T.C.
NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI SONLU CİSİMLER ÜZERİNDE ESNEK POLİNOM KODLAR

Tezi Hazırlayan
Şerif ÖZLÜ

Tez Danışmanı
Doç. Dr. Hacı AKTAŞ

Matematik Anabilim Dalı
Doktora Tezi

Nisan 2015
NEVŞEHİR

T.C.
NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI SONLU CİSİMLER ÜZERİNDE ESNEK POLİNOM KODLAR

Tezi Hazırlayan
Şerif ÖZLÜ

Tez Danışmanı
Doç. Dr. Hacı AKTAŞ

Matematik Anabilim Dalı
Doktora Tezi

Nisan 2015
NEVŞEHİR

Doç. Dr. Hacı AKTAŞ danışmanlığında **Şerif ÖZLÜ** tarafından hazırlanan **"Bazı Sonlu Cisimler Üzerinde Esnek Polinom Kodlar"** başlıklı bu çalışma, jürimiz tarafından Nevşehir Hacı Bektaş Veli Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalında **Doktora Tezi** olarak kabul edilmiştir.

27/04/2015

JÜRİ

Başkan : (Doç. Dr. Necdet BATIR) imza

Üye : (Doç. Dr. Hacı AKTAŞ) imza

Üye : (Doç. Dr. Sezer SORGUN) imza

Üye : (Doç. Dr. Aytekin ERYILMAZ) imza

Üye : (Yard. Doç. Dr. Tufan Sait KUZPINARI) imza

ONAY:

Bu tezin kabulü Enstitü Yönetim Kurulunun 28.04.2015 tarih ve 2015/2004 sayılı kararı ile onaylanmıştır.

28/4/2015

Doç. Dr. Şahlan ÖZTÜRK

Enstitü Müdürü

TEZ BİLDİRİM SAYFASI

Tez yazım kurallarına uygun olarak hazırlanan bu çalışmada yer alan bütün bilgilerin bilimsel ve akademik kurallar çerçevesinde elde edilerek sunulduğunu ve bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Şerif ÖZLÜ

TEŞEKKÜR

Desteği, bilgisi ve tecrübesi ile bana yol gösteren saygı değer danışmanım Doç. Dr. Hacı AKTAŞ'a, hayat boyu üzerime titreyen ve beni bugünlere getiren aileme ve tüm sevdiklerime sonsuz teşekkürlerimi sunarım.

BAZI SONLU CİSİMLER ÜZERİNDE ESNEK POLİNOM KODLAR
(Doktora Tezi)

Şerif ÖZLÜ

NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Nisan 2015

ÖZET

Bu tezin amacı, esnek kümeler kullanılarak devirli esnek gruplar inşa etmek ve bu gruplarla devirli esnek kodlar tanımlamaktır.

Birinci bölümde, esnek kümeler ve kodlama teorisinin tarihçesi, gelişim aşamaları, bu kavramlara duyulan ihtiyaç ve günümüzde bu kavramların ulaştığı noktalar ifade edilmiştir.

İkinci bölümde, kodlama teorisi üzerine geniş bir literatür taraması yapılmış ve kodlama teorisine ait temel özellikler verilmiştir.

Üçüncü bölümde, esnek kümelerle ilgili geniş bir literatür çalışması yapılmış ve esnek kümelerler üzerinde yapılan teorik ve pratik çalışmalardan söz edilmiştir. Ayrıca esnek kümelerin temel özelliklerine yer verilmiştir.

Dördüncü bölümde, esnek kümelerin mertebesi, devirli esnek gruplar ve bu grupların cebirsel özellikleri çalışılmıştır. Aynı bölümde devirli esnek kodlar inşa edilmiş ve devirli esnek kodların tanımı kullanılarak yeni bir üreteç matrisi elde edilmiştir. Bu matrisin hamming kodlarla olan ilişkisine değinilmiştir.

Beşinci bölümde ise esnek kümeler üzerinde vektörel çarpım tanımlanmış ve bu çarpım kullanılarak lineer olmayan kodlar elde edilmiştir. Ayrıca bu metot için kodlama ve kod çözme algoritması geliştirilmiştir.

Anahtar kelimeler: Esnek küme, esnek kümelerde mertebe, esnek devirli gruplar, kodlama teorisi, esnek devirli kodlar, esnek kodlama, esnek kod çözme.
Tez Danışman: Doç. Dr. Hacı AKTAŞ
Sayfa Adeti: 70

SOFT POLYNOMIAL CODES OVER SOME FINITE FIELDS
(Ph. D. Thesis)

Şerif ÖZLÜ

NEVŞEHİR HACI BEKTAŞ VELİ UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

April 2015

ABSTRACT

The purpose of this thesis, is to construct cyclic soft groups by using soft sets and to define cyclic soft codes by using these groups.

In the first section, history and progressing steps of coding theory and soft sets has been presented. In addition requriment of these concepts has been stated.

In the second section, a widely literature searching has been made about coding theory and basic properties of coding theory has been defined.

In the third section, a widely literature searching has been made and theoretical and practical studies has been mentioned about soft sets.

In the fourth section, orders of soft sets, cyclic soft groups and algebra properties of these groups has been studied. Also in this section cyclic soft codes has been constructed and anew generator matrix has been consisted of by using definition of cyclic soft codes. Hamming codes have been with these generator matrices.

In the fifth section, a new encoding method has been mentioned by using soft sets. This method creats soft encoding and error correcting algortithm.

Keywords: Soft sets, orders of Soft groups, soft cyclic groups, coding theory, soft cyclic codes, soft coding, soft decoding.
Thesis Supervisor: Assoc. Prof. Dr. Hacı AKTAŞ
Page Number: 70

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

BÖLÜM 1

GİRİŞ

Günümüzde matematik ve bilimin en önemli problemlerinden biri belirsizliktir. Ünlü fizikçi Einstein belirsizliği "Matematiğin kavramları kesin oldukları sürece gerçeği yansıtmazlar, gerçeği yansıttıkları sürece de kesin değillerdir" şeklinde ifade etmiştir. Belirsizliği matematiksel olarak ifade etmek için 1965 yılında Zadeh tarafından fuzzy (bulanık) kümeler isimli bir makale yayımlanmıştır. Klasik mantığın tanımlayamadığı belirsiz kavramların matematiksel olarak ifade edilebilmesi otomatik çamaşır makineleri, otomatik fotoğraf makineleri, buzdolapları gibi birçok otomatik makinenin çalıştırılmasında fuzzy kümeler önemli bir yer tutmaktadır.

Klasik matematikte bir A kümesi için x, A nın elemanı ise A ya aitlik derecesi 1, değilse 0 olarak belirtilir. Fuzzy kümelerinde bir elemanın kümeye aitlik derecesi 0 ile 1 arasında reel sayı değerleri alır. Yani klasik kümenin karakteristik fonksiyonu

$$\mu_A(x) = \begin{cases} 1, x \in A \\ 0, x \notin A \end{cases}$$

ile ve bir fuzzy kümesinin üyelik fonksiyonu da $A \subset X$ olmak üzere $\mu_A(x): X \to [0,1]$ fonksiyonu ile ifade edilir. Buna göre bir elemanın kümeye aitlik derecesi 0'a ne kadar yakın ise kümeye aitliği o kadar azdır, 1' e ne kadar yakın ise kümeye aitliği o kadar çoktur. $\mu_A(x)$ değerine x elemanın üyelik değeri, bu değeri ifade eden μ_A fonksiyonuna da üyelik fonksiyonu denir. Bulanık kümelerde birçok kavram üyelik fonksiyonları ile tanımlanır. Üyelik fonksiyonunun belirlenmesi bulanık kümelerinin kullanımını zorlaştıran bir durumdur. Bu yüzden 1999 yılında Molodtsov üyelik fonksiyonlarının belirlenmesi zorluğundan kurtulmak için "Soft sets theory-First results" isimli makalesini yayınlamıştır.

U boştan farklı bir küme ve $P(U)$, U 'nun kuvvet kümesi olsun. E parametrelerin kümesi, $A \subset U$ ve $F: A \to P(U)$ tanımlı fonksiyon olmak üzere (F, A) ikilisine esnek(soft) küme denir. Bir başka ifade ile esnek küme U nün parametreleştirilmiş alt ailesidir.

Molodtsov'un makalesinde daha çok esnek kümelerin matematik ve sosyal alanlarda uygulamaları verilmiştir. Ayrıca bu çalışmada her bulanık kümenin bir esnek küme olarak ifade edilebileceği yani fuzzy kümenin, esnek kümenin özel hali olduğu gösterilmiştir. Esnek kümeler üzerinde birleşim, kesişim, AND ve OR gibi küme işlemleri Maji ve arkadaşları tarafından 2003 yılında yayımlanan "soft set theory" makalesinde tanımlanmış ve bu işlemlerin çeşitli cebirsel özellikleri incelenmiştir.

Belirsizlik ifade eden diğer bir küme de yaklaşımlı kümelerdir. U evrensel küme ve R, U üzerinde bir bağıntı ve $X \subset U$ ve boştan farklı bir alt küme olsun. Bu durumda $\underline{A}(X) = \{x: [x]_R \subseteq X\}$ ve $\overline{A}[x] = \{x: [x]_R \cap X = \emptyset\}$ kümeleri sırasıyla X in alt ve üst yaklaşımıdır. Alt ve üst yaklaşımların oluşturduğu $A(X) = (\underline{A}(X), \overline{A}(X))$ ikililerin kümesi X in yaklaşım kümesidir. Yaklaşımlı küme bir alt kümeye yine kümelerle yaklaşılarak oluşturulan bir kümedir.

Sonlu cisimlerin önemli ve ilginç uygulama alanlarından biri de cebirsel kodlama teorisidir. Haberleşme sırasında oluşan bazı problemleri çözmek için ortaya çıkan yaklaşık altmış yıllık bir geçmişe sahip olan kodlama teorisinde, kısa geçmişine rağmen, önemli gelişmeler kaydedilmiştir.

Kodlama teorisini kriptoloji biliminden ayıran asıl mantık hata bulma özelliğidir." Hata bulma" cümlesinden de anlaşılabileceği gibi hatadan, parazitten dolayı bir tarafın mesajının karşı tarafa hatalı bir şekilde taşındığı görülmüştür. Hatalar her hangi bir cihazdaki hatalar, insan kaynaklı hatalar olabilir. Bu hatalar alınan iletinin hatalı olmasına yol açar. Bir hata düzeltici kodlama sisteminin amacı verilere ilave bir miktar hata düzeltme dijiti ekleyerek kodlamaktadır. İşte kodlama teorisi iletişimin hatasız bir şekilde yapılmasını amaçlayan, eğer iletişim sırasında bir gürültü oluşmuşsa bu hatanın nerde olabileceğini araştıran, bundan daha önemlisi de hatalı bir şekilde iletilen mesajdan doğru mesaj elde etmek için çok farklı teknikler geliştiren bir teoridir.

Claude Elwood Shannon, elektronik iletişim çağının önemli bilim adamlarındandır. 1948 yılında yayınladığı makale ile birlikte hala günümüzde bilgi iletişiminin büyük bir kısmını oluşturmaktadır. Bu makale 20. yüzyılın büyük başarılarından biri olarak sayılmaktadır. Claude Elwood Shannon, hamming kodlara benzer bir yöntemle kodlama gerçekleştirmiştir.

Hata doğrulama kod teorisi 1948 yılında Claude Shannon'un [1] "A Mathematical Theory of Communication" makalesi ile birlikte cebirsel yapıları içeren matematiksel teorilerde kullanılmaya başlanmıştır. 1948 yılında ortaya atılan bu teori günümüzde birçok bilgisayar sisteminin yapısında iletişim araçlarında kullanılmaya çalışılmıştır. Bir gürültülü kanal üzerinde bilginin daha güvenilir iletimi için yapılan kodlama ve kod çözme teknikleri bugün hayatımızda çok büyük önem teşkil etmektedir.

Gilbert, n uzunlukta ki bir kod için bir minimum uzaklık belirlemiş ve bu konu ile ilgili çeşitli metotlar ortaya sürmüştür. Bu metotlar Gilbert- Varshamov sınırları olarak bilinir. Bu sayede ise devirli kodlar üretilmiştir.

Bell laboratuarlarında çalışan Hamming çalıştığı makinelerde bir hata oluştuğu durumda bu hatanın nasıl tespit edileceği konusunda bazı yöntemler ortaya atmıştır. Hamming, bu yöntemler sayesinde oluşan hatayı tek hataya kadar tespit etmiştir. Böylece Hamming tarafından isimi verilen, bu gün halen kullanılmakta olan "Hamming kodlama" yöntemi açıklanmıştır.

Hamming kodlama sistemi iletişimde kullanılan bir çeşit doğrusal hatanın var olup olmaması durumunu kontrol ve düzeltme yöntemidir. Golay, Hamming kodların gelişimine yardım etmek için bazı çalışmalar yapmıştır. Bu sayede Golay kodlar elde edilmiştir.

Bu tezde bilginin iletimi konusunda önemli bir yere sahip olan kodlama teorisinin esnek kümelerle olan ilişkisine değinilmiştir. Bu kapsamda 4 bölüm oluşturulmuş ilk bölümde kodlama teorisinin temel tanım ve teoremlerinden, gelişim aşamalarından ve çeşitli cebirsel yapılar üzerindeki uygulamalarından bahsedilmiştir. Ayrıca bu bölüm de kodlama teorisinin günümüzdeki uygulamalarından, kodlamanın temel mantığı olan hata bulma algoritmasından ve tezde yer alan kodlama ve kod çözme mantığının nasıl olacağı konusunda çeşitli bilgiler verilmiştir. Kodlama üzerinde önem teşkil eden ağırlık, minimum uzaklık gibi çok önemli tanımlar ve bu tanımların hata bulma yapıları ile olan ilişkilerinden bahsedilmiştir. Buna ilaveten Hamming kodlardan özellikle genişletilmiş hamming kodundan ve bu kod çeşidinin tanımından, hata bulma algoritmasından da bahsedilmiş ve bu kod çeşidinin üreteç matrisi ve parity kontrol matrisinin nasıl üretileceği örneklerle gösterilmiştir. İkinci bölümde ise kümeler

teorisinde bulanık kümeler ve yaklaşımlı kümelerden sonra tanımlanan ve bağımsızlık ifade eden esnek küme kavramından, esnek kümeler üzerine kurulan cebirsel yapılardan ve bunların bazı özelliklerinden bahsedilmiştir. Esnek küme teorisi günümüzde eğitim alanında, oyun teoride ve daha birçok alanda kullanım alanı bulmuştur. Bu teorinin uygulamaları işlevsel araştırmalarda ve oyun teoride detaylı bir şekilde tartışılmıştır. Zamanla grup teori üzerine genişleyen esnek küme teorisi üzerinde tanımlanmış olan kartezyen çarpım, birleşim ve kesişim gibi temel tanım ve teoremler bu bölümde açıklanmıştır. Ayrıca bu tanımlarla ilgili çeşitli teoremler ve önermeler verilmiştir. Üçüncü bölümde ise esnek kümelerin kodlarla olan ilişkisi incelenmiştir. Bu bölümün en temel özelliği esnek grupların mertebeleri önemi ölçüde açıklanmış ve bu mertebelerin esnek kümeler üzerindeki kartezyen çarpım, birleşim ve kesişim tanımları üzerinde nasıl uygulanacağı konusunda çeşitli tanım ve teoremler verilerek, mertebe tanımı esnek kümeler üzerinde incelenmiştir. Ayrıca bu bölümde esnek devirli gruplar tanımlanmış olup bu esnek devirli grupların çeşitli özellikleri verilmiştir.

Bu bölümde elde edilen sonuçlar 2014 yılında *Scientific World Journal* adlı dergide yayınlanmıştır [45].

Aynı bölümün devamı olan üçüncü kısmında ise devirli esnek kod kümeleri tanımlanmış bu kümelerin temel bazı özellikleri incelenmiş ve çeşitli cebirsel özelliklerine çalışılmıştır. Öncelikle bu kısımda esnek devirli kodlar tanımlanmış ve bu yapının çeşitli cebirsel özellikleri araştırılarak sonuçlar elde edilmiştir. Devirli esnek kodlar kullanılarak elde edilen idempotent polinom yapılarının esnek kümeler üzerindeki uygulamaları incelenmiş ve bu yapı sayesinde esnek devirli kod yapılarının üreteç polinomu kümesi olan A kümesinin elemanlarının nasıl üretileceğine dair bilgiler verilmiştir. Esnek devirli kodların ortogonalliğine bakılmış ve bu tanım sayesinde iki esnek kümenin dikliğine dair bir teorem ve örnek verilmiştir.

Kodlama teorisinde üreteç matrisi, üreteç polinomu kod üretmek için önemli kavramlardır. Bir sonraki alt başlıkta esnek devirli kodların tanımları kullanılarak kodlamanın temel mantığı olan üreteç küme yapısı sayesinde elde edilen esnek devirli kodların üreteç kümeleri yeni bir tanımla bir araya getirilerek bir üreteç kümesi elde edilmiştir. Esnek devirli kodların üreteç tanım kullanılarak mevcut kodlardan olan Hamming kodların nasıl üretileceğine dair tanım ve teoremler verilmiştir. Yeni bir üreteç kümesine sahip olan esnek devirli kodların üreteç kümesi farklı bir kod

ürettiğinden bu kodun uzunluğu, tabanındaki eleman sayısı, minimum uzaklığı nasıl olması gerektiği teoremlerle ifade edilmiştir. Özellikle minimum uzaklığın ağırlıkla olan ilişkisine değinilmiş esnek devirli kodlar üzerinde minimum uzaklık ve ağırlık arasındaki ilişki incelenmiştir. Beşinci bölümde ise $(n/2)-1$ den daha az veya eşit sayıda olan tek sayılarda hata düzeltebilen bir kodlama yöntemi geliştirilmiştir. Bu yöntemin üzerine bir kod çözme metodu oluşturulmuştur. Kodlama teorisini kriptoloji biliminden ayıran özelliği olan hata bulma algoritması bu metot üzerine kurulmuştur. Bu metodun işlerliğini göstermek için bölümün temelini oluşturan vektörel çarpımın çeşitli özelliklerini anlatan temel iki teorem tanımlanmış olup bu sayede hata bulma algoritmasının nasıl olacağı konusunda da çeşitli bilgiler verilmiştir. Bu teoremler sayesinde hata bulma algoritması inşa edilmiş ve son olarak da bu algoritmanın çalıştığını gösteren bir örnek verilmiştir. Makalede tanımlanan bu vektörel çarpımın sonucu oluşan esnek kodların herhangi bir elemanının üzerinde oluşan $(n/2)-1$ den daha az veya eşit sayıda oluşan hata yapısının nasıl çözüleceği konusunda algoritmanın her adımı işlenerek öncelikle hatalı kod kelimesi belirlenmiş arkasından hatalı kod kelimesinin hatalı dijitlerinin doğrusu bulunarak hatalı kod kelimesine eklenmiş ve hata yapısı düzeltilmiştir. *Journal of New Theory* adlı bir dergide yayınlanan bu sonuçlar esnek kümelerin çeşitli özelliklerini de içermektedir. Esnek kümelerin en temel özellikleri olan birleşim, tümeyen ve değili özellikleri de sağlatılmış ve bu özelliklerin üzerine çeşitli teoremler ve önermeler ifade edilmiştir.

