = d + 1$ ve $d < qb$ olduğundan $\dim_{\mathbb{F}_q}(V_2) = d_0$ olduğunu elde ederiz. Ayrıca, $s_1 = 0 = s_2$ olur. Buna ek olarak $k = 0$ olduğundan $s_3 = dd_0 - \frac{b}{2}(d_0^2 + d_0)$ olur. Sonuç olarak, $(d_0 + 1)(d + 1 - \frac{bd_0}{2})$ elde ederiz.

d değerinin $q+1 \leq d \leq qb$ aralığında olduğunu varsayalım. $d > q$ olduğundan $\dim_{\mathbb{F}_q}(V_1) = q+1$ ve $\dim_{\mathbb{F}_q}(V_2) = 0$ olduğu açıktır. Ayrıca $d_0 \leq q$ olduğu da açıktır. Dolayısıyla $s_1 = 0$ olur. $\eta_1 = 0$ olduğundan $s_2 = kq$ elde ederiz. Ayrıca $s_3 = d(d_0-k) - \frac{b}{2}((d_0-k)(d_0+k+1))$ olur. Böylece, istenilen sonucu elde ederiz.

$d > qb$ ve $k < q$ olduğunu varsayalım. $d > qb$ olduğundan $d_0 > q$ olur. Dolayısıyla $\eta_1 \geq 0$. $d \geq q$ olduğundan $\dim_{\mathbb{F}_q}(V_1) = q+1$ ve ayrıca $d > qb$ olduğundan b, d'yi bölerse $\dim_{\mathbb{F}_q}(V_2) = q$ veya eğer bölmezse $\dim_{\mathbb{F}_q}(V_2) = q-1$ olur. $s_1 \geq 0$, $s_2 \geq 0$ ve ayrıca $s_3 \geq 0$ olduğu açıktır. Sonuç olarak, $\dim_{\mathbb{F}_q}(V_3) = s_1+s_2+s_3 = (q-1)(d-\frac{qb}{2})+k(q-d)+\frac{kb}{2}(k+1)$ durumunu elde ederiz. Bu formülü düzenlediğimizde boyut için verdiğimiz formülü elde ederiz, gerçekten, eğer b, d'yi bölüyorsa $(k+q)(k-q+1)\frac{b}{2}+q(d+k+1)-bd_0-r_0+q-kd+1$ olur. Tersine, eğer b, d'yi bölmüyorsa $(k+q)(k-q+1)\frac{b}{2}+q(d+k+1)-bd_0-r_0+q-kd$ olduğunu elde ederiz. κ ifadesini aşağıdaki biçimde tanımlayalım:

$$\kappa = \begin{cases} q+1-r_0 & \text{eğer } b \mid d, \\ q-r_0 & \text{eğer } b \nmid d. \end{cases} \tag{22}$$

Eğer b, d'yi bölerse $r_0 = 0$ elde ederiz veya tersine bölmezse $0 < r_0 < b$ olduğunu elde ederiz. Sonuç olarak, istediğimiz iddiayı bu durumlarda da elde ederiz.

Son olarak, $d > qb$ ve $k \geq q$ olduğunu varsayalım. Bu durumda $d_0 = k$. Benzer şekilde, $d \geq q$ olduğundan $\dim_{\mathbb{F}_q}(V_1) = q+1$ ve ayrıca $d > qb$ olduğundan, b değeri d'yi bölerse $\dim_{\mathbb{F}_q}(V_2) = q$ veya bölemezse $\dim_{\mathbb{F}_q}(V_2) = q-1$ olur. $d_0 \geq q$ olduğu açıktır ve dolayısıyla $s_1 = q-r_0$. Ayrıca $s_2 = q^2-2q$ ve $d_0 = k+1$ olduğundan $s_3 = r_0$ elde ederiz. Toplamda eğer b, d'yi bölerse, $q^2-2q+2q+r_0+q-r_0+1$ elde ederiz. Aksi takdirde $q^2-2q+2q+r_0+q-r_0$ elde ederiz. κ'yı, (22) eşitliğindeki gibi tanımlarsak $q^2+r_0+\kappa$ elde ederiz. □

3.2.4 Düzenlilik Kümesi ve Yarı(Quasi) Polinomlar

Sonuç 3.2.13. *$Y = \mathbb{P}(1,1,b)(\mathbb{F}_q)$'nin düzenlilik kümesini (regularity set) aşağıdaki gibi elde ederiz.*

$$reg(Y) = \{d \in \mathbb{N} : d_0 \geq q + \lfloor (q-1)/b \rfloor \text{ olmak üzere } \} = (q + \lfloor (q-1)/b \rfloor)b + \mathbb{N}b$$

Kanıt. $d = d_0 b + r_0$ ile $0 \leq r_0 < b$ olduğu durumu ele alalım.

Durum A: İlk olarak $q \leq b$ olduğunu varsayalım. Bu durumda, $\lfloor (q-1)/b \rfloor = 0$ olduğundan, aşağıdaki eşitliği göstermek yeterlidir:

$$\mathrm{reg}(Y) = \{d \in \mathbb{N} : d = d_0 b \text{ ile } d_0 \geq q\} = qb + \mathbb{N}b.$$

Durum A.I: $0 \leq d_0 \leq q-1$ ve $0 \leq r_0 \leq q-1$ olduğunu varsayalım. (3.2.9) ile verilen sonucu dikkate aldığımızda, Hilbert fonksiyonunun değerini $H_Y(d) = d_0(q+1) + r_0 + 1$ olarak elde ederiz. Dolayısıyla,

$$H_Y(d) \leq (q-1)(q+1) + q = q^2 - 1 + q < q^2 + q + 1.$$

Bu nedenle, $0 \leq d_0 \leq q-1$ ve $0 \leq r_0 \leq q-1$ için $d \notin \mathrm{reg}(Y)$ olur.

Durum A.II: $0 \leq d_0$ ve $q \leq r_0 < b$ olduğunu varsayalım. Benzer şekilde, (3.2.9) ile verilen sonucu dikkate aldığımızda, $H_Y(d) = (d_0+1)(q+1) \leq q(q+1)$ elde ederiz. Bu durumda, $H_Y(d) < q^2 + q + 1$ olduğu açıktır. Dolayısıyla, $d \notin \mathrm{reg}(Y)$ olur.

Durum A.III: $d_0 \geq q$ ve $0 < r_0 < b$ olduğunu varsayalım. (3.2.9) ile verilen sonuçtan $H_Y(d) = q(q+1)$ elde ederiz. Bu durumda, $H_Y(d) < q^2 + q + 1$ olduğu açıktır. Dolayısıyla, $d_0 \geq q$ ve $0 < r_0 < b$ için de $d \notin \mathrm{reg}(Y)$ olur.

Durum A.IV: $d_0 \geq q$ ve $r_0 = 0$ olduğunu varsayalım. Benzer şekilde, $H_Y(d) = q^2 + q + 1$ olduğunu biliyoruz. Dolayısıyla, bu durumda $d = d_0 b \in \mathrm{reg}(Y)$ olur.

Yukarıdaki durumların sadece biri mümkün olduğundan, şu sonucu elde ederiz:

$$\mathrm{reg}(Y) = \{d \in \mathbb{N} \mid d = d_0 b \text{ ile } d_0 \geq q\} = qb + \mathbb{N}b.$$

Durum B: $q > b$ olduğunu varsayalım.

Durum B.I: $0 \leq d \leq b-1$ olduğunu varsayalım. (3.2.10) ile verilen sonucu dikkate aldığımızda, $H_Y(d) = d + 1$ elde ederiz. Bu durumda, $H_Y(d) < q^2 + q + 1$ olduğu açıktır. Dolayısıyla, $0 \leq d \leq b-1$ için $d \notin \mathrm{reg}(Y)$ olur.

Durum B.II: $b \leq d \leq q$ olduğunu varsayalım. $d_0 \geq 1$ olduğundan (aksi takdirde $d = d_0 b + r_0 = r_0 < b$ çelişkisi ortaya çıkar), aşağıdaki eşitsizliği elde ederiz:

$$H_Y(d) = (d_0+1)(d+1) - b\left(\frac{d_0(d_0+1)}{2}\right) < (d_0+1)(d+1) \leq q(q+1).$$

Bu nedenle, $H_Y(d) < q^2+q+1$ elde ederiz. Dolayısıyla, $b \leq d \leq q$ için $d \notin \mathrm{reg}(Y)$ olur.

Durum B.III: $q+1 \leq d \leq qb$ olduğunu varsayalım. Aşağıdaki toplamı dikkate alalım:

$$H_Y(d) = (k+1)(q+1) + (d_0-k)(d+1) - b\sum_{i=k+1}^{d_0} i.$$

Bu toplamı düzenleyip sadeleştirirsek, aşağıdaki sonucu elde ederiz:

$$H_Y(d) = q+1+\frac{bd_0^2}{2}+\frac{bd_0}{2}+d_0-\frac{k^2b}{2}-kr+\frac{kb}{2}.$$

Bilindiği gibi, $q+1 \leq d = d_0 b + r_0$ olduğundan, $q \leq d_0 b + r_0 - 1$ elde ederiz. Ayrıca,

$$d_0 \leq q \leq d_0 b + r_0 - 1 \Rightarrow d_0 \leq \frac{r_0-1}{1-b}.$$

Bu eşitsizlikleri kullanarak, aşağıdaki sonuçları elde ederiz:

$$\begin{aligned} H_Y(d) &< \frac{q}{2}+1+d_0+\frac{b}{2}(d_0(d_0+1))+\frac{b}{2}(q-\frac{q+r}{b}+1)-r \\ &= \frac{bd_0+r_0}{2}+\frac{1}{2}+\frac{r_0-1}{1-b}+\frac{bd_0}{2}(d_0+1)+\frac{qb}{2}+\frac{b}{2}-\frac{3r}{2}. \end{aligned}$$

Bu eşitsizlikler ile,

$$H_Y(d) \leq qb+b-\frac{(3r+1)}{2} < q^2+q < q^2+q+1.$$

durumu elde edildiğinden, bir başka deyişle $H_Y(d) < q^2+q+1$ olduğundan dolayı, $q+1 \leq d \leq qb$ için $d \notin \mathrm{reg}(Y)$ olur.

Durum B.IV: $d > qb$ ve $k < q$ olduğunu varsayalım. Şu toplamı dikkate alalım:

$$H_Y(d) = \frac{b}{2}(k+q)(k-q+1) + q(k+d+1) - dk - bd_0 + \kappa.$$

Bu formül, $d = q+kb+r$ formülündeki k değerine bağlıdır. $k = q-1$ olduğunda, şu sonucu elde ederiz:

$$H_Y(d) = q^2 + d - bd_0 + \kappa = q^2 + r_0 + \kappa.$$

- Eğer $0 < r_0 < q$ ise, $\kappa = q - r_0$ olur ve $H_Y(d) = q^2 + q < q^2 + q + 1$ olduğunu elde ederiz. Dolayısıyla, $d > qb$, $k = q-1$ ve $0 < r_0 < q$ için $d \notin \operatorname{reg}(Y)$ olur.
- Eğer $r_0 = 0$ ise, $\kappa = q+1$ olur ve $H_Y(d) = q^2+q+1$ elde ederiz. Dolayısıyla, $d > qb$, $k = q-1$ ve $r_0 = 0$ için $d \in \operatorname{reg}(Y)$ olur.

Benzer şekilde, $k < q-1$ olduğunda, $H_Y(q+kb+r) < H_Y(q+(q-1)b+r)$ olduğundan, $k < q-1$ ise $d \notin \operatorname{reg}(Y)$ olduğu sonucu çıkar.

Durum B.V: $d > qb$ ve $k \geq q$ olduğunu varsayalım. Bu durumda, şu eşitsizlikleri elde ederiz:

$$\begin{aligned} H_Y(d) &= \frac{b}{2}q(q+1) + q^2 - bd_0 + \kappa - k(d+1) + \frac{q(d+1)}{b} \\ &< \frac{q^2+q+b}{2} - bd_0 + \kappa - \kappa d_0 + \frac{q(d+1)}{b} \\ &= \frac{q^2+q+b}{2} - bd_0 + qd_0 + 1 + qd + 1 < q^2 + q < q^2 + q + 1. \end{aligned}$$

Bu nedenle, $d > qb$, $k \geq q$ olduğunda $H_Y(d) < q^2+q+1$ olur. Dolayısıyla, $d \notin \operatorname{reg}(Y)$ olur. Özetle, yukarıdaki tüm durumları göz önünde bulundurduğumuzda, şu sonucu elde ederiz:

$$\operatorname{reg}(Y) = \{d \in \mathbb{N} : d = qb + \mathbb{N}b\}.$$

□

Aşağıda verilen tablolarda kırmızı renk ile gösterilen d değerleri düzenlilik indeksini belirtmektedir. Bir başka deyişle, Hilbert fonksiyonunun maksimum değere ulaştığı ilk dereceye karşılık gelen (düzenlilik kümesinin ilk elemanı olan) d değeri kırmızı renk

ile gösterilmiştir. Ayrıca Hilbert fonksiyonunun değerleri hesaplanırken Macaulay2 [44] programı kullanılmıştır.

Tablo 3.1 $Y = \mathbb{P}(1,1,2)(\mathbb{F}_5)$ için Hilbert Fonksiyonunun Değerleri

d	0	1	2	3	4	5	6	7	8	9	10	11	12
$H_Y(d)$	1	2	4	6	9	12	15	18	21	24	27	28	30
d	13	14	15	16	17	18	19	20	21	22	23	24	25
$H_Y(d)$	30	31	30	31	30	31	30	31	30	31	30	31	30

Tablo 3.2 Sırasıyla $b = 5, 7$ olmak üzere $Y = \mathbb{P}(1,1,b)(\mathbb{F}_5)$ için Hilbert Fonksiyonunun Değerleri

d	0	1	2	3	4	5	6	7	8	9	10	11	12
$H_Y(d)$	1	2	3	4	5	7	8	9	10	11	13	14	15
d	13	14	15	16	17	18	19	20	21	22	23	24	25
$H_Y(d)$	16	17	19	20	21	22	23	25	26	27	28	29	31
d	26	27	28	29	30	31	32	33	34	35	36	37	38
$H_Y(d)$	30	30	30	30	31	30	30	30	30	31	30	30	30

d	0	1	2	3	4	5	6	7	8	9	10	11	12
$H_Y(d)$	1	2	3	4	5	6	6	7	8	9	10	11	12
d	13	14	15	16	17	18	19	20	21	22	23	24	25
$H_Y(d)$	12	13	14	15	16	17	18	18	19	20	21	22	23
d	26	27	28	29	30	31	32	33	34	35	36	37	38
$H_Y(d)$	24	24	25	26	27	28	29	30	30	31	30	30	30
d	39	40	41	42	43	44	45	46	47	48	49	50	51
$H_Y(d)$	30	30	30	31	30	30	30	30	30	30	31	30	30

Teorem 3.2.14. *[40, Theorem 4.3.5] R, pozitif dereceli bir $\mathbb{K}$-cebiri ve $M \neq 0$ sonlu üretilmiş dereceli bir R-modül olmak üzere,*

(i) Her $d \gg 0$ için $H_M(d) = P_M(d)$ durumunu sağlayan tek bir şekilde tanımlı P_M yarı polinomu vardır.

(ii) $\operatorname{der}(HS_M(t)) = \max\{d : H_M(d) \neq P_M(d)\}$

Burada $\operatorname{der}(HS_M(t))$, $HS_M(t)$ *rasyonel fonksiyonunun derecesi olarak tanımlıdır ve ayrıca M'nin a-değişmezi (a-invariant) olarak bilinir. Ayrıca, $a(M)$ ile gösterilir.*

Uyarı 3.2.15. Serre'nin bu Teoremi 3.2.14 Y'nin Hilbert fonksiyonunun her $d > a(Y)$ için **Hilbert yarı-polinomu** P_Y olduğunu kanıtlar, bir başka deyişle, periyot olarak adlandırılan

bir g pozitif tam sayısı ve $P_0, \ldots, P_{g-1}$ polinomları vardır öyle ki $d > a(Y)$ ve $d \equiv i \mod g$ için $H_Y(d) = P_i(d)$ koşulunun sağlandığını söyler.

Buradan, Y'nin yarı-polinomu ile ilgili olarak aşağıdaki sonucu elde ederiz.

Sonuç 3.2.16. *$Y = \mathbb{P}(1,1,b)(\mathbb{F}_q)$ olmak üzere, Y'nin Hilbert yarı-polinomu aşağıdaki şekilde elde edilir.*

$$P_Y(d_0 b + r_0) = \begin{cases} q(q+1)+1 & \text{eğer } d_0 \in \mathbb{Z} \text{ ve } r_0 = 0 \\ q(q+1) & \text{eğer } d_0 \in \mathbb{Z} \text{ ve } 1 \leq r_0 \leq b-1. \end{cases}$$

Kanıt. Burada,

$$d \geq a(Y) + 1 = (q-1)(b+1) + 1 = (q-1)b + q = qb + q - b$$

olduğu tüm d dereceleri için $H_Y(d) = P_Y(d)$ olduğunu kanıtlamamız gerekiyor. Sonuç 3.2.13'in kanıtı, $d \leq a(Y)$ için $H_Y(d) < q(q+1)$ olduğunu ve ancak ve ancak $d = (q-1)b + r_0$ ile $q \leq r_0 < b$ olduğunda veya $d = d_0 b + r_0$ ile $d_0 \geq q$ ve $0 < r_0 < b$ olduğunda $H_Y(d) = q(q+1)$ olduğunu ortaya koyar; bu durum, $q \leq b$ olduğu yani **Durum A** için geçerlidir. Son olarak, eğer $d = d_0 b$ ile $d_0 \geq q$ ise, $H_Y(d) = q(q+1)+1$ olur ve bu, **Durum A** için iddiayı kanıtlar. $q > b$ olduğu yani **Durum B** için, $d \geq a(Y) + 1 = qb + q - b > qb$ elde ederiz. Bu nedenle, $d > qb$ ve $0 < r_0 < q$ olduğunda Sonuç 3.2.13'in kanıtı gösterir ki, $H_Y(d) = q^2 + q$ olur. Benzer şekilde, eğer $d_0 > q$ ise, $H_Y(d_0 b) = q(q+1) + 1$ olur. Dolayısıyla, bu durumda da $H_Y(d) = P_Y(d)$ elde ederiz, bu da istenen durumu sağlar. □

Yukarıda verilen Sonuç 3.2.16 ile birlikte şunu söyleyebilirz ki; $a(Y)$ ile gösterilen a-değişmezi olmak üzere eğer $d \geq a(Y) + 1$ ise Hilbert fonksiyonu ya $q(q+1)$ değerini ya da $q(q+1)+1$ değerini alacaktır. Örneğin, $q = 5$ değeri için bu değerler $30, 31$ olmak üzere düzenlilik kümesinin ilk elemanı olan d derecesinden sonraki her b birimde de Hilbert fonksiyonunun maksimum değeri olan 31 değerini aldığı görülür. (Örnek için bknz. Tablo 3.1 ve Tablo 3.2)

Bir sonraki bölümde ise diğer bir temel parametre olan minimum uzaklık ile ilgili elde edilenler verilecektir.

3.2.5 Minimum Uzaklık

$$Y = \{[1 : y_2 : y_3] : y_2, y_3 \in \mathbb{F}_q\} \cup \{[0 : y_2 : 1] : y_2 \in \mathbb{F}_q\} \cup \{[0 : 1 : 0]\}$$

Yukarıda verilen Y kümesi,$X = \mathbb{P}(1, 1, b)$ ağırlıklı projektif uzayının $\overline{\mathbb{F}}_q$ cebirsel kapalı cismi üzerinde, $\mathbb{F}_q$-rasyonel noktalarının kümesi olmak üzere aşağıdaki teorem ile $C_{d,Y}$ kodunun minimum uzaklığı verilir.

Teorem 3.2.17. *$C_{d,Y}$ kodunun minimum uzaklığı aşağıdaki şekilde verilir.*

$$\delta = \begin{cases} q(q-d+1) & \textit{eğer } 1 \le d < q \\ q-k & \textit{eğer } d = q + kb + r < qb \textit{ ile } 0 \le r < b \textit{ ve } 0 \le k \le q-2, \\ 1 & \textit{eğer } d = q + kb + r \textit{ ile } 0 \le r < b \textit{ ve } k \ge q-1 \end{cases}$$

Kanıt. **Durum I:** $1 \le d < q$ olsun. $d = d_0 b + r_0$ şeklinde yazalım. Burada $0 \le d_0 \le d$ ve $0 \le r_0 < b$. Sıfır olmayan bir $F \in S_d$ polinomu için, $J = \{y_3 \in \mathbb{F}_q : \mathrm{F}, y_3 x_1^b - x_3$ tarafından bölünür.$\}$ şeklinde bir küme tanımlayalım. Açıkça görülür ki eğer $y_3 \in J$ ise $|J| \le d_0$ ve $F(1, y_2, y_3) = 0$ ve $y_1 = 1$ olduğunda Y üzerinde $q|J|$ tane bu formda nokta vardır.

Diğer yandan, eğer $y_3 \notin J$ ise $f(x_2) = F(1, x_2, y_3) \in \mathbb{F}_q[x_2]\backslash\{0\}$ olur. Bu durumda, $y_3 \notin J$ olduğunda f en fazla $\mathrm{der}_{x_2}(F) = \mathrm{der}(f)$ köke sahip olabilir. Dolayısıyla F en fazla $|\mathbb{F}_q\backslash J| \,\mathrm{der}_{x_2}(F) = (q - |J|)\,\mathrm{der}_{x_2}(F)$ kadar köke sahiptir. Bu yüzden aşağıdaki eşitsizlik elde edilir:

$$|V_Y(F) \cap U_1| \le q|J| + (q - |J|)\,\mathrm{der}_{x_2}(F), \tag{23}$$

burada $V_Y(F) = \{P \in Y : F(P) = 0\}$ ve $U_1 = \{[x_1 : x_2 : x_3] \in Y : x_1 = 1\}$.