BÖLÜM 2

KODLAMA TEORİSİNE GİRİŞ

2.1.Giriş

Sonlu cisimlerin önemli ve ilginç uygulama alanlarından biri de cebirsel kodlama teorisidir. Haberleşme sırasında oluşan bazı problemleri çözmek için ortaya çıkan yaklaşık altmış yıllık bir geçmişe sahip olan kodlama teorisinde, kısa geçmişine rağmen, önemli gelişmeler kaydedilmiştir.

Kodlama teorisinin asıl amacı olan hatasız iletişimdir.“ Hatasız iletişim” ifadesinden de anlaşılabileceği gibi hatadan, parazitten dolayı bir tarafın mesajının karşı tarafa hatalı bir şekilde ulaşabildiği görülmüştür. İşte kodlama teorisi iletişimin hatasız bir şekilde yapılmasını amaçlar. Eğer iletişim sırasında bir gürültü oluşmuşsa bu hatanın nerde olabileceğini araştırır. Bundan daha önemlisi de hatalı bir şekilde iletilen mesajdan doğru mesaj elde etmek için çok farklı teknikler geliştiren bir teoridir. Kodlama teorisi’nin önemli bir teori olduğunu anlamak için şu örneğe bakılabilir. Örneğin bir uzay aracı dünyadan jüpitere gönderilsin. Uzay aracının jüpitere indiği 1 ile aksi takdirde 0 ile kodlansın. Uzay aracına eğer 1 yerine 0 yollanırsa olabilecek hatanın verdiği zararı telafi edilemeyeceği görülür. Bu örnekle birlikte kodlama teorisi’nin gerekliliği daha iyi anlaşılmış olur.

Bilgi kavramı ile uğraşan, bilgiyi ölçmeye çalışan ve kullanım alanlarını inceleyen bilim alanına *bilgi teorisi* denilebilir.

Genel bakış açısıyla, bilgi kavramı 3’e ayrılır:

1. Sözdizimsel Bilgi: Mesajları oluşturan semboller ve bu sembollerin arasındaki ilişkileri ile alakalıdır.
2. Anlamsal Bilgi: Mesajların ne anlama geldiği ile ilgilenir.
3. İşlevsel Bilgi: Mesajların nasıl kullanıldığı ve etkileri üzerinedir.

Harry Nyquist 1924 yılında "Certain Factors Affecting Telegraph Speed" adlı makalesi ile telgraf üzerinden maksimum hızda ve bozulma olmadan mesaj göndermenin yolunu açıkladı. Kullanılan devreye göre iletişim kanalının limitlerinin var olduğundan bahsetti. Kullanılan devreye göre iletişim kanalının limitlerinin oluşması durumunda oluşan sınırlılıkların nasıl giderileceğine dair bir teori geliştiremedi.

Claude Elwood Shannon, Nyquist ve Hartley'nin kuramlarını genişleterek günümüz bilgi kuramını oluşturmuştur. Bir mesajın içerisindeki belirsizliği olasılık kavramı ile ilişkilendirirek mesajın içerisindeki bilgi miktarını tanımlamıştır. Tüm karakterlerin oluşma olasılıklarının eşit olduğu varsayıldığında Hartley'nin ölçüsüne dönülmektedir. Bu sebeple Hartley'nin ölçüsü Shannon ölçüsünün özel bir durumudur denilebilir.

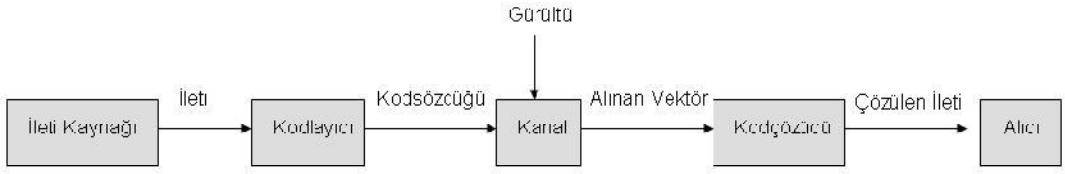
Hata doğrulama kod teorisi 1948 yılında Claude Shannon'un [1] "A Mathematical Theory of Communication" makalesi ile birlikte cebirsel yapıları içeren matematiksel teorilerde kullanılmaya başlanmıştır. 1948 yılında ortaya atılan bu teori günümüzde birçok bilgisayar sisteminin yapısında iletişim araçlarında kullanılmaya başlanmıştır. Bir gürültülü kanal üzerinde bilginin daha güvenilir iletimi için yapılan kodlama ve kod çözme teknikleri bugün hayatımızda çok büyük önem teşkil etmektedir.

1950 yılında Hamming tarafından isimini verdiği, bu gün halen kullanılmakta olan "Hamming kodlama" yöntemi açıklandı.

Hamming kodlama sistemi iletişimde kullanılan bir çeşit doğrusal hatanın var olup olmaması durumunu kontrol ve düzeltme yöntemidir. Hamming kelimesi bu yöntemi bulan kişi olan Richard Hamming'in isminden gelmektedir. Hamming kodlama yöntemi ile gönderilen mesajlardaki tek bitlik hatalar bulunup düzeltilebilir. Yine bu yöntem iki bitlik hataları da tespit edebilir fakat düzeltemez.

Kodlama teorisi sonlu bir alfabenin sonlu bir dizisinden meydana gelir. Örneğin alfabe 0, 1, 2 den meydana geliyorsa dizide 0, 1, 2 den meydana gelen bir dizidir. Bu şekildeki kod biçimine *ternary*(üçlü) *kodlar* denir. Kodlama sistemlerinde bu dizilerin aktarımları sırasında hatasız bir şekilde iletim her zaman temel amaçtır. Fakat gürültü kanalının olduğu her yerde bir şekilde hata oluşumu her zaman olma ihtimali vardır.

Bir kanal üzerinde hata olma ihtimali varsa akla şu soru gelecektir. “Hata sonlu dizinin neresinde meydana gelmiştir?” işte tam olarak bu soru karşılığını kodlama teorisin de bulmuştur. Kodlama teorisi geliştirilen yöntemler sayesinde kanal üzerinde hatanın nerde nasıl yapıldığını belirler. Aşağıda bir dijital bilgi sistemi verilerek kodlama sisteminde ki yöntemlerle kodun hatasının nasıl çözülüp kodun nasıl elde edilebileceğine dair bir şema verilmiştir.



Şekil 2.1. Dijital Bilgi Sistemi

Gürültü bu süreçteki en önemli kısımdır. Çünkü gürültü yoksa kodlama teorisine olan ihtiyaçta ortadan kalkacaktır. Gürültü, teknik bir terim olup kodlama sırasında oluşabilecek hataların tamamına denir. Gürültüye örnek olarak radyo karışıklılığına sebep olan parazitler verilebilir. Şimdi de yukarıda ki bilgi sistemini bir örnekle açıklayalım.

A, B, C, D harflerini aşağıda olduğu gibi kodlayalım. A→00, B→01, C→10, D→11 olsun. Öncelikle gürültü kanalı üzerinde 00 olarak kodlanan A yollansın. Bu gönderi üzerinde herhangi bir bozulma gerçekleşsin ve A 10 olarak alınsın. Ancak büyük olasılıkla alıcı gönderim sırasında hata olduğunu düşünmeyecek ve iletişim başarısız olacaktır. İşte böyle bir durumda sadece kaynağı kodlamak yani mesajı kodlamak yerine kanal kodlaması da yapmak hatanın var olup olmadığı konusunda bize kesin sonuçlar verecektir. Görüldüğü gibi sadece kaynak kodlaması yapmak karmaşık yapılarda oldukça zordur. Şimdi yukarıda ki kaynak kodlamaya bir basamak ekleyelim.

A→000, B→011, C→101, D→110 olsun. Daha önce yaptığımız gibi A harfini gönderelim ve bir tane hata yapalım. Buna göre alınan harf 100, 010 veya 001 sembollerinden biri olacaktır. Bu mesajın kelimelerimiz arasında olmayışı gönderilen

mesajın hatalı olduğu anlamına gelir. Fakat hatalı kod kelimesini yine bulunamaz. Şimdi her kelimeye ikişer bit daha ekleyip mesajı tekrar gönderelim.

A→00000, B→01111, C→10110, D→11001 olsun. Şimdi yine A harfini gönderelim ve gönderdiğimiz harf üzerinde herhangi bir dijitte hata yapalım. Örneğin mesaj 10000 olarak alınsın bu durumda 10000 iletisinin 00000 olduğu görülecektir. Çünkü 10000 mesajı $\{01111, 10110, 11001\}$ arasında en az iki hata vardır. Böylece aktarımın hızını azaltırken hatanın anlaşılması ve hatanın çözülmesi bakımından bir sınır var olduğunu düşünürüz. İşte kodlama teorisi tam olarak burada devreye girer ve çeşitli yöntemler kullanılarak bu hataları belirleyip çözer.

2.2. Temel Kavramlar

Kod kelimesini ve kodlama fonksiyonunu açıklamadan önce dijital bilgi sisteminde yer alan alfabe 0 ve 1 den oluştuğu için bundan sonra yapacağımız tüm çalışmalar F_2 cismi üzerinde olacaktır.

Tanım 2.2.1. [2] $F_2^n = \{a_i | i = 1, 2, \dots, n\}$ olmak üzere F_2^n kümesi üzerinde toplama işlemi "+", $a_i = a_1 a_2 \dots a_n$ ve $b_i = bb_2 \dots b_n$ olmak üzere $a_i + b_i = c_i (mod 2)$ olarak tanımlanır. Bu şekilde tanımlanan toplama işlemi F_2^n kümesinde değişmeli gruptur.

Tanım 2.2.2. [2] $F_2^n = \{a_i | i = 1, 2, \dots, n\}$ olmak üzere F_2^n kümesi üzerinde çarpma işlemi × işlemi, $a_i = a_1 a_2 \dots a_n$ ve $b_i = b_1 b_2 \dots b_n$ olmak üzere $c \in \{0, 1\}$ için şeklinde tanımlanır.

$$a_i \times b_i = a_1 b_1 + \dots + a_n b_n = c \ (mod\ 2).$$

Tanım 2.2.3. [2] $A = \{a_1 a_2 \dots a_q\}$ kümesini ele alalım. A kümesine kod alfabesi ve kümenin elemanlarına da kod sembolleri denir.

Tanım 2.2.4. [2] Aynı n uzunluğuna sahip kod kümesine blok kod denir. Bu küme C harfi ile gösterilir. C kümesinin her bir elemanına kod kelimesi denir. C kümesinin eleman sayısı $|C|$ şeklinde gösterilir. Uzunluğu n olan ve küme içinde M tane elemana sahip olan kod için (n, M) gösterimi kullanılır.

Tanım 2.2.5. [2] x ve y bir A kümesinde ki n uzunluğuna sahip iki kod kelimesi olsun. İki kod kelimesi arasında ki uzaklık (*distance*) $d(x,y)$ şeklinde gösterilir ve aşağıda ki gibi tanımlanır. $x = x_1x_2 \dots x_n$ ve $y = y_1y_2 \dots y_n$ olmak üzere

$$d(x,y) = \begin{cases} 1 & x_i \neq y_i \\ 0 & x_i = y_i \end{cases}$$

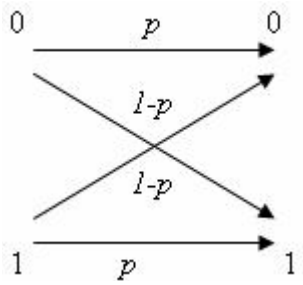
böylece $d(x,y) = d(x_1,y_1) + d(x_2,y_2) + \cdots + d(x_n,y_n)$ olur.

Tanım 2.2.6. [2] İki kod kelimesinin birbirinden farklı olan konumlarının sayısına *Hamming* uzaklık denir. *Hamming uzaklığı* $(GF(q))^n$ üzerinde bir metriktir. x ve y iki kod kelimesi olmak üzere $d(x,y)$ aşağıdaki özellikleri sağlar.

(a) $d(x,y) > 0$ olup $d(x,y) = 0 \iff x = y$,
(b) $d(x,y) = d(y,x)$,
(c) $d(x,y) + d(y,z) \geq d(x,z)$ olduğu kolayca görülür.

Hatasız bir kanalda gönderilen dijitler olduğu gibi alınır. Böylece hata düzeltme gibi bir durumla karşılaşılmaz. Aşağıda verilecek olan bir kodun hatalı alınma olasılığını göstermektedir.

İkili bir kanalda 0 ve 1 basamakları eşit olarak dizilir ise bu kanala ikili simetrik kanal denir. Aşağıda kullanılacak olan p reel sayısı $0 \leq p \leq 1$aralığında olup herhangi bir basamağın nasıl alındığını göstermektedir.



Şekil 2.2. İkili Simetrik Kanal

Bu ikili simetrik kanal için şunları söylenebilir.

(1) $p = 1$ olduğunda kanal mükemmeldir.

(2) p sayısı $\frac{1}{2} < p < 1$ arasında olduğunda kanalın incelenmesi gerektiği düşünülür. Kısacası hatasız bir şekilde gönderilme olasılığının hatalı bir şekilde gönderilme olasılığından daha büyük olduğu bir durumu teşkil eder.

Tanım 2.2.7. [3] Herhangi v ve w sözcükleri için $\Phi_p(v,w)$ sayısı v kod kelimesi p güvenirlilikle gönderildiğinde w' nın alınma olasılığını göstermek üzere $d(v,w) = d \rightarrow n - d$ tane basamaktan d tanesi hatalı iletilmiştir. Bu durumda

$$\Phi_p(v,w) = (1-p)^d p^{n-d}$$

olur. Bu yapıya *Maksimum Olabilirlik Çözümü* denir.

Tanım 2.2.8. [3] $\forall \boldsymbol{x} \in F^n$ için x kod kelimesinin ağırlığı x dizisinin sıfırdan farklı bileşenlerinin sayısıdır. Yani

$$wt(x) = \sum_{i=1}^{n} a_i$$

dır.

Teorem 2.2.9. [3] Aşağıdaki özellikler sağlanır.

(1) $d(C) \geq s + 1$ ise C kodu, s veya daha az hataya kadar belirlenebilir.
(2) $d(C) \geq 2t + 1$ ise C kodu t veya daha az hataya kadar düzeltebilir.

Önerme 2.2.10. [4] Bir C kodunda minumum uzaklık d olarak verilsin. Buna göre aşağıda ki özellikler sağlanır.

(1) En fazla $d - 1$ hata belirlenebilir.
(2) $\left\lfloor \frac{d-1}{2} \right\rfloor$ hata da düzeltilebilir.

Teorem 2.2.11. [4] C kodu p hata olasılıklı bir simetrik kanalda n uzunluklu bir kod olsun. Bu durumda alınan bir kelimede k ağırlıklı bir hata olma olasılığı $p^k(1-p)^{(n-k)}$ dır ve k ağırlıklı hata vektörlerinin toplam sayısı $\binom{n}{k} p^k (1-p)^{(n-k)}$ şeklinde bulunur.

Tanım 2.2.12. [4] Her bir kod kelimesi sadece x_1 mesaj sembollerinden oluşuyor ve geriye kalan $n-1$ tane sembol $x_2 = x_3 = \cdots = x_n$ kontrol sembollerinin hepsi x_1'e eşitse bu koda tekrarlama kodu denir.

Tanım 2.2.13. [10] C bir (n,k) kodu olsun.

(1) G, C kodu için $k \times n$ şeklinde taban elemanlarından oluşan matrisi teşkil ediyorsa G matrisine *Üreteç Matris* denir.

(2) $H, C^{\perp}$ için $(n-k) \times n$ şeklinde bir üreteç matris oluşturuyorsa H matrisine C için bir *Parity Kontrol Matris* denir. Burada C kodu için aşağıdaki özelliği yazabiliriz.

$$C = \{x \in F_2^n : H.x = 0\}$$

olur.

C, n uzunluklu lineer bir kod olmak üzere $v \in F_q^n$ için $C^e(v)$ kodu $n+1$ uzunluklu olmak ve genişletilmiş kodu göstermek üzere aşağıdaki gibi tanımlanır. $(c_1, \dots, c_n) \in C$ olmak üzere $c^e(v)$ kod kelimesini inşa etmek için c kod kelimesinin sonuna $c_{n+1}(v) \in C$ olacak şekilde ve aşağıdaki gibi parity kontrol yapısı oluşturularak eklenir.[5]

$$v_1 c_1 + \cdots + v_n c_n = 0$$

Bu kodun üreteç matrisleri aşağıdaki gibi bulunur. C bir $[n,k]$ kodu olmak üzere $C^e(v)$ kodu F_q^{n+1} in bir alt uzayı olmak üzere k boyutludur. $G^e(v)$ ve $H^e(v)$ sırasıyla bir genişletilmiş kodun üreteç matrisi ve parity kontrol matrisi ise bu matrisler aşağıdaki gibi tanımlanır.

$$G^e(v) = \begin{pmatrix} G & \begin{matrix} g_{1n+1} \\ g_{2n+1} \\ \vdots \\ g_{kn+1} \end{matrix} \end{pmatrix}$$

$G^e(v)$ nin en son kolonu $g_{in+1} = -\sum_{j=1}^{n} g_{ijv_j}$ şeklinde bulunur.

$$H^e(v) = \left(\begin{array}{ccc|c} v_1 & v_2 & \cdots & v_n & 1 \\ & H & & & 0 \\ & & & & \vdots \\ & & & & 0 \end{array} \right)$$

2.3. Lineer Kodlar

Lineer kodlar kodlama teorisinde hata bulma algoritmasının yapısında kullanılmaktadır. Bu kod çeşidi kodlamanın büyük bir kısmını oluşturmaktadır. Aşağıda bu kod çeşidine dair tanımlar, önermeler ve teoremler verilmiştir.

Tanım 2.3.1. [6] Bir $C \subset F_2^n$ kodu aşağıdaki şartları sağlarsa lineer kod denir.

(1) $0 \in C$,
(2) $x, y \in C$ iken $x + y \in C$dir.

Burada C kodu F_2^n nin F_2 üzerinde alt vektör uzayıdır.

Tanım 2.3.2. [6] Bir C kodunun rankı F_2 vektör uzayında olduğu gibi onun boyutunu belirtmektedir. Bir n uzunluklu ve rankı k olan lineer kod (n, k) kodu şeklinde gösterilir. Ayrıca bu kod d minimum uzaklığına sahipse kodu (n, k, d) şeklinde gösterilir. $v_1, \ldots, v_k$ C kodu için taban temsil etmek üzere

$$C = \left\{ \sum_{i=1}^{k} \lambda_i v_i \,\middle|\, \lambda_1, \ldots, \lambda_k \in F_2 \right\}$$

olur. Bu nedenle $|C| = 2^k$ dir. Böylece (n, k) kodunu $(n, 2^k = M)$ şeklinde temsil eder ve bilgi oranı $P(C) = \frac{k}{n}$ şeklinde bulunur.

Tanım 2.3.3. [7] $x \in F_2^n$ şeklindeki bir kod kelimesinin ağırlığı $w(x)$ şeklinde gösterilir ve $w(x) = d(x, 0)$ dir.

$q-$bileşenli (n, M, d) kodunun var olması için M' nin en büyük değeri olan $A_q(n, d)$ tanımlanır. $u \in A^n$ vektörü ve $r \leq n$ negatif olmayan bir r tamsayısı için $S_r(u) = \{v \in A^n | d(u, v) \leq r\}$ kümesine u merkezli r yarıçaplı küre denir. q sembollerinin

kümesi A ve $u, v \in A^n$ olmak üzere $u \neq v$ olsun ve ayrıca $d(u,v) = m$ olsun. v vektörlerinin sayısı $\binom{n}{m}(q-1)^m$ dir. Buna göre aşağıdaki eşitliği yazabiliriz.

$$|S_r(u)| = \sum_{m=0}^{r} \binom{n}{m} (q-1)^m$$

Minimum uzaklığı d ve $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ olacak şekilde bir $C \subset A^n$ kodunu ele alalım. Bu durumda merkezleri *C'* de olan kod kelimesi *t*-yarıçaplı olan küreler ayrıktır.

Örnek 2 .3.4. $A^4 = \{0000, 1000, 0100, 0010, 0001, 1100, 1010, 1001, 0110, 0101,$ $0011, 1110, 1011, 1101, 0111, 1111\}$ olsun. Bu durumda $d(1000, x) = 2$ olacak şekilde x kod kelimelerinin sayısını $\binom{4}{2}$ şeklinde bulabiliriz. Bu da x kod kelimelerinin sayısının 6 olduğunu bize belirtecektir. Böylece x kod kelimesi {0100, 0010, 0001, 1110, 1101, 1011} kod kelimelerinden herhangi biri olacaktır. Ayrıca t-yarıçaplı kürelerin birbirinden ayrık olduğunu göstermek için u kod kelimesinin yerine $\{1000, 1100\}$ kod kelimelerini alalım. Böylelikle tanımlanan $S_2(1000)$ ve $S_2(1100)$ kürelerinin birbirinden ayrık olduğunu gösterelim.

$$S_2(1000) = \{0100, 0010, 0001, 1110, 1101, 1011\}$$

$$S_2(1100) = \{0000, 1010, 0110, 0101, 1001, 1111\}$$

olur. Böylece $S_2(1000) \cap S_2(1100) = \emptyset$ yani ayrık olur.

Teorem 2.3.5. [7] C, q bileşenli (n, M, d) kodu ve $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ olmak üzere

$$M \sum_{m=0}^{t} \binom{n}{m} (q-1)^m \leq q^n$$

Bu eşitsizliğe; *Sphere- Packing Bound* denir, verilen q, n ve d değerleri için $A_q(n,d)$ sayısı için bir üst sınır adı verilir.

$$A_q(n,d) \leq \frac{q^n}{M \sum_{m=0}^{t} \binom{n}{m} (q-1)^m}$$

olur. Birçok kodda kod kelimelerinin gerçek M sayısı *Sphere- Packing Bound'*dan daha azdır.

Tanım 2.3.6. [7] $d(C) = 2t + 1$ olacak şekilde $C \subset A^n$ tanımlansın. Eğer $\forall y \in A^n$ vektörü için $d(x, y) \leq t$ için $x \in C$ varsa o zaman C' ye mükemmel kod denir.

Teorem 2.3.7. [7] q bileşenli (n, M, d) kodunu ele alalım. $d = 2t + 1$ için bu kodun mükemmel olabilmesi ancak ve ancak aşağıdaki şartı sağlaması ile gerçekleşir.

$$M \sum_{m=0}^{t} \binom{n}{m} (q-1)^m = q^n$$

dir.

Teorem 2.3.8. [8] d tek bir sayı olmak üzere bu durumda ikili bir (n, M, d) kodunun var olması için ancak ve ancak ikili bir $(n + 1, M, d + 1)$ kodu vardır.

Teorem 2.3.9. [8] İkili bir lineer kodda tüm kod kelimelerinin ağırlığı ya çifttir ya da yarısı çift yarısı tektir.

Lemma 2.3.10. [9] Bir lineer kod'un minimum uzaklığı sıfırdan farklı en az ağırlıklı kod kelimelerinin ağırlığına eşittir.

Tanım 2.3.11. [9] $p \subset F_2^n$ olsun. $C = \{x \in F_2^n : p.x = 0, \forall p \in P\}$ şeklinde tanımlanan P koduna *parity kontrol kod* denir.

Teorem 2.3.12. [10] Her *parity kontrol kod* lineer bir koddur.

Tanım 2.3.13. [10] $C \subset F_2^n$ lineer bir kod olsun. Aşağıdaki gibi tanımlanan koda dual kod denir. $C^{\perp} = \{x \in F_2^n : x.y = 0, \forall y \in C\}$ şeklinde tanımlanan koda dual kod denir.

Dual kod bir *parity kontrol kod*'dur. Bu nedenle lineer bir koddur.

Lemma 2.3.14. [10] C bir lineer kod olsun. $(C^{\perp})^{\perp} = C$ dir.

Tanım 2.3.15. [11] İki $k \times n$ tipindeki matris $[n, k]$ şeklindeki kodların üreteç matrisleri olsun. Aşağıdaki özelliklerin bazılarının uygulanmasıyla F_2^n üzerinde biri diğerinden elde ediliyorsa bu iki matrise denk matris denir.

1. Satırların yer değiştirilmesi.
2. Bir satırın sıfırdan farklı bir skalerle çarpılması.
3. Bir satırın skalerle çarpılıp başka bir satıra eklenmesi.
4. Sütunların yer değiştirilmesi.
5. Bir sütunun sıfırdan farklı bir skalerle çarpılması.

F_2^n üzerindeki bir $[n, k]$ kodunun üreteç matrisi $k \times n$ şeklindeki bir matris olan standart formu $[I_k : A]$ şeklinde yazabiliriz. Burada A matrisi $k \times (n - k)$ tipinde bir matristir.

2.4. Lineer Kodlarda Kodlama

F_2^k üzerinde bir $[n, k, d]$ lineer kodu olan bir C kodu alalım. C kodunun eleman sayısı 2^k tanedir. $v \in F_2^k$ için C' nin üreteç matrisi G olsun. Bir mesaj kodlanmak isteniyorsa mesaj kelimesi w olmak üzere $w.G$ şeklinde kodlanır.

2.4.1. (7,4) Hamming Kodlama

Hamming kod ilk olarak 1950 yılında Hamming tarafından oluşturulmuştur. Bu kod (7,4) Hamming kod olarak bilinir. Bu kodlama yönteminde her 4 bitlik data için 3 bit kontrol biti eklenir. Hamming' in geliştirdiği bu (7,4) algoritması her hangi bir tek bitlik hatayı düzeltebilir ya da bütün tek veya iki bitlik hataları tespit edebilir.

Tanım 2.4.1.1. [11] (7,4) lük Hamming kodlama da birbirleriyle bağlantılı olan 2 çeşit matris kullanılır. Kod üreteç matrisi G ve parity kontrol matrisi H dır.

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

G matrisinin ilk 4 satırını, 4×4'lük birim matris oluştururken son 3 satırı ise 4 veri bitinin 3 parity biti ile 4×3 şeklinde bir matristen oluşur. G' deki satır vektörleri H matrisinin elemanlarını oluşturur. Birim matrisi çarpım işlemi sırasında mesaj vektörünü aktarır. Yukarıdaki açıklamanın aksine mesaj bitleri ilk 4 pozisyondadır, parity bitleri ise son 3 pozisyona yerleştirilmiştir. Ayrıca bu matrisler asıl Hamming matrislerinden biraz farklı olsa da, Hamming kodlamayı anlamamızı kolaylaştıracak temel özellikleri taşımaktadır.

H matrisinin oluşturulması G matrisine benzerlik göstermektedir. H matrisinde her satırın son 3 sütunu 3×3'lük birim matrisidir. İlk 4 sütun ise yine G matrisinde de kullanılan ve data bitleri ve parity bitlerinin birleşmesinden oluşan $4 \times 3'$ lük matristir.

Yukarda bahsedildiği ve isminden de anlaşılabileceği gibi bu yöntemde 4 bit veri iletilir. Örneğin göndereceğimiz 4 bitlik mesaj "1000" olsun. Bu datayı göndermek için kullanacağımız vektör;

$$x = (1 \quad 0 \quad 0 \quad 0)$$

olacaktır.

Mesaj kodlamak için G üreteç matrisi kullanılır. 7×4'lük G matrisi ile gerçek mesaj olan 4×1'lik x matrisinin $mod2$ ye göre çarpılmasından elde edilecek 7×1'lik bir y matrisi $(7,4)$ lük Hamming kodlama yöntemi ile kodlanmış mesajı gösterecektir.

$$x.G = (1 \quad 0 \quad 0 \quad 0) \times \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = y$$

Eğer mesajın gönderimi sırasında bir hata oluşmazsa alınan mesaj ile iletilen mesaj birbirine eşit olmalıdır.

Eğer varsa hatalı dijiti bulmak için kullanılacak f matrisini elde etmek için H ve r matrisleri çarpılır. Matrislerin çarpımı yine $mod2$ ye göre yapılır.

$$H \times r = H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Eğer mesajın gönderimi sırasında tek dijitte bir hata meydana gelirse r ve y matrisleri birbirinden farklı olacaktır ve bu fark aşağıdaki gibi matematiksel olarak ifade edilebilir;

$$r = y + e$$

e burada hata vektörüdür. Aşağıdaki ifadeler $n.$ sıradaki tek dijitte meydana gelen hatanın belirlenişini gösterir.

Eğer r matrisini H matrisi ile çarparsak;

$$Hr = H(y + e) = Hy + He$$

ifadesi elde edilir. Bu ifadede y asıl iletilen mesaj olduğu için H matrisi ile çarpımı sıfır olacaktır. Buna göre;

$$Hy + He = 0 + He = He$$

$$r = y + e = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Şimdi ise bu hatalı r matrisi H ile çarpıldığı zaman elde edilecek f matrisi bize hatalı olan dijitin nerede olduğuna dair bilgi verecektir.

Burada f matrisinin gösterdiği 3×1'lik matris$H$ matrisindeki sütunlardan birine eşittir. İşte bu sütunun sırası aynı zamanda bize iletilen mesajın bozulan dijitin sırasıdır. Yukarıdaki örnek için hatalı dijit;

$$H \times r = H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ matrisi H parity kontrol matrisinde 4. sırada yer aldığından hatalı dijitin $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ iletilen mesajda 4. sıradadır. Bu yüzden kelime $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ olmak zorundadır.

2.5. Lineer Kodlarda Kod Çözme:

Burada bir lineer kod için şifre çözme yöntemi verilecektir. Şifre çözmenin genel kuralı, alınan vektöre en yakın kod kelimesini seçmektir. Bunun için bir tablo oluşturulur, bu tablo da alınan her vektör için verilen en yakın kod kelimesini aranır. Bir alt uzay olarak bir lineer kodun cebirsel yapısı böyle bir tabloyu hazırlamak için uygun bir metot sağlar. C, F_2^n de bir alt uzay olsun. $\forall a \in F_2^n$ için

$$a + C = \{a + c : c \in C\}$$

şeklinde tanımlanan kümeye C' nin bir koseti denir. $x, y \in F_2^n$ aynı koset de olması için gerek ve yeter şart $x - y \in C$ olmasıdır. Dolayısıyla F_2^n C' nin farklı kosetlerin birleşimidir. y, F^n de bir vektör $x \in C$ de y'ye en yakın kod kelimesi olsun. y kod kelimesi $y + C = \{y + c : c \in C\}$ kosetindedir. $\forall c \in C$ için; $d(x, y) \leq d(y, c)$ dir. Yani $w(y - x) \leq w(y - c)$ dir. Buradan $y - x$, y' yi içeren koset de en küçük ağırlıklı vektör olduğu anlaşılır. $e = y - x$ ise $x = y - e$ olur.

Teorem 2.5.1. [11] $C \subset F^n$ de bir lineer kod olsun. $y \in F^n$ verilsin. y kod kelimesine en yakın x kod kelimesi $x = y - e$ eşitliği ile verilir. e, y kod kelimesini içeren koset

de en küçük ağırlıklı vektördür. Eğer y kod kelimesini içeren koset birden çok en küçük ağırlıklı vektöre sahipse bu durumda birden fazla y kod kelimesine yakın kelimeleri vardır.

Tanım 2.5.2. [11] $C \subset F^n$ de bir lineer kod olsun. Verilen koset de en küçük ağırlıklı vektöre koset lideri denir.

Eğer koset içerisinde birden fazla en küçük ağırlıklı vektör varsa onlardan herhangi biri de koset lideri olarak seçilebilir. t hata düzeltebilen bir C kodunda minimum uzaklık t den daha küçük ve eşit olamaz. Eğer e vektörü ağırlığı t den daha küçük ve eşit olan bir koset lideri ise bu durumda e vektörü koset içerisinde en küçük ağırlıklı tek vektördür. C, F_q üzerinde bir $[n, k]$ kodu olsun. F^n, q^n tane elemana sahiptir. C nin her kosetinde q^k tane eleman vardır. Böylece C nin q^{n-k} tane farklı koseti vardır. Koset liderlerini $e_1, e_2, \dots, e_{q^{n-k}}$ olarak tanımlayalım ve $C = \{c_1, c_2, \dots, c_M\}$ $M = q^k$ olacak şekilde C kodunu gösterelim. Aşağıda belirtilen tablo da bir C kodunu kullanarak standart satır elde edilir ve hata bulma algoritması bunun üzerine inşa edilir.

$c_1 = 0 = e_1$	c_2	…	….	…	c_M
e_2	$c_2 + e_2$	…	…	…	$e_2 + c_M$
…	…	…	…	…	…
…	…	…	…	…	…
e_i	$c_2 + e_i$	…	…	…	$e_i + c_M$
…	…	…	…	…	…
$e_{q^{n-k}}$	$e_{q^{n-k}} + c_2$	…	…	…	$e_{q^{n-k}} + c_M$

Standart satır kodlama için kullanılır. $y \in F^n$ vektörü alındığını kabul edelim. Bu y vektörünün durumları tablodan bulunabilir. Eğer y tabloda *i.* satır da *j.* sütun da ise o zaman $y = e_i + c_j$ olur. e_i koset de en küçük ağırlığa sahip olan vektör olduğundan bir önceki teoreme göre y kod kelimesine en yakın kod kelimesi $x = y - e_i = c_j$ olacaktır. Böylece y vektörü en üst sütunda ki bir kod kelimesi olarak çözülür. Bir x vektörü gönderilsin ve bir y vektörü alınsın. O zaman $e = y - x$ bir hata vektörü olarak adlandırılır. Böylece bir koset lideri koset de bulunan her y vektörü için bir hata vektörü teşkil eder.

Örnek 2.5.3. [11] Üreteç matrisi aşağıda verilen bir ikili kodun üreteç matrisi olmak üzere bu kodun standart satırını yazalım.

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

Verilen kod $[5, 2]$ kodudur ve C nin elemanları $C = \{00000, 10101, 01011, 11110\}$ olur. Böylece 8 tane farklı koseti vardır. Standart satır 8 satırdan oluşacaktır. C nin minumum uzaklığı $d(C) = 3$ dür ve $t = 1$ olur. Ağırlığı 1 olan 5 vektör 5 farklı koset oluşturacak, kalan 2 satır ise sırayla önceki satırlarda olmayan ağırlığı 2 olan vektörlerden seçilecektir. Aşağıdaki tabloya dikkat edilirse son iki vektör ağırlığı 2 olan vektörlerdendir.