F'nin $x_1 = 0$ olduğunda kök sayısını elde etmeye çalışalım.

$$F(x_1, x_2, x_3) = x_1^{\ell} \prod_{y_3 \in J} (y_3 x_1^b - x_3) F'(x_1, x_2, x_3) \text{ burada } F' = x_1 F_1 + F_2,$$

ve $F_2(x_2, x_3)$, $x_1 \nmid F_2$ koşulunu olan $d - \ell - |J|b$ dereceli homojen bir polinomdur.

Eğer $\ell > 0$ ise, $x_1 = 0$ iken F'nin $q+1$ kökü vardır. Bu nedenle, (23) ile aşağıdaki durumu elde ederiz:

$$\begin{aligned} |V_Y(F)| &\leq q+1+q|J|+(q-|J|)(d-\ell-|J|b). \\ &= q+1+q(d-\ell)+|J|(q-qb-d+\ell+|J|b) \\ &\leq q+1+q(d-\ell) \leq qd+1, \end{aligned}$$

Burada $q-qb-d+\ell+|J|b \leq 0$ olduğu açıktır.

Varsayalım ki $\ell = 0$ olsun. Eğer $F(0,y_2,1) = 0$ ise $F'(0,y_2,1) = 0$ olur, yani $F' \in I([0:y_2:1])$ olur. [43, Proposition 3.4]'ye göre,

$$x_1F_1 + F_2 = F' \in I([0:y_2:1]) = \langle x_1, x_2^b - y_2^b x_3 \rangle$$

ve dolayısıyla $y_2 \neq 0$ iken $x_2^b - y_2^b x_3$, F_2'nin bir çarpanıdır. Ayrıca, F_2 en fazla $d_0 - |J|$ tane bu formda çarpana sahip olabilir, çünkü d'nin içerisinde $d_0 b$ vardır ve dolayısıyla d'de b'li kısımdan d_0 tane vardır ve $\mathrm{der}_{x_2}(F_2) = d-|J|b$'dir. Bu nedenle, $[0:y_2:1]$ formunda en fazla $d_0 - |J|$ kök vardır. Bu durumda,

$$F(x_1,x_2,x_3) = \prod_{y_3 \in J}(y_3x_1^b - x_3)[x_1F_1 + x_2^{r_0}\prod_{y_2=1}^{d_0-|J|}(x_2^b - y_2^b x_3)].$$

Ama $I([0:0:1]) = \langle x_1, x_2 \rangle$ ve $r_0 > 0$ olduğunda, $F'(0,0,1) = 0$ olur. $J \neq \emptyset$ olduğunda, $y_3x_1^b - x_3$ F'nin bir çarpanı olduğu için $[0:1:0]$ noktası da bir köktür. Toplamda, $x_1 = 0$ olduğunda en fazla $2 + d_0 - |J|$ kök vardır. Dolayısıyla, (23) ile şunu elde ederiz:

$$\begin{aligned} |V_Y(F)| &\leq 1+d_0+qd+|J|(q-qb-d+|J|b) \\ &\leq 1+qd+|J|(d_0+q-qb-d+|J|b) \leq qd+1, \end{aligned}$$

çünkü $b > 1$ olduğu için $d_0 + q \leq qb$ olur ve bu nedenle $d_0+q-qb-d+|J|b \leq 0$ elde ederiz.

$J = \emptyset$ olsun. $\mathrm{der}_{x_2}(F) \leq d$ olduğundan, (23) ile F, $[1:y_2:y_3]$ formunda en fazla qd köke sahip olabilir. Şimdi $x_1 = 0$ olduğunda kök sayısını sayalım. Eğer $\mathrm{der}_{x_2}(F) = d$ ise, x_2^d F'de bulunur, bu yüzden $F \notin I(0,1,0) = \langle x_1, x_3 \rangle$ olur. Bu durumda $F(0,1,0) \neq 0$. Eğer F, $[1{:}y_2{:}y_3]$ formunda qd köke sahipse, herhangi bir $y_2 \in \mathbb{F}_q^*$ için $I(0,y_2,1) = \langle x_1, y_2^b x_3 - x_2^b \rangle$

idealinde olamaz. Dolayısıyla, $x_1 = 0$ olduğunda F'nin tek kökü $[0:0:1]$ olabilir. Toplamda F en fazla $qd+1$ köke sahip olabilir. Eğer $\mathrm{der}_{x_2}(F) \leq d-1$ ise, (23) eşitsizliğinden F, $x_1 = 1$ iken en fazla $q(d-1)$ köke sahip olabilir. Ve F, $x_1 = 0$ iken en fazla $q+1$ köke sahip olabilir, dolayısıyla

$$|V_Y(F)| \leq q(d-1) + q + 1 = qd + 1.$$

Bu nedenle, her durumda $\ell = 0$ için $|V_Y(F)| \leq qd+1$ eşitsizliğini elde ederiz.

$$F_0(x_1, x_2, x_3) = \prod_{y_2=1}^{d} (x_2 - y_2 x_1) \in S_d$$

polinomu tam olarak $qd+1$ köke sahiptir, bu nedenle son olarak iddiamızdaki eşitliği elde ederiz:

$$\delta = N - (qd+1) = q^2 + q + 1 - qd - 1 = q(q-d+1).$$

Durum II: $q \leq d < qb$ olsun. $0 \leq r < b$ olacak şekilde $d = q + kb + r$ olarak alalım. S_d'de sıfır olmayan bir F polinomu, aşağıdaki formdadır:

$$F = x_1^{\ell} \prod_{y_3 \in J} (y_3 x_1^b - x_3) F'(x_1, x_2, x_3) \tag{24}$$

Bu ifade, Durum I'deki gibi bir alt küme olan $J \subseteq \mathbb{F}_q$ ve derecesi $\mu = d - \ell - |J|b$ olan homojen bir polinom F' için geçerlidir.

$0 \leq |J| \leq k$ olduğunu varsayalım. $f_3 = x_1^q x_2 - x_1 x_2^q \in I(Y)$ ve $|V_Y(F)| = |V_Y(\bar{F})|$ olduğu zaman $F - \bar{F} \in I(Y)$ olduğunu kullanarak, $x_1 x_2^q$ yerine $x_1^q x_2$'yi F'ye koyabiliriz ve F'nin $x_1 x_2^q$ ile bölünebilir terimi olmadığını varsayabiliriz.

Eğer $\ell > 0$ ise, x_1, F'yi böler ve böylece $\mathrm{der}_{x_2}(F) < q$ olur ve bu, her $y_3 \in \mathbb{F}_q \setminus J$ için tek değişkenli polinom $f(x_2) : = F(1, x_2, y_3) \in \mathbb{F}_q[x_2] \setminus \{0\}$'ın en fazla $q-1$ köke sahip olmasına yol açar. Bu nedenle, $0 \leq |J| \leq k$ olduğu için, aşağıdaki eşitsizliği elde ederiz:

$$\begin{aligned} |V_Y(F)| &\leq q + 1 + q|J| + (q - |J|)(q-1) \\ &\leq q + 1 + q|J| + q^2 - q - q|J| + |J| \\ &\leq q^2 + k + 1. \end{aligned}$$

Eğer $\ell = 0$ ve $f(x_2)$ en fazla $q-1$ köke sahipse, aynı mantıkla $|V_Y(F)| \leq q^2 + k + 1$ olduğunu ispatlarız. Bu nedenle, $\ell = 0$ ve $f(x_2)$'nin q köke sahip olduğunu varsayalım. Bu

durumda, $x_2 - y_2$ f'yi böler, bu da $x_2 - y_2$'nin F'yi bölmesini sağlar. $d < qb$ olduğu için şu sonuca varırız:

$$F' = x_2^{d-q-|J|b} \prod_{y_2 \in \mathbb{F}_q} (x_2 - y_2 x_1).$$

Böylece, $|V_Y(F) \cap U_1| = q^2$ olur. $F(0, x_2, x_3) = (-1)^{|J|} x_3^{|J|} x_2^{d-|J|b}$ olduğundan, $F(0, 0, 1) = 0$ ve $F(0, 1, y_3) = 0$ durumları yalnızca $y_3 = 0$ ve $|J| \geq 1$ olduğunda geçerlidir. Bu nedenle, $0 \leq |J| \leq k$ olduğunda, $|V_Y(F)| \leq q^2 + k + 1$ olur.

Öte yandan, $|J| > k$ ise $|J| = k + j_0$ olacak şekilde yazabiliriz, burada $j_0 \geq 1$.

Öncelikle $\ell > 0$ durumunu ele alalım. Bu durumda, $|J| < q$ olur. Eğer $|J| = q$ ise, aşağıdaki eşitlik sağlandığında $F \in I(Y)$ olur:

$$|V_Y(F)| = q + 1 + q|J| + (q - |J|) \operatorname{der}_{x_2}(F) = q^2 + q + 1.$$

Sonuç olarak,

$$\begin{aligned} d - \ell - b|J| &= d - \ell - bk - b(j_0 - 1 + 1) \\ &= q + r - b - b(j_0 - 1) - \ell \quad (\text{çünkü } d - bk = q + r) \\ &\leq q - 1 - \ell - b(j_0 - 1) \quad (\text{çünkü } r - b \leq -1) \\ &\leq q - 2 - b(j_0 - 1) \quad (\text{çünkü } -\ell \leq -1). \end{aligned}$$

Bu nedenle,

$$\begin{aligned} |V_Y(F)| &\leq q + 1 + q|J| + (q - |J|)(d - \ell - |J|b) \\ &\leq q + 1 + q|J| + (q - |J|)(q - 2 - b(j_0 - 1)) \\ &= q + 1 + q|J| + q^2 - 2q - qbj_0 + qb - q|J| + 2|J| + bj_0|J| - b|J| \\ &= q + 1 + q^2 - 2q - qb(j_0 - 1) + 2|J| + b|J|(j_0 - 1) \\ &= q^2 + 1 - q + (j_0 - 1)b(|J| - q) + 2|J| + k - k \\ &= q^2 + k + 1 + (j_0 - 1)b(|J| - q) + |J| - k + |J| - q \\ &\leq q^2 + k + 1 + (j_0 - 1)b(-1) + j_0 - 1 \quad (\text{ burada, } |J| - q \leq -1.) \\ &\leq q^2 + k + 1 - (j_0 - 1)(b + 1) \\ &\leq q^2 + k + 1. \end{aligned}$$

Şimdi, $|J| > k$ ve $\ell = 0$ olduğunu varsayalım. $|J| = k + j_0$ ve $j_0 \geq 1$ olduğundan, $d - b|J| = d - bk - bj_0 = q + r - b - b(j_0 - 1) \leq q - 1 - b(j_0 - 1)$ olur. Bu nedenle,

$$\begin{aligned} |V_Y(F)| &\leq q + 1 + q|J| + (q - |J|)(q - 1 - b(j_0 - 1)) \\ &\leq q^2 + k + 1 - b(j_0 - 1) + j_0 \quad (\text{eğer } |J| - q \leq -1) \\ &\leq q^2 + k + 1 \quad (\text{çünkü } j_0 \geq 2 \text{ ve } b \geq 2). \end{aligned}$$

Bu nedenle, $j_0 = 1$ veya $|J| = q$ olduğunda da aynı eşitsizliği kanıtlamamız gerekiyor. İlk olarak, varsayalım ki $j_0 = 1$ olsun, bu durumda $|J| = k + 1$ olur. $y_2 \in \mathbb{F}_q^*$ için $[0 : y_2 : 1]$ formundaki köklerin sayısı $d_0 - |J| = d_0 - k - 1 < q - 1$ kadar olabilir çünkü $d_0 < k + q$'dur. $[0 : 1 : 0]$ ve $[0 : 0 : 1]$ köklerini de dahil ettiğimizde, $x_1 = 0$ için en fazla q kök vardır. Bu nedenle, aşağıdaki eşitsizlik geçerlidir:

$$\begin{aligned} |V_Y(F)| &\leq q + q(k + 1) + (q - (k + 1))(d - b(k + 1)) \\ &\leq q^2 + k + 1. \end{aligned}$$

Öte yandan, $|J| = q$ ise,

$$|V_Y(F)| \leq 2 + d_0 - |J| + q|J| + (q - |J|)(d - |J|b) \leq q^2 + k + 1 \quad (\text{ çünkü } d_0 < k + q)$$

Dolayısıyla, tüm ℓ ve tüm $|J|$ için $|V_Y(F)| \leq q^2 + k + 1$ olur. Son olarak, $0 \leq r < b$ ve $d = q + kb + r$ olduğu durumda aşağıdaki polinomu düşünelim:

$$F_0(x_1, x_2, x_3) = x_1^{r+1} \prod_{y_3=1}^{k} (y_3 x_1^b - x_3) \prod_{y_2 \in \mathbb{F}_q^*} (x_2 - y_2 x_1) \in S_d.$$

F_0, y_3'ün k değeri için ve tüm $y_2 \in \mathbb{F}_q$ için $[1 : y_2 : y_3]$ noktasında sıfır olur ve kalan $q - k$ y_3 değeri için ve tüm $y_2 \in \mathbb{F}_q^*$ için $[1 : y_2 : y_3]$ noktasında sıfır olur. Böylece $qk + (q-1)(q-k) = q^2 - q + k$ köke sahip olur. Ek olarak, $r + 1 \geq 1$ olduğundan, F_0, $[0 : y_2 : 1]$ noktasında tüm $y_2 \in \mathbb{F}_q$ için ve ek olarak $[0 : 1 : 0]$ noktasında sıfır değerini alır. Toplamda, F_0 tam olarak $q^2 + k + 1$ köke sahiptir. Bu nedenle, son olarak istenen eşitliği elde ederiz:

$$\delta = N - (q^2 + k + 1) = q^2 + q + 1 - q^2 - k - 1 = q - k.$$

Durum III: $0 \leq r < b$ ve $k \geq q-1$ olmak üzere $d = q + kb + r$ olsun.

$$F_0 = x_1^{\ell_0} \prod_{y_3 \in \mathbb{F}_q^*} (y_3 x_1^b - x_3) \prod_{y_2 \in \mathbb{F}_q^*} (y_2 x_1 - x_2) \in S_d$$

tam olarak $q^2 + q = q + 1 + (q-1)q + (q-1)$ noktada sıfır olur, çünkü x_1'in kuvveti olan $\ell_0 := d - q - (q-1)b + 1 \geq 1$ olur, bu durum ise kod kelimesi $ev_Y(F_0)$'ın ağırlığının 1 olduğu anlamına gelir. □

3.2.6 Kodların Parametreleri için Örnekler

Aşağıdaki tablolarda örnek olması açısından kodların parametreleri verilmiştir. Bu tablolarda sırasıyla $q = 2, 5$ ve $b = 2, 5, 7$ değerleri için parametreler hesaplanmıştır. Bu parametreler hesaplanırken hızlı olması açısından SageMath [45] programı kullanılmıştır. Burada mavi renk ile gösterilen d derecelerinde (her b birimde) kodun boyutunun maksimum değere ulaştığı görülür. Benzer şekilde, kırmızı ile gösterilen d dereceleri ise düzenlilik indeksini göstermektedir. Yani, kodun boyutunun maksimum değere ulaştığı ilk d derecesini belirtmektedir.

Tablo 3.3 Sırasıyla $b = 2, 5, 7$ olmak üzere $Y = \mathbb{P}(1,1,b)(\mathbb{F}_2)$ üzerindeki kodların temel parametreleri

b	**Derece**	**N**	**K**	δ	b	**Derece**	**N**	**K**	δ	b	**Derece**	**N**	**K**	δ
$b=2$	$d=2$	7	4	2	$b=5$	$d=2$	7	3	2	$b=7$	$d=2$	7	3	2
	$d=3$	7	5	2		$d=3$	7	3	2		$d=3$	7	3	2
	$d=4$	7	7	1		$d=4$	7	3	2		$d=4$	7	3	2
	$d=5$	7	6	1		$d=5$	7	4	2		$d=5$	7	3	2
	$d=6$	7	7	1		$d=6$	7	5	1		$d=6$	7	3	2
	$d=7$	7	6	1		$d=7$	7	6	1		$d=7$	7	4	1
	$d=8$	7	7	1		$d=8$	7	6	1		$d=8$	7	5	1
	$d=9$	7	6	1		$d=9$	7	6	1		$d=9$	7	6	1
	$d=10$	7	7	1		$d=10$	7	7	1		$d=10$	7	6	1
	$d=11$	7	6	1		$d=11$	7	6	1		$d=11$	7	6	1
	$d=12$	7	7	1		$d=12$	7	6	1		$d=12$	7	6	1
	$d=13$	7	6	1		$d=13$	7	6	1		$d=13$	7	6	1
	$d=14$	7	7	1		$d=14$	7	6	1		$d=14$	7	7	1
	$d=15$	7	6	1		$d=15$	7	7	1		$d=15$	7	6	1

Tablo 3.4 Sırasıyla $b = 2, 5, 7$ olmak üzere $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_5)$ üzerindeki kodların temel parametreleri

b	**Derece**	**N**	**K**	δ	b	**Derece**	**N**	**K**	δ	b	**Derece**	**N**	**K**	δ
$b = 2$	$d = 2$	31	4	20	$b = 5$	$d = 2$	31	3	20	$b = 7$	$d = 2$	31	3	20
	$d = 3$	31	6	15		$d = 3$	31	4	15		$d = 3$	31	4	15
	$d = 4$	31	9	10		$d = 4$	31	5	10		$d = 4$	31	5	10
	$d = 5$	31	12	5		$d = 5$	31	7	5		$d = 5$	31	6	5
	$d = 6$	31	15	5		$d = 6$	31	8	5		$d = 6$	31	6	5
	$d = 7$	31	18	4		$d = 7$	31	9	5		$d = 7$	31	7	5
	$d = 8$	31	21	4		$d = 8$	31	10	5		$d = 8$	31	8	5
	$d = 9$	31	24	3		$d = 9$	31	11	5		$d = 9$	31	9	5
	$d = 10$	31	27	3		$d = 10$	31	13	4		$d = 10$	31	10	5
	$d = 11$	31	28	2		$d = 11$	31	14	4		$d = 11$	31	11	5
	$d = 12$	31	30	2		$d = 12$	31	15	4		$d = 12$	31	12	4
	$d = 13$	31	30	1		$d = 13$	31	16	4		$d = 13$	31	12	4
	$d = 14$	31	31	1		$d = 14$	31	17	4		$d = 14$	31	13	4
	$d = 15$	31	30	1		$d = 15$	31	19	3		$d = 15$	31	14	4
	$d = 16$	31	31	1		$d = 16$	31	20	3		$d = 16$	31	15	4
	$d = 17$	31	30	1		$d = 17$	31	21	3		$d = 17$	31	16	4
	$d = 18$	31	31	1		$d = 18$	31	22	3		$d = 18$	31	17	4
	$d = 19$	31	30	1		$d = 19$	31	23	3		$d = 19$	31	18	3
	$d = 20$	31	31	1		$d = 20$	31	25	2		$d = 20$	31	18	3
	$d = 21$	31	30	1		$d = 21$	31	26	2		$d = 21$	31	19	3
	$d = 22$	31	31	1		$d = 22$	31	27	2		$d = 22$	31	20	3
	$d = 23$	31	30	1		$d = 23$	31	28	2		$d = 23$	31	21	3
	$d = 24$	31	31	1		$d = 24$	31	29	2		$d = 24$	31	22	3
	$d = 25$	31	30	1		$d = 25$	31	31	1		$d = 25$	31	23	3
	$d = 26$	31	31	1		$d = 26$	31	30	1		$d = 26$	31	24	2
	$d = 27$	31	30	1		$d = 27$	31	30	1		$d = 27$	31	24	2
	$d = 28$	31	31	1		$d = 28$	31	30	1		$d = 28$	31	25	2
	$d = 29$	31	30	1		$d = 29$	31	30	1		$d = 29$	31	26	2
	$d = 30$	31	31	1		$d = 30$	31	31	1		$d = 30$	31	27	2
	$d = 31$	31	30	1		$d = 31$	31	30	1		$d = 31$	31	28	2
	$d = 32$	31	31	1		$d = 32$	31	30	1		$d = 32$	31	29	2
	$d = 33$	31	30	1		$d = 33$	31	30	1		$d = 33$	31	30	1
	$d = 34$	31	31	1		$d = 34$	31	30	1		$d = 34$	31	30	1
	$d = 35$	31	30	1		$d = 35$	31	31	1		$d = 35$	31	31	1

KISIM II

4. AĞIRLIKLI PROJEKTİF UZAYLARDAKİ KODLARA GEOMETRİK BAKIŞ

İlk olarak, bu bölümdeki çalışmalarda kullanılan bazı tanım, teorem ve kavramları vererek (daha önce kullandığımız ve tanıttığımız kavramları, teoremleri vb. hatırlatarak) başlayacağız.