00000	10101	01011	11110
10000	00101	11011	01110
01000	11101	00011	10110
00100	10001	01111	11010
00010	10111	01001	11100
00001	10100	01010	11111
11000	01101	10011	00110
10010	00111	11001	01100

Örneğin 01111 kelimesi çözülmek istenirse 3. sütuna gidilir. Kelimeyi bulup C kodundaki karşılığına yani üstteki kod kelimesine bakılır. En üstteki kod 01011 kelimesidir. Bu durumda 01111 kelimesi 01011 kelimesi olarak çözülür. Standart sıra şifre çözmek için elverişli olmasına rağmen büyük n değerleri için elverişli bir teknik değildir.

Şimdi ise çok daha etkili bir şifre çözme metodu tanımlayalım.

2.5.4. Şifre Çözme Metodu

[11] F cismi üzerinde *parity kontrol matrisi* H olan bir $C, [n, k]$ kodu tanımlansın. $\forall y \in F$ için y' nin syndrome $s(y)$ ile gösterilir. $s(y) = yH^T$ dir. Dikkat edilmesi gereken şey ise syndrome, özel bir *parity kontrol matrisi* ile uyumlu olarak tanımlanır. $[n, k]$ kodu için $s(y)$, $(n - k)$ uzunluğunda bir vektördür. Syndrome yH^T satır vektörü

yada Hy^T sütun vektörü olarak yazılabilir. $s(y) = Hy^T = y_1H^1 + \cdots + y_nH^n$ biliniyor $C = \{x \in F^n : xH^T = 0 = Hx^T\}$ teoremi gereğince $s(y) = 0 \leftrightarrow y \in C$ olur. O halde $S(y) = S(y') \leftrightarrow (y - y')H^T = 0$ olur. Yani $y - y' \in C$ dir. İki vektörün aynı syndrome sahip olması için gerek ve yeter şart aynı koset de olmasıdır. Böylece C'nin kosetleri ile syndromları arasında birebir uyum vardır. Koset lideri e_i ve $S(e_i)$ koset liderinin syndorm olmak üzere iki sütunlu tabloya syndrom tablosu denir. Alınan bir y vektörünü çözmek için $S(y)$ hesaplanmıştır. Daha sonra $S(e) = S(y)$ için koset lideri e nin tabloda ki yeri bulunur. Böylece $x = y - e$ olacak şekilde y çözülür. Bu aşamaya ise syndrom şifre çözme denir.

Örnek 2.5.5. Daha önceki örnekte 11010 vektörünü çözmek için syndrome tablosunu yazıp bu tablo ya göre çözmeye çalışalım. Üreteç matris aşağıdaki gibi verilmişti bu üreteç matrisden *parity kontrol matrisi* elde edilir.

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

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

Koset Liderleri	**Syndrome**
10000	101
01000	011
00100	100
00010	010
00001	001
11000	110
10010	111

Verilen y vektörünün syndrome ise aşağıdaki gibi bulunur.

$$s(y) = yH^T = [11010] \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [100]$$

Syndrome tablosundan 100 syndrome ile koset lideri bulunur. $e = 00100$ olur böylece $x = 11110$ olarak çözülür.

Teorem 2.5.6. [11] Aşağıdaki özellikler sağlanır.

(1) $S(y) = 0 \leftrightarrow y \in C$

(2) $S(y) = s(w) \leftrightarrow y + C = w + C$ olacak şekilde y ile w aynı koset içerisindedir.

2.6. Polinom Kodlar

Polinom kodları anlatmadan önce kodlamada önemli bir yere sahip olan polinomlarla ilgili bazı temel özellikleri verelim.

Tanım 2.6.1. [12] $p(x) = a_0 + a_1x + \cdots + a_nx^n$ şeklinde bir x belirsizine bağlı olarak yazılabilen terimleri bir reel sayının elemanları olan $(a_0, a_1, \dots, a_n, 0_R, 0_R, \dots)$ şeklindeki diziye reel sayılar üzerinde tanımlanmış bir polinom denir. $(a_0, a_1, \dots, a_n)$ sayılarına polinomun katsayıları $\forall i \geq 1$ olmak üzere $a_i = 0$ ise $f = (a_0, 0_R, 0_R, \dots)$ polinomuna sabit polinom $\forall r \geq 0$ için ise $f = (0_R, 0_R, 0_R, \dots)$ şeklindeki polinoma ise sıfır polinom denir. Eğer f bir sıfır polinom değilse $a_i \neq 0_R$ olan i lerin en büyüğüne f in derecesi denir. $der(f)$ şeklinde gösterilir. f, g polinom olmak üzere $f = (a_0, a_1, \dots)$ ve $g = (b_0, b_1, \dots)$ olsun. $\forall i > m$ için $a_i = 0_R$ ve $\forall i > n$ ve $b_i = 0_R$ olacak şekilde $m, n \geq 0$ tamsayılar vardır. Böylece $\forall i > 0$ için $a_i = b_i$ ise $f = g$ olur. Buna iki polinomun eşitliği denir. Şimdi de iki polinomun nasıl toplanacağına bakalım. f, g polinom olmak üzere $f = (a_0, a_1, \dots)$ ve $g = (b_0, b_1, \dots)$ olsun. $f + g = (a_0 + b_0, a_{1+}b_1, \dots)$ şeklinde tanımlanır. İki polinomun çarpımı ise aşağıdaki gibi ifade edilir. f, g polinom olmak üzere $\forall k \geq 0$ için

$$c_k = \sum_{i=0}^{k} a_k b_{k-i} = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$$

olmak üzere $f.g = (c_0, c_1, \dots, c_k)$ şeklinde tanımlanır. Ayrıca bir polinomu sabit bir sayı ile çarpımı f bir polinom ve $r \in R$ için $r.f = (r.a_0, r.a_1, \dots)$ şeklindedir.

$$f(x) = \sum_{i=0}^{m} a_i x^i$$

polinomununda da $a_m \neq 0_R$ olsun. a_m ye baş katsayısı denir ve $a_m = 1$ ise bu polinoma monik polinom denir.

Lemma 2.6.2. [12] D bir tamlık bölgesi olsun. $f(x), g(x) \in D(x)$ olsun. Buna göre aşağıdaki özellikler sağlanır.

(i) $der(f(x) + g(x)) \leq maks\{derf(x), derg(x)\}$,

(ii) $der\big(f(x).g(x)\big) = der\big(f(x)\big) + der(g(x))$.

Teorem 2.6.3. [12] D tamlık bölgesi $f(x), g(x) \in D(x)$ $g(x) \neq 0_D$ ve $g(x)$ in baş katsayısı tersinir olsun. O zaman

$$f(x) = q(x)g(x) + r(x)$$

ve $der(r(x)) < der(g(x))$ olacak şekilde $q(x)$, $r(x) \in D(x)$ vardır. Ayrıca $q(x), r(x)$ tektir.

Tanım 2.6.4. [12] $p(x) \in F(x)$ olsun. Eğer

1. $p(x)$ sabit polinom değilse,
2. $p(x)$ her birinin çarpımı kendinden daha küçük olan polinomların çarpımı olarak yazılamıyorsa,

$p(x)$ polinomuna indirgenemez polinom denir.

Tanım 2.6.5. [12] $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in Z[X]$ ve $f(x) \neq 0$ olmak üzere $a_0, a_1, a_2, \ldots, a_n$ sayılarının en büyük ortak bölenine $f(x)$ in içeriği denir. Eğer $C\big(f(x)\big) = 1$ ise $f(x)'$ e ilkel polinom denir.

Temel polinom tanım ve teoremlerini verdikten sonra şimdi de kodlama teorisi için önemli olan polinom kodlarla ilgili bazı temel temel kavramları verelim. Kodlama teorisinde kodlama yapılırken en çok kullanılan yöntem polinom çarpımıdır. Bu yöntemle bulunan kodlara polinom kod denir.

Tanım 2.6.6. [13] Derecesi k olacak şekilde $g(x) = g_0 + g_1x + \cdots + g_kx^k$ bir polinom tanımlayalım. Vektörel olarak ifade edilen m uzunluklu olan $h = (h_0, h_1, \dots, h_{m-1})$ mesaj kelimesini $c = (c_0, c_1, \dots, c_{m-1})$ şeklinde kod kelimesine dönüştüren $g(x)$ polinomuna üreteç polinom denir. $c = (c_0, c_1, \dots, c_{m-1})$ mesaj kelimesine karşılık gelen $c(x) = c_0 + c_1x + \cdots + c_{m+k-1}x^{m+k-1}$ polinomuna da polinom kod denir.

2.7. $Z_2[X]$ de Polinom Kodlar

$m, n \in N$ için $n > m$ olduğunu kabul edilsin. Buna göre kodlama fonksiyonu

$$\alpha: Z_2^m \to Z_2^n$$

şeklinde ifade edilsin. $\forall w = w_1 \dots w_m \in Z_2^m$ için $w(x) = w_1 + w_2x + \cdots + w_mx^{m-1} \in Z_2[x]$. Şimdi $g(X) \in Z_2[x]$, $n-m$ dereceli bir polinom olmak üzere $w(x)g(x) \in Z_2[x]$ en çok $n-1$ dereceli bir polinom olsun. $w(x)g(x)$ aşağıdaki gibi yazılabilir.$c_1, \dots, c_2 \in Z_2^n$

$$w(x)g(X) = c_1 + c_2x + \cdots + c_nx^{n-1}$$

Bu durumda $\alpha(w) = c_1 \dots c_2 \in Z_2^n$ olacaktır [44].

Önerme 2.7.1.[44] $m, n \in N, n > m$ için $g(x) \in Z_2[x]$, derecesi $n-m$ olan kodlama fonksiyonu aşağıdaki gibidir. $\alpha: Z_2^m \to Z_2^n$ her $w = w_1 \dots w_m \in Z_2^m$ için $C = \alpha(Z_2^m)$ bir grup koddur.

Önerme 2.7.2. Bir öneki önermeden $\forall c \in C$ için $g(x)$ polinomu tarafından bölünen $(c+e)(x)$ polinomundan kalan $e = 0 \dots 010 \dots 0 \in Z_2^n$, $g(x)$ polinomunun x^{j-1} polinomunu böldüğünde kalana eşittir. Burada $j-1$, e vektöründeki birden önceki sıfır sayısıdır.

2.8. Polinom Kodlarda Kod Çözme Algoritması

$v \in Z_2^n$ kod kelimesi alınırsa aşağıdaki hata bulma algoritması uygulanarak kod kelimesi üzerindeki hata bulunur.

1. $g(x)$, $v(x) \in Z_2[x]$ kelimesini bölerse alınan kod kelimesinde hata bulunmamaktadır. Kodu çözmek için $v(x) = g(x)q(x) \in Z_2[x]$ olmak üzere $q \in Z_2^m$ için kod kelimesi bulunur.
2. $g(x)$, $v(x) \in Z_2[x]$ kelimesini bölmez $g(x)$, $v(x)$'in böldüğünde elde edilen kalan ile x^{j-1} i böldüğünde elde edilen kalan aynı ise bu bizim hatalı olan

dijitimizdir. $x^{j-1} + v(x) = g(x).q(x) \in Z_2[x]$ olacak şekilde hata bulunarak $q \in Z_2^m$ kod kelimesi elde edilir.

3. $g(x)$, $v(x) \in Z_2[x]$ kelimesini bölmez $g(x)$, $v(x)$'in böldüğünde elde edilen kalan ile x^{j-1} i böldüğünde elde edilen kalan farklı ise bu durum bir hatadan daha fazla hata olduğunu gösterir. Bunun çözümü için bölüm algoritması güvenilir bir metot olmayacaktır.

Örnek 2.8.1. $\alpha: Z_2^4 \to Z_2^7$ tanımlı olsun. $1 + x + x^3$, $g(x)$ polinomu olmak üzere $w = 1011$ için $w(x) = 1 + x^2 + x^3$ olur. $c(x) = w(x)g(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ polinom kodu elde edilir. Bu kod kelimesi $1111111 \in C$ dir kod kelimesi $v = 1110111$ olarak alınsın. Bu durumda $v(x) = 1 + x + x^2 + x^4 + x^5 + x^6 = g(x)(x^2 + x^3) + x + 1$. Diğer tarafdan $x^3 = g(x) + x + 1$ eğer $v(x)$ polinomuna x^3 polinomunu eklersek ve $g(x)$ polinomuna bölünsün $w(x)$ elde edilir.

Gönderilen kod üzerinde 2 hata yapılsın. Bu durumda $v = 1010111$ olur.

$$v(x) = 1 + x^2 + x^4 + x^5 + x^6 = g(x)(x^2 + x^3) + 1.$$

Diğer tarafdan $1 = g(x)0 + 1$. $v(x)$'e 1 eklenirse ve $g(x)$ tarafından bölünürse $x^2 + x^3$ elde edilir. $w = 0011 \in Z_2^4$ eşit olur. Yöntem yapılan hatayı bulamamıştır.

BÖLÜM 3

ESNEK KÜME TEORİSİNE GİRİŞ

3.1.Giriş

Tıp biliminde, sosyal bilimlerde, mühendislikte, ekonomide birçok problem klasik metotlarla çözülemez. Çünkü klasik metotlarla çözüm zorlukları çözmek yerine daha da karmaşık haline getirilebilir. Bu zorlukların sebebi genelde parametrelerin seçiminden kaynaklıdır. Belirsiz şekildeki bu zorlukların çözümü için olasılık teorisi, bulanık kümeler teorisi, yaklaşımlı kümeler teorisi ve en son olarak da esnek kümeler teorisi ortaya atılmıştır. Esnek küme teorisi oyun teorileri Reiman integrali, Perron integrali olasılık teorisi ve ölçüm teorisi gibi birçok konuda uygulamalara sahiptir. Bu teorinin uygulamaları işlevsel araştırmalarda ve oyun teoride detaylı bir şekilde tartışılmıştır. Ayrıca esnek küme yapısı tıp alanında da çeşitli problemler üzerinde konuşulmaya başlamıştır. Gerçek hayattaki problemler ve diğer konular üzerindeki esnek küme çalışmaları momentuma kadar ulaşmıştır. Bulanık esnek kümeler üzerine yapılan çalışmalar karar verme problemleri üzerine yoğunlaştırılmıştır. Sınıflandırma algoritmasını temel alan esnek küme teorisi, belirli nitelikteki sınıflandırmalar ile karşılaştırılmıştır. Bu teklif edilen algoritma, Bayos sınıflandırma tekniği ile karşılaştırılabilen daha az karmaşık bir yapıya sahiptir. Ayrıca esnek küme yaklaşımları, semi gruplar üzerinde sezgisel bulanık esnek kümelerin yapısının uygulamaları üzerinde yayılmaya başlamıştır. 2010 yılında K. V. Babitha ve J. J. Sunil [15] tarafından esnek kümeler üzerinde kartezyen çarpımın bir esnek alt kümesi üretilmiş ve bu yapı üzerinde ki birleşim, kesişim, OR ve AND gibi işlemler tanımlanmıştır. Aynı zamanda A. Kharal ve B. Ahmat [16] esnek küme üzerinde dönüşümler tanımlanmış ve bu tanım üzerinde çeşitli görüntü ve ters görüntü özelliklerini örnek ve ters örnekler ile açıklanmıştır. T. Harawan ve M. M. Deris [17] 2009 yılında yaklaşımlı kümeler Pawlak ve Iwiki [18] yaklaşımlı kümelerle ilgili çeşitli bilgiler vermiş ve bu düşüncesini çeşitli teoremlerle ispat etmiştir. M. M. Mushrif [18] 2006 yılında esnek küme teorisi üzerine basit bir sınıflandırma yöntemi uygulamış, 2010 yılında ise Wei Xu [19] esnek küme yapısına ek olarak bulanık esnek küme yapısını üretmiş ve bu makalede belirsiz esnek küme

kavramını temel özellikleri açıklanmıştır. M. A. Öztürk ve E. İnan [20] esnek kümeler içerisinde çeşitli işlemler arasındaki bağlantıyı göstermiş ve esnek kümelerin sınırlı simetrik farklılıkları tanımlamış ve çeşitli özelliklerini incelemiştir. G bir grup ve μ üyelik fonksiyonu olmak üzere $\forall x, y \in G$ için $\mu(x.y) \geq \min\{\mu(x), \mu(y)\}$ ve $\forall x \in G$ için şeklinde $\mu(x^{-1}) \geq \mu(x)$ üyelik fonksiyonları yardımıyla oluşturulan cebirsel yapı bulanık grup yapısıdır.

Benzer şekilde çok işlemli cebirsel yapı olan bulanık halka yapısı, R bir halka ve μ , R üzerinde bir bulanık alt küme olmak üzere $\forall x, y \in R$ için $\mu(x - y) \geq \min\{\mu(x), \mu(y)\}$ ve $\mu(x.y) \geq \min\{\mu(x), \mu(y)\}$ olarak inşa edilen cebirsel yapıdır. Bulanık halkada verilen ikinci özellik $\mu(x.y) \geq \max\{\mu(x), \mu(y)\}$olarak değiştirildiğinde R halkasının bulanık ideali elde edilmiş olur.

Bu cebirsel yapılar, klasik grup ve halka yapısına ek olarak üyelik fonksiyonu ve max, min işlemlerinin kullanıldığı bir ve iki işlemli farklı cebirsel yapılardır. Burada kümeden alınan herhangi iki elemanın çarpımının kümeye ait olması için çarpımın üyelik derecesinin çarpımdaki elemanlardan en az birinin üyelik değerinden büyük olması yeterlidir.

Bulanık kümeler üzerinde bu iki cebirsel yapının dışında da oldukça fazla sayıda cebirsel yapı ve özelliklerinden söz etmek mümkündür.
U üzerinde ikili işlem tanımlı bir evrensel küme ve G, U nun boştan farklı bir alt kümesi olsun.
(i) $\forall x, y \in G, x.y \in \overline{A}(G)$.

(ii) G de birleşme özelliği sağlanır.

(iii) $\forall x \in G, x.e = e.x = x$ önermesini doğrulayan $\exists e \in A(G)$ vardır.

(iv) $x.y = y.x = e$ eşitliğini sağlayan vardır. $\forall x \in G, \exists y \in G$.

$A(G) = (\underline{A}(G), \underline{A}(G))$ yaklaşımlı kümesi verilen dört özelliği sağlıyor ise bir yaklaşımlı gruptur.