$X = \mathbb{P}(1, a, b)$, ağırlık projektif düzlemi bir basit simitli çeşitlemdir. Burada, ağırlıklı projektif uzayın da tanımını göz önünde bulundurduğumuzda bu simitli çeşitlem $\mathrm{der}(x_0) = 1$, $\mathrm{der}(x_1) = a$ ve $\mathrm{der}(x_2) = b$ derecelendirmeleri ile birlikte $S = \mathbb{F}_q[x_0, x_1, x_2]$ dereceli polinom halkası ile ilişkilidir. $d \in \mathbb{N}$ bir derece olmak üzere, bu d derecesinin tanımladığı bir çokgen aşağıdaki şekilde verilir,

$$P_d = \{(x, y) \in \mathbb{R}^2 : x \geq 0, y \geq 0, ax + by \leq d\} \tag{25}$$

ayrıca, bu P_d çokgeninin integral noktaları bize derecesi d olan monomları verecektir, bir başka deyişle aşağıdaki küme ile çokgenin integral noktaları ve d dereceli monomlar arasındaki ilişkiyi verebiliriz.

$$\mathbb{M}_d = \left\{ \mathbf{x}^{\mathbf{a},d} = x_0^{d-aa_1-ba_2} x_1^{a_1} x_2^{a_2} : \mathbf{a} = (a_1, a_2) \in P_d \cap \mathbb{Z}^2 \right\}. \tag{26}$$

Buradan S polinom halkasını $S_d = \mathrm{Span}\, \mathbb{M}_d$ olmak üzere, $S = \bigoplus_{d \geq 0} S_d$ şeklinde yazabiliriz. Daha öncede belirttiğimiz üzere tekrar hatırlatmak gerekirse bir lineer kod elde etmek için derecesi $d \geq 1$ olan homojen polinomların $Y = \{P_1, \ldots, P_n\} \subseteq \mathbb{P}(1, a, b)(\mathbb{F}_q)$, F_q-rasyonel noktalar kümesindeki noktalarda hesaplanması ile elde edilir. Bir başka deyişle, aşağıdaki biçimde tanımlanan hesaplama dönüşümünün görüntüsü bize bir lineer kod verir.

$$\begin{array}{rccc} ev_Y & : & S_d & \to & \mathbb{F}_q^n \\ & & f & \mapsto & \big(f(P_1), \ldots, f(P_n)\big) \end{array} \tag{27}$$

Bu bölümdeki çalışmalarda, ağırlıklı projektif uzayların simitli (toric) çeşitlem olduğu gerçeğinden yararlanılmıştır ve [22] makalesinde verilen yöntemler referans alınarak, $Y =$

$\mathbb{P}(1, a, b)$ kümesi ile ilişkili $C_{d,Y}$ kodunun temel parametreleri elde edilmiştir. Bu makaledeki yöntemler, yukarıda tanımını verdiğimiz (bknz. (25)) P_d çokgeninin ve $C_{d,Y}$ kodunun temel parametreleri arasındaki kombinatoriği birbirine bağlar. Dolayısıyla ilk bölümdeki cebirsel yöntemlerin yanısıra bu çalışmada geometrik yöntemler göz önünde bulundurularak da kodun parametreleri için sonuçlar elde edileceğini söyleyebiliriz.

Bir hesaplama kodu olan $C_{d,Y}$ kodu, S_d'nin Y'nin sıfırlayan idealinin d dereceli kısmı olan I_d tarafından bölünmesiyle elde edilen bölüme izomorfur. Bir başka deyişle, $I(Y)$, Y'nin her noktasında sıfırlanan, S halkası üzerindeki homojen polinomlar tarafından üretilen homojen bir ideal olmak üzere, bu sıfırlayan ideal ile ilişkili kodların boyutu ile idealin Hilbert serisi arasında cebirsel bir ilişki olduğu bir önceki bölümde anlatılmıştır.

Yukarıda tanımladığımız hesaplama dönüşümünün (bknz. (27) ile verilen dönüşüm) çekirdeği, $I(Y)$ idealinin, d dereceli $I_d(Y)$ homojen kısmına eşit olduğundan dolayı $S_d/I_d(Y) \cong C_{d,Y}$ izomorfizmasını elde ederiz. İlgilendiğimiz durumda, yani $Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$ olduğunda, Y'nin sıfırlayan idealinin bir üreteç kümesini biliyoruz. Bu üreteç kümesinin bir Gröbner tabanı olduğunu kanıtlayarak ve ayrıca derecesi d olan standart monomlara karşılık gelen *projektif indirgeme* adı verilen bir kombinatoryal küme tanımlayarak, $C_{d,Y}$'nin boyutu için bir formül vereceğiz.

4.1 Geometrik Yöntemlere Hazırlık

4.1.1 Sıfırlayan İdealin Evrensel Gröbner Bazı ve Graver Bazı

Öncelikle, $I(Y)$ sıfırlayan ideali için hem evrensel Gröbner bazı hem de Graver bazı olan, minimal üreteç kümesi verilecektir.

$\lambda \in \mathbb{K} \setminus \{0\}$ için $\mathbf{x^u} - \lambda\mathbf{x^v}$ binomlarıyla üretilen bir ideale **binom ideal** denir. Aşağıdaki teoremin ifadesine göre, $I(\mathbb{P}(1, a, b)(\mathbb{F}_q))$ idealinin **saf binomsal (pure binomial)** olduğunu, yani saf fark binomları $\mathbf{x^u} - \mathbf{x^v}$ ile üretilmiş olduğunu söyleyebiliriz. Aşağıdaki teorem bir önceki bölümdeki sonuçların elde edilmesinde de kullanıldığı için o bölümde de verilmiştir. Bu bölümde üreteçleri hatırlatmak için tekrar veriyoruz.

Teorem 4.1.1. *[43] $X = \mathbb{P}(1, a, b)$ ve $Y = X(\mathbb{F}_q)$ olmak üzere, Y kümesinin ideali aşağıdaki şekilde elde edilir.*

$$I(X) = \langle f_0, f_1, f_2 \rangle$$

Burada $f_0 = x_1^{(q-1)b+1}x_2 - x_1x_2^{(q-1)a+1}$, $f_1 = x_0^{(q-1)b+1}x_2 - x_0x_2^q$ *ve* $f_2 = x_0^{(q-1)a+1}x_1 - x_0x_1^q$

Kanıt. İspatı için [43, Corollary 5.8]'de verilen ispata bakılabilir. □

Uyarı 4.1.2. Açıkça görülüyor ki f_0, f_1, f_2 monomları birbirlerini bölemezler ve dolayısıyla [46] makalesindeki notasyon gereği G, bir monom idealin minimal monomsal üreteçlerinin tek (veya eşsiz (unique)) kümesi olmak üzere, $|G(M_{I(Y)})| = 6$ olur. Böylece, [46, Corollary 3.6]'nın sonucu olarak f_0, f_1, f_2 binomları *vazgeçilmezdir (indispensable)*, yani $I(Y)$ idealinin her minimal binom üreteç kümesinde (sıfır olmayan bir sabite kadar) bulunurlar. Başka bir deyişle, (sıfır olmayan bir sabite kadar) $\{f_0, f_1, f_2\}$ eşsiz minimal üreteç kümesidir.

Bir terim sırası seçerek ve $\{f_0, f_1, f_2\}$ minimal üreteç kümesinden başlayarak, $I(Y)$'nin bir Gröbner bazının elde edilebilir olduğunu biliyoruz.

$I(Y)$'nin **evrensel** Gröbner bazı da herhangi bir monom sıralamasına göre bir Gröbner bazıdır. Sadece sonlu sayıda farklı indirgenmiş Gröbner bazı olduğundan, bunların birleşimi **evrensel Gröbner bazıdır**. Bir binomun evrensel Gröbner bazında olmasının **ilkel** olması gerektirdirdiğini söyleyen [46, Proposition 4.2]'nin verdiği fikirle aşağıdaki tanımı verebiliriz.

Tanım 4.1.3. [46, Definition 4.1] Saf bir binom idealindeki sıfır olmayan $\mathbf{x^u} - \mathbf{x^v} := x_0^{u_0}x_1^{u_1}x_2^{u_2} - x_0^{v_0}x_1^{v_1}x_2^{v_2}$ binomuna, eğer $I \setminus \{0\}$'da $\mathbf{x^{u'}} - \mathbf{x^{v'}}$ gibi başka bir binom yoksa ve $\mathbf{x^{u'}}$, $\mathbf{x^u}$'yu, ayrıca $\mathbf{x^{v'}}$ de $\mathbf{x^v}$'yu bölerse, I idealinin **ilkel binomu** denir. I'nin tüm ilkel binomlarının kümesine **Graver bazı** denir.

Bir idealin hem evrensel Gröbner bazı hem de Graver bazı olması durumu nadir gözlenen bir durumdur. Aşağıdaki teorem ile birlikte Y'nin sıfırlayan idealinin üreteç kümesinin hem evrensel Gröbner bazı hem de Graver bazı olduğu ve bu üreteç kümesinin tek minimal üreteç kümesi olduğu ifade edilecektir. Bu, $\mathbb{F}_q$ cisminin bir cebirsel genişlemesi üzerinde $Y = \mathbb{P}^m(\mathbb{F}_q)$ kümesi için aynı zamanda evrensel bir Gröbner baz olan indirgenmiş bir Gröbner bazı veren [47, Theorem 2.8] referansındaki teoremi geneller.

Teorem 4.1.4. $I(Y)$ *idealinin üreteç kümesi* $\{f_0, f_1, f_2\}$ *olmak üzere bu üreteç kümesi hem evrensel Gröbner bazı hem de Graver bazıdır.*

Kanıt. $I(Y)$ idealinin evrensel Gröbner bazı olan homojen bir binom $\mathbf{x^u} - \mathbf{x^v}$ alalım. Bu binomun [46, Proposition 4.2]'e göre, ilkel olması gereklidir. Dolayısıyla, f_0, f_1, f_2 dışında başka bir ilkel homojen binom olmadığını göstermek yeterlidir. [43, Önerme 5.6] ve [43, Teorem 3.7]'nin ispatına göre, $I(Y)$ içindeki homojen bir binom şu formdadır:

$$\mathbf{x^u} - \mathbf{x^v} = \mathbf{x^a}(\mathbf{x}^{m^+} - \mathbf{x}^{m^-}) \text{ ve } \operatorname{supp}(\mathbf{x}^{m^+}) \cap \operatorname{supp}(\mathbf{x}^{m^-}) = \emptyset,$$

burada $\operatorname{supp}(\mathbf{x^a}) := \{j \in \{0,1,2\} : x_j \mid \mathbf{x^a}\}$ ve $m^+ - m^- \in (q-1)L_{\beta(\varepsilon)}$ şeklindedir. $\beta = \begin{pmatrix} 1 & a & b \end{pmatrix}$ olduğunu, $\beta(\varepsilon)$'nin β matrisinin $\varepsilon = \operatorname{supp}(\mathbf{x^a}) \subseteq \{0,1,2\}$'deki β_{j+1} sütunlarına sahip alt matrisi olduğunu ve $L_{\beta(\varepsilon)}$'nin $\beta(\varepsilon)$ matrisi tarafından temsil edilen doğrusal dönüşümün çekirdeğinin rasyonel noktaları olan kafes (latis) olduğunu hatırlayalım.

Varsayalım ki $\varepsilon = \{0,1,2\}$. Bu durumda, genel geçerliliği bozmadan, $\mathbf{x^u} - \mathbf{x^v} = x_0^{a_0}x_1^{a_1}x_2^{a_2}(x_2^{m_2^+} - x_0^{m_0^-}x_1^{m_1^-})$ olduğunu kabul edebiliriz ve burada a_0, a_1, a_2 pozitiftir. O zaman,

$$\mathbf{x^u} - \mathbf{x^v} = x_0^{a_0-1}x_1^{a_1-1}x_2^{a_2-1}(x_0x_1x_2^{m_2^+ +1} - x_0^{m_0^- +1}x_1^{m_1^- +1}x_2).$$

Dolayısıyla, $\mathbf{x^u} - \mathbf{x^v}$ ilkel binom değildir, çünkü $\mathbf{x^{u'}} - \mathbf{x^{v'}} := x_0x_1x_2^{m_2^+ +1} - x_0^{m_0^- +1}x_1^{m_1^- +1}x_2$, $I(Y)$'ye aittir ve hem $\mathbf{x^{u'}}$ $\mathbf{x^u}$'yu böler hem de $\mathbf{x^{v'}}$ $\mathbf{x^v}$'yu böler.

$L_{\beta(\varepsilon)} = \{0\}$ olduğundan, $|\varepsilon| = 1$ olur, dolayısıyla sadece $|\varepsilon| = 2$ olduğu durumu düşünmemiz gerekmektedir. Eğer $\varepsilon = \{1,2\}$ ise $\beta(\varepsilon) = [a\ b]$, $L_{\beta(\varepsilon)}\ (b, -a)$ tarafından genişletilmiş $\mathbb{Z}^2$ alt kafesi olup, bazı pozitif tam sayılar a_1, a_2 için $\mathbf{x^u} - \mathbf{x^v} = x_1^{a_1}x_2^{a_2}(x_1^{m_1^+} - x_2^{m_2^-})$ ve pozitif tam sayı l_0 için $(m_1^+, 0) - (0, m_2^-) = (q-1)l_0(b, -a)$ olur. Dolayısıyla, $x_1x_2x_1^{(q-1)b} \mid \mathbf{x^u}$ ve $x_1x_2x_2^{(q-1)a} \mid \mathbf{x^v}$ olacak şekilde tek ilkel binom açıkça f_0'dır. Diğer iki durum da yani f_1, f_2'nin de ilkel binom olduğunu benzer şekilde gösterebiliriz. Şimdi, f_1'in binom olduğunu aynı yöntemle gösterelim. Aynı sebepten dolayı, bu sefer eğer $\varepsilon = \{0,2\}$ ise $\beta(\varepsilon) = [1\ b]$, $L_{\beta(\varepsilon)}\ (b, -1)$ tarafından genişletilmiş $\mathbb{Z}^2$ alt kafesi olacağından, bazı pozitif tam sayılar a_0, a_2 için $\mathbf{x^u} - \mathbf{x^v} = x_0^{a_0}x_2^{a_2}(x_0^{m_0^+} - x_2^{m_2^-})$ ve pozitif tam sayı l_1 için $(m_0^+, 0) - (0, m_2^-) = (q-1)l_1(b, -1)$ olur. Dolayısıyla, $x_0x_2x_0^{(q-1)b} \mid \mathbf{x^u}$ ve $x_0x_2x_2^{(q-1)} \mid \mathbf{x^v}$ olacak şekilde tek ilkel binom açıkça f_1'dir. Son olarak, f_2 için eğer $\varepsilon = \{0,1\}$ ise $\beta(\varepsilon) = [1\ a]$, $L_{\beta(\varepsilon)}\ (a, -1)$ tarafından genişletilmiş $\mathbb{Z}^2$ alt kafesi olacağından, bazı pozitif tam sayılar a_0, a_1 için $\mathbf{x^u} - \mathbf{x^v} = x_0^{a_0}x_1^{a_1}(x_0^{m_0^+} - x_1^{m_1^-})$ ve $l_2 \geq 0$ tam sayısı için $(m_0^+, 0) - (0, m_1^-) = (q-1)l_2(a, -1)$ olur. Dolayısıyla, $x_0x_1x_0^{(q-1)a} \mid \mathbf{x^u}$ ve $x_0x_1x_1^{(q-1)} \mid \mathbf{x^v}$ olacak şekilde tek ilkel binom açıkça f_2'dir. □

4.1.2 Çokgenler üzerinde Projektif İndirgeme

Bu alt kısımda, P_d çokgeninin projektif indirgeme kavramını, bir başka deyişle $S_d/I(Y)_d$'deki sınıflar için kanonik temsilciler sağlayan ve P_d'nin kafes noktalarını S_d'deki monomlarla tanımlayan projektif indirgeme kavramının tanımını vereceğiz. Buradaki notasyonlar [22, §3.1]'de tanıtılan notasyonları takip etmektedir ve bu tanım [47, §2.1]'de verilen klasik projektif uzaylar için projektif indirgeme kavramını genelleştirir.

Kafes (latis) çokgenleri hakkında bazı tanımları hatırlayalım. P konveks bir kafes çokgeni olsun. P'nin bir yüzünü $Q \prec P$ ile gösteririz ve *iç kısmını*, herhangi bir yüz üzerinde yatmayan noktaların kümesi olarak tanımlarız, yani

$$P^\circ = P \setminus \bigcup_{\substack{Q \prec P \\ Q \neq P}} Q.$$

Tanım 4.1.5. Q, P birer kafes (lattice) çokgen olsun. $P \cap \mathbb{Z}^N$'nin elemanlarının mod P'de temsillerinin kümesi **projektif indirgeme** olarak adlandırılır. Bir başka deyişle,

$$m \sim_P m' \iff \exists Q \preceq P \text{ öyle ki } m, m' \in Q^\circ \text{ olmak üzere } m - m' \in (q-1)\mathbb{Z}^N$$

Burada, Q° ile Q çokgeninin içi belirtilmiştir. P çokgeninin projektif indirgemesi $\mathrm{Red}(P)$ ile gösterilecektir.

Bu çalışmalarda, [22, Definition 4.3] (bu tanımda belli bir sıralamaya göre indirgeme tanımlanıyor) tarafından önerildiği gibi, bir monomsal sıralamadan gelen, P_d'nin belirli bir projektif indirgemesini dikkate alıyoruz. Bu tez çalışmasının bu bölümünde $x_2 > x_1 > x_0$ olacak şekilde sözlük sıralamasını dikkate alacağız. Bir başka deyişle, derecesi d olan bir monom $x^{\mathbf{a},d} = x_2^{a_2} x_1^{a_1} x_0^{d-aa_1-ba_2}$, derecesi d' olan bir monom $x^{\mathbf{a}',d'} = x_2^{a_2'} x_1^{a_1'} x_0^{d'-aa_1'-ba_2'}$'den küçüktür, ancak ve ancak, $(a_2 - a_2', a_1 - a_1', a(a_1' - a_1) + b(a_2' - a_2))$'deki en soldaki sıfır olmayan sayı negatiftir. Bu durumda, $x^{\mathbf{a},d} <_{\text{lex}} x^{\mathbf{a}',d'}$ yazarız.

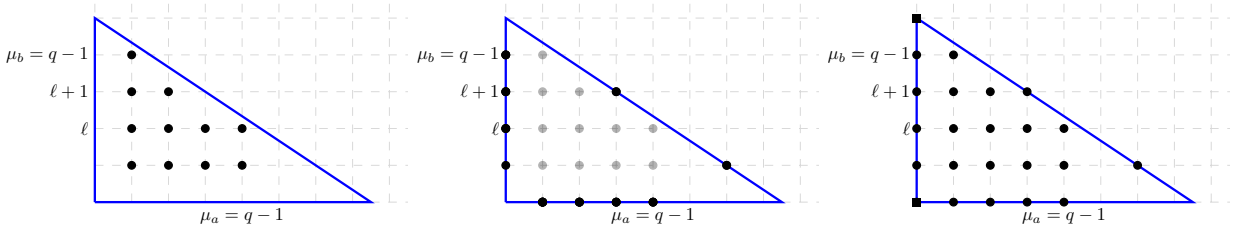
$(a_2 - a_2', a_1 - a_1', a(a_1' - a_1) + b(a_2' - a_2))$'deki en soldaki sıfır olmayan sayının negatif olması, $(a_2 - a_2', a_1 - a_1')$'deki en soldaki sıfır olmayan sayının negatif olmasına eşdeğerdir, yani $(a_1, a_2) <_{\text{lex}} (a_1', a_2')$ olur.

$\mathrm{Red}(d)$'yi yukarıda belirtilen sıralamaya göre projektif indirgeme olarak adlandırıyoruz, (bknz. Şekil 4.1'de yer alan üçüncü figür), yani,

$$\mathrm{Red}(d) = \left\{ \min_{\text{lex}} \{m \in \theta\} : \theta \in (P_d \cap \mathbb{Z}^2)/\sim_{P_d} \right\} \tag{28}$$

$$= \bigcup_{Q \prec P} \left\{ \min_{\text{lex}} \{m \in \theta\} : \theta \in (Q^\circ \cap \mathbb{Z}^2)/(q-1)\mathbb{Z}^2 \right\}. \tag{29}$$

Aşağıda verilen figürlerde (bknz. Şekil 4.1) indirgeme kavramı bir örnek üzerinden açıklanmaya çalışılmıştır. Şekil 4.1'de yer alan ilk figürde çokgenin iç rasyonel noktaları, ikinci figürde kenarlarına karşılık gelen rasyonel noktaları ve son olarak üçüncü figürde ise tüm rasyonel noktaları gösterilmektedir.



Şekil 4.1 $q = 5$ ve $d = 15$ için $\mathbb{P}(1,2,3)$ uzayına karşılık gelen bir çokgenin indirgemesi.

Teorem 4.1.6. *[22, Theorem 3.5] PC_P, P çokgenine karşılık gelen simitli kod olmak üzere,*

$$\mathrm{Ker}(ev_P) = Span\{\chi^m - \chi^{\bar{m}} : m \in (P \cap \mathbb{Z}^N)^2, \bar{m} \in Red(P) \text{ öyle ki } m \neq \bar{m}\}$$

Bu kodun bir bazı da aşağıdaki formdadır.

$$\{ev_P(\chi^{\langle \bar{m}, P\rangle}) : \bar{m} \in Red(P)\}$$

Buradan kodun boyutunun $Red(P)$ kümesinin eleman sayısı ile verileceğini söyleyebiliriz.

Yukarıdaki teoremin bir sonucu olarak, $C_{d,Y}$ kodu için bir baz, Tanım 4.1.5 ile verilen eşdeğerlik ilişkisine göre P_d'nin belirli rasyonel noktaları tarafından verilir. Bir başka deyişle, eğer $X = \mathbb{P}(1,a,b)$ düzlemine karşılık gelen çokgenlerin projektif indirgenmesinin kafes noktalarını göz önünde bulundurursak kodun boyutuna ulaşabiliriz.

Kodun boyutunu verirken kullanacağımız bazı kavramları verelim:

$$\mu_a = \min\left\{\left\lfloor \frac{d-1}{a} \right\rfloor, q-1\right\}, \qquad E_x(d) = \left\{(x,0) : 0 \le x \le \mu_a\right\}$$
$$\mu_b = \min\left\{\left\lfloor \frac{d-1}{b} \right\rfloor, q-1\right\}, \qquad E_y(d) = \left\{(0,y) : 0 \le y \le \mu_b\right\}.$$

$N_0 = (x', y')$, P_d üçgeninin hipotenüsü üzerindeki ilk iç latis (kafes) noktası olmak üzere, bir başka deyişle y-koordinatı $x' > 0$ ile birlikte en küçük pozitif tam sayı olan nokta olmak üzere

$$t = \min\left\{q-2, \left\lfloor \frac{d-by'-1}{ab} \right\rfloor\right\} \tag{30}$$

kümesini ve

$$E_h(d) = \left\{(x'-ib, y'+ia) \in \mathbb{N}^2 : 0 \le i \le t\right\}, \tag{31}$$

kümesini tanımlayalım. Eğer böyle bir N_0 noktası yoksa $E_h(d) = \emptyset$ olur.

Şimdi $H(d)$ kümesinin eleman sayısını ifade etmek için kullanacağımız, nümerik yarıgruplar teorisinde çok klasik bir fonksiyonun tanımını vereceğiz. Dolayısıyla, bir sonraki bölümde verilecek olan kodun boyutu ile ilgili sonuçta bu tanım kullanılacaktır.

Tanım 4.1.7. [48] a, b ve d pozitif tamsayılar olsun. $\mathrm{den}(d; a, b)$ ile gösterilen **denumerant** fonksiyonu , d'nin a ve b tam sayıları ile gösterimlerinin sayısı olarak tanımlanır, yani

$$d = m_a a + m_b b$$

eşitliğini sağlayan $(m_a, m_b) \in \mathbb{N}^2$ çözümlerinin sayısıdır.

$\mathrm{den}(d; a, b)$ değeri, ancak ve ancak, d, $\mathbb{N}$ üzerinde a ve b tarafından oluşturulan yarıgrup $\langle a, b\rangle_{\mathbb{N}}$'a ait ise pozitiftir. Literatürde (bknz. [48, Chapter 4] veya [49]), eğer $d = \lambda ab + s$ ve $0 \le s < ab$ ise, $\mathrm{den}(d; a, b) = \lambda + \mathrm{den}(s; a, b)$ olup, $\mathrm{den}(s; a, b) \in \{0, 1\}$'dir. Daha ayrıntılı olarak,

$$\mathrm{den}(s; a, b) = \begin{cases} 0 \text{ veya } 1 & \text{eğer } 0 < s < ab \\ 1 & \text{tüm } ab - a - b < s < ab \\ 0 & \text{eğer } s = ab - a - b. \end{cases}$$

Uyarı 4.1.8. Literatürde geleneksel olarak yarıgrubun *boşlukları (gaps)* olarak adlandırılan $\mathrm{den}(d; a, b) = 0$ olduğu durumdaki d tamsayıları, Miura tarafından [50] makalesinde detaylı bir şekilde incelenmiştir.

4.2 SONUÇLAR VE YÖNTEMLER-II

Bu bölümde [2] referansı ile verilen **"Codes on Weighted Projective Planes"** adlı makalesindeki yöntem ve sonuçlar ele alınacaktır.

İlk olarak kodun boyutu ile ilgili sonuçları vereceğiz. $X = \mathbb{P}(1, a, b)$ uzayına karşılık gelen çokgeni P ile gösterelim. P çokgeninin kafes noktaları ile kodun boyutu arasında ilişki olduğu kullanılarak bir önceki bölümde verdiğimiz tanımlar doğrultusunda aşağıda verilen sonuçlar elde edilmiştir.

4.2.1 Kodun Boyutu

Uyarı 4.2.1. $\alpha_2 = \left\lfloor \frac{d-1-a(q-1)}{b} \right\rfloor$ ve $\ell = \max\left\{0, \min\left\{q-1, \alpha_2\right\}\right\}$ sayıları bu çalışmalar boyunca kullanacağımız önemli kavramlar olduğundan dolayı bu sayılarla ilgili olarak aşağıdaki durumları vereceğiz. ℓ sayısı, $a(q-1) + by \leq d-1$ koşulunu sağlayan en büyük pozitif $y \in [1, \mu_b]$ tamsayısı olmak üzere (bir başka deyişle, $(q-1, y)$ kafes noktasının P_d° üzerinde olma koşulunu sağlayan tam sayı olmak üzere), aşağıdaki durumlar sağlanır.

$$\begin{cases} \mu_a = \lfloor \frac{d-1}{a} \rfloor, & \alpha_2 < 0 & \text{ve } \ell = 0 & \text{eğer } d \leq a(q-1), \\ \mu_a = q-1, & \alpha_2 = 0 & \text{ve } \ell = 0 & \text{eğer } a(q-1) < d \leq a(q-1)+b, \\ \mu_a = q-1, & 1 \leq \alpha_2 \leq q-2 & \text{ve } \ell = \alpha_2 & \text{eğer } a(q-1)+b < d \leq (q-1)(a+b), \\ \mu_a = q-1, & q-1 \leq \alpha_2 & \text{ve } \ell = q-1 & \text{eğer } (q-1)(a+b) < d. \end{cases}$$

Lemma 4.2.2. *ℓ sayısı Uyarı 4.2.1'da verildiği gibi tanımlansın.* $\mathrm{Red}(d)$ *belli bir* $x_2 > x_1 > x_0$ *sıralamasına karşılık gelen projektif indirgeme olmak üzere bu* $\mathrm{Red}(d)$ *kümesi aynı zamanda aşağıdaki birleşime eşittir.*

$$R(d) \cup T(d) \cup H(d), \text{ burada,}$$

$$\begin{aligned} R(d) &= \left\{(x,y) \in \mathbb{Z}^2 : 0 \leq x \leq \mu_a \text{ ve } 0 \leq y \leq \ell\right\}, \\ T(d) &= \left\{(x,y) \in \mathbb{Z}^2 : 0 \leq x \leq \left\lfloor \frac{d-1-by}{a} \right\rfloor \text{ ve } \ell+1 \leq y \leq \mu_b \right\}, \\ H(d) &= E_h(d) \cup \left[\left\{(0, d/b), (d/a, 0)\right\} \cap \mathbb{Z}^2\right]. \end{aligned}$$

Kanıt. (29) eşitliğindeki gibi tanımlanan $\mathrm{Red}(d)$ kümesinin elemanlarını belirlemek için, $Q \prec P_d$ yüzeylerine bakarız ve yukarıda bahsedilen sözlük sıralamasına göre eşdeğer olmayan en küçük $\mathbf{a} \in Q^\circ$ noktalarını seçeriz.

Öncelikle, $(0,0)$ köşesi $R(d)$ kümesinde yer alır. $\left(0, \frac{d}{b}\right)$ ve $\left(\frac{d}{a}, 0\right)$ köşeleri, sırasıyla, $b|d$ veya $a|d$ olduğunda açıkça $H(d)$ kümesine aittir.

Şimdi, P_d çokgeninin kenarları ile ilgilenelim. Eğer Q, x ekseninde P_d'nin kenarıysa, Q'nun iç kısmı olan Q°'deki kafes noktaları $1 \leq x \leq \left\lfloor \frac{d-1}{a} \right\rfloor$ için $(x,0)$ şeklindedir. İndirgemenin tanımına göre, aşağıdaki durumun geçerli olduğu kolayca kontrol edilebilir.

$$Q^\circ \cap \mathrm{Red}(d) = \left\{(x,0) : 1 \leq x \leq \mu_a\right\} = E_x(d) \subseteq R(d).$$

Eğer Q, P_d'nin y eksenindeki kenarı ise, o zaman aşağıdaki durum sağlanır:

$$Q^\circ \cap \mathrm{Red}(d) = \left\{(0,y) : 1 \leq y \leq \mu_b\right\} = E_y(d) \subseteq R(d) \cup T(d).$$

Q'nun P_d üzerinde $ax + by = d$ doğrusunda yatan kenar olduğunu varsayalım. Eğer $N_0 = (x', y')$, Q° üzerindeki en küçük kafes noktasıysa (en küçük pozitif y koordinatına sahip olan nokta), o zaman Q° üzerindeki tüm kafes noktaları, bazı pozitif olmayan i tamsayısı için $N_i = (x' - ib, y' + ia)$ şeklindedir.

Q° üzerindeki en büyük kafes noktasının (en büyük y koordinatına sahip olan ve $ax+by = d$ doğrusu üzerinde pozitif x koordinatına sahip olan nokta) $N_{i_{max}} = (x' - i_{max}b, y' + i_{max}a)$ olduğunu söyleyebiliriz. Burada, $i_{max} = \left\lfloor \frac{d-by'-1}{ab} \right\rfloor$ şeklinde tanımlıdır. Gerçekten de, taban kısmının tanımına göre, $N_{i_{max}}$'in koordinatları

$$\begin{aligned} x' - i_{max}b &\in \left[\frac{1}{a}, \frac{1}{a} + b\right), \\ y' + i_{max}a &\in \left(\frac{d-1}{b} - a, \frac{d-1}{b}\right]. \end{aligned}$$

koşullarını sağlar.

Ayrıca, herhangi iki pozitif olmayan i ve j tamsayısı için, ve a ve b aralarında asal olmak üzere, $N_i - N_j = (i-j)(-b, a)$ olduğunu hatırlarsak, eğer $q-1$, $i-j$'yi bölerse ancak

ve ancak bu durumda N_i ve N_j eşdeğerdir. Bu nedenle, $t = \min\{q-2, i_{max}\}$ olduğunda (bknz. Denklem (30)), $Q^\circ \cap \mathrm{Red}(d)$ indirgemesi tam olarak $E_h(d)$'dir.

Son olarak, Q'nun kendisinin P_d olduğunu varsayalım. Yatay ve dikey kenarlar için aynı mantıkla, Q°'nun indirgemesinin $[1, \mu_a] \times [1, \mu_b]$ karesinde olduğunu söyleyebiliriz. Daha açık bir şekilde, aşağıdaki durum geçerlidir:

$$Q^\circ \cap \mathrm{Red}(d) = P_d^\circ \cap \left([1, \mu_a] \times [1, \mu_b]\right).$$

Şimdi ise, $P_d^\circ \cap \left([1, \mu_a] \times [1, \mu_b]\right)$ kesişimini $1 \le y_0 \le \mu_b$ olmak üzere, her yatay doğru $y = y_0$ için daha ayrıntılı inceleyeceğiz.

$y = y_0$ doğrusunda, $\left\lfloor \frac{d-1-by_0}{a} \right\rfloor$, P_d°'nun en sağdaki kafes noktasının x koordinatıdır. Böylece,

$$P_d^\circ \cap \mathrm{Red}(d) = \bigcup_{1 \le y \le \mu_b} \left\{ (x, y) : 1 \le x \le \min\left\{ q-1, \left\lfloor \frac{d-1-by}{a} \right\rfloor \right\} \right\}. \qquad (32)$$

- Eğer $\ell = 0$ ise, o zaman (4.2.1) uyarınca $d - 1 < a(q-1) + b$ olur. Bu durumda, her $y \ge 1$ için $\lfloor \frac{d-1-by}{a} \rfloor < \left\lfloor \frac{d-1-b}{a} \right\rfloor \le q-1$ olur. (32)'de verilen küme aşağıdaki gibidir:

$$P_d^\circ \cap \mathrm{Red}(d) = \bigcup_{1 \le y \le \mu_b} \left\{ (x, y) : 1 \le x \le \left\lfloor \frac{d-1-by}{a} \right\rfloor \right\} \subset T(d).$$

  Bu durumda, $\mathrm{Red}(d)$ kümesi,

  - $R(d) = \{(0,0)\} \cup E_x(d)$, bu küme köşe $(0,0)$'ın ve yatay kenarın indirgemelerini içerir,
  - $T(d) = \{(x, y) : 0 \le x \le \left\lfloor \frac{d-1-by}{a} \right\rfloor$ ve $1 \le y \le \mu_b\}$, bu küme dikey kenarın $E_y(d)$ ve P_d'nin iç kısmının indirgemelerini içerir,
  - $H(d)$, son iki köşe arasındaki kafes noktaları ve $ax + by = d$ doğrusunda yatan kenarın iç kısmının indirgemeleridir.

- Eğer $\ell \geq 1$ ise, o zaman Uyarı 4.2.1'in gereği olarak, (32)'de verilen eşitliği şu şekilde yeniden yazabiliriz:

$$P_d^\circ \cap \mathrm{Red}(d) = \bigcup_{1\leq y\leq \ell} \{(x,y) : 1 \leq x \leq q-1 = \mu_a\} \cup \bigcup_{\ell+1\leq y\leq \mu_b} \left\{(x,y) : 1 \leq x \leq \left\lfloor \frac{d-1-by}{a} \right\rfloor \right\}.$$

İlk birleşim dikdörtgen alan $R(d)$'de yer alırken, ikinci birleşim trapez alan $T(d)$'de yer alır.

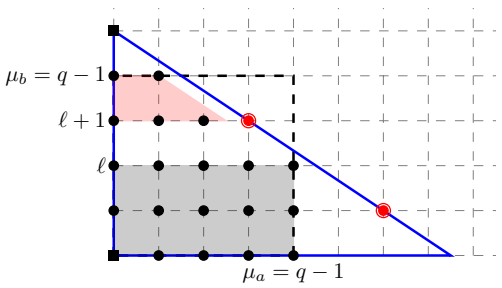
Böylece, hem (29)'de verilen $\mathrm{Red}(d)$ tanımı hem de Lemma'nın ifadesi birbirini karşıladığı için ispat tamamlanmış olur. □

Örnek 4.2.1. *Aşağıda verilen Figürler 4.2 ve 4.3'de kodun boyutu ile ilgili olarak verilen kavramların çokgenlerde tam olarak hangi noktalara ve bölgelere karşılık geldiği görselleştirilmiştir. Eğer* $q = 5$ *ve* $Y = \mathbb{P}(1,2,3)(\mathbb{F}_q)$ *olarak alınırsa ilk olarak* $d = 7$ *ve* $d = 11$ *için bakıldığından* (4.2)*'da görüldüğü üzere sırasıyla* $\mathrm{Red}(d)$*'nin nokta sayılarını aşağıdaki gibi sayabiliriz. Açıkça,* $R(d) = \{(0,0),(1,0),(2,0),(3,0)\}$ *ve* $\ell = 0$ *olur* $d = 7$ *için. Dolayısıyla* $|R(d)| = 4$ *olarak elde ederiz. Benzer şekilde trepazoid olarak adlandırılan kırmızı ile gösterilen bölgedeki elamanlar da* $T(d) = \{(0,1),(1,1),(0,2)\}$ *olduğundan dolayı* $|T(d)| = 3$ *olarak elde edilir. Ayrıca,* $H(d)$ *olarak gösterdiğimiz kümedeki elemanlar ise* $H(d) = \{(2,1)\}$ *olduğundan* $|H(d)| = 1$ *olur ve sonuç olarak,* $\dim_{\mathbb{F}_5}(C_{7,Y}) = |Red(7)| = 4+3+1 = 8$ *elde edilir.*

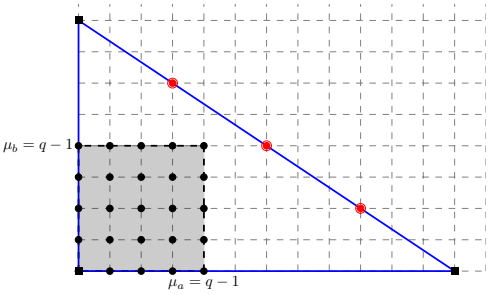
(a) $\mathrm{Red}(7) = P_7 \cap \mathbb{Z}^2$ ve $\ell = 0$, $\mu_a = 3$ *ve* $\mu_b = 2$.

(b) $\mathrm{Red}(11)$ ve $\ell = 0$, $\mu_a = 4$ ve $\mu_b = 3$

Şekil 4.2 $d = 7, 11$ ve $(q,a,b) = (5,2,3)$ durumlarına karşılık gelen $\mathrm{Red}(d)$ kümesi



(a) $\mu_a = \mu_b = q-1$ ve $T(15) \neq \varnothing$



(b) $\ell = \mu_a = \mu_b = q-1$ ve $T(24) = \varnothing$

Şekil 4.3 $d = 15, 24$ ve $(q, a, b) = (5, 2, 3)$ durumlarına karşılık gelen $\mathrm{Red}(d)$ kümesi

Örnek 4.2.1, Teorem 4.1.6 ve Lemma 4.2.2'i kullanarak $C_{d,Y}$ kodunun boyutunun nasıl kombinatorik olarak hesaplanabileceğini göstermektedir.

Şimdi kodun boyutunu hesaplayabilmemizi sağlayan Teoremi vereceğiz.

Teorem 4.2.3. *$Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$ ve burada $a \leq b$ olan iki pozitif ve aralarında asal tam sayılar olsun. $d \geq 1$ ve ℓ Uyarı 4.2.1 verildiği gibi tanımlı olsun. Böylece, $C_{d,Y}$ kodunun boyutu,*

$$\dim_{\mathbb{F}_q}(C_{d,Y}) = (\ell+1)\mu_a + \mu_b + 1 + \sum_{y=\ell+1}^{\mu_b} \left\lfloor \frac{d-1-by}{a} \right\rfloor + |H(d)| \tag{33}$$

ifadesi ile verilir, burada,

$$|H(d)| = \begin{cases} \mathrm{den}(d; a, b) & \text{eğer } d \leq ab(q-1), \\ q - 1 + \mathbf{1}_{a|d} + \mathbf{1}_{b|d} & \text{eğer } d > ab(q-1). \end{cases}$$

Kanıt. Teorem 4.1.6 göz önünde bulundurulduğunda, $C_{d,Y}$ kodunun boyutu $\mathrm{Red}(d)$ içindeki kafes noktalarının sayısına eşit olduğu görülür. Ayrıca, Lemma 4.2.2 ile aşağıdaki eşitliğin sağlandığı gösterilmişti.

$$\mathrm{Red}(d) = R(d) \cup T(d) \cup H(d).$$

Açıkça, dikdörtgen alanının kafes noktalarının kümesi olan $R(d)$ kümesinin eleman sayısı aşağıda verilen toplama eşittir:

$$|R(d)| = (\ell+1)(\mu_a+1) = (\ell+1)\mu_a + \ell + 1 \tag{34}$$

ℓ ile gösterilen ifadenin tanımı $\mu_b \geq \ell$ olmasını sağladığından, $\mu_b = \ell$ olduğunda $T(d)$ kümesi boş kümedir, bu yüzden bu durum (33) ile verilen toplamın 0'a eşit olduğu anlamına gelir. Ayrıca, $\mu_b \geq \ell + 1$ olduğunda, $T(d)$ bir yamuk içindeki kafes noktalarının kümesidir ve büyüklüğü

$$|T(d)| = \sum_{y=\ell+1}^{\mu_b} \left(\left\lfloor \frac{d-1-by}{a} \right\rfloor + 1 \right) = \mu_b - \ell + \sum_{y=\ell+1}^{\mu_b} \left\lfloor \frac{d-1-by}{a} \right\rfloor \tag{35}$$

$H(d) = E_h(d) \cup [\{(0, \frac{d}{b}), (\frac{d}{a}, 0)\} \cap \mathbb{Z}^2]$ kümesinin eleman sayısını da hesaplarsak teoremin ispatını tamamlamış olacağız, yani şimdi, $\mathrm{Red}(d)$ kümesindeki, çokgenin hipotenüsünün üzerinde yatan kafes noktalarının kümesinin eleman sayısını hesaplayacağız. Açıkça, $\mathrm{den}(d; a, b)$ fonksiyonu, P_d üçgeninin hipotenüsü üzerindeki (köşeleri de içeren) ve eşdeğer olabilecek kafes noktalarının sayısıdır. Bu nedenle,

$$|E_h(d)| = \min\left\{q-1, \mathrm{den}(d; a, b) - \epsilon\right\} \text{ burada } \epsilon = \mathbf{1}_{a|d} + \mathbf{1}_{b|d}, \tag{36}$$

ve $|H(d)|$ eleman sayısı şu şekilde yeniden ifade edilebilir:

$$|H(d)| = \min\left\{q-1+\epsilon, \mathrm{den}(d; a, b)\right\}. \tag{37}$$

Hatırlatmak gerekirse, eğer $d = \lambda ab + s$ ve $0 \leq s < ab$ ise, $\mathrm{den}(d; a, b) = \lambda + \mathrm{den}(s; a, b)$ ve $\mathrm{den}(s; a, b) \in \{0, 1\}$ olur ve bu durum s'in $\langle a, b\rangle_{\mathbb{N}}$ içinde olup olmamasına bağlıdır.

- $d < ab(q-1)$ olduğunda, $\lambda < q-1$ ve $\mathrm{den}(d; a, b) \leq q-1$ olur. $\epsilon \geq 0$ olduğundan, $|H(d)| = \mathrm{den}(d; a, b)$ olur.
- Eğer $d = (q-1)ab$ ise, hem $a|d$ hem de $b|d$ olur bu yüzden $\epsilon = 2$ olur. Ayrıca, aşağıdaki durum sağlanır:

  $$\mathrm{den}(d; a, b) = q - 1 + \mathrm{den}(0; a, b) = q \leq q - 1 + \epsilon.$$

  Bu nedenle, $|H(d)| = \mathrm{den}(d; a, b)$ olur.
- Şimdi $d > ab(q-1)$ olduğunu varsayalım. O zaman $\mathrm{den}(d; a, b) \geq q-1+\mathrm{den}(s; a, b)$ olur.

– Eğer $\epsilon = 0$ ise, (37) eşitliği $|H(d)| = q - 1$ verir.

– Eğer $\epsilon = 1$ ise, ya a ya da b s'yi böler, bu da $\mathrm{den}(s; a, b) = 1$ demektir. Böylece $\mathrm{den}(d; a, b) \geq q = q - 1 + \epsilon$, dolayısıyla $|H(d)| = q$ olur.

– Eğer $\epsilon = 2$ ise, hem a hem de b d'yi böler, bu da $d = \lambda ab$ olduğunu gösterir ve $\lambda \geq q$ olur. O zaman

$$\mathrm{den}(d; a, b) = \lambda + \mathrm{den}(0; a, b) = \lambda + 1 \geq q - 1 + \epsilon,$$

ve böylece, $|H(d)| = q + 1$ olur.

Buradan, (34), (35) ve (37) eşitliklerinden elde edilen değerler, (33) eşitliğinde belirtilen formülde göz önünde bulundurulursa istenilen elde edilir ve böylece ispat tamamlanır. □

Şimdi ise yukarıdaki teoremin bir sonucu olarak, $a = 1$ durumuna, yani $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$ durumuna karşılık gelen kodların boyutunu veren sonucu vereceğiz.