Yaklaşımlı kümeler üzerinde tek ve iki işlemli cebirsel yapı olarak yaklaşımlı grup ve yaklaşımlı halka cebirsel yapıları en temel yapılardır. Bunlar dışında da üzerinde çalışılmış cebirsel yapı ve özellikleri görülebilir. G bir grup olmak üzere $F: A \to P(G)$ tanımlı F fonksiyonu verilsin. Her $x \in A$ için $F(x)$, G nin bir alt grubu ise (F, A) ikilisine bir esnek grup denir.

Yaklaşımlı kümeler üzerinde iki işlemli cebirsel yapı tanımlamak için G nin bir halka yapısına sahip olması yeterlidir. Bu durumda her $x \in A$ için $F(x)$, G nin bir alt halkası ise (F, A) ikilisine esnek halka denir.

Belirsizlik ifade eden kümeler üzerinde tanımlanan cebirsel yapılar klasik cebirsel yapılara dayandırılarak elde edilen ve daha geniş cebirsel yapılardır. Bu nedenle belirsizlik ifade eden cebirsel yapıların özel halleri klasik cebirsel yapıları vermektedir. "Soft sets and soft group" isimli makalede esnek grupların birçok cebirsel özelliklerinin yanı sıra belirsizlik ifade eden bulanık küme yaklaşımlı küme ve esnek kümeler karşılaştırılmıştır. Esnek grup kavramı teorik matematik çalışan araştırmacılar için oldukça büyük ilgi kaynağı olmuştur.
Ayrıca S. V. Maneman [22] 2011 yılında bulanık esnek kümelerin cebirsel özelliklerini ve bulanık esnek grupları tanımlamıştır. Bulanık esnek gruplar üzerine verilen bazı sonuçları ispat etmiştir. Ayrıca bulanık esnek fonksiyonlarının tanımını ve bulanık esnek homomorfizma yapısını tanımlamıştır. Sonuç olarak, homomorfik görüntü ve homomorfik ters görüntü J. Glosh [23] tarafından açıklanmış ve halka teorisi ve mevcut bulanık esnek ideal teorisi üzerine yaygınlaşmıştır. H. Prade ve D. Dubois [24] konu ile ilgili uygulamaları bulanık kümeler ile ilgili teoriler üzerine çalışmıştır. A. O. Atagün ve A. Sezgin [25] 2011 yılında esnek alt halkalar ve bir halkanın esnek idealleri üzerine çalışmıştır. Ayrıca bir cismin esnek alt cisimleri ve bir R-modülünün esnek alt modülünü tanımlamıştır. Cisimlerin, modüllerin, halkaların esnek alt yapıları hakkında bazı kavramlar örneklerle gösterilmiştir. Esnek küme yapıları sezgisel bulanık esnek küme yapıları üzerine yaygınlaşmış ve sezgisel bulanık esnek küme yapıları ise semi grup yapıları üzerinde çalışılmaya başlanmıştır. Bir semigrup üzerindeki sezgisel bulanık esnek idealler yapısı ve temel özellikleri J. Zhou tarafından çalışılmıştır. Aynı zamanda bir semi grubun yapısının sezgisel bulanık esnek ideallerin kümesinin latis yapıları ele alınmıştır. Bu teoriler içerisinde 1965 yılında Zadeh tarafından ortaya atılan

ve birçok araştırmacı tarafından ilgi ile çalışılmış bulanık küme teorisi en çok dikkat çeken teoridir. Böylece yıllardan beri kullanılan klasik mantık olarak tanınan doğru ve yanlış mantığından kurtulup bu üyelik fonksiyonu sayesinde değerler kendi içerisinde derecelendirilmiştir. Molodtsov (1999) da üyelik fonksiyonun doğası çok fazla bireysel olduğundan ve her durum için üyelik fonksiyonu inşa etmek zor olduğundan üyelik fonksiyonu olmayan yeni bir kümeler teorisine ihtiyaç olduğunu belirtmiştir. Molodtsov[26] kesinlik içermeyen esnek küme teorisine yeni bir matematiksel teori tanımlamıştır. Daha sonra birçok yazar tarafından esnek kümeler üzerine cebirsel yapılar kurulmuştur. Molodtsov' un bu çalışmasından sonra esnek kümelerin çeşitli özellikleri üzerine Maji [27] tarafından bir çalışma yapıldı. Daha sonra Maji bulanık esnek küme yapısı üzerine çalışmalar yapmıştır. Rosenfeld' de bulanık kümelerin cebirsel yapısını incelemiştir. Aktaş ve Çağman [28] tarafından bulanık kümeler ve yaklaşımlı kümeler esnek kümeler ile karşılaştırılmış ve esnek kümeler üzerine grup yapılarını kurmuşlardır. Bu yapının kurulması üzerine bazı yazarlar [29] tarafından bulanık esnek grup yapısı tanımı verilmiştir. Bunun üzerine F. Feng [30] tarafından esnek semi halka yapıları tanımlanmış U. Acar tarafından ise esnek halka yapıları tanımlanmıştır. Bazı yazarlar ise bulanık modül yapıları üzerine çalışmalar başlatmıştır ve Qiu-Mei Sun [31] tarafından bulanık esnek modüller ve onların temel özellikleri çalışılmıştır. Xiao [32] ise esnek kümelerin sosyal hayat üzerine etkilerini araştırmış ve bulanık kümeler ile ilgili çeşitli uygulamaları esnek kümeler üzerinde nasıl sonuç verdiğine dair çalışmalara imza atmıştır. Pei ve Miaono [33] ise esnek kümelerin bilgi sistemleri üzerine çalışmalar başlatmıştır. Bu bilgi sistemleri Daouwu Pei ve Duoqion Miaono [34] ya temel oluşturmuş ve bu bilgi sistemlerinin bulanık esnek kümeler üzerindeki işlerliğini araştırmışlardır. Park [35] ise esnek ws-cebirleri ve esnek alt cebirleri üzerine çeşitli çalışmalar üzerine yoğunlaşmıştır. Jun [36] uygulamalı esnek cebirler üzerine BCK / BCI- cebirlerinin cebirsel yapıları üzerine ile ilgili çeşitli araştırmalar yapmıştır. Jun ve Park [37] hilbert cebirleri üzerine esnek kümelerin uygulamaları incelemiştir. Ayrıca Jun [38] d- cebirleri içindeki ideallerin esnek kümeler üzerine uygulamalarını ve Pseudo d- cebirlerinin üzerine çalışmalar yapmıştır. Sun [39] ise esnek modüller üzerine çeşitli tanımlar vermiştir. Maji [40] bulanık kümeler yapısını daha da güçlendirmek için fs- kümelerini tanımlamış bu tanımı ise bazı araştırmacılar kullanarak fs-kümelerinin çok çeşitli özelliklerini incelemiştir. Som [41] esnek kümelerinin teorisi üzerine bulanık esnek ilişkiler tanımlamıştır.

3.2. Temel Kavramlar

Bu kısımda dört ve beşinci bölümde esnek kümeler üzerinde tanımlanan devirli grup ve devirli kod kavramlarını inşa etmede kullanılacak olan genel kavramlar verilmiştir.

Tanım 3.2.1. [28] U evrensel küme ve E parametrelerin ailesi olmak üzere $P(U)$ U' nun kuvvet kümesi için $A \subset E$ olarak gösterilsin. (F, A) sıralı ikilisi U üzerinde esnek küme olarak adlandırılır. F fonksiyonu $F: A \to P(U)$ bir dönüşümdür. U üzerindeki esnek küme U evrensel kümesinin alt kümelerinin parametreleştirilmiş ailesidir.

Tanım 3.2.2. [28] $E = \{e_1, e_2, \dots, e_n\}$ parametrelerin kümesi olsun. E'nin değili $\urcorner E$ şeklinde gösterilir ve $i = 1 \dots n$ için $\urcorner e_i$, e_i nin değili şeklinde ifade edilir ve aşağıdaki gibi tanımlanır. $\urcorner E = \{\urcorner e_1, \urcorner e_2, \dots, \urcorner e_n\}$.

Önerme 3.2.3. [28] $E = \{e_1, e_2, \dots, e_n\}$ parametrelerin kümesi olsun. $A, B \subseteq E$ olsun. Buna göre aşağıdaki özellikler sağlanır.

1. $\urcorner(\urcorner A) = A$
2. $\urcorner(A \cup B) = \urcorner A \cup \urcorner B$
3. $\urcorner(A \cap B) = \urcorner A \cap \urcorner B$

Tanım 3.2.4. [28] (F, A) esnek kümesinin tümleyeni $(F, A)^c$ şeklinde gösterilir ve $\forall \alpha \in \urcorner A$ için $F^c: \urcorner A \to P(U)$ şeklinde tanımlı bir dönüşüm $F^c(\alpha)$, $U - F(\urcorner \alpha)$ olarak tanımlı $(F, A)^c = (F^c, \urcorner A)$ kümesidir.

Tanım 3.2.5. [28] (F, A) ve (G, B), U evrensel kümesi üzerinde tanımlı iki esnek küme olsun. $B \subseteq A$ $\forall b \in B$ için ve $G(b) \subset F(b)$ ise (G, B) esnek kümesine (F, A) esnek kümesinin alt kümesi denir.

Tanım 3.2.6. [28] $(F, A), U$ evrensel kümesi üzerinde esnek küme olmak üzere $\forall e \in A$ için $F(e) = \emptyset$ ise (F, A) esnek küme yapısına boş esnek küme denir. Φ şeklinde gösterilir

Tanım 3.2.7. [28] $(F, A), U$ evrensel kümesi üzerinde esnek bir küme olmak üzere $\forall e \in A$ için $F(e) = U$ ise (F, A) esnek küme yapısına tam esnek küme denir. $\tilde{A}$ şeklinde gösterilir.

Tanım 3.2.8. [28] (F,A) ve (G,B), U evrensel kümesi üzerinde tanımlı iki esnek küme olsun. $\forall c \in C$ ve $C = A \cup B$ olmak üzere (H,C) esnek kümesine iki esnek kümenin birleşimi denir ve aşağıdaki gibi tanımlanır.

$$H(c) = \begin{cases} F(c) & c \in A/B \\ G(c) & c \in B/A \\ F(c) \cup G(c) & c \in A \cap B \end{cases}$$

$(F,A) \cup (G,B) = (H,C)$ şeklinde gösterilir.

Tanım 3.2.9. [28] (F,A) ve $(G,B), U$ evrensel kümesi üzerinde tanımlı iki esnek küme olsun. $\forall c \in C$ ve $C = A \cap B$ olmak üzere (H,C) esnek kümesine iki esnek kümenin kesişimi denir ve aşağıdaki gibi tanımlanır. $H(e) = F(e)$ veya $G(e)$ dir ve $(F,A) \cap (G,B) = (H,C)$ şeklinde gösterilir.

Tanım 3.2.10. [28] (F,A) G üzerinde bir esnek küme olsun. $\forall x \in A$ için $F(x)$, G nin bir altgrubu ise (F,A) esnek kümesine G üzerinde bir esnek grup denir.

Tanım 3.2.11. [28] (F,A) ve (H,B), G ve K grupları üzerinde sırasıyla iki esnek grup ve $f: G \to K$ ve $g: A \to B$ ye tanımlı iki fonksiyon olsun. Aşağıdaki şartları sağlayan (f,g) ikilisine esnek homomorfizma (F,A) esnek grubuna ise (H,B) esnek grubuna homomorfik denir ve (F,A)~(H,B) şeklinde gösterilir.

1. f, G den K ya bir homomorfizmadır.
2. g, A dan B ye bir örten dönüşümdür.
3. $\forall x \in A$ için $f\big(F(x)\big) = H(g(x))$.

Esnek homomorfizma tanımında f, G den K ya bir izomorfizma ve g de A'dan B' ye bire bir bir dönüşüm ise (f,g)ikilisine esnek izomorfizma (F,A) esnek grubu (H,B) esnek grubuna esnek izomorf denir ve $(F,A) \approx (H,B)$ şeklinde gösterilir.

Tanım 3.2.12. [28] (F,A) ve (G,B) U evrensel kümesi üzerinde tanımlı iki esnek küme olsun. VE ve VEYA tanımı aşağıdaki gibi verilir sırasıyla $\wedge$ ve $\vee$ ile gösterilir.

(a) $\cap$ sembolü kümelerin kesişim işlemini göstersin ve $\forall(\alpha,\beta) \in A \times B$ için $H(\alpha,\beta) = F(\alpha) \cap G(\beta)$ olmak üzere $(F,A) \wedge (G,B) = (H, A \times B)$ şeklinde tanımlanır.

(b) $\cup$ sembolü kümelerin birleşimini göstersin ve $\forall(\alpha,\beta) \in A \times B$ için $K(\alpha,\beta) = F(\alpha) \cup G(\beta)$ olarak tanımlanır. $(F,A)\vee(G,B) = (K, A \times B)$ şeklinde gösterilir.

Önerme 3.2.13. [42] (F,A), (G,B) ve (H,C) U üzeride üç esnek kümeler olsun. Buna göre aşağıdaki özellikler sağlanır.

1. $(F,A)\vee\big((G,B)\vee(H,C)\big) = \big((F,A)\vee(G,B)\big)\vee(H,C)$,
2. $(F,A)\wedge\big((G,B)\wedge(H,C)\big) = \big((F,A)\wedge(G,B)\big)\wedge(H,C)$,
3. $(F,A)\vee\big((G,B)\wedge(H,C)\big) = ((F,A)\vee(G,B))\wedge((F,A)\vee(H,C))$,
4. $(F,A)\wedge\big((G,B)\vee(H,C)\big) = ((F,A)\wedge(G,B))\vee((F,A)\wedge(H,C))$.

Önerme 3.2.14. [42] (F,A) ve $(G,B), U$ üzerinde esnek kümeler olsun. Birleşim ve kesişim işlemleri aşağıdaki özellikleri sağlar.

(a)$((F,A) \cup (G,B))^c = (F,A)^c \cup (G,B)^c$,

(b) $((F,A) \cap (G,B))^c = (F,A)^c \cap (G,B)^c$.

Önerme 3.2.15. [42] (F,A) U üzerinde esnek küme olsun. Aşağıdaki özellikler sağlanır.

(a) $(F,A) \cup (F,A) = (F,A)$,

(b) $(F,A) \cap (F,A) = (F,A)$,

(c) $(F,A) \cup \Phi = \Phi$,

(d) $(F,A) \cap \Phi = \Phi$,

(e) $(F,A) \cup \hat{A} = \hat{A}$,

(f) $(F,A) \cap \hat{A} = (F,A)$.

BÖLÜM 4

ESNEK DEVİRLİ GRUPLAR VE KODLAMA TEORİSİ ÜZERİNE UYGULAMALARI

Aktaş ve Çağman tarafından 2007 yılında "Soft Sets and Soft Groups" isimli makalesi ile esnek kümeler üzerine ilk cebirsel yapı tanımlanmıştır. Bu makalenin yazımıyla birlikte esnek kümeler üzerine yapılan çalışmalar hızlanmıştır. Bu bölümde esnek grup tanımını kullanarak bir esnek kümenin kuvveti ve mertebesi tanımlanmış ve çeşitli özellikleri incelenmiştir. Ayrıca kuvvet ve mertebe tanımları kullanılarak devirli esnek grup yapısı oluşturulmuş ve çeşitli özellikleri verilerek ispatlanmıştır. Ayrıca klasik gruplarla ayrıştığı ve birleştiği durumlar incelenmiştir.
Bu bölümde oluşturulan kavramlar ve elde edilen sonuçlar orijinal olup yayınlamıştır.

4.1. Esnek Küme Mertebesi

Tanım 4.1.1. $F: A \to P(U)$ tanımlı bir örten dönüşüm olmak üzere (F, A) ikilisine U üzerinde örten esnek küme denir.

Bu bölüm boyunca G bir grup yapısını ve (F, A) ise örten esnek kümeyi gösterecektir. (F, A) nın bir elemanı olan $(a, F(a))$ elemanın yerine $F(a)$ kullanılacaktır.

Tanım 4.1.2. (F, A), G üzerinde bir esnek küme ve $\forall x \in A$ için $F(x) \in (F, A)$ olsun. Bu durumda $F(x)$ in n. kuvveti aşağıdaki gibi tanımlanır.

$$F(x)^n = \{a^n : a \in F(x), n \in Z\}$$

Örnek 4.1.3. $A = S_3$ olmak üzere (F, A) esnek küme S_3 üzerinde aşağıdaki gibi tanımlansın. $(F, A) = \{F(e) = \{e\}, F(12) = \{e, (12)\}, F(13) = \{e, (13)\}, F(23) = \{e, (23)\}, F(123) = \{e, (123), (132)\}\}$

kümesi S_3 grubu üzerinde bir esnek kümedir. $F(123)$ ün üçüncü kuvveti kümelerdeki her bir elemanın 3. mertebesi olarak hesaplanır. $F(123)^3 = \{e^3, (123)^3, (132)^3\} = \{e, e, e\} = \{e\}$. Eğer grup yapısı toplamsal bir grup ise $F(x)$ in n.kuvveti

$$n.F(x) = \{n.a : a \in F(x), n \in Z\}$$

şeklinde hesaplanır yani $F(x)$ in n katı hesaplanarak elde edilir.

Teorem 4.1.4. $(F, A), G$ üzerinde esnek küme olmak üzere $\forall x, y \in A$ için $\forall F(x), F(y) \in (F, A)$ olsun. Buna göre $\forall n \in Z$ için aşağıdaki özellikler sağlanır.

1. $\forall n \in Z$ için, $(F(x) \cap F(y))^n \subseteq F(x)^n \cap F(y)^n$,
2. $\forall n \in Z$ için, $(F(x) \cup F(y))^n = F(x)^n \cup F(y)^n$,
3. $\forall n \in Z$ için, $(F(x) \times F(y))^n = F(x)^n \times F(y)^n$.

İspat

1. $\forall n \in Z$ için $a^n \in (F(x) \cap F(y))^n$ olsun. $a \in F(x) \cap F(y)$ ve buradan $a \in F(x)$ ve $a \in F(y)$ olacaktır. Böylece $a^n \in F(x)^n$ ve $a^n \in F(y)^n$ olur. Tanım 4.1.2 den $a^n \in F(x)^n \cap F(y)^n$ anlamına gelmektedir. Böylece ispat tamamlanır.
2. $\forall n \in Z$ için $a^n \in (F(x) \cup F(y))^n$ olsun. Buradan $a \in (F(x) \cup F(y))$ olduğundan $a \in F(x)$ veya $a \in F(y)$ olur. Bu durumda $a^n \in F(x)^n \cup F(y)^n$ olacaktır. Böylece $(F(x) \cup F(y))^n \subseteq F(x)^n \cup F(y)^n$ olur. Şimdi $a^n \in F(x)^n \cup F(y)^n$ olarak alalım. $a^n \in F(x)^n$ veya $a^n \in F(y)^n$ olur. Bu durumda $a \in F(x)$ veya $a \in F(y)$ olacaktır. Böylece $a \in F(x) \cup F(y)$ durumu elde edilir. Buda $a^n \in (F(x) \cup F(y))^n$ anlamına gelir. Buradan $(F(x) \cup F(y))^n = F(x)^n \cup F(y)^n$ sonucu bulunur.
3. $\forall n \in Z$ için $(a, b)^n \in (F(x) \times F(y))^n$ olsun. $(a, b) \in F(x) \times F(y)$ olur. Bu ise $a \in F(x)$ ve $b \in F(y)$ olur. $a^n \in F(x)^n$ ve $b^n \in F(y)^n$ olacaktır. $(a, b)^n \in F(x)^n \times F(y)^n$dır. $(F(x) \times F(y))^n \subseteq F(x)^n \times F(y)^n$ anlamına gelir.
   $(a^n, b^n) \in F(x)^n \times F(y)^n$ olsun. $a^n \in F(x)^n$ ve $b^n \in F(y)^n$ olacaktır. Bu durumda $a \in F(x)$ ve $b \in F(y)$ elde edilir. $(a, b) \in F(x) \times F(y)$ olur. Böylece $(a, b)^n \in (F(x) \times F(y))^n$ olacaktır. Buda $F(x)^n \times F(y)^n \subseteq$

$(F(x) \times F(y))^n$ anlamına gelir. Sonuç olarak $(F(x) \times F(y))^n = F(x)^n \times F(y)^n$ elde edilir.

Teorem 4.1.4 (1) in tersinin doğru olmadığını aşağıdaki örnekle gösterelim.

Örnek 4.1.5. $A = \{0,1\}$ ve $F: A \to P(Z)$tanımlı bir fonksiyonu $F(0)$ ve $F(1)$ aşağıdaki gibi tanımlı $F(0) = \{2k: k \in Z\}$ ve $F(1) = \{2k+1: k \in Z\}$ olsun. Bu durumda $F(0) \cap F(1) = \emptyset$ olur. Bu nedenle $(F(0) \cap F(1))^2 = \emptyset$ olur. Ama diğer taraftan $F(0)^2 \cap F(1)^2 \neq \emptyset$ dır. Bu da sonuç olarak $(F(x) \cap F(y))^n \neq F(x)^n \cap F(y)^n$ olduğunu gösterir.

Tanım 4.1.6. (F, A), Ggrubu üzerinde bir esnek küme ve $F(x) \in (F, A)$ olsun. $F(x)^n = \{e\}$ olacak şekilde bir n pozitif tamsayısı varsa bu n tamsayılarının en küçüğüne $F(x)$ in mertebesi denir. Eğer böyle bir n tamsayısı yoksa $F(x)$ sonsuz mertebelidir denir. $F(x)$ in mertebesi $|F(x)|$ şeklinde gösterilir. (F, A), G grubu üzerinde bir esnek grup ise $F(x) \in (F, A)$ nin mertebesi, G grubunun bir altgrubu olan $F(x)$ in mertebesi ile aynıdır. Doğal olarak eğer $F(x)$ grubu birim elemana eşit ise yani $F(x) = \{e\}$ ise $F(x)$ in mertebesi 1 olur.

Örnek 4.1.7. $F(123)$ alt grubunun mertebesi 3 dür.

Şimdi de (F, N) esnek grubunu ele alalım ve F dönüşümünü N doğal sayılar kümesinden $P(Z)$ tam sayıların kuvvet kümesi üzerine tanımlayalım. Doğal sayılar kümesi olan N kümesinden bir n elemanı alıp F dönüşümü ile $P(Z)$ kuvvet kümesi üzerinde $n.Z$ olacak şekilde tanımlayalım.

$$F: N \to P(Z)$$
$$n \to F(n) = nZ$$

şeklinde olsun. $F(n)^m = \{0\}$ olacak şekilde bir m pozitif tam sayısının olmadığı açıktır. Bu durumda $F(n)$, $\forall n \in N - \{0\}$ için sonsuz mertebelidir.

Teorem 4.1.8. G sonlu grup ve (F, A) da G üzerinde esnek grup olsun. (F, A) nın elemanlarının mertebeleri sonludur.

İspat: Lagrange Teoremine göre sonlu bir grubun her alt grubunun mertebesi grubun mertebesini böleceğinden ve (F,A) nın her bir elemanı G nin alt grubu olduğundan (F,A) nın her elemanın mertebesi G nin mertebesini böler

Teorem 4.1.9. $(F,A),G$ sonlu grubu üzerinde bir esnek küme ve $\forall x \in A$ için $F(x) \in (F,A)$ olsun. $F(x)$ in mertebesi $F(x)$ in elemanlarının mertebelerinin en küçük ortak katıdır.

İspat: n, $F(x)$ in mertebesi olsun. Buradan $F(x)^n = \{e\}$ olur. Böylece $\forall a \in F(x)$ için $a^n = \{e\}$ olacaktır. Klasik gruplarda bildiğimiz gibi $\forall a \in F(x)$ elemanlarının mertebesi grubun mertebesini böler. Yani $|a||n$ olur. Böylece n , $F(x)$ in elemanlarının mertebesinin ortak katıdır. Ayrıca m sayısı $F(x)$ in elemanlarının mertebelerinin ortak katı olsun. $\forall a \in F(x)$ için $a^m = \{e\}$ olacak şekilde $F(x)^m = \{e\}$ olur. $F(x)^n = \{e\}$ olacak şekilde en küçük n sayısına sahip ve n sayısı en küçük ortak kat olduğundan $n|m$ olacaktır. Buda ispatı tamamlar.

Teorem 4.1.10. G sonlu bir grup olsun. (F,A), G üzerinde bir esnek grup ve $F(x)$ ve $F(y)$, (F,A) esnek grubunun elemanları olsun. $\forall x,y \in A$ için aşağıdaki şartlar sağlanır.

1. $\forall x,y \in A$ için, $|F(x) \cap F(y)| \leq ebob(|F(x)|,|F(y)|)$,
2. $\forall x,y \in A$ için, $|F(x) \cup F(y)| = ekok(|F(x)|,|F(y)|)$,
3. $\forall x,y \in A$ için, $|F(x) \times F(y)| = |F(x)|.|F(y)|$.

İspat:

1. $F(x) \cap F(y)$, $F(x)$ ve $F(y)$ nin birer alt grubu olduğundan Langrange teoremi gereği alt grubun mertebesi grubun mertebesini böler. Yani $|F(x) \cap F(y)||F(x)|$ ve $|F(x) \cap F(y)||F(y)|$ ayrı ayrı böler. Bu durumda $|F(x) \cap F(y)| \leq ebob(|F(x)|,|F(y)|)$ olur.
2. $|F(x) \cup F(y)| = k$, $|F(x)| = m$ ve $|F(y)| = n$ olsun. $(F(x) \cup F(y))^k = F(x)^k \cup F(y)^k = \{e\}$ olduğunu biliyoruz. Ayrıca alt grubun mertebesi grubun mertebesini böleceğinden $n|k$ ve $m|k$ olur. Böylece k sayısı m ve n sayılarının ortak katı olur. m ve n sayılarının diğer bir ortak katı olarak t olsun.

$(F(x) \cup F(y))^t = F(x)^t \cup F(y)^t = \{e\}$ olur. k sayısı $(F(x) \cup F(y))^k = \{e\}$ olacak şekilde en küçük pozitif tamsayısı olduğundan k sayısı t sayısını böler. Böylece k sayısı $F(x)$ ve $F(y)$ altgruplarının mertebelerinin en küçük ortak katı olur.

3. $F(x)$ ve $F(y), G$ nin birer alt grubu olduğundan 3 ün ispatı açıktır.

Tanım 4.1.11. G bir grup ve (F, A) esnek kümesi de G grubu üzerinde bir esnek grup olsun. $(F, A)^n = \{F(x)^n : x \in A, n \in Z\}$ kümesine (F, A) esnek grubunun n. kuvveti denir.

Örnek 4.1.12. (F, A) esnek kümesi daha önceki örnekte de olduğu gibi S_3 kümesi üzerinde bir esnek küme olsun. (F, A) esnek kümesinin ikinci kuvveti aşağıdaki gibi alınır. $(F, A)^2 = \{F(e)^2 = \{e\}, F(12)^2 = \{e\}, F(13)^2 = \{e\}, F(23)^2 = \{e\}, F(123)^2 = F(132)\}$.

Teorem 4.1.12. (F, A) ve $(E, B), G$ grubu üzerinde iki esnek küme olsun. Buna göre aşağıdaki özellikler sağlanır.

1. $\big((F, A) \vee (E, B)\big)^n = (F, A)^n \vee (E, B)^n$,
2. $\forall a \in A$ için, $A \subseteq B$ ise $F(a)$ ve $E(a)$ aynı yaklaşımlı olmak üzere $\big((F, A) \wedge (E, B)\big)^n \subseteq (F, A)^n \wedge (E, B)^n$ olur.

İspat:

1. $(F, A) \vee (E, B) = (H, A \times B)$ ve $(F, A)^n \vee (E, B)^n = (T, A \times B)$ olduğu bilinmektedir. Ayrıca $\big((F, A) \vee (E, B)\big)^n = (H, A \times B)^n$ şeklinde yazılabilir. Tanım 4.1.2. ve Teorem 4.1.10. kullanılarak aşağıdaki eşitlikler yazılabilir.

$$\begin{aligned}(H, A \times B)^n &= \{H(a, b)^n : (a, b) \in A \times B\} \\ &= \{\big(F(a) \cup E(b)\big)^n : (a, b) \in A \times B\} \\ &= \{F(a)^n \cup E(b)^n : (a, b) \in A \times B\} \\ &= \{T(a, b) : (a, b) \in A \times B\} \\ &= (F, A)^n \vee (G, B)^n.\end{aligned}$$

2. $(F,A)\wedge(E,B)=(H,A\times B)$ ve $(F,A)^n\wedge(E,B)^n=(T,A\times B)$ şeklinde yazıldığı bilinmektedir. (1) in ispatı kullanılarak aşağıdaki ifadeler yazılır.

$$(H,A\times B)^n=\{H(a,b)^n:(a,b)\in A\times B\}$$
$$=\{(F(a)\cap E(b))^n:(a,b)\in A\times B\}$$
$$\subseteq\{F(a)^n\cap E(b)^n:(a,b)\in A\times B\}$$
$$=\{T(a,b):(a,b)\in A\times B\}$$
$$=(F,A)^n\wedge(E,B)^n.$$

(F,A) ve (E,B) esnek grup ise $\forall a,b\in A$ için $F(a)$, ve $E(b), G$ nin alt gruplarıdır. Dolayısıyla $F(a)$ ve $E(b)$, G nin birim elemanı olan e yi içerir. Böylece $F(a)\cap E(b)\neq\emptyset$ dır. Bunun anlamı Teorem 4.1.12. (2) maddesinde (F,A) ve (E,B) esnek küme değil de esnek grup alınırsa Teorem 4.1.12. (2) ye ekstra şartlar eklenir.
Klasik gruplarda, bir grubun mertebesi grupta bulunan elemanların sayısı olarak tanımlanır. Mertebe kavramı esnek gruplarda, klasik gruplardan farklıdır.

Tanım 4.1.13. $(F,A), G$ üzerinde bir esnek grup olsun. G sonlu bir grup ise (F,A) nın elemanlarının mertebelerinin en küçük ortak katına (F,A) nın mertebesi denir. G, sonsuz grup ise (F,A) nın mertebesi (F,A) nın elemanlarının sayısı olarak adlandırılır. (F,A) esnek grubunun mertebesi $|(F,A)|$ şeklinde gösterilir. Ayrıca (F,A) örten ise (F,A) nın elemanlarının sayısı A daki elemanların sayısına eşittir.

Örnek 4.1.14. Örnek 4.1.3. de (F,A) nın mertebesi 6 ve Örnek 4.1.7. deki N doğal sayılar kümesini $N_5=\{0,1,2,3,4\}$ olarak seçersek ve $F(n)=n.Z$ şeklinde tanımlanırsa $\forall n\in N_5$ için (F,N_5) esnek grubunun mertebesi 5 olur.

Şimdi de aşağıda grup teoride verilen Langrange teoremine benzer sonuçları esnek gruplar üzerine verelim.

Teorem 4.1.15. (F,A), G sonlu grubu üzerinde esnek grup olsun ve $F(x)\in(F,A)$ için aşağıdaki özellikler sağlanır.

1. $F(x)$ in mertebesi (F,A) nın mertebesini böler ve $F(x)^{|(F,A)|}=\{e\}$ dır.
2. (F,A) nın mertebesi G nin mertebesini böler.

İspat:

1. $|F(x)| = k$ için Tanım 4.1.2. göre $0 \neq m \in N$ için $|(F,A)| = k.m$ olmalıdır. Bu durumda $F(x)^{k.m} = \{e\}$ olur. Çünkü $F(x)^k = \{e\}$ dir ve k sayısının her kuvveti de $F\ (x)$ kümesini birim elemana götürür.
2. Alt grubun mertebesi grubun mertebesini böleceğinden (F,A) nın elemanlarının mertebesinin en küçük ortak katı G nin mertebesini böler.

G grubu sonlu bir grup olduğundan (F,A) nın mertebesi de sonludur. (F,A) nın elemanlarının mertebeleri (F,A) nın mertebesini böler. G sonsuz bir grup olduğunda (F,A) nın mertebesi sonlu ya da sonsuz olabilir. Ama yukarıdaki teorem sonsuz gruplar için doğru değildir.

Teorem 4.1.16. G sonlu bir grup ve (F,A) ve $(G,B), G$ üzerinde iki esnek grup olsun. Buna göre aşağıdaki özellikler sağlanır.

1. $|(F,A) \wedge (G,B)| \leq |(F,A)|$,
2. $|(F,A) \wedge (G,B)| \leq |(G,B)|$.

İspat:

1. $(F,A) \wedge (G,B) = (H,C)$ ve $C = A \times B$olsun. Tanım 4.1.13. ve Teorem 4.1.12. den ve $|(F,A)|$ nın tanımını kullanarak aşağıdaki ifadeyi yazabiliriz.$\forall (a_i, b_i) \in A \times B$ için
   $|(F,A) \wedge (G,B)| = ekok(|H(a_i,b_i)|) = ekok(|F(a_i) \cap G(b_i)|) \leq$
   $ekok|F(a_i)| = |(F,A)|$.
2. $(F,A) \wedge (G,B) = (H,C)$ olsun. Tanım 4.1.13 ve Teorem 3.2.13 ve $|(G,B)|$ nın tanımını kullanarak aşağıdaki ifadeyi yazabiliriz.$\forall (a_i, b_i) \in A \times B$için
   $|(F,A) \wedge (G,B)| = ekok(|H(a_i,b_i)|) = ekok(|F(a_i) \cap G(b_i)|) \leq$
   $ekok|G(b_i)| = |(G,B)|$.

4.2. Devirli Esnek Gruplar

Devirli gruplar, grup teori içinde önemli bir yere sahiptir. Bu bölümde $P(G)$ nin bir elemanı tarafından üretilen esnek grup yapıları çalışılacaktır. Devirli esnek grup tanımı ve klasik gruplardaki özelliklere benzer sonuçlar verilecektir.

Tanım 4.2.1. (F,A), G üzerinde bir esnek grup ve X de $P(G)$ nin bir elemanı olsun. Aşağıdaki gibi tanımlanan (F,A) esnek kümesinin bir alt kümesi olan kümeye X kümesi tarafından üretilen küme denir. $\{(a,<x>):F(a)=<x>,x\in X\}$ ve bu küme $<X>$ şeklinde gösterilir. $(F,A)=<X>$ ise (F,A) esnek grubu X tarafından üretilen devirli esnek grup olarak adlandırılır.

$(F,A),G$ üzerinde devirli esnek grup ise, $(F,A)=\{F(a)=<x>:a\in A,x\in G\}$ şeklinde yazılır. Bu durum ancak (F,A) nın tüm elemanlarının $P(G)$ nin bir X elemanı tarafından üretiliyorsa mümkündür. Böylece (F,A), G grubu üzerinde devirli esnek bir gruptur.

G devirli bir grup ise devirli bir grubun her alt grubu devirli olduğundan $(F,A),G$ üzerinde devirli bir esnek gruptur, fakat bunun tersi doğru değildir. Bu durum aşağıdaki örnekle ifade edilir.

Örnek 4.2.2. $G=S_3$ simetrik bir grup ve $A=\{e,(12),(13),(23),(123)\}$ parametrelerin kümesi olsun. Şimdi G üzerinde (F,A) esnek kümesi inşa edelim.$\forall x\in A$ için $F(x)=\{y\in G:y=x^n,n\in Z\}$ şeklinde tanımlanırsa G devirli bir grup olmamasına rağmen $(F,A),G$ üzerinde esnek devirli bir grup olur. $(F,A),G$ üzerinde devirli esnek grup ise $\{<x>:x\in G\}$, $P(G)$ nin bir elemanı olmak üzere $(F,A)=\{F(a)=<x>:a\in A,x\in G\}$ şeklinde yazılır.

Aşağıdaki teoremle esnek devirli grupların klasik gruplarla olan benzer bazı özellikleri verilmiştir.