Sonuç 4.2.4. *Pozitif bir tamsayı b ve $d \geq 1$ için $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$ olsun. $\ell = \max\{\min\{0, q-1, \left\lfloor \frac{d-q}{b} \right\rfloor\}\}$ olmak üzere, kodun boyutu $\dim_{\mathbb{F}_q}(C_{d,Y})$ aşağıdaki şekilde verilir:*

$$(\ell + 1)(\mu_a + 1) + (\mu_b - \ell)d - b\binom{\mu_b + 1}{2} + b\binom{\ell + 1}{2} + \mu_b + 1 + \mathbf{1}_{b|d}.$$

Ek olarak, $d \leq q$ ise $\ell = 0$ ve $\mu_a = d - 1$ olur.

Kanıt. $a = 1$ ise, $\mu_a = \min\{q - 1, d - 1\}$ olur ve (33)'de verilen eşitlik aşağıdaki hale gelir:

$$\dim_{\mathbb{F}_q}(C_{d,Y}) = (\ell + 1)\mu_a + \mu_b + 1 + \sum_{y=\ell+1}^{\mu_b} (d - 1 - by) + |H(d)|.$$

Bu toplamı düzenlersek aşağıdaki formülü elde ederiz:

$$\begin{aligned}
\dim_{\mathbb{F}_q}(C_{d,Y}) &= (\ell + 1)\mu_a + \mu_b + 1 + (\mu_b - \ell)(d - 1) - b \sum_{y=\ell+1}^{\mu_b} y + |H(d)| \\
&= \mu_a\ell + \mu_a + 1 + \mu_b d - \ell d + \ell - b\left(\frac{\mu_b(\mu_b + 1)}{2} - \frac{\ell(\ell + 1)}{2}\right) + |H(d)| \\
&= (\ell + 1)(\mu_a + 1) + (\mu_b - \ell)d - b\binom{\mu_b + 1}{2} + b\binom{\ell + 1}{2} + |H(d)|.
\end{aligned}$$

$d \leq b$ olduğunda $E_h(d) = \emptyset$ olur ve $d > b$ olduğunda $N_0 = (x', y') = (d - b, 1)$ noktası, ilk iç kafes noktası olduğundan, Denklem (31)'den şu sonucu elde ederiz:

$$E_h(d) = |\{(d - by, y) : 1 \leq y \leq \mu_b\}| = \mu_b.$$

Bu nedenle, $|H(d)| = |E_h(d)| + 1 + \mathbf{1}_{b|d} = \mu_b + 1 + \mathbf{1}_{b|d}$ olur. Özetle, istenildiği gibi $|H(d)| = \mu_b + 1 + \mathbf{1}_{b|d}$ elde ederiz. □

Uyarı 4.2.5. Kodun boyutu için verilen formül, $a = b = 1$ durumu için [14, Theorem 6.4] referansındaki Teorem ile uyuşmaktadır.

$Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$ olduğu durumda düzenlilik kümesi ile ilgili sonuçlar Bölüm (3.2)'de verilmiştir. Şimdi ise $Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$ kümesinin düzenlilik kümesi ile ilgili sonuçlar verilecektir.

4.2.2 Düzenlilik Kümesi

Bu alt bölümde, ağırlıklı projektif düzlemin $\mathbb{P}(1, a, b)$ üzerindeki $\mathbb{F}_q$-rasyonel noktalarından oluşan $Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$ kümesinin düzenlilik kümesini vereceğiz. Kısaca açıklamak gerekirse, bu kümenin önemi, aşikar kodlar olarak adlandırdığımız minimum uzaklığı 1 olan kodların açığa çıkarmasından kaynaklanmaktadır. Bir ağırlıklı projektif düzlem $\mathbb{P}(1, a, b)$'nın *sıfır boyutlu* alt çeşitlemi Y'nin Hilbert fonksiyonu, $S/I(Y)$ halkasının Hilbert fonksiyonu olarak tanımlanır:

$$H_Y(d) = \dim_{\mathbb{K}} S_d - \dim_{\mathbb{K}} I_d(Y) = \dim_{\mathbb{F}_q} S_d - \dim_{\mathbb{F}_q} I_d(Y),$$

burada $I_d(Y) = I(Y) \cap S_d$, Y üzerinde sıfırlanan homojen polinomlar tarafından oluşturulan $I(Y)$ sıfırlayan idealinin d dereceli kısmıdır. Hatırlatmak gerekirse, $Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$ ise, (27)'teki hesaplama dönüşümünün çekirdeği $I_d(Y)$'dir ve bu nedenle $C_d(Y)$ kodunun boyutu $H_Y(d) \leq |Y|$ olur. $H_Y(d) = |Y|$ olduğu durumda Hilbert fonksiyonu alabileceği maksimum değere ulaşır ve bu durumu sağlayan $d \in \mathbb{N}\mathbf{w}$ (burada $\mathbf{w}$ ile gösterilen $\mathbf{w} = (w_0, \ldots, w_n)$ ağırlığıdır) derecelerinin kümesi olan düzenlilik kümesi aşağıdaki şekilde tanımlıdır.

Tanım 4.2.6. $Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$ kümesinin düzenlilik kümesi,

$$\mathrm{reg}(Y) = \{d \in \mathbb{N}\mathbb{W} : H_Y(d) = |Y|\}$$

olarak tanımlanır.

Uyarı 4.2.7. Eğer $d \in \mathrm{reg}(Y)$ ise, kodun boyutu maksimum olur, yani $C_{d,Y} = \mathbb{F}_q^n$ olur, burada $n = |Y|$'dir. Bu nedenle, bu kod $[n, n, 1]$ parametrelerine sahip aşikar (trivial) bir koddur.

Önerme 4.2.8. *a ve b aralarında asal olan iki pozitif tam sayılar olsun ve $1 \leq a \leq b$ olsun. Bir d tam sayısı, $Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$ kümesinin düzenlilik kümesine aittir ancak ve ancak $d = d_0ab$ olacak şekilde bir $d_0 \geq q$ ve $(a + b)(q - 1) < d$ vardır.*

Kanıt. Bu sonuç, Lemma 4.2.2 tarafından verilen $\mathrm{Red}(d)$ projektif indirgenmiş kümenin tanımından yola çıkılarak elde edilmektedir. Buna göre, $d \in \mathrm{reg}(Y)$ olabilmesi için $|\mathrm{Red}(d)| = |Y| = q^2 + q + 1 = (q - 1)^2 + 3(q - 1) + 3$ durumu sağlanmalıdır. Bu da $a \mid d$ ve $b \mid d$ olmak üzere $|P_d^\circ| = (q - 1)^2$, $|E_x(d)| = |E_y(d)| = |E_h(d)| = q - 1$ durumuna eşdeğerdir.

$(q-1)^2$ koşulunun sağlanması için $(q-1, q-1)$ noktasının P_d'nin içinde yer alması gereklidir ki bu da $(a + b)(q - 1) < d$ koşuluna eşdeğerdir. Bu durumda, $(q - 1, 0) \in E_x(d)$ ve $(0, q - 1) \in E_y(d)$ olduğundan $|E_x(d)| = |E_y(d)| = q - 1$ olur.

a ve b tam sayıları aralarında asal olduğundan $a \mid d$ ve $b \mid d$ olması $ab \mid d$ ile eşdeğerdir. Buradan $d = d_0ab$ olacak şekilde bir d_0 tam sayısının varlığını garanti edebiliriz. Ve $\mathrm{den}(d; a, b) = d_0 + 1$ olur. (36)'te verilen eşitliğe göre,

$$|E_h(d)| = \min\left\{q - 1, \mathrm{den}(d; a, b) - 2\right\} = q - 1 \iff d_0 \geq q,$$

olur ki bu da kanıtı tamamlar. □

Teorem 4.2.9. *a ve b, $1 < a < b$ olacak şekilde iki aralarında asal pozitif tam sayı olsun. $Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$ kümesinin düzenlilik kümesi aşağıdaki gibi verilmektedir.*

$$\mathrm{reg}(Y) = \{d \in \mathbb{N} : d_0 \geq q \text{ olmak üzere } d = d_0ab\} = qab + \mathbb{N}ab.$$

Kanıt. Önerme 4.2.8'e göre, $d = d_0ab$ şeklinde yazarsak, $d_0 \geq q$ olmak üzere bu durumun $(a+b)(q-1) < d$ koşulunu sağladığını kontrol etmek yeterlidir. $a \geq 2$ ve $b > a$ olduğundan, $ab \geq 2b > a + b$ olduğu için şu sonucu elde ederiz:

$$d = d_0ab \geq qab \geq q(a + b) > (q - 1)(a + b).$$

Bu da ispatı tamamlar. □

Uyarı 4.2.10. $a = 1$ durumunda [1, Corollary 3.9] referansıyla verilen ayrıca bu tez çalışmasında da Sonuç 3.2.13 ile verilen sonucu yukarıdaki teoremden de elde edebileceğimiz açıktır. Bu Teoremin bize sağladığı kolaylık geometrik bakış açısından kaynaklı olarak Sonuç 3.2.13 ispatındaki gibi Hilbert fonksiyonunun değer aralıklarına göre d derecelerinin düzenlilik kümesine düşüp düşmediğini kontrol etmemize gerek yoktur. Hatta, kısaca göstermek gerekirse, $a = 1$ için, $Y = \mathbb{P}(1,1,b)(\mathbb{F}_q)$ olmak üzere, düzenlilik kümesi aşağıdaki gibidir:

$$\mathrm{reg}(Y) = \{d \in \mathbb{N} : d = d_0 b \text{ olmak üzere } d_0 \geq q + \lfloor (q-1)/b \rfloor\} = \left(q + \left\lfloor \frac{q-1}{b} \right\rfloor\right) b + \mathbb{N}b.$$

Buradan,

$$d_0 b > (1+b)(q-1) \iff d_0 \geq \left\lfloor \frac{q-1}{b} \right\rfloor + q,$$

olduğu kolayca görülür.

Şimdi düzenlilik kümesi ile ilgili olarak aşağıdaki örneği ele alalım.

Örnek 4.2.2. *$X = \mathbb{P}(1,a,b)$ olmak üzere $a = 2$, $b = 3$ olarak alalım. Sırasıyla $q = 3, 5, 7$ olmak üzere $Y = X(\mathbb{F}_q)$ rasyonel noktalar kümesini ele alalım. Y kümesinin Hilbert fonksiyonlarının değerleri aşağıda verilen tablolarda sunulmuştur. Burada kırmızı renk ile gösterilen d dereceleri Hilbert fonksiyonunun maksimum değere ulaştığı değerlerdir. Bir başka deyişle düzenlilik kümesinin elemanları olan d dereceleri kırmızı renk ile gösterilmiştir.*

Tablo 4.1 $Y = \mathbb{P}(1,2,3)(\mathbb{F}_3)$'in Hilbert fonksiyonunun değerleri

d	0	1	2	3	4	5	6	7	8	9	10	11	12
$H_X(d)$	1	1	2	3	4	5	7	7	9	10	10	11	12
d	13	14	15	16	17	18	19	20	21	22	23	24	25
$H_X(d)$	11	12	12	12	11	13	11	12	12	12	11	13	11
d	26	27	28	29	30	31	32	33	34	35	36	37	38
$H_X(d)$	12	12	12	11	13	11	12	12	12	11	13	11	12

Tablo 4.2 $Y = \mathbb{P}(1,2,3)(\mathbb{F}_5)$'in Hilbert fonksiyonunun değerleri

d	0	1	2	3	4	5	6	7	8	9	10	11	12
$H_X(d)$	1	1	2	3	4	5	7	8	10	12	14	15	18
d	13	14	15	16	17	18	19	20	21	22	23	24	25
$H_X(d)$	19	21	23	24	25	27	27	28	29	29	29	30	29
d	26	27	28	29	30	31	32	33	34	35	36	37	38
$H_X(d)$	30	30	30	29	31	29	30	30	30	29	31	29	30
d	39	40	41	42	43	44	45	46	47	48	49	50	51
$H_X(d)$	30	30	29	31	29	30	30	30	29	31	29	30	30

Tablo 4.3 $Y = \mathbb{P}(1,2,3)(\mathbb{F}_7)$'in Hilbert fonksiyonunun değerleri

d	0	1	2	3	4	5	6	7	8	9	10	11	12
$H_X(d)$	1	1	2	3	4	5	7	8	10	12	14	15	18
d	13	14	15	16	17	18	19	20	21	22	23	24	25
$H_X(d)$	16	19	21	24	26	29	31	34	36	39	41	43	45
d	26	27	28	29	30	31	32	33	34	35	36	37	38
$H_X(d)$	47	48	50	51	52	53	54	54	55	55	55	56	55
d	39	40	41	42	43	44	45	46	47	48	49	50	51
$H_X(d)$	56	56	56	55	57	55	56	56	56	55	57	55	56
d	52	53	54	55	56	57	58	59	60	61	62	63	64
$H_X(d)$	56	56	55	57	55	56	56	56	55	57	55	56	56

4.2.3 Minimum Uzaklık

Bu kısımda, $a \leq b$ aralarında asal pozitif tam sayılar olmak üzere, $\mathbb{P}(1,a,b)$ uzayına karşılık gelen Ağırlıklı Projektif Reed-Muller kodların temel parametrelerinden biri olan minimum uzaklıkla ilgili olan hesaplamalar ve sonuçlar verilecektir. Hatırlatmak gerekirse, tez boyunca $\mathbb{P}(1,a,b)$ uzayının $\mathbb{F}_q$-rasyonel noktalarının kümesi aşağıdaki şekilde alınacaktır:

$$Y = \mathbb{P}(1,a,b)(\mathbb{F}_q) = \left\{[1 : y_1 : y_2] : y_1, y_2 \in \mathbb{F}_q\right\} \cup \left\{[0 : y_1 : 1] : y_1 \in \mathbb{F}_q\right\} \cup \{[0 : 1 : 0]\}.$$

Her $f \in S_d \setminus I_d(Y)$, için Y_f ile f'nin köklerini içeren Y'nin $V_Y(f)$ alt çeşitlemini (variety) göstereceğiz ve $n_f = |Y_f|$ olarak tanımlayacağız. Hesaplama kodlarının minimum uzaklığının tanımı gereği aşağıdaki eşitliği yazabiliriz.

$$d_{min}(C_{d,Y})(= \delta(C_{d,Y})) = n - \max\{n_f : f \in S_d \setminus I_d(Y)\}.$$

Minimum uzaklık için verilecek olan alt sınır hesaplanırken, literatürde, **ayakizi sınırı**

(footprint bound) olarak da bilinen ve Gröbner baz teorisine dayanan sınır kullanılarak n_f üzerine bir üst sınır verilmiştir. Literatürde afin ve projektif uzay durumları için [47, 51, 52], Hirzebruch yüzeyleri için [23], ve daha genel simitli çeşitlemler (toric varieties) için [22] makalelerinde bu sınır kullanılarak minimum uzaklıkla ilgili çalışmalar yapılmıştır.

S halkası üzerindeki monomların kümesi M üzerinde tanımlı olan $\prec$ monomsal sıralamasına karşılık gelen S halkasının bir I homojen idealinin *ayakizi* aşağıdaki şekilde tanımlanır:

$$\Delta(I) = \{M \in \mathbb{M} : M \neq \text{LM}(g) \text{ herhangi bir } g \in I \text{ ve } g \neq 0 \text{ için }\}.$$

Burada, $\text{LM}(g)$ notasyonu ile gösterilmek istenen g polinomunun baş monomudur (leading monomial). Aşağıda vereceğimiz Lemma sayesinde $f \in S_d \setminus I_d(Y)$ olmak üzere, f'nin kök sayılarını ifade eden n_f için bir üst sınır elde edeceğimizden dolayı minimum uzaklık için de bir alt sınır elde etmiş olacağız.

Lemma 4.2.11. *[22, Lemma 5.5]* $Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$ *olsun ve* $I(Y, f)$ *ile* $f \in S$ *bir homojen polinomu için* $I(Y) + (f)$ *idealini gösterelim. Buradan, herhangi bir* $f \in S_d \setminus I_d(Y)$ *ve* $\tilde{d} \in \text{reg}(Y)$ *olmak üzere,* $n_f \leq \tilde{n}_f(\tilde{d}) = H_{I(Y,f)}(\tilde{d}) = |\Delta_{\tilde{d}}(I(Y, f))|$ *olur.*

Kanıt. Düzenlilik kümesi $\text{reg}(Y)$, $H_{I(Y)}(d) = N$ olan d elemanlarından oluştuğundan, $\tilde{d} \in \text{reg}(Y)$ için $ev_{\tilde{d},Y} : S_{\tilde{d}} \mapsto \mathbb{F}_q^n$ lineer dönüşümü örtendir. $S_d \setminus I_d(Y)$'deki herhangi bir f için, $Y_f = \{P \in Y : f(P) = 0\}$ kümesini doğal projeksiyon dönüşümü $\mathbb{F}_q^n \mapsto \mathbb{F}_q^{n_f}$ ile birleştirerek, aşağıdaki örten fonksiyonu elde ederiz: $ev_{\tilde{d},Y_f} : S_{\tilde{d}} \mapsto \mathbb{F}_q^{n_f}$. Böylece, $n_f = H_{I(Y_f)}(\tilde{d})$ ve $\tilde{d} \in \text{reg}(Y_f)$ olur. $I(Y, f) \subseteq I(Y_f)$ kapsama ilişkisi,

$$I_{\tilde{d}}(Y, f) = I_{\tilde{d}}(Y) + S_{\tilde{d}-d} \cdot (f) \subseteq I_{\tilde{d}}(Y_f)$$

sonucunu verir. Dolayısıyla, n_f için bir üst sınır şu şekilde verilir:

$$\tilde{n}_f(\tilde{d}) = H_{I(Y,f)}(\tilde{d}) \geq n_f = H_{I(Y_f)}(\tilde{d}).$$

$H_{I(Y,f)}(\tilde{d}) = |\Delta_{\tilde{d}}(I(Y, f))|$ olduğundan ispat tamamlanır. □

Yarı polinomlardan, (3.2.4) bölümünde bahsedilmiştir. Fakat tekrar hatırlatmak gerekirse, [40, Theorem 4.3.5] referansındaki Teoreme göre, $M = S/I(Y, f)$ modülü için $H_M(d) = P_M(d)$ olacak şekilde $d > a(M)$ için belirlenmiş bir yarı-polinom (quasi polynomial) P_M

vardır. Burada $a(M)$, Hilbert serisi $HS_M(t)$'yi temsil eden rasyonel fonksiyonun derecesini ifade eder ve a-invaryantı veya değişmezi olarak adlandırılır. Diğer bir deyişle, g (periyot) pozitif bir tam sayı ve bazı $P_0, \ldots, P_{g-1}$ polinomları vardır öyle ki $d > a(M)$ ve $d \equiv i \mod g$ için $H_M(d) = P_i(d)$ eşitliği geçerlidir.

$I(Y) \subseteq I(Y, f) \subseteq I(Y_f)$ olduğundan, eğer f, $S/I(Y)$'nin bir sıfır böleni ise, $I(Y, f)$'nin Krull boyutu 1'dir. Bu nedenle, $J = I(Y, f)$ ve f, $S/I(Y)$'nin bir sıfır böleni ise, S/J'nin Hilbert yarı-polinomunun derecesi 0'dır. (bknz. [53, Proposition 5] veya [54]). Bu nedenle, $\tilde{n}_f(\tilde{d})$'nin yeterince büyük $\tilde{d}$ için aldığı değerler olarak ortaya çıkan sonlu sayıda sabit vardır. Böylece, bu sabitlerin tümünün maksimumu olarak $\tilde{n}_f$'yi tanımlıyoruz. Dolayısıyla, tüm bunların doğrultusunda ve yukarıdaki Lemma'nın bir sonucu olarak öncesinde de bahsettiğimiz gibi minimum uzaklık üzerine aşağıdaki sınırı verebiliriz.

$$d_{min}(C_{d,Y}) \geq N - \max\left\{\tilde{n}_f : f \in S_d \setminus I_d(Y), S/I(Y) \text{ halkasının bir sıfır böleni. }\right\} \quad (38)$$

Fakat $\tilde{n}_f$'i elde etmek için Hilbert yarı-polinomlarını hesaplamak kolay değildir. Bu nedenle, $\tilde{n}_f(\tilde{d})$ için kolay bir üst sınır vermek amacıyla Gröbner baz teorisinin aşağıdaki Lemma ile verilecek olan kolaylık sağlayacak klasik bir hilesine başvurulacaktır ve bu sınır $\tilde{d}$'den bağımsız olacaktır.

Lemma 4.2.12. *[52, Lemma 2.5] $I \subset S$, $\mathcal{G} = \{g_0, \ldots, g_r\}$ tarafından üretilen bir ideal olmak üzere, aşağıdaki durum sağlanır:*

$$\Delta_\prec(I) \subset \Delta_\prec(LM_\prec(g_1), \ldots LM_\prec(g_r)).$$

eğer bu $\mathcal{G}$, Gröbner baz ise yukarıdaki kapsama, eşitliğe dönüşür.

Lemma 4.2.13. *[22] X bir basit simitli (toric) çeşitlem ve $Y \subset X$ bir alt çeşitlem olsun. $\mathcal{G}$, $I(Y)$'nin bir terim sıralaması olan $\prec$'e göre Gröbner bazını göstersin.*

$$\overline{\Delta}_{\tilde{d}}(f) = \{M \in \mathbb{M}_{\tilde{d}} : \forall g \in \mathcal{G} \cup \{f\},\ LM(g) \nmid M\}.$$

Böylece, $f \in S_d \setminus I_d(Y)$ için

$$\tilde{n}_f(\tilde{d}) = H_{I(Y,f)}(\tilde{d}) \leq |\overline{\Delta}_{\tilde{d}}(f)|, \quad (39)$$

olur. Ve $\tilde{n}_f(\tilde{d}) = |\overline{\Delta}_{\tilde{d}}(f)| \iff \mathcal{G} \cup \{f\}$, $I(Y, f)$'nin $\prec$ sıralamasına göre Gröbner bazıdır.

Uyarı 4.2.14. $X = \mathbb{P}(1,a,b)$ ve $Y = X(\mathbb{F}_q)$ olmak üzere, derecesi $\tilde{d}$ olan ve her $g \in \mathcal{G}$ (Burada $\mathcal{G}$ ile kast edilen Gröbner baz) için $\text{LM}(g)$ ilk monomuna bölünmeyen monomların kümesi, ($\prec$ için $= <_{\text{lex}}$) $\overline{\mathbb{M}}_{\tilde{d}}$ kümesidir. Böylece,

$$\overline{\Delta}_{\tilde{d}}(f) = \left\{ M \in \overline{\mathbb{M}}_{\tilde{d}} : \text{LM}(f) \nmid M \right\}. \tag{40}$$

$|\overline{\Delta}_{\tilde{d}}(f)|$ üst sınırı için, Lemma 4.2.13 vasıtasıyla $\overline{\Delta}_{\tilde{d}}(f) = \overline{\Delta}_{\tilde{d}}(\text{LM}(f))$ olduğundan, f'yi bir monom olarak kabul etmek yeterlidir. Ayrıca $\text{LM}(f) = \mathbf{x}^{\mathbf{a},d}$ ve $\mathbf{a} \in \text{Red}(d)$ olduğunu da varsayabiliriz. Bu nedenle, sabit bir $\mathbf{a} \in \text{Red}(d)$ ve $\tilde{d} \geq d$ için, derecesi $\tilde{d}$ olan $\mathbf{x}^{\mathbf{a},d}$ monomunun **projektif gölgesi** (projective shadow) aşağıdaki biçimde tanımlanır:

$$\overline{\nabla}_{\tilde{d}}(\mathbf{x}^{\mathbf{a},d}) = \{\mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}} \in \overline{\mathbb{M}}_{\tilde{d}} : \mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}}, \mathbf{x}^{\mathbf{a},d} \text{ tarafından bölünsün. } \} = \overline{\mathbb{M}}_{\tilde{d}} \setminus \overline{\Delta}_{\tilde{d}}(\mathbf{x}^{\mathbf{a},d}).$$

Sonuç 4.2.15. *Sözlük sıralamasını $\prec = <_{lex}$ olarak düşünelim ve $\tilde{d} \in \text{reg}(Y)$ olduğunu varsayalım. Böylece, her $f \in S_d \setminus I(Y)$ için*

$$|\overline{\Delta}_{\tilde{d}}(f)| = |\overline{\Delta}_{\tilde{d}}(LM(f))| = N - \overline{\nabla}_{\tilde{d}}(LM(f)).$$

Kanıt. $\tilde{d} \in \text{reg}(Y)$ olduğunda, $|\overline{\mathbb{M}}_{\tilde{d}}| = H_{I(Y)}(\tilde{d}) = N$ olur. $|\overline{\Delta}_{\tilde{d}}(f)|$'nin değeri doğrudan eşitlik (40)'dan elde edilir. □

Her $\mathbf{a} \in \text{Red}(d)$ ve $\tilde{d} \in \text{reg}(Y)$ için, aşağıdaki eşitliği tanımlayalım:

$$L(\mathbf{a},\tilde{d}) : = |\overline{\nabla}_{\tilde{d}}(\mathbf{x}^{\mathbf{a},d})| = n - |\overline{\Delta}_{\tilde{d}}(\mathbf{x}^{\mathbf{a},d})|. \tag{41}$$

Lemma 4.2.16. *$d \in \mathbb{N} \setminus \text{reg}(Y)$ ve $\tilde{d} \in \text{reg}(Y)$ olsun. Böylece minimum uzaklık için bir alt sınır aşağıdaki gibi elde edilir:*

$$d_{min}(C_{d,Y}) \geq \min\{\ L(\mathbf{a},\tilde{d}) : \mathbf{a} \in \text{Red}(d)\}.$$

Kanıt. Açıkça görüldüğü gibi,

$$d_{min}(C_{d,Y}) = n - \max\{\ |V_Y(f)| : f \in S_d \setminus I_d(Y)\}.$$

$f \in S_d \setminus I_d(Y)$ ve $\text{LM}(f) = \mathbf{x}^{\mathbf{a},d}$ olarak alalım. Teorem 4.1.6 ile $\mathbf{a} \in \text{Red}(d)$ olduğunu varsayabiliriz. Lemma 4.2.11 ve Lemma 4.2.13'den dolayı $|V_Y(f)| \leq |\overline{\Delta}_{\tilde{d}}(\text{LM}(f))|$

olduğunu söyleyebiliriz ve dolayısıyla istenilen durum aşağıdaki gibi elde edilir:

$$d_{min}(C_{d,Y}) \geq n - \max\{|\overline{\Delta}_{\tilde{d}}(\mathbf{x}^{\mathbf{a},d})| : \mathbf{a} \in \mathrm{Red}(d)\} = \min\{L(\mathbf{a},\tilde{d}) : \mathbf{a} \in \mathrm{Red}(d)\}.$$

□

Uyarı 4.2.17. $\mathbf{a} \in \mathrm{Red}(d)$ olsun. $\tilde{d} \in \mathrm{reg}(Y)$ olduğunda, $x_0^{\tilde{d}}$, $x_1^{\tilde{d}/a}$ ve $x_2^{\tilde{d}/b}$ monomları, $\overline{\mathbb{M}}_{\tilde{d}}$'e ait olmalıdır. Hatırlatmak gerekirse,

$$\overline{\mathbb{M}}_{\tilde{d}} = \left\{ M \in \mathbb{M}_{\tilde{d}} : \mathbf{LM}(g) \nmid M \right\}.$$

Dolayısıyla, tanım gereği eğer $\mathbf{x}^{\mathbf{a},d}$ bu monomlardan ikisini bölerse, sabit bir sayı olmalı ve $d = 0$ olmalıdır. O zaman, $d \geq 1$ ise, $L(\mathbf{a},\tilde{d}) \leq n-2$ olur. Ayrıca, $d \leq \tilde{d}$ ise, $\mathbf{x}^{\mathbf{a},d}$ monomu, $\mathbf{x}^{\mathbf{a},\tilde{d}}$'yi böler ve $L(\mathbf{a},\tilde{d}) \geq 1$ olur, çünkü $d \notin \mathrm{reg}(Y)$'dir. Sonuç olarak, Lemma 4.2.16 tarafından sağlanan sınır aşikar, önemsiz bir sınır (trivial) değildir.

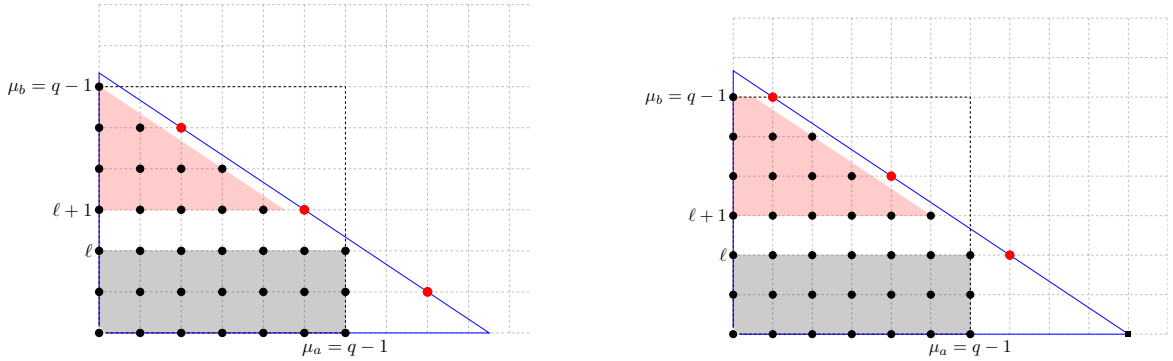
Burada, minimum uzaklığı, Lemma 4.2.16 tarafından sağlanan alt sınırın yeterince büyük $\tilde{d}$ için eşitlik olduğunu kanıtlayarak belirlemek amaçlanmaktadır. Bu doğrultuda aşağıdaki adımlar izlenerek çalışmalar yapılmıştır.

Öncelikle, $\tilde{d}$ derecesine olan bağımlılığı ortadan kaldırarak, $\tilde{d}$'ye bağlı olmayan derecede $\overline{\mathbb{M}}_d$ içindeki monomların **projektif gölgesinin** eleman sayısının bir formülünü vererek alt sınırın bağımlılık durumunun ortadan kaldırılması amaçlanmaktadır. (bknz. Önerme 4.2.18).

Sonrasında, Lemma 4.2.21 ve doğrultusunda verilen sonuçlarla birlikte $L = L(\cdot,\tilde{d})$ fonksiyonunun $\mathrm{Red}(d) \cap \{a_2 \leq \mu_b\}$ konveks alanındaki minimumu belirlenecektir. Aşağıdaki durumların $\mathrm{Red}(d)$ tanımından elde edildiği kolayca kontrol edilebilir, öyle ki

- eğer $d \leq bq-1$ ise, $\mu_b = \left\lfloor \frac{d-1}{b} \right\rfloor$ ve $a_2 \leq \mu_b$ durumu her $\mathbf{a} \in \mathrm{Red}(d)$ için geçerlidir, fakat eğer $b \mid d$ ise, $\mathbf{a} = (0, d/b)$ hariç olmak üzere diğer durumlar aynı şekilde geçerlidir.

Önerme 4.2.18. *$\tilde{d} \in \mathrm{reg}(Y)$ ve $\tilde{d} \geq d + (q-1)\max\{a+b, ab\}$ koşullarını sağlayan her durumda ve her $\mathbf{a} = (a_1, a_2) \in \mathrm{Red}(d)$ için, $L(\mathbf{a},\tilde{d})$'nin değeri $\tilde{d}$'ye bağlı değildir ve $L(\mathbf{a})$*



(a) $d < bq-1$,
$\mu_b = \left\lfloor \frac{d-1}{b} \right\rfloor$ ve
Her $\mathbf{a} \in Red(d)$ için $a_2 < \mu_b$

(b) $d = bq-1 < bq$,
$\mu_b = \left\lfloor \frac{d-1}{b} \right\rfloor$ ve
Her $\mathbf{a} \in Red(d)$ için $a_2 \leq \mu_b$

Şekil 4.4 Sırasıyla $d = 19, 20$ dereceleri ve $\mathbb{P}(1,2,3)(\mathbb{F}_7)$ kümesi için verilen minimum uzaklıkların alt sınırlarının karşılaştırılması.

olarak göstereceğimiz fonksiyon aşağıdaki durumları sağlar:

$$\begin{cases} (q-a_1)(q-a_2) & \text{eğer } aa_1+ba_2 \neq d \\ \max\{q-a_1,0\}\max\{q-a_2,0\}+q-1-\left\lfloor \frac{a_2-1}{a} \right\rfloor & \text{eğer } aa_1+ba_2 = d \text{ ve } a_1 \neq 0, \\ q\cdot\max\{q-\frac{d}{b},0\}+\max\{q-\left\lfloor \frac{d-b}{ab} \right\rfloor,1\} & \text{eğer } (a_1,a_2)=(0,\frac{d}{b}) \text{ ve } b \mid d. \end{cases}$$

Kanıt. $\mathbf{a} = (a_1,a_2) \in \mathrm{Red}(d)$ ve $\mathbf{x}^{\mathbf{a},d} = x_0^{d-aa_1-ba_2}x_1^{a_1}x_2^{a_2}$ olarak alalım. $\mathbf{x}^{\mathbf{a},d}$ monomunu bölen $\mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}} = x_0^{\tilde{d}-a\tilde{a}_1-b\tilde{a}_2}x_1^{\tilde{a}_1}x_2^{\tilde{a}_2}$ olan $\tilde{\mathbf{a}} = (\tilde{a}_1,\tilde{a}_2) \in \mathrm{Red}(\tilde{d})$ çiftlerinin sayısını sayarsak aşağıdaki denkliği elde ederiz:

$$\mathbf{x}^{\mathbf{a},d} \text{ böler } \mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}} \iff \begin{cases} a_1 \leq \tilde{a}_1, \\ a_2 \leq \tilde{a}_2 \\ d-aa_1-ba_2 \leq \tilde{d}-a\tilde{a}_1-b\tilde{a}_2. \end{cases} \tag{42}$$

Burada, $\tilde{d} \in \mathrm{reg}(Y)$ kabulünün $|\mathrm{Red}(\tilde{d})| = q^2+q+1$ olduğunu garanti ettiğini belirtelim. Özellikle, $\mathrm{Red}(\tilde{d}) = R(\tilde{d}) \cup H(\tilde{d})$ koşulu aşağıdaki eşitlikler doğrultusunda sağlanır:

$$R(\tilde{d}) = \{(\tilde{a}_1,\tilde{a}_2) \in \mathbb{Z}^2 : 1 \leq \tilde{a}_1 \leq q-1 \text{ ve } 1 \leq \tilde{a}_2 \leq q-1\} \tag{43}$$

ve

$$H(\tilde{d}) = \{(b(d_0-y_0), y_0a) \in \mathbb{Z}^2 : 0 \leq y_0 \leq q-1 \text{ ve } y_0 = d_0\}, \tag{44}$$

Burada, $\tilde{d} = d_0 ab$ eşitliği, $d_0 \geq q$ olan bazı $d_0 \in \mathbb{N}$ için geçerlidir (bknz. Önerme 4.2.8).

Eğer $\mathbf{a} = (a_1, a_2) \in \mathrm{Red}(d) \backslash H(d)$ ise, $aa_1 + ba_2 < d$ olur ve dolayısıyla (42) içindeki üçüncü koşulun sağlanması için $a\tilde{a}_1 + b\tilde{a}_2 < \tilde{d}$'yi de içermesi gerekmektedir. Bu, $(\tilde{a}_1, \tilde{a}_2) \in R(\tilde{d})$ olduğu ve dolayısıyla $\tilde{a}_1 \leq q-1$ ile $\tilde{a}_2 \leq q-1$ durumlarının sağlandığı anlamına gelir. Sonuç olarak,

$$\tilde{d} - d \geq (q-1)(a+b) \geq a\tilde{a}_1 + b\tilde{a}_2 \geq a(\tilde{a}_1 - a_1) + b(\tilde{a}_2 - a_2),$$

olur ve bu durum da (42)'deki üçüncü koşulu sağlar. Bu nedenle, (42)'deki tüm koşullar $0 \leq a_1 \leq \tilde{a}_1 \leq q-1$ ve $0 \leq a_2 \leq \tilde{a}_2 \leq q-1$ için sağlanır. Bu durumda, $\tilde{a}_1$ ve $\tilde{a}_2$ sırasıyla, $q - a_1$ ve $q - a_2$ olası değerlerine sahiptir, bu da L fonksiyonunun ilk koşulunu sağlar.

Şimdi $\mathbf{a} \in H(d) \setminus \{(0, d/b)\}$ olduğunu varsayalım. Bu durumda, $aa_1 + ba_2 = d$ olur ve böylece, (42)'deki üçüncü koşul sağlanmış olur. Ve $\mathbf{x}^{\mathbf{a},d}$, $\mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}}$'yi böler ancak ve ancak $a_1 \leq \tilde{a}_1$ ve $a_2 \leq \tilde{a}_2$ durumları sağlanır. $R(\tilde{d})$'deki bu tür çiftlerin sayısı, a_1 ve a_2, $q-1$'den büyük olabilse de $\tilde{a}_1 \leq q-1$ ve $\tilde{a}_2 \leq q-1$ olduğundan, $\max\{q-a_1, 0\}\max\{q-a_2, 0\}$ olarak verilir. $\mathbf{a} \neq (0, d/b)$ eşitsizliği $a_1 \geq 1$ ve $0 \leq a_2 < aq$ olduğunu ifade eder. (44) eşitliği ile, her $\tilde{\mathbf{a}} = (\tilde{a}_1, \tilde{a}_2) \in H(\tilde{d})$ için, aşağıdaki durumlar sağlanır:

$$\begin{aligned} a_1 \leq \tilde{a}_1 &\iff d - ba_2 \leq \tilde{d} - aby_0 \\ &\iff aby_0 \leq \tilde{d} - d + ba_2 \end{aligned}$$

Bu nedenle $\tilde{d} \geq d + (q-1)\max\{a+b, ab\}$ durumu, $a_1 \leq \tilde{a}_1$ koşulunun $\tilde{a}_1 \leq 1$ koşuluna indirgenmesini her $(\tilde{a}_1, \tilde{a}_2) \in H(\tilde{d}) \backslash \{(0, \tilde{d}/b)\}$ için sağlar. $\tilde{a}_2 = ay_0 < a_2$ koşulunu sağlayan tam olarak $\left\lfloor \frac{a_2 - 1}{a} \right\rfloor$ tane $\tilde{\mathbf{a}}$ çifti olduğundan, aşağıdaki formülü elde ederiz:

$$L(\mathbf{a}) = \max\{q-a_1, 0\}\max\{q-a_2, 0\} + q - 1 - \left\lfloor \frac{a_2 - 1}{a} \right\rfloor$$

bu da ikinci durumu kanıtlar.

Son olarak, $\mathbf{a} = (0, d/b)$ ve $b \mid d$ olduğunu varsayalım. Önceki durumdan farkı, $\tilde{a}_1$'in 0 olabilmesidir. Yani, önceki formüle $a_1 = 0$, $a_2 = d/b$'yi ekleyip, $(0, \tilde{d}/b)$ köşesi için 1 ekleyerek son formülü elde ederiz: $q \cdot \max\{q - \frac{d}{b}, 0\} + \max\{q - \left\lfloor \frac{d-b}{ab} \right\rfloor, 1\}$, ve böylece ispat tamamlanır. □

Uyarı 4.2.19. Önerme 4.2.18'deki $L(\mathbf{a})$ için ikinci formül 0 değerini alabilir, ancak bu sadece $\mathbf{a} \notin \mathrm{Red}(d)$ ise mümkündür, bu da Uyarı 4.2.17 ile doğrulanmış olur.

Önerme 4.2.18'ye $a = b = 1$ durumlarını ekleyerek [47, Lemma 4.1]'u tekrar elde ederiz.

Örnek 4.2.3. *Varsayalım ki, $q = 2$, $X = \mathbb{P}(1,1,3)$ ve $Y = X(\mathbb{F}_q)$ olsun. Teorem 4.1.4'e göre, aşağıda verilen eşitlik, $I(Y)$ için evrensel Gröbner tabanını vermektedir.*

$$\mathcal{G} = \{f_0 = x_2^2x_1 + x_2x_1^4, f_1 = x_2^2x_0 + x_2x_0^4, f_2 = x_1^2x_0 + x_1x_0^2\}.$$

Şahin ve Baldemir tarafından [55] makalesinde verilen algoritmalardan birini kullanarak, $C_{4,Y}$ kodunun minimum uzaklığının 2 olduğunu hesaplayabiliriz. Bu, maksimum olası kök sayısına sahip bir homojen polinom olan f'nin kök sayısının $n_f = |Y| - 2 = 5$ olduğunu ortaya koyar. Ve Önerme 4.2.18'nin çalıştığı en küçük olası $\tilde{d}$ elemanını analiz etmek için kullanılır.

$d = (q-1)(a+b) = 4$ için, $S_d/I_d(Y)$ için bir baz aşağıdaki şekilde verilir:

$$\overline{\mathbb{M}}_4 = \{x_2x_1,\ x_2x_0,\ x_1^4,\ x_1x_0^3,\ x_0^4\}.$$

Sonuç 3.2.13'ye göre, $\mathrm{reg}(Y) = 6 + 3\mathbb{N}$ olduğundan, önce her $f \in \overline{\mathbb{M}}_4$ için $I(Y) + \langle f\rangle$'nin Hilbert fonksiyonunun değerlerine bakarız ve aşağıdaki durumları elde ederiz:

$$H_{I(Y)+\langle f\rangle}(6) = \begin{cases} 6 & \text{eğer } f = x_1x_0^3, \\ 5 & \text{eğer } f \in \overline{\mathbb{M}}_4 \setminus \{x_1x_0^3\}. \end{cases}$$

Bu durum, $f = x_1x_0^3$ için $H_{I(Y)+\langle f\rangle}(6)$'nin en büyük $n_f = 5$'ten büyük olduğunu ortaya koyar.

Ancak, $\tilde{d} \geq 2(q-1)(a+b) = 8$ alırsak, yani $\tilde{d} \in 9 + 3\mathbb{N}$ alırsak, bu sorunu çözebiliriz. Gerçekten de, $f = x_1x_0^3$ için tüm $\tilde{d} \in 9 + 3\mathbb{N}$ için $\tilde{n}_f(\tilde{d}) = |\overline{\Delta}_{\tilde{d}}(f)| = 5$ olduğunu görürüz, çünkü $I(Y) + \langle f\rangle$'nın Gröbner bazı $\mathcal{G} \cup \{f\}$ şeklindedir ve $S_{\tilde{d}}/I_{\tilde{d}}(Y, f)$ için bir baz ise, $\{x_2^{\tilde{d}/3}, x_2x_1^{\tilde{d}-3}, x_2x_0^{\tilde{d}-3}, x_1^{\tilde{d}}, x_0^{\tilde{d}}\}$ ile verilir.

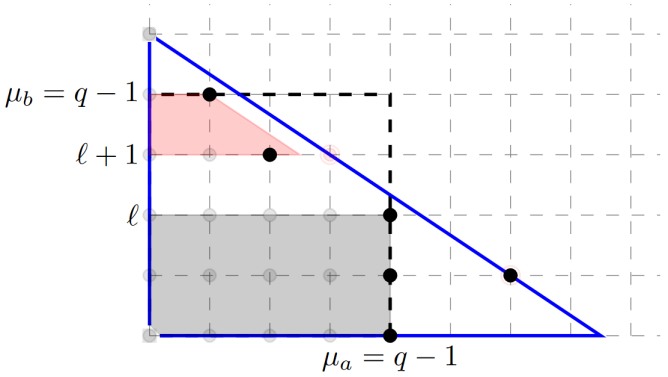
Şimdi $\mathbf{a} \in \mathrm{Red}(d)$ olmak üzere yani $\mathrm{Red}(d)$ kümesi üzerinde minimumu tam olarak 1 olan $L(\mathbf{a}, \tilde{d})$ fonksiyonunun hangi d derecelerine karşılık geldiğini veren Önermeyi verelim.