Teorem 4.2.3. Aşağıdaki ifadeler sağlanır.

1. $(F,A),X$ tarafından üretilen sonlu devirli bir grup ise $x_i\in X$ için $|(F,A)|=ekok\{|x_i|\}$ dir.
2. $(F,A),X$ tarafından üretilen sonuz devirli bir grup ise, $|(F,A)|=|X|$ dir.
3. (F,A) birim esnek grup ise, bu grup $\{e\}$ tarafından üretilen devirli esnek gruptur.
4. (F,A) , G üzerinde tanımlanan tam esnek grup ise, G devirli grup olmak üzere (F,A) devirli esnek gruptur.
5. $(F,A),G$ üzerinde esnek grup olsun. G nin mertebesi asal ise (F,A) devirli esnek gruptur.

6. Bir devirli esnek grubun her esnek alt grubu devirli esnek gruptur.

İspat:

1. $i = 1, \dots, n$ için $F_i(x) \in (F, A)$ için $F_i(x) =< x >$ olsun. Böylece $| < x_i > | = m$ olduğunu kabul edelim. Bu durumda $|F_i(x)| = m$ olacaktır. Tanım 4.2.1 den G sonlu bir grup ise (F, A) nın elemanlarının en küçük ortak katı (F, A) nın mertebesi olarak bilinir. Bu durumda $|(F, A)| = ekok(|x_i|)$ olur.
2. (F, A) sonsuz devirli bir grup olduğundan $F(x) =< x >$ olacak şekilde $x \in X$ ile üretilir. Bu durumda (F, A) devirli grup olduğundan $(F, A) =< X >$ olacaktır. Tanım 4.2.1 e göre (F, A) nın mertebesi (F, A) nın elemanlarının sayısını gösterir. Bu durumda X kümesinin her x_i elemanı için (F, A) esnek kümesinin $F(x)$ elemanını üreteceğinden , $|(F, A)| = |X|$ olur.
3. Tanım 4.2.3 den $\forall x \in A$ için $F(x) = \{e\}$ olacağından devirli esnek gruptur.
4. $\forall x \in A$ için $F(x) = G$ dir. G devirli olduğundan (F, A) devirli esnek gruptur.
5. $(F, A), G$ üzerinde esnek grup olsun. G grubunun mertebesi asal ve G grubu içerisindeki herhangi bir elemanın mertebesi G grubunun mertebesini böleceğinden G nin elemanlarının mertebesi ya 1 ya da grubun mertebesi olacaktır. Bu durumda $a \in G \setminus \{e\}$ olsun. p asal sayısı için $| < a > | = p = |G|$ olsun. Bu durumda G grubu devirli olduğundan $F(x) \in (F, A)$ için $|F(x)| = | < a > |$ olur. Böylece(F, A) da devirli olacaktır.
6. (F, A), (H, B) esnek grubunun bir alt grubu olsun. Bu durumda $F(x) < H(x)$ dir. $H(x)$ devirli olduğundan $F(x)$ de devirlidir. O halde (F, A) da esnek devirli gruptur.

Teorem 4.2.4. $(f, g), K$ grubu üzerindeki (H, B) esnek grubundan G grubu üzerindeki (F, A) esnek grubuna bir esnek homomorfizma olsun. $(F, A), G$ grubu üzerinde devirli esnek grup ise $(f(F), g(A)),\ K$ grubu üzerinde devirli esnek gruptur.

İspat: İlk olarak $\big(f(F), g(A)\big), K$ grubu üzerinde bir esnek grup olduğunu gösterelim. f, G den K ya bir esnek homomorfizma olduğu biliniyor. $\forall g(x) \in g(A)$ için K nın bir alt grubu $f\big(F(x)\big) = H(g(x))$ dir. Böylece $(f(F), g(A)), K$ grubu üzerinde esnek gruptur. $F(x)$, A kümesindeki her x için devirli bir alt grup olduğundan, $F(x)$ in f altındaki görüntüsü de devirli olur ve bu durumda $\forall g(x) \in g(A)$ için K nın devirli bir

alt grubu $f\big(F(x)\big) = H(g(x))$ olur. Sonuç olarak, $(f(F), g(A))$, K grubu üzerinde devirli esnek gruptur.

Teorem 4.2.5. (F, A) ve (H, B) sırasıyla G ve K grupları üzerinde iki izomorf esnek grup olsun. (F, A) devirli esnek grup ise, (H, B) de devirli esnek gruptur.

İspat: (F, A) ve (H, B) izomorf gruplar olduklarından $\forall x \in A$ için$f\big(F(x)\big) = H(g(x))$ olacak şekilde G grubundan K ya f izomorfizması vardır. Burada g, A dan B ye birebir örten bir dönüşümdür.$\forall x \in A$ için $F(x)$ devirli bir alt grup olduğundan $H(g(x))$, K grubunun devirli bir alt grubudur. Böylece (H, B) esnek kümesinin her elemanı da devirli olur. Bu yüzden (H, B) esnek devirli gruptur.

Teorem 4.2.6. (F, A) ve (H, B), G grubu üzerinde esnek grup olsun. $(F, A) \wedge (H, B)$ de G grubu üzerinde devirli esnek gruptur.

İspat: $\forall(\alpha, \beta) \in A \times B$ ve $E(\alpha, \beta) = F(\alpha) \cap H(\beta)$ olacak şekilde $(F, A) \wedge (H, B) = (E, A \times B)$ olsun. $\forall \alpha \in A$ ve $\forall \beta \in B$ için $F(\alpha)$ ve $H(\beta), G$ nin devirli alt grupları ve $F(\alpha) \cap H(\beta)$, $F(\alpha)$ ve $H(\beta)$ gruplarının alt grupları olduğundan $\forall(\alpha, \beta) \in A \times B$ için $F(\alpha) \cap H(\beta)$, Gnin devirli bir alt grubu olur. Bu yüzden $(H, A \times B)$, G üzerinde devirli bir esnek gruptur.

Teorem 4.2.7. (F, A) ve (H, B), G grubu üzerinde devirli esnek bir grup ve $A \cap B = \emptyset$ olsun. $(F, A) \cup (H, B)$ de G grubu üzerinde devirli esnek gruptur.

İspat: $C = A \cup B$olmak üzere $(F, A) \cup (H, B) = (G, C)$ şeklinde gösterilsin. Buna göre iki esnek kümenin birleşimi aşağıdaki gibi tanımlanır. $A \cap B = \emptyset$ olduğundan $\forall c \in C$ için,

$$G(c) = \begin{cases} F(c) & c \in A \setminus B \\ H(c) & c \in B \setminus A \end{cases}$$

Bu durumda $c \in A \setminus B$ için $G(c) = F(c)$ olur. $F(c)$ esnek devirli bir grup olduğundan $G(c)$ de esnek devirli grup olur. $c \in B \setminus A$ için $G(c) = H(c)$ olur ve $H(c)$ esnek devirli bir grup olduğundan $G(c)$ de esnek devirli bir grup olur.

Teorem 4.2.8. (F,A)ve (H,B), sırasıyla G ve K üzerinde m ve n mertebeli iki devirli esnek grup olsun. m ve n sayıları aralarında iki asal sayı ise $(F,A)\times(H,B)$ de devirli esnek gruptur.

İspat: $(m,n)=1$olsun. Langrange Teoremine göre $\forall x\in A$ ve $\forall y\in B$ için $|F(x)||m$ ve $|H(y)||n$ dir. $(m,n)=1$ olduğundan $|F(x)|$ ve $|H(y)|$ aralarında asaldır. Bu nedenle $\forall(x,y)\in A\times B$ için, $F(x)\times H(y)$ de devirli esnek bir gruptur. Böylece ispat tamamlanmış olur.

4.3. Esnek Devirli Kodlar

Bu bölümde devirli kodların esnek kümeler üzerine uygulamaları çalışılmış olup devirli kod yapılarının çeşitli özellikleri esnek kümeler üzerinde tanımlanmıştır. Öncelikle devirli esnek kod tanımı verilecek ve bu tanım kullanılarak bazı cebirsel özellikler ifade edilecektir. Bu bölüm boyunca A kümesi üreteç polinomların kümesini ve $g(x)$ üreteç polinomunu gösterecektir.

Tanım 4.3.1. U evrensel polinomların kümesini göstersin $A\subset U$ olsun. Buna göre aşağıdaki gibi tanımlanan kümeye esnek devirli kod kümesi denir.

$i=0,1,\dots,n-1$ için

$$F: A\to P(U)$$
$$g(x)\to F\big(g(x)\big)=<x^i g(x)>\ mod(1+x^n)$$

Devirli esnek kod kümesi $(F,<x^i g(x)>)$ şeklinde gösterilir.

Örnek 4.3.2. $A=\{1+x^2,1+x\}$ üreteç polinomların kümesi olsun. Sırasıyla $n=4,3$ için A kümensin polinomları tanımlansın. Buna göre esnek devirli kodlar aşağıdaki tanımlanır.

$$F: A\to P(U)$$
$$1+x^2\to F(1+x^2)=<x^i(1+x^2)>\ mod(1+x^4),\ i=0,1,2,3$$
$$1+x\to F(1+x)=<x^i(1+x)>\ mod(1+x^3),\ i=0,1,2$$

(F,A)

$=\{\{0,1+x^2,x+x^3,1+x^3,x^2+x^3,1+x,1+x^2+x+x^3\},\{1+x,x+x^2,1+x^2,0\}\}=\{\{0000,1010,1001,0011,1100,0101,0110,1111\},\{000,110,101,011\}\}$

Bu bölüm boyunca U evrensel kümesi ile E parametrelerin kümesi aynı küme olarak alınacaktır.

$a(x) = a_0 + a_1x + \cdots + a_mx^m$ polinomu ile (F, A) esnek devirli kodunu çarpmak demek $F(x) \in (F, A)$ için $a(x)F(x) = \{a(x)f_i(x): f_i(x) \in F(x)\}$ anlamına gelir. $a(x)F(x)$ polinom kümesinin derecesi aşağıdaki gibi ifade edilir.

$$der\big(a(x)F(x)\big) = \max\{der(a(x)f_i(x)): f_i(x) \in F(x)\}$$

Teorem 4.3.3. (F, A) esnek devirli kod olsun. $\forall F(x) \in (F, A)$ ve herhangi bir $a(x)$ polinomu için $a(x)F(x)\ mod(1 + x^n)$, (F, A) nın elemanıdır.

İspat: (F, A) devirli esnek kod olsun. $F(x) \in (F, A)$ ve $a(x)$ elemanını tanımlayalım. $F(x) = \{f_i(x): i \in N\}$ ve $a(x) = a_0 + a_1x + \cdots + a_lx^l$ şeklinde olsun. $der\big(a(x)F(x)\big) = \max\{der(a(x)f_i(x)): f_i(x) \in F(x)\}\} = m$ diyelim

$der\big(a(x)F(x)\big) = m$ olsun. Bu durumda iki seçenek vardır.

1. $m < n$ olsun. Bu durumda $a(x)F(x)$, $F(x)$ in elemanı olacaktır.
2. $m \geq n$ durumu mevcuttur. Bu durumda $m = nq + r$ olacak şekilde $q, r \in Z$ tamsayıları vardır. Bölme algoritmasından bildiğimiz gibi $r < n$ olacaktır. nq ifadesi $mod(1 + x^n)$ için 1 e denk olduğundan $x^r \in F(x)$ olacaktır.

Klasik kodlarda her devirli kod bir lineer koddur. Bu durum esnek devirli kodlar içinde aşağıdaki durumu ifade eder.

Teorem 4.3.4. Her esnek devirli kod bir lineer koddur.

İspat: (F, A) esnek devirli bir kod olsun. Bu durumda $F(x) \in (F, A)$ olsun. (F, A) nın esnek lineer devirli bir kod olabilmesi için aşağıdaki şartları sağlaması gerekmektedir.

1. $a(x) = a_0 + a_1x + \cdots + a_mx^m$ polinomunun kod olarak ifade şekli $(a_0a_1 \ldots a_m)$ dir.

$$(a_0a_1 \ldots a_m) \in F(x) \Leftrightarrow (a_ma_0a_1 \ldots a_{m-1}) \in F(x)$$

2. $f_i(x) \in F(x)$ ve $f_i(x)^* \in F(x)$ olsun. Bu durumda $f_i(x) + f_i(x)^* \in F(x)$

Buradan da görüldüğü gibi her $F(x)$ devirli kodu lineer bir koddur. (F, A) esnek lineer devirli bir koddur.

Teorem 4.3.5. (F, A) esnek devirli kod kümesinin her elemanının üreteci tekdir.

İspat: $g_1(x), g_2(x)$; $F(x)$ in iki üreteç polinomu ve $\deg(g_1(x)) = \deg(g_2(x)) = k$ olsun. Her bir $F(x)$ elemanı lineer olduğundan $g(x) + g_2(x)$ de $F(x)$ kümesinin bir elemanı olur. $deg\ (g_1(x) + g_2(x)) < \deg\{g_1(x), g_2(x))$ eşitsizliği vardır. Bu üreteç polinomun en küçük dereceli polinom olması gerekliliği ile çelişir.

Teorem 4.3.6. (F, A) esnek devirli kod olsun. $\forall F(x) \in (F, A)$ için $|F(x)| = 2^{|<x^i g(x)>|}$dir.

İspat: $| < x^i g(x) > | = n$ olsun. $|F(x)|$ bulmak için şimdi aşağıdaki permütasyon yöntemini uygulayalım. $|F(x)| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$olur.

İdempotent polinom, kodlar için önemli bir kavramdır. Burada idempotent polinomların esnek kümelerde ki uygulamaları incelenip esnek grupların mertebelerinin bulunma yöntemile çeşitli kuvvetleri incelenecektir.

Tanım 4.3.7. $U = \{0,1,2,,..,n-1\}$ olacak şekilde N doğal sayılar kümesinin bir alt kümesi olsun. $A = \{Z_n : n \in N\}$ olmak üzere bir F dönüşümü $F(Z_n) = \{f(i) : \forall i \in Z_n\}$ şeklinde tanımlansın. Buna göre

$$F : A \to P(U)$$

$$Z_n \to F(Z_n) = \{2^j . i(mod\ n) : j = 0,..,r, 1 = 2^r mod(n)\}$$

olsun. $a_i \in \{0,1\}$ için $\sum_{j \in f(i)} a_i x^j$ şeklinde yazılan $F(x)$ kümesine idempotent polinom kümesi ve (F, A) esnek kümesine ise esnek idempotent polinom kümesi denir.

Örnek 4.3.8. $A = \{Z_3, Z_7\}$ ve U evrensel kümesi doğal sayılar kümesi olmak üzere f dönüşümünü tanımlayalım.

$$F : A \to P(U)$$

$$Z_3 \to F(Z_3) = \{f(0\}, f(1), f(2)\}$$

$$Z_7 \to F(Z_7) = \{f(0), f(1), f(2), f(3), f(4), f(5), f(6)\}$$

Bu durumda yukarıdaki kümeyi yazarsak $\{\{\{0\},\{1,2\}\},\{\{0\},\{1,2,4\},\{3,5,6\}\}\}$ şeklinde olacaktır. (F, A) esnek idempotent polinom kümesini yazarsak aşağıdaki gibi yazılır.

$$(F, A) = \{\{a_0x^0 + a_1(x + x^2)\}, \{a_0x^0 + a_1(x + x^2 + x^4) + a_2(x^3 + x^5 + x^6)\}\}$$

$$= \{\{0,1, x + x^2, 1 + x + x^2\}, \{0,1, x + x^2 + x^4, x^3 + x^5 + x^6, 1 + x + x^2 + x^4, 1 + x^3 + x^5 + x^6, x + x^2 + x^4 + x^3 + x^5 + x^6\}\}.$$

Esnek idempotent polinomlar üzerinde bazı işlemler aşağıdaki gibi yapılır.

1. $ebobF(x_i) = \{g_i(x): i \in N\}$,
2. $1 + (F, A) = \{1 + f_i(x): f_i(x) \in (F, A)\}$,
3. Bir esnek idempotent polinomun 2. kuvveti Tanım 4.1.17 kullanılarak yapılır.

Esnek idempotentpolinomların bazı özellikleri aşağıdaki gibi yazılabilir.

1. (F, A) esnek idempotent polinom olsun. $1 + (F, A)$ da esnek bir idempotent polinomdur.
2. (F, A) esnek idempotent polinom olsun. $\forall F(x) \in (F, A)$ için $F(x)^2 = F(x^2) = F(x)\ mod(1 + x^n)$.
3. (F, A) esnek idempotent polinom olsun. $A = \{g_i(x): i \in N\}$ üreteç polinomların kümesi $ebob(F(x), 1 + x^n) = g_i(x)$.

Örnek 4.3.9. Örnek 4.2.8. kullanarak yukarıdaki özelliklerin var olduğunu gösterelim.

1. $1 + (F, A) = \{\{0,1,1 + x + x^2, x + x^2\}, \{0,1,1 + x + x^2 + x^4, 1 + x^3 + x^5 + x^6, x + x^2 + x^4, x^3 + x^5 + x^6, 1 + x + x^2 + x^4 + x^3 + x^5 + x^6\}\}$ olur. Buda (F, A) esnek idempotent kümesine eşit olduğundan yine $1 + (F, A)$ idempotent polinomdur.
2. $(F, A)^2 = \{\{0,1,1 + x + x^2, x + x^2\}, \{0,1,1 + x + x^2 + x^4, 1 + x^3 + x^5 + x^6, x + x^2 + x^4, x^3 + x^5 + x^6, 1 + x + x^2 + x^4 + x^3 + x^5 + x^6\}\} = (F, A)$ olduğundan $(F, A)^2$ idempotent polinomdur.