Önerme 4.2.20. *Eğer* $\tilde{d} \geq d > (a+b)(q-1)$ *ise, o zaman* $\min_{\mathbf{a}\in \mathrm{Red}(d)} L(\mathbf{a}, \tilde{d}) = 1$.

Kanıt. $d > (a+b)(q-1)$ koşulu, $(q-1, q-1)$ noktasının P_d° içinde yer aldığı, dolayısıyla $\mathrm{Red}(d)$ içinde yer aldığı anlamına gelir. Minimum L açıkça bu noktada elde edilir, çünkü $\mathbf{x}^{\tilde{\mathbf{a}},\tilde{d}}$, $\mathbf{x}^{\mathbf{a},d} = x_0^{d-(q-1)(a+b)} x_1^{q-1} x_2^{q-1}$ tarafından bölünebilirdir ancak ve ancak $\tilde{a}_1 = q-1$, $\tilde{a}_2 = q-1$ ve $\tilde{d} \geq d$ koşulları sağlanır. Bu da ispatı tamamlar. □

Şimdi ise, $L(a_1, a_2)$ fonksiyonunun $\mathrm{Red}(d) \cap \{a_2 \leq \mu_b\}$ alanı üzerindeki minimumu ile ilgili sonuçlar ve gözlemler verilecektir. Bu durum, Figür 4.4'de verilen ilk iki Figürde görülen çokgenlere karşılık gelmektedir.

İlk olarak gözlemlediğimiz durum, $L(a_1, a_2)$ fonksiyonunun minimum değerine ulaşmadığı $\mathrm{Red}(d) \cap \{a_2 \leq \mu_b\}$ kümesindeki birçok (a_1, a_2) noktasını ortadan kaldırır. Diğer bir deyişle, minimum değerin bir iç noktada elde edildiğini söylemekle kalmaz, aynı zamanda her yatay çizgi $y = a_2$ üzerindeki böyle bir noktanın a_1 koordinatını da tanımlar (bknz. Şekil 4.5).



Şekil 4.5 L'nin, Lemma 4.2.21 sayesinde elde edilen $\mathrm{Red}(d) \cap \{a_2 \leq \mu_b\}$ üzerindeki olası minimum noktalarının gösterimi

Lemma 4.2.21. $a_2 \in \{0, \ldots, \mu_b\}$ *olarak alalım. Ayrıca,* $\mathcal{X}_{a_2} = \{a_1 \in \mathbb{N} : (a_1, a_2) \in \mathrm{Red}(d)\}$ *ve* $M_{a_2} = \max \mathcal{X}_{a_2}$ *olsun.*

Eğer $aM_{a_2} + ba_2 < d$ *ise,* $\mathcal{X}_{a_2}$ *üzerinde* $a_1 \mapsto L(a_1, a_2)$ *tek değişkenli fonksiyonunun minimumu tam olarak* $a_1 = M_{a_2}$ *noktasında elde edilir.*

Eğer $aM_{a_2} + ba_2 = d$ *ise, minimum*

$$\operatorname*{argmin}_{a_1 \in \mathcal{X}_{a_2}} L(\cdot, a_2) = \begin{cases} \{\min\{M_{a_2}, q\} - 1, M_{a_2}\} & \text{eğer } a_2 = 0, 1 \text{ ya da } a = 1, \\ \{\min\{M_{a_2}, q\} - 1\} & \text{aksi takdirde.} \end{cases}$$

noktasında elde edilir.

Kanıt. Eğer $aM_{a_2} + ba_2 \neq d$ ise, $(M_{a_2}, a_2) \notin H(d)$ anlamına gelir ve bu da $M_{a_2} \leq q-1$ demektir. Dolayısıyla, $\mathcal{X}_{a_2}$ kümesi üzerinde $a_1 \mapsto L(a_1, a_2)$ fonksiyonu Önerme 4.2.18 ile $L(a_1, a_2) = (q-a_1)(q-a_2)$ olarak tanımlanır. Bu fonksiyon a_1'e göre kesinlikle azalan bir fonksiyondur.

Aksi halde, $aM_{a_2} + ba_2 = d$ olur. Bu durumda $M_{a_2} \geq 1$ (çünkü $a_2 \leq \mu_b$) ve $a_1 \mapsto L(a_1, a_2)$ fonksiyonunun $\mathcal{X}_{a_2} \setminus \{M_{a_2}\}$ üzerinde kesinlikle azalan olduğunu söyleyebiliriz ve aşağıdaki iki durumun da sağlandığını açıkça görürüz:

1. $M_{a_2} \leq q$ ise, bu $\mathcal{X}_{a_2} = \{0, \ldots, M_{a_2}\}$ anlamına gelir.
2. $M_{a_2} > q$, bu da $\mathcal{X}_{a_2} = \{0, \ldots, q-1\} \cup \{M_{a_2}\}$ durumuna karşılık gelir.

İlk durum için aşağıdaki iki durumu karşılaştıracağız:

$$L(M_{a_2}, a_2) = (q - M_{a_2})(q - a_2) + q - 1 - \left\lfloor \frac{a_2 - 1}{a} \right\rfloor$$

ve $L(M_{a_2} - 1, a_2) = (q - M_{a_2} + 1)(q - a_2) = (q - M_{a_2})(q - a_2) + q - a_2$. Bu iki fonksiyon arasındaki farkı hesaplayarak şu sonuca ulaşırız:

$$\begin{aligned} L(M_{a_2}, a_2) - L(M_{a_2} - 1, a_2) &= -1 - \left\lfloor \frac{a_2 - 1}{a} \right\rfloor + a_2 \\ &= \left\lceil \frac{(a-1)(a_2-1)}{a} \right\rceil \geq 0 \end{aligned}$$

İkinci durumda, sadece $L(M_{a_2}, a_2) = q - 1 - \left\lfloor \frac{a_2-1}{a} \right\rfloor$ ve $L(q-1, a_2) = q - a_2$'yu karşılaştırmak kalır. Benzer şekilde farka bakarsak:

$$L(M_{a_2}, a_2) - L(q-1, a_2) = \left\lceil \frac{(a-1)(a_2-1)}{a} \right\rceil.$$

olduğu elde edilir. Her iki durumda da, $\mathcal{X}_{a_2}$ kümesi üzerinde $a_1 \mapsto L(a_1, a_2)$ fonksiyonunun minimumu $\min\{M_{a_2}, q\} - 1$ ile ve ayrıca $a_2 \in \{0, 1\}$ veya $a = 1$ ise M_{a_2} ile elde edilir. $\square$

Yukarıda verilen Lemmadan yola çıkarak aşağıdaki tek değişkenli fonksiyonu tanımlayalım:

$$a_2 \mapsto \tilde{L}(a_2) = L\left(\min\left\{\left\lfloor\frac{d-1-ba_2}{a}\right\rfloor, q-1\right\}, a_2\right) \tag{45}$$

Burada amacımız, fonksiyonun hangi (a_1, a_2) değerlerinde minimum değere ulaştığını gözlemleyebilmek olduğundan yukarıdaki lemma ve sonrasında tanımladığımız (45) fonksiyonu doğrultusunda aşağıdaki sonucu elde ederiz.

Sonuç 4.2.22. *Yukarıdaki varsayımlar altında,*

$$\min_{\substack{(a_1,a_2)\in \mathrm{Red}(d)\\ a_2\leq \mu_b}} L(a_1, a_2) = \min_{a_2\in\{0,\ldots,\mu_b\}} \tilde{L}(a_2)$$

olduğu elde edilir.

Kanıt. Bu sonuç Lemma 4.2.21'in doğrudan bir sonucudur, gerçekten, aşağıdaki durumları düşünürsek,

$$\min\left\{\left\lfloor\frac{d-1-ba_2}{a}\right\rfloor, q-1\right\} = \begin{cases} M_{a_2} & \text{eğer } aM_{a_2} + ba_2 < d, \\ \min\{M_{a_2}, q\} - 1 & \text{eğer } aM_{a_2} + ba_2 = d, \end{cases}$$

bu durumlarla birlikte kanıt tamamlanır. □

Uyarı 4.2.1'de verilen $\alpha_2 = \left\lfloor\frac{d-1-a(q-1)}{b}\right\rfloor$ sayısını hatırlarsak, $\mathrm{Red}(d) \cap \{a_2 \leq \mu_b\}$ üzerinde $L(a_1, a_2)$ fonksiyonunun minimum değerini elde etmek için, $\tilde{L}$ tek değişkenli fonksiyonunun $\{0, \ldots, \mu_b\}$ üzerinde nasıl değiştiğini gözlememiz gereklidir.

Uyarı 4.2.23. En genelde ağırlıklar üzerindeki $a \leq b$ varsayımı, $(a_1, a_2) \in \mathrm{Red}(d) \setminus H(d)$ ve $a_2 > a_1$ olduğunda (a_2, a_1)'in de aynı kümede olduğunu ifade eder. Ayrıca, Önerme 4.2.18'de tanımlanan L fonksiyonu P_d'nin iç kısmında, simetriktir, yani eğer hem (a_1, a_2) hem de (a_2, a_1) $\mathrm{Red}(d) \setminus H(d)$'ye aitse, $L(a_1, a_2) = L(a_2, a_1)$'dir. Bu nedenle, $\mathrm{Red}(d) \setminus H(d)$ üzerindeki L fonksiyonunun minimumunu araştırırken, $\mathbf{a_2} \leq \mathbf{a_1}$ alt kümesine sınırlayabiliriz.

Uyarı 4.2.23 ile açıklananlar doğrultusunda $\tilde{L}$ fonksiyonunu $\left\{0, \ldots, \left\lfloor \frac{d-1}{a+b} \right\rfloor \right\}$ kümesi üzerinde incelemek yeterlidir. Böylece, $\left\{0, \ldots, \left\lfloor \frac{d-1}{a+b} \right\rfloor \right\}$ kümesi üzerinde $\tilde{L}$ fonksiyonunun aldığı değerleri inceleyerek aşağıdaki lemmayı elde ederiz.

Lemma 4.2.24. $\left\{0, \ldots, \left\lfloor \frac{d-1}{a+b} \right\rfloor \right\}$ *kümesi üzerinde,* (45) *eşitliğinde tanımlanan* $\tilde{L}$ *fonksiyonu aşağıdaki gibi verilir.*

1. *Eğer* $d \leq a(q-1)$ *(yani* $\alpha_2 < 0$*), ise*

$$\tilde{L}(a_2) = \left(q - \left\lfloor \frac{d-1-ba_2}{a} \right\rfloor \right) (q - a_2).$$

2. *Eğer* $d > a(q-1)$ *(yani* $\alpha_2 \geq 0$*), ise*

$$\tilde{L}(a_2) = \begin{cases} q - a_2 & \text{eğer } a_2 \leq \alpha_2, \\ \left(q - \left\lfloor \frac{d-1-ba_2}{a} \right\rfloor \right) (q - a_2) & a_2 \leq \alpha_2 \text{ durumu dışında kalan diğer durumlarda.} \end{cases}$$

Kanıt. İlk durum, Önerme 4.2.18 ve (45) eşitliği ile verilen $\tilde{L}$'nin tanımı ile $\left\lfloor \frac{d-1-ba_2}{a} \right\rfloor \leq \left\lfloor \frac{d}{a} \right\rfloor \leq q-1$ gözlemi doğrultusunda elde edilir. İkinci kısım da benzer şekilde, aşağıdaki durumu göz önünde bulundurarak elde edilir.

$$\left\lfloor \frac{d-1-ba_2}{a} \right\rfloor \geq q-1 \iff a_2 \leq \left\lfloor \frac{d-1-a(q-1)}{b} \right\rfloor = \alpha_2, \tag{46}$$

ve böylece kanıt tamamlanır. □

Lemma 4.2.25. *Eğer,* $\tilde{L}(a_2)$ *fonksiyonu, Lemma 4.2.24'de verildiği gibi,* $\tilde{L}(a_2) = \left(q - \left\lfloor \frac{d-1-ba_2}{a} \right\rfloor \right) (q - a_2)$ *ise,* $\left\{ \max\{0, \alpha_2\}, \ldots, \left\lfloor \frac{d-1}{a+b} \right\rfloor \right\}$ *kümesinde kesinlikle artandır.*

Kanıt. a_2'nin aşağıdaki durumu sağlayan tüm değerleri için

$$\max\left\{0, \left\lfloor \frac{d-1-a(q-1)}{b} \right\rfloor\right\} + 1 \leq a_2 \leq \min\left\{ \left\lfloor \frac{d-1}{a+b} \right\rfloor, q-1 \right\}$$

$\tilde{L}(a_2) - \tilde{L}(a_2 - 1)$ farkı şu şekildedir:

$$(q - a_2 + 1)\left(\left\lfloor \frac{d-1-b(a_2-1)}{a} \right\rfloor - \left\lfloor \frac{d-1-ba_2}{a} \right\rfloor\right) - q + \left\lfloor \frac{d-1-ba_2}{a} \right\rfloor.$$

Eğer $a = 1$ ise, yukarıdaki ifade aşağıdaki hale gelir:

$$\tilde{L}(a_2) - \tilde{L}(a_2 - 1) = d + (q+1)(b-1) - 2a_2 b$$

Ve bu ifade pozitiftir çünkü $a_2 \leq \left\lfloor \frac{d-1}{b+1} \right\rfloor$ ve $a_2 \leq q - 1$ durumu sağlanır.

Eğer $a \neq 1$ ise, $x, y \in \mathbb{Z}$ için

$$\left\lfloor \frac{x}{a} \right\rfloor - \left\lfloor \frac{y}{a} \right\rfloor = \left\lfloor \frac{x}{a} \right\rfloor - \left\lceil \frac{y+1}{a} \right\rceil + 1 \geq \left\lfloor \frac{x-y-1}{a} \right\rfloor. \tag{47}$$

durumu sağlanır. Bu durumu $x = d-1-b(a_2-1)$ ve $y = d-1-ba_2$ için uyguladığımızda, aşağıdaki sonucu elde ederiz:

$$\tilde{L}(a_2) - \tilde{L}(a_2 - 1) \geq (q - a_2 + 1)\left\lfloor \frac{b-1}{a} \right\rfloor - q + \left\lfloor \frac{d-1-ba_2}{a} \right\rfloor.$$

$a_2 \leq \left\lfloor \frac{d-1}{a+b} \right\rfloor$ olduğundan, bu durum $\left\lfloor \frac{d-1-ba_2}{a} \right\rfloor \geq a_2$ anlamına gelir, ve dolayısıyla

$$\tilde{L}(a_2) - \tilde{L}(a_2 - 1) \geq (q - a_2 + 1)\left(\left\lfloor \frac{b-1}{a} \right\rfloor - 1\right) + 1$$

olur, ve bu ifade pozitiftir çünkü $q > a_2$ ve $b > a$'dır. □

Yukarıdaki lemma, $\tilde{L}(a_2)$ fonksiyonunun a_2'nin belirli bir aralığında kesinlikle artan olduğunu gösterir. Ve $\tilde{L}(a_2)$ ve $\tilde{L}(a_2 - 1)$ arasındaki farkın pozitif olduğunu ispatlamak için farklı durumlar ele alınarak ispatlanmıştır.

Önerme 4.2.26. $\{0, \ldots, \mu_b\}$ *kümesindeki* $\tilde{L}$ *fonksiyonunun minimum değeri aşağıdaki şekilde elde edilir:*

$$\tilde{L}(\ell) = \begin{cases} q(q - \mu_a) & \textit{eğer } \ell = 0, \\ q - \ell & \textit{eğer } \ell = \alpha_2. \end{cases}$$

Kanıt. $d \leq (a+b)(q-1)$ varsayımı $\alpha_2 = \left\lfloor \frac{d-1-a(q-1)}{b} \right\rfloor \leq q-2$ ifadesine denktir. Bu nedenle, Uyarı 4.2.1 ile anlatılmak istenilene göre, $\ell = \max\{0, \alpha_2\}$ olur.

1. Eğer $d \leq a(q-1)$ (yani $\alpha_2 < 0$) ise, Lemma 4.2.24 (1)'de verilen $\tilde{L}$ fonksiyonu, Lemma 4.2.25'a göre, $\left\{0, \ldots, \min\left\{\left\lfloor \frac{d-1}{a+b} \right\rfloor, q-1\right\}\right\}$ kümesinde kesinlikle artan bir fonksiyondur. Bu yüzden, $\tilde{L}$'nin minimum değeri $\ell = 0$ durumunda elde edilir.

2. Eğer $a(q-1) < d$ ise, $\ell = \alpha_2 \geq 0$'dır. $\tilde{L}$ fonksiyonu, Lemma 4.2.24 (2)'de verilmiştir. Bu nedenle, Lemma 4.2.25'a göre sadece $\tilde{L}(\ell) = q - \ell$ ile

$$\tilde{L}(\ell+1) = (q-\ell-1)\left(q - \left\lfloor \frac{d-1-b(\ell+1)}{a} \right\rfloor\right)$$

ifadelerini karşılaştırmamız gerekir.

Tanım gereği, $\ell \leq \frac{d-1-a(q-1)}{b} < \ell+1$ olduğundan,

$$\left\lfloor \frac{d-1-b(\ell+1)}{a} \right\rfloor < q-1$$

olduğu kolayca kontrol edilebilir, bu yüzden $\tilde{L}(\ell+1) > q-\ell-1$'dir.

Sonuç olarak, $\tilde{L}(\ell+1) - \tilde{L}(\ell) \geq (q-\ell) - (q-\ell) = 0$. Bu durumda minimum değer her zaman $\tilde{L}(\ell)$ değerinde elde edilir, dolayısıyla kanıt tamamlanır. □

Şimdi ise Lemma 4.2.16 tarafından sağlanan alt sınırın tam olarak $\tilde{L}(\ell)$ olduğunu, diğer yandan $\tilde{L}$'nin minimum değeri olan $\tilde{L}(\ell)$ ile $b \mid d$ iken $d < bq$ olduğu durumdaki $L(0, d/b)$ değerini karşılaştırarak göstereceğiz.

Fakat öncesinde $a = b = 1$ olduğu durumu ele alıp bir uyarı ile bu duruma karşılık gelen minimum uzaklık verilecektir.

Uyarı 4.2.27. Eğer $a = b = 1$ ise,

$$\tilde{L}(0) = q(q-d+1) \geq q(q-d) + q - (d-1) = L\left(0, \frac{d}{b}\right),$$

olduğundan dolayı, bu durum $d_{\min}(C_{d,Y}) = \tilde{L}(0) = q(q-d+1)$ olmasına karşılık gelir. Bu durumda, Lemma 4.2.16'in sağladığı sınır kesin değildir.

Ancak, bu sorun projektif düzlem $\mathbb{P}^2$'nin 3-geçişli yapısı kullanılarak aşılabilir. Bir başka deyişle, eğer bir projektif düzlem, noktalar üzerinde geçişli bir otomorfizm grubuna izin veriyorsa geçişlidir. Projektif düzlemlerin geçişliliği üzerine kapsamlı araştırma için [56] makalesine bakılabilir. Öncelikle bu sorun için bu geçişlilik sayesinde literatürde **Serre Eşitsizliği** olarak da bilinen önermeye bakacağız.

Öncesinde bazı notasyonları verelim. İlk olarak, [18] makalesinde tanımlandığı gibi r boyutlu projektif uzayın $\mathbb{F}_q$-rasyonel noktalar kümesinin eleman sayısını p_r notasyonu ile gösterelim, yani, $p_r = |\mathbb{P}^r(\mathbb{F}_q)| = q^r + q^{r-1} + \cdots + 1$ olsun.

Önerme 4.2.28. *[47, Proposition 4.2] (Serre Eşitsizliği) $F \in \mathbb{F}_q[x_0, \ldots, x_m]$, sıfırdan farklı derecesi $d \leq q$ koşulunu sağlayan homojen bir polinom ve $V(F)$, F'nin, $\mathbb{P}^m$ m boyutlu projektif uzayı üzerindeki F_q-rasyonel sıfırlarını içeren bir hiperyüzey olmak üzere bu hiperyüzeyin eleman sayısı üzerine bir sınır aşağıdaki şekilde verilir:*

$$|V(F)| \leq dq^{m-1} + p_{m-2}.$$

Önerme 4.2.28 ile verilen Serre eşitsizliğinden, $F \in \mathbb{F}_q[x_0, x_1, x_2]$ için $|V(F)| \leq qd + 1$ olduğu açıktır. Dolayısıyla buradan, $\delta = N - |V(F)| \leq q(q - d + 1)$ eşitsizliği elde edilir. Lemma 4.2.16'in verdiği sınıra göre ise $\delta \geq q(q-d+1)$ elde edileceğinden $\delta = d_{\min}(C_{d,Y}) = \tilde{L}(0) = q(q - d + 1)$ durumu elde edilir.

Şimdi, $\tilde{L}$'nin minimum değeri olan $\tilde{L}(\ell)$ ile $b \mid d$ iken ve $d < bq$ olduğu durumdaki $L(0, d/b)$ değerini karşılaştıracağız. Buradan, varsayalım ki $d < bq$ olsun.

Eğer $b \nmid d$ ise, o zaman her $\mathbf{a} \in \mathrm{Red}(d)$ için, $a_2 \leq \mu_b$ durumu ve Önerme 4.2.26, doğrudan Lemma 4.2.16 tarafından verilen alt sınırı verir.