4.4. Esnek Dual Devirli Kodlar

[2] Devirli kodlarda bir kodun dualini bulmak istiyorsak herhangi bir $a(x)$ ve $b(x)$ polinomların vektörel hali a ve b olarak olsun.

$$a.b = 0 \Longrightarrow \pi(a).\pi(b) = 0$$

oluyorsa bu durumda a ve b vektörleri birbirinin duali denir. Yukarıda verilin bu çarpım şu şekilde ifade edilir $\pi(a).\pi(b) = a_1b_1 + a_2b_2 + \cdots + a_nb_n + a_0b_0 = a.b = 0'$ dır. $C =< \{v, \pi(v), \dots, \pi(v)^{n-1}\} >$ olsun. $i = 0,1, \dots, n-1$ için $u \in C^{\perp}$ ise $\pi^i(v).u = 0$. Ayrıca $u \in C^{\perp}$ için $\pi(u) \in C^{\perp}$ olduğundan $C^{\perp}$ de devirlidir.

Lemma 4.4.1. [2]$a(x)$, $b(x)$ ve $b'(x) = x^n bx^{-1}(mod\ 1 + x^n)$ polinomların vektörel hali a, b ve b' olarak gösterilmek üzere bu durumda kodlar arasındaki duallik $k = 0,1, \dots, n-1$ için aşağıdaki gibi tanımlanır.

$$a(x)b(x)mod(1 + x^n) = 0 \Leftrightarrow \pi^k(a)b' = 0$$

Teorem 4.4.2. (F, A) ve (G, B) esnek devirli kodlar olmak üzere bu iki esnek devirli kodun dual olması için gerek ve yeter şart aşağıdaki gibi ifade edilir.

$$(F, A)^{\perp} = (G, B) \Leftrightarrow A^{\perp} = B$$

olmasıdır.

İspat: $\Rightarrow$) Kabul edelim ki $(F, A)^{\perp} = (G, B)$ ve $A^{\perp} \neq B$ olsun. $A = \{g_i(x): i = 1, \dots, n\}$ ve $B = \{g_i^*(x): i = 1, \dots, n\}$ olarak tanımlayalım.

$$(F, A) = \{F(x_i): F(x_i) =< x^n g_i(x) >, i = 1 \dots n\}$$

$$(G, B) = \{F^*(x_i): F^*(x_i) =< x^n g_i^*(x) >, i = 1 \dots n\}$$

olur. Yukarıdaki kabulümüzden $g_i^{\perp}(x) \neq g_i^*(x)$ olduğundan $F_i^{\perp}(x) \neq F_i^*(x)$ olur. Bu durumda $(F, A)^{\perp} \neq (G, B)$ olur. Bu ise kabulümüzle çelişir. Böylece $(F, A)^{\perp} = (G, B)$ olduğu görülür.

$\Leftarrow$) Kabul edelim ki $A^{\perp} = B$ ve $(F, A)^{\perp} \neq (G, B)$ olsun. $A = \{g_i(x): i = 1 \ldots n\}$ ve $B = \{g_i^*(x): i = 1 \ldots n\}$ olarak tanımlayalım. Bu durumda $g_i^{\perp}(x) = g_i^*(x)$ olacaktır. Bu ise $(F, A)^{\perp} \neq (G, B)$ olması ile çelişir. Böylece $(F, A)^{\perp} = (G, B)$ dir.

Örnek 4.4.3. Yukarıdaki örnek 4.3.2 teki devirli esnek kod kümesini kullanalım. $A = \{1 + x^2, 1 + x\}$ üreteç polinom kümesi ve $A^{\perp} = \{1 + x^2, 1 + x + x^2\}$ için(F, A) ve $(F, A)^{\perp}$ esnek kod kümesi aşağıdaki gibi yazılır.

$$(F, A) = \{\{0000,1010,0101,1001,0011,1100,1111\}, \{110,011,101,000\}\}$$

$(F, A)^{\perp} = \{\{0000,1010,0101,1001,0011,1100,1111\}, \{111\}\}$ şeklinde olur.

Esnek devirli kodlar üzerinde esnek kümelerin bazı temel kavram ve özellikleri ifade edilmiştir.

Tanım 4.4.4. (F, A) ve (G, B) iki esnek devirli kod kümesi olmak üzere $A \subset B$ ise $(F, A) \subset (G, B)$ olur. (F, A) devirli esnek kod kümesine (G, B) devirli esnek kod kümesinin alt kümesi denir.

Tanım 4.4.5. (F, A) ve (G, B) iki esnek devirli kod kümesi olmak üzere $A = B$ ise $(F, A) = (G, B)$ olur.

Tanım 4.4.6 A üreteç polinomlarının kümesi olmak üzere $\sqsubset A = 1_n - A$ şeklinde ifade edilen kümeye A kümesinin değili denir.

Önerme 4.4.7. Aşağıdaki özellikler sağlanır.

1. $\sqsubset(A \cup B) = \sqsubset A \cup \sqsubset B$
2. $\sqsubset(\sqsubset A) = A$
3. $\sqsubset(A \cap B) = \sqsubset A \cap \sqsubset B$

Tanım 4.4.8. Esnek devirli bir kod olan (F, A) kümesinin tümleyeni$(F, A)^c$ şeklinde gösterilir ve aşağıdaki gibi tanımlanır.

$(F, A)^c = (F^c, \sqsubset A)$ dir.

Örnek 4.4.9. Örnek 4.3.2 teki üreteç polinomlar kümesini kullanalım. $A = \{1 + x^2, 1 + x\}$ için $A = \{1 + x^2, 1 + x\} = \{1010{,}110\}$ kümesinin değili $\vdash A = \{0101, 001\}$ olur. Bu durumda

$$F: A \rightarrow P(U)$$

$$1 + x^2 \rightarrow F(1 + x^2) = < x^i(1 + x^2) > mod(1 + x^4), i = 0, 1, 2, 3$$

$$1 + x \rightarrow F(1 + x) = < x^i(1 + x) > mod(1 + x^3), i = 0, 1, 2$$

$$(F, A) = \{\{0, 1 + x^2, x + x^3, 1 + x^3, x^2 + x^3, 1 + x, 1 + x^2 + x + x^3\}, \{1 + x, x + x^2, 1 + x^2, 0\}\}$$

$$(F^c, \vdash A) = \{\{0000{,}1010{,}1001{,}0011{,}1100{,}0101{,}0110\}, \{000{,}110{,}101{,}011\}\}$$

Tanım 4.4.10. (F, A) ve (G, B) esnek devirli kodlar olsun. $(H, C), (F, A)$ ve (G, B) nin birleşimi $C = A \cup B$ olmak üzere $\forall e \in C$ için

$$H(e) = \begin{cases} F(e) & e \in A - B \\ G(e) & e \in B - A \\ F(e) \cup G(e) & e \in A \cap B \end{cases}$$

şeklinde tanımlanır.

$(F, A) \cup (G, B) = (H, C)$ şeklinde de gösterilir.

Önerme 4.4.11. (F, A) esnek devirli kod olmak üzere aşağıdaki özellikler sağlanır.

1. $(F, A) \cup (F, A) = (\mathrm{F}, \mathrm{A})$,
2. $((F, A) \cup (G, B))^c = (F, A)^c \cup (G, B)^C$,
3. $(F, A) \cup \big((G, B) \cup (H, C)\big) = \big((F, A) \cup (G, B)\big) \cup (H, C)$,

İspat: Yukarıdaki ifadeler Tanım 4.4.9 ve Tanım 4.4.10 kullanılarak kolayca ispat edilir.

Teorem 4.4.12. $(F, A), (H, B)$ esnek devirli kodlar olsun. $A \cap B \neq \emptyset$ olmak üzere $(F, A) \cup (H, B)$ esnek devirli koddur.

İspat: $(F,A) \cup (H,B) = (U,C)$ olsun. $C = A \cup B \neq \emptyset$ olduğundan $\forall x \in C$ için $x \in A - B$, $x \in B - A$ veya $x \in A \cap B$ dır. $x \in A - B$ ise $U(x) = F(x)$ olur. Bu durumda $U(x)$ esnek devirli koddur. $x \in B - A$ ise $U(x) = H(x)$ için durumda $U(x)$ esnek devirli koddur. $U(x) \in (F,A) \cap (H,B)$ olmak üzere bu durumda $U(x)$ esnek devirli koddur.

4.5. Esnek Devirli Kodların Hamming Kodlar Üzerine Uygulamaları

Bu bölümde esnek devirli kod tanımı kullanılarak esnek devirli kodların üreteç matrisler inşa edilmiştir. Ayrıca bu üreteç matrisler yardımı ile bir hamming kodun nasıl elde edileceği konusunda teoremler verilmiştir. Bu teoremler sayesinde elde edilen yeni kodun uzunluğu, tabanındaki eleman sayısı ve minimum uzaklığının nasıl hesaplanacağı hakkında bazı metotlar geliştirilmiştir.

Tanım 4.5.1 (F,A) esnek devirli bir kod olmak üzere $F(x_i) \in (F,A)$ için $F(x_i)$ kümeleri (n_i, k, d_i) şeklinde tanımlansın. Buna göre (F,A) esnek devirli kodun üreteç matrisi $G_{(F,A)}$ olarak gösterilir ve $i = 1 \ldots m$ için aşağıdaki gibi tanımlanır.

$$G_{(F,A)} = (G_{F(x_1)} | G_{F(x_2)} | \ldots | G_{F(x_m)})$$

Örnek 4.5.2. $A = \{1, 1 + x + x^2\}$ olsun. Bu durumda $n = 4$ için esnek küme üzerine tanımladığımız esnek devirli kod yapısını belirleyelim.

$$F: A \to P(U)$$

$$1 \to F(1) =< x^i(1) >, n = 4$$

$$1 + x + x^2 \to F(1 + x + x^2) =< x^i(1 + x + x^2) >, n = 4$$

Buna göre esnek devirli kod aşağıdaki gibi bulunur.

$$(F,A) = \{\{< 1 + x + x^2, x + x^2 + x^3, 1 + x^2 + x^3, 1 + x + x^3 >\}, \{< 1, x, x^2, x^3 >\}\}$$

Böylece üreteç matris

$$G_{(F,A)} = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right)$$

olarak oluşturulmuştur.

Bu elde edilen üreteç matris genişletilmiş hamming kod olarak bilinen $(8,4,4)$ kodudur.

Teorem 4.5.3. (F, A) esnek devirli bir kod ve $G_{(F,A)}$ esnek devirli kodun üreteç matrisi olsun. $F(x_i) \in (F, A)$ için $F(x_i)$ kodları (n_i, k, d_i) şeklinde gösterilsin. (F, A) nın üreteç matrisi $G_{(F,A)}$ olan $(n_1 + n_2 + \cdots + n_m, k, d \geq d_1 + d_2 + \cdots + d_m)$ koddur.

İspat: $G_{(F,A)}$ üreteç matrisinin oluşturduğu kod kümesinin her bir elemanının uzunluğunun $n_1 + n_2 + \cdots + n_m$ olduğu ve tabanındaki eleman sayısının k olduğu açıktır.

Bir lineer kodun minimum uzaklığı kod içerisindeki sıfırdan farklı en az ağırlıklı kod kelimesi olduğu bilinmektedir. Şimdi $y \in F_2^k$ elemanını alalım. Buna göre

$$yG_{(F,A)} = y(G_{F(x_1)}|G_{F(x_2)}| \ldots |G_{F(x_m)})$$

$$(yG_{F(x_1)}|yG_{F(x_2)}| \ldots |yG_{F(x_m)})$$

elde edilir. Bu durumda üreteç matrislerin matrisi olan

$$G_{(F,A)} = (G_{F(x_1)}|G_{F(x_2)}| \ldots |G_{F(x_m)})$$

matrisinin elemanları yeni oluşturulacak kodun üreteç matrisi olur. $(yG_{F(x_1)}|yG_{F(x_2)}| \ldots |yG_{F(x_m)})$ de bu kodun elemanı olduğu bilinmektedir. Bu elde edilen kodun minimum uzaklığı en az $d_1 + d_2 + \cdots + d_m$ kadar olur. Çünkü en az bir kod kelimesinin ağırlığı $d_1 + d_2 + \cdots + d_m$ dır. Sonuç olarak yeni elde edilen kodun minimum uzaklığı $d \geq d_1 + d_2 + \cdots + d_m$ olmalıdır.

Aşağıdaki teoremde yukarıdaki gibi tanımlanan devirli esnek kodun üreteç matrisinden elde edilen kodun uzunluğu, minimum uzaklığı ve tabandaki eleman sayılarının nasıl tanımlanması ile ilgili başka bir teorem daha ifade ve ispat edilmiştir.

Teorem 4.5.4. (F, A) esnek devirli bir kod ve $G_{(F,A)}$ esnek devirli kodun üreteç matrisi olsun. $F(x_i) \in (F, A)$ için $F(x_i)$ kodları (n_i, k, d_i) şeklinde tanımlansın. $G_{(F,A)}$ üreteç matrisli kod $(n_1 + n_2 + \cdots + n_m, k, d \geq d_1 + d_2 + \cdots + d_m)'$ e eşit bir kod kümesidir.

İspat:

$$G_{(F,A)} = \begin{pmatrix} x_1 & y_1 & \cdots & z_1 \\ x_2 & y_2 & \cdots & z_2 \\ \vdots & \vdots & \cdots & \vdots \\ x_k & y_k & \cdots & z_k \end{pmatrix}_{n \times k}$$

$$wt(x_1|y_1| \ldots |z_1) = wt(x_1) + wt(y_1) + \cdots + wt(z_1) \geq d_1 + d_2 + d_3 + \cdots + d_m$$

$$wt(x_2|y_2| \ldots |z_2) = wt(x_2) + wt(y_2) + \cdots + wt(z_2) \geq d_1 + d_2 + d_3 + \cdots + d_m$$

……..…..

$$wt(x_{k_1}|y_{k_2}| \ldots |z_{k_2}) = wt(x_{k_1}) + wt(y_{k_2}) + \cdots + wt(z_{k_2}) \geq d_1 + d_2 + d_3 + \cdots + d_m$$

Eşitsizlikler taraf tarafa toplanırsa

$wt(x_1|y_1| \ldots |z_1) + wt(x_2|y_2| \ldots |z_2) + \cdots + wt(x_k|y_k| \ldots |z_k) \geq kd_1 + kd_2 + \cdots + kd_m$buradan anlaşıldığı gibi

$$wt(x_1|y_1| \ldots |z_1) \geq d,$$

$$wt(x_2|y_2| \ldots |z_2) \geq d,$$

… … … … … ….

$$wt(x_k|y_k| \ldots |z_k) \geq d.$$

Eşitsizlikler taraf tarafa toplanırsa

$wt(x_1|y_1| \ldots |z_1) + wt(x_2|y_2| \ldots |z_2) + \cdots + wt(x_k|y_k| \ldots |z_k) \geq kd$ olduğu açıktır. Yukarıdaki eşitsizlikte yerine yazarsak ifadeyi

$$kd \geq kd_1 + kd_2 + \cdots + kd_m$$

$$d \geq d_1 + d_2 + d_3 + \cdots + d_m$$

Yeni üretilen ve üreteç matrisi $G_{(F,A)}$ olan kodun minimum uzaklığı hesaplanmıştır.

BÖLÜM 5

$(\frac{n}{2}-1)$ 'DEN DAHA AZ VEYA EŞİT SAYIDA VE SADECE TEK SAYILARDAKİ HATAYI DOĞRULAYAN ESNEK KODLAR

Bu bölüm de 4. Bölümde tanımlanan esnek lineer devirli kodlardan farklı olarak lineer olmayan kodlar çalışılacaktır. Esnek kümeler üzerine kod sistemleri tanımlanarak bir çarpım işlemi verilmiş ve bu işlem ile kodlama yapma algoritması tanımlanmıştır. Verilen bir mesaj kümesinin kodlandıktan sonra kodlanan kelimelerin çözülüp mesaj kümlerinin elde edilmesi yöntemleri oluşturulmuştur. Kodlanan kelimelerin transferi sırasında oluşan hataların belirlenmesi ve çözülmesi için bir algoritma belirlenmiştir. Ayrıca esnek kümeler üzerine tanımlanan bazı tanımlar esnek kod yapısı üzerinde de ifade edilmiştir. Bu bölümün son kısımda ise bir örnekle kodlama teorisinin temel mantığı olan hata bulma algoritmasının çalıştığı gösterilmiştir. Bu bölüm boyunca U evrensel kümesi kodların kümesi, n ise bir kodun uzunluğunu ve w kodun ağırlığını gösterecektir.

5.1.Esnek Kodlar

Tanım 5.1.1. U vektörlerin kümesini göstermek üzere $P(U)$, U nun kuvvet kümesi olsun. E kod kelimelerinin ağırlığını göstersin ve $A \subseteq E$ olsun. Buna göre $F: A \rightarrow P^*(U)$ şeklinde bir esnek kod yapısı aşağıdaki gibi tanımlanır ve $(F,A)_n^w$ şeklinde gösterilir. Burada $P^*(U)$, kuvvet kümesinin bir alt kümesi, w, $\forall x \in A$ için kodun ağırlığını, n ise kodun uzunluğunu göstermektedir.

$(F,A)_n^w = \{(w, F(w), n): e \in A\}$.

Örnek 5.1.2. $(F,A)_n^w$ esnek bir kod olmak üzere U evrensel kümesi aşağıdaki gibi tanımlanır. $U = \{0,1,00,10,01,11,000,100,010,001,110,101,011,111 \ldots\}$ $n = 3, A = \{1,2\}$, $E = \{1,2\}$ için $P(U)$ kuvvet kümesinin bir alt kümesi aşağıdaki gibi tanımlansın.

$P^*(U) = \{\{000,100,010,001,110,101,011,111\}\}$ böylece esnek kod yapısı aşağıdaki gibi ifade edilir. $(F,A)_n^w = \{(1,\{100,010,001\},3),(2,\{110,101,011\},3)\}$.

Tanım 5.1.3. U üzerinde bir esnek kod yapısı olan $(F,A)_n^w$ kodu için;

1. $A = \{0\}$ ise $(F, A)_n^w$ yapısına sıfır esnek kod denir. $(F, A)_n^w = 0_n$ şeklinde gösterilir.
2. $A = N$ ise $(F, A)_n^w$ yapısına evrensel esnek kod denir. $(F, A)_n^w = F_2^n$ şeklinde gösterilir.

Tanım 5.1.4. U evrensel kümesi üzerinde $(F, A)_n^w$, $