Eğer $b \mid d$ ise, $q - \frac{d}{b} \geq 1$ olur ve Önerme 4.2.18 şunu belirtir:

$$L\left(0, \frac{d}{b}\right) = q\left(q - \frac{d}{b}\right) + \max\left\{q - \left\lfloor \frac{d-b}{ab} \right\rfloor, 1\right\}.$$

i. Eğer $d \leq a(q-1)$ ise, $\alpha_2 < 0$ ve bu yüzden $\ell = 0$ olur. Ve dolayısıyla, aşağıdaki durum geçerlidir:

$$\frac{d-b}{ab} \leq \frac{d-b}{a} \leq q - 1 \text{ ve bu yüzden } q - \left\lfloor \frac{d-b}{ab} \right\rfloor \geq 1.$$

Eğer $a \nmid d$ ise, o zaman Lemma 4.2.24 (1)'e göre,

$$\tilde{L}(0) = q\left(q - \left\lfloor \frac{d-1}{a} \right\rfloor\right) = q\left(q - \left\lfloor \frac{d}{a} \right\rfloor\right) \leq q\left(q - \frac{d}{b}\right) \leq L\left(0, \frac{d}{b}\right)$$

olur. Eğer $a \mid d$ ve $b > 1$ ise, $d_0 \geq 1$ ve $d/a - 1 = d_0 b - 1 \geq d_0 a = d/b$ için, $b \geq a+1$, $d = d_0 ab$'dir. Böylece, Lemma 4.2.24 (1)'e göre, aşağıdaki durum elde edilir:

$$\tilde{L}(0) = q\left(q - \left\lfloor \frac{d-1}{a} \right\rfloor\right) = q\left(q - \left\lfloor \frac{d}{a} \right\rfloor + 1\right) \leq q\left(q - \frac{d}{b}\right) \leq L\left(0, \frac{d}{b}\right).$$

Dolayısıyla, $a = b = 1$ olmadıkça L'nin minimumu $\tilde{L}(0) = q(q - \mu_a)$ olur.

ii. Eğer $a(q-1) < d$ ise, o zaman $\ell = \alpha_2 \geq 0$ olur. Lemma 4.2.24 (2)'ye göre, aşağıdaki durum elde edilir:

$$\tilde{L}(\ell) = q - \ell \leq q < q + 1 \leq L\left(0, \frac{d}{b}\right).$$

Bu nedenle, Lemma 4.2.16'e göre, minimum uzaklık için bir alt sınır aşağıdaki gibi verilir:

$$d_{\min}(C_{d,Y}) \geq \tilde{L}(\ell) = \begin{cases} q(q - \mu_a) & \text{eğer } d \leq a(q-1), \\ q - \ell & \text{eğer } a(q-1) < d < bq. \end{cases}$$

Bu bölümde şuana kadar yapılan tüm çalışmalar L ve $\tilde{L}$ şeklinde tanımlanan fonksiyonların minimum değeri hangi noktalar ve durumlarda aldıklarını gözlemlemek üzerine odaklanmıştır. Bu doğrultuda ağırlıklı projektif uzaya karşılık gelen çokgenin kafes noktaları baz alınarak bu noktalara göre tüm durumlar incelenmeye çalışılmıştır. Sonuç olarak, şimdi vereceğimiz bu bölümün ana teoremi olan minimum uzaklığı veren teoreme ulaşılmıştır.

Teorem 4.2.29. *$C_{d,Y}$'nin minimum uzaklığı aşağıdaki şekilde elde edilir:*

$$d_{\min}(C_{d,Y}) = \tilde{L}(\ell) = \begin{cases} q(q - \mu_a) & \textit{eğer } d \leq a(q-1), \\ q - \ell & \textit{eğer } a(q-1) < d \leq (a+b)(q-1) < bq, \\ 1 & \textit{eğer } d > (a+b)(q-1) \end{cases}$$

Kanıt. $a = b = 1$ olduğunda minimum uzaklık ve minimum ağırlıklı kod kelimeleri [14, Corollary 3.3 & Theorem 4.3] tarafından verilmiştir. Bu yüzden $b > a$ olduğunu varsayalım.

$d_{\min}(C_{d,Y}) \geq \tilde{L}(\ell)$ eşitsizliği bir önceki sonuçlardan gelmektedir. Tersini elde etmek için, her durum için $n_f = n - \tilde{L}(\ell)$ olan bir f polinomu bulmalıyız. Bu doğrultuda durumlara göre aşağıdaki polinomlar elde edilmiştir.

i. Eğer $d \leq a(q-1)$ ise, $\alpha_2 < 0$ ve $\ell = 0$ olur. Buradan,

$$f = x_0^{r+1} \prod_{y_1 \in J} (x_1 - y_1 x_0^a)$$

burada r, $d-1$'in a ile bölünmesinden kalan ve J, $|J| = \left\lfloor \frac{d-1}{a} \right\rfloor$ olan $\mathbb{F}_q$'nin herhangi bir alt kümesidir. Böylece, $\deg(f) = r+1+a|J| = d$ olur. Polinom f, $x_0 = 0$ ile $q+1$ köke ve $[1{:}y_1{:}y_2]$ formunda $q|J|$ köke sahiptir. Toplamda, $q+1+q|J| = q+1+q\left\lfloor \frac{d-1}{a} \right\rfloor$ kökü vardır. Çünkü,

$$n - n_f = q^2 + q + 1 - (q + 1 + q\left\lfloor \frac{d-1}{a} \right\rfloor) = q\left(q - \left\lfloor \frac{d-1}{a} \right\rfloor\right) = \tilde{L}(0)$$

olur ve böylece minimum uzaklık $\tilde{L}(0) = q(q - \mu_a)$.

ii. Eğer $a(q-1) < d \leq a(q-1) + b$, o zaman $\ell = \alpha_2 = 0$ olur. Buradan,

$$f = x_0^{d-(q-1)a} \prod_{y_1 \in \mathbb{F}_q^*} (x_1 - y_1 x_0^a)$$

$x_0 = 0$ ile $(q+1)$ köke ve $[1 : y_1 : y_2]$ formunda $(q-1)q$ köke sahiptir. Toplamda, q^2+1 kökü vardır. Böylece, $n - n_f = q^2 + q + 1 - (q^2+1) = q = \tilde{L}(0)$. Dolayısıyla, minimum uzaklık $\tilde{L}(0) = q$.

iii. Eğer $a(q-1) + b < d \leq (a+b)(q-1)$ ise, o zaman $d - 1 - a(q-1) = \ell b + r$ ve $\ell = \alpha_2 \geq 1$ ve $0 \leq r < b$ olur. J' $\mathbb{F}_q$'nin herhangi bir alt kümesi olup $|J'| = \ell$ ise,

$$f = x_0^{r+1} \prod_{y_1 \in \mathbb{F}_q^*} (x_1 - y_1 x_0^a) \prod_{y_2 \in J'} (x_2 - y_2 x_0^b)$$

derecesi $d = r + 1 + (q-1)a + \ell b$ ve $n_f = q^2 + \ell + 1$ olan bir polinomdur, çünkü f, $x_0 = 0$ ile $q+1$ köke, $[1 : y_1 : y_2]$ formunda $y_2 \in \mathbb{F}_q \setminus J'$ ve $q\ell$ köke ve $[1 : y_1 : y_2]$

formunda $y_2 \in J'$ köklere sahiptir. Böylece,

$$d_{\min}(C_{d,Y}) = q^2 + q + 1 - (q^2 + \ell + 1) = q - \ell = \tilde{L}(\ell).$$

iv. Eğer $(a+b)(q-1) < d < bq$, o zaman $\ell = q - 1$ olur. Buradan,

$$f = x_0^{d-(q-1)(a+b)} \prod_{y_1 \in \mathbb{F}_q^*} (x_1 - y_1 x_0^a) \prod_{y_2 \in \mathbb{F}_q^*} (x_2 - y_2 x_0^b) \in S_d$$

polinomu $x_0 = 0$ ile $q+1$ köke, $[1{:}y_1{:}y_2]$ formunda $(q-1)q$ köke ve $[1{:}0{:}y_2]$ formunda $(q-1)$ köke sahip olup toplamda $q^2 + q$ köke sahiptir. Bu, $ev_Y(f)$ kod sözcüğünün ağırlığının $\tilde{L}(\ell) = 1$ olduğunu gösterir.

□

4.2.4 Kodların Parametreleri için Örnekler

Bu son bölümde örnek olması açısından ağırlığı belli bir uzaya karşılık gelen kodların tüm parametrelerini vereceğiz. Burada düzenlilik kümesinin tanımından dolayı kodun boyutunun maksimum değere ulaştığı d derecesi kırmızı renk ile gösterilmiştir.

Tablo 4.4 $Y = \mathbb{P}(1,2,3)(\mathbb{F}_3)$ üzerindeki kodların temel parametreleri

q	a	b	Derece (d)	Uzunluk (N)	Boyut (K)	Minimum Uzaklık (δ)
3	2	3	2	13	2	9
3	2	3	3	13	3	6
3	2	3	4	13	4	6
3	2	3	5	13	5	3
3	2	3	6	13	7	3
3	2	3	7	13	7	3
3	2	3	8	13	9	2
3	2	3	9	13	10	1
3	2	3	10	13	10	2
3	2	3	11	13	11	1
3	2	3	12	13	12	1
3	2	3	13	13	11	1
3	2	3	14	13	12	1
3	2	3	15	13	12	1
3	2	3	16	13	12	1
3	2	3	17	13	11	1
3	2	3	18	13	13	1

Tablo 4.5 $Y = \mathbb{P}(1,2,7)(\mathbb{F}_3)$ üzerindeki kodların temel parametreleri

q	a	b	Derece (d)	Uzunluk (N)	Boyut (K)	Minimum Uzaklık (δ)
3	2	7	2	13	2	9
3	2	7	3	13	2	6
3	2	7	4	13	3	6
3	2	7	5	13	3	3
3	2	7	6	13	4	3
3	2	7	7	13	4	3
3	2	7	8	13	5	3
3	2	7	9	13	5	3
3	2	7	10	13	6	3
3	2	7	11	13	6	3
3	2	7	12	13	7	2
3	2	7	13	13	7	2
3	2	7	14	13	8	2
3	2	7	15	13	8	2
3	2	7	16	13	9	2
3	2	7	17	13	9	2
3	2	7	18	13	10	2
3	2	7	19	13	10	1
3	2	7	20	13	11	1
3	2	7	21	13	11	1
3	2	7	22	13	11	1
3	2	7	23	13	11	1
3	2	7	24	13	11	1
3	2	7	25	13	11	1
3	2	7	26	13	11	1
3	2	7	27	13	11	1
3	2	7	28	13	12	1
3	2	7	29	13	11	1
3	2	7	30	13	12	1
3	2	7	31	13	11	1
3	2	7	32	13	12	1
3	2	7	33	13	11	1
3	2	7	34	13	12	1
3	2	7	35	13	11	1
3	2	7	36	13	12	1
3	2	7	37	13	11	1
3	2	7	38	13	12	1
3	2	7	39	13	11	1
3	2	7	40	13	12	1
3	2	7	41	13	11	1
3	2	7	42	13	13	1

5. SONUÇ VE ÖNERİLER

Bu tez çalışmasında literatürde Ağırlıklı Projektif Reed-Muller Kodları (kısaca WPRM kodları) olarak bilinen kod ailelerinin $X = \mathbb{P}(1, a, b)$ ve $X = \mathbb{P}(1, 1, b)$ ağırlıklı projektif uzaylarına karşılık gelen sınıfları çalışılmıştır. Bu tez çalışmasının ilk hedefi doğrultusunda $a = 1$ durumu ile çalışmalara başlanmış olup, bu uzayın cebirsel değişmezleri (algebraic invariants) olarak adlandırılan sıfırlayan ideali (vanishing ideal), dereceli minimal serbest çözülümü (graded minimal free resolution), Hilbert serisi ve fonksiyonu elde edilmiştir. Ek olarak, bir başka cebirsel değişmez olan düzenlilik kümesi de elde edilmiştir. Ayrıca $a \geq 1$ olduğu durumda yani $X = \mathbb{P}(1, a, b)$ ve $Y = X(\mathbb{F}_q)$ olduğu durumda da cebirsel değişmezlerle ilgili sonuçlar elde edilmiştir. Cebirsel değişmezler ile kodların temel parametreleri arasındaki ilişki literatürde bilinmektedir. Bu ilişki tanıtılarak, cebirsel değişmezlerle ilgili elde edilen sonuçlar doğrultusunda kodun yapısı anlaşılmaya çalışılmıştır. İlk olarak, $Y = X(\mathbb{F}_q)$ rasyonel noktalar kümesindeki noktaların sıfır olduğu polinomların bir kümesi olan sıfırlayan ideal $I(Y)$'nin dereceli minimal serbest çözülümünün formu elde edilmiş ve bu ispatlanmıştır, [1, Theorem 3.2]. Buradan, serbest çözülümler ve Hilbert serileri arasındaki ilişki kullanılarak Y kümesinin Hilbert serisi ve dolayısıyla Hilbert fonksiyonu elde edilmiştir, [1, Proposition 3.3, Corollary 3.4, Theorem 3.5, Theorem 3.6]. Hesaplama dönüşümü (bknz. (27)) olarak adlandırılan dönüşümün görüntüsü olarak elde edilen hesaplama kodlarından biri olan ve bu tez çalışmasında ele alınan WPRM kodlarının boyutu, dönüşümün tanımından dolayı Hilbert fonksiyonu vasıtasıyla hesaplanabilirdir. Bu bilgi doğrultusunda, Y kümesinin Hilbert fonksiyonunun değerlerini veren sonuçlar aynı zamanda kodun boyutunu da elde etmemizi sağlamıştır, [1, Corollary 3.7, 3.8]. Ayrıca, literatürde kullanılan başka bir yöntem kullanılarak S_d/I_d koordinat halkasının bazı bulunmuş ve bu kümelerin boyutları hesaplanarak bu uzaya karşılık gelen kodların boyutları farklı bir yöntemle de hesaplanmıştır, [1, Theorem 3.10, Corollary 3.11]. Bir başka önemli cebirsel değişmez olan düzenlilik kümesi de hesaplanarak Hilbert fonksiyonunun maksimum değere ulaştığı, bir başka deyişle, $H_Y(d) = |Y|$ olduğu d derecelerinin kümesi elde edilmiştir. Bu küme ilk olarak [1] makalesinde sadece $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$ durumu için elde edilmiştir. Bu kümedeki d derecelerinde kod maksimum boyuta ulaşacağından bu kodların minimum uzaklığı 1 değerindedir ve aşikâr (trivial) kodlar olarak adlandırılır. Dolayısıyla, bu küme bize aşikâr kodları elemek için referans olacaktır, [1, Corollary 3.12]. Ek olarak, literatürde Hilbert yarı-polinomu (Hilbert quasi-polynomial) olarak bilinen Hilbert fonksiyonunun bir yerden sonraki bazı

d derecelerinde aldığı değerlerin belirli bir düzenlilik gösterdiğini de aktaran polinomlarla ilgili olarak da $Y = \mathbb{P}(1,1,b)(\mathbb{F}_q)$ kümesi için sonuç verilmiştir, [1, Corollary 3.15]. $Y = \mathbb{P}(1,1,b)(\mathbb{F}_q)$ kümesinin Hilbert fonksiyonlarının değerlerini anlamak ve hesaplamak için yapılan örnekler doğrultusundaki gözlemlerde dikkat çeken durumlardan biri; Hilbert fonksiyonunun maksimum değere ulaştığı ilk d derecesinden sonra belirli bir düzenlilik gösterdiğidir. Yarı-polinomlarla ilgili verilen sonuç doğrultusunda bu durum net bir şekilde ifade edilmiş ve bu düzenli yapı gösterilmiştir. Ayrıca, bu uzaya karşılık gelen kodların parametrelerinden minimum uzaklık da formülize edilip sunulmuştur, [1, Theorem 4.1]. Tüm bu çalışmaları destekleyecek şekilde örnekler *Macaulay2* [44] ve *SageMath* [45] gibi cebirsel hesaplama programları kullanılarak tablolaştırılmış ve bu tez çalışmasında sunulmuştur. Böylece bu tez çalışmasının başlangıcındaki planlanan hedeflerden ilki başarıyla tamamlanmış olup, tüm bu çalışmaların bir genellemesi olacak nitelikte $a > 1$ durumu da ele alınarak farklı yöntemler ve bakış açılarıyla bu durum için de sonuçlar elde edilmiştir. Bu sebeple bu tez çalışması **Kısım I** (bknz. Kısımlar (3.), (3.2)) ve **Kısım II** (bknz. Kısımlar (4.),(4.2)) şeklinde iki ayrı kısıma ayrılmıştır. Şuana kadar anlattığımız çalışmalar tezin ilk kısmını oluşturmakla birlikte şimdi ise ikinci kısımda yaptığımız çalışmalar doğrultusunda elde edilenler açıklanacaktır. **Kısım II.** adı altında verilen çalışmalarda $a \leq b$ aralarında asal iki pozitif tam sayılar olmak üzere, $X = \mathbb{P}(1,a,b)$ ağırlıklı projektif uzayı ile ilişkili kod aileleri ele alınmış olup, diğer kısımdaki sonuçlarda izlenen yöntemlerden farklı olarak geometrik ve kombinatorik bakış açısı dikkate alınmıştır. $Y = X(\mathbb{F}_q)$ bu uzayın $\mathbb{F}_q$-rasyonel noktalar kümesi olmak üzere, bu uzayın sıfırlayan idealinin evrensel Gröbner bazı ve Graver bazı olduğu gösterilmiştir, [2, Theorem 2.4]. Bu doğrultuda bu tez çalışmasında Gröbner baz, evrensel Gröbner baz, Graver baz tanımları ele alınmıştır. Y kümesine karşılık gelen $C_{d,Y}$ kodunun boyutu, uzaya karşılık gelen P_D kafes çokgeninin rasyonel noktalarının sayısı ile bu kodun bazı arasındaki ilişki kullanılarak elde edilmiştir. Bu doğrultuda öncelikle projektif indirgeme kavramı göz önünde bulundurulmuş bu uzaya karşılık gelen çokgenlerin projektif indirgeme kümesi elde edilmiştir, [2, Theorem 2.7]. Böylece, kodun bazı hesaplanırken bu çokgenlerin rasyonel noktalarından hangilerini göz önünde bulundurmamız gerektiği konusunda bu küme referans alınmaktadır. Bu doğrultuda dikkate aldığımız uzayla ilişkili çokgenlerin rasyonel noktalarının detaylı analizleri yapılarak bazı kümeler tanımlanmış, bu kümelerin eleman sayıları hesaplanmıştır. Bu hesaplamalarda ihtiyacımız olan kavramlardan nümerik yarıgruplarla da ilişkisi olan önemli bir kavram, denumerant kavramı da bu çalışmalarda göz önünde bulundurulmuş ve tez çalışmasında tanıtılmıştır. Böylece, $C_{d,Y}$ kodunun boyutu geometrik bir yöntemle elde edilmiş olup,

bunun bir sonucu olarak $a = 1$ durumu için de kodun boyutu farklı bir yöntemle tekrar ispatlanmıştır, [2, Theorem 2.12, Corollary 2.13]. Önceki kısımda ele aldığımız önemli cebirsel değişmezlerden biri olan düzenlilik kümesi,$Y = X(\mathbb{P}(1, a, b)(\mathbb{F}_q)$ kümesi için de elde edilmiş olup, hem aşikâr kodları eleyebilmek hem de minimum uzaklık kavramının hesaplanmasında d dereceleri hakkında fikir vermesinden dolayı önemli bir kavram bu uzay için de elde edilmiştir, [2, Theorem 3.4]. Son olarak, temel parametrelerden minimum uzaklık ile ilgili çalışmalar yapılmış olup bu kısımda literatürde ayakizi sınırı (footprint bound) olarak bilinen temeli Gröbner baz teorisine dayanan bir sınır kullanılarak minimum uzaklığa bir sınır verilmeye çalışılmıştır. Bu doğrultuda, bu teori, çalışmalarda ele aldığımız uzaya uygulanarak bu uzaya karşılık gelen kodun minimum uzaklığına alt sınır elde edilmiştir, [2, Lemma 4.5]. Bu alt sınır daha önce bahsettiğimiz projektif indirgeme kümesindeki noktalara ve düzenlilik kümesindeki $\tilde{d}$ derecelerine bağlı olarak elde edilmiştir. Verilen alt sınır ayakizi sınırının ana fikrine dayanarak elde edilmiş bir küme ile verilmiştir. Ve dolayısıyla bu kümenin eleman sayısı elde edilerek minimum uzaklık için alt sınırın değerleri hesaplanmıştır. Bu hesaplamalarda her durum ayrıntılı bir şekilde ele alınmış olup, çokgenlerin kafes noktalarına da bakılarak minimum uzaklığa sınır verebilmek için tanımlanan fonksiyonların hangi noktalarda minimum değer aldığı incelenmiştir, [2, Section 4.2]. Böylece d derecelerinin durumlarına göre minimum uzaklık için bir alt sınır elde edilmiş olup, minimum kod kelimeleri için minimum uzaklığı veren tam kök sayısına sahip olan d dereceli homojen polinomlar da elde edilerek bu sınırın minimum uzaklığı tam olarak verdiği de gösterilmiştir, [2, Section 4.3, Theorem 4.18].

Sonuç olarak, bu tez çalışması boyunca $X = \mathbb{P}(1, a, b)$ ve $Y = X(\mathbb{F}_q)$ olmak üzere bu uzaya karşılık gelen $C_{d,Y}$ ağırlıklı projektif Reed-Muller kod ailelerinin (WPRM) temel parametreleri hesaplanmış olup, bu doğrultuda cebirsel değişmezlerle ilgili de sonuçlar verilerek bu detaylı çalışmalar ve incelemeler doğrultusunda kod ailesinin yapısı anlaşılmıştır. Bu tez çalışmasının sonucunda farklı durum, gözlemler ve yöntemler doğrultusunda iki ayrı makale çıktısı elde edilmiştir, [1], [2]. Bu tez çalışmasında kullanılan tüm figürler Latex programındaki Tikz paketi kullanılarak elde edilmiş olup, benzer şekilde tablolarla sunulan farklı kod ailelerinin parametreleri de SageMath ve Macaulay2 programı vasıtasıyla elde edilmiştir. Bu çalışma doğrultusunda, kullanılan fikir ve yöntemlerin daha genel durumlara da uygulanabileceği öngörülmektedir. Bu sonuçlar doğrultusunda üzerinde durulan kod ailelerinin yapıları anlaşıldığından dolayı bu kod ailelerine çalışma noktasında da fikir oluşturduğu düşüncesinden hareketle literatüre bu anlamda da bir katkı sağlandığı düşünülmektedir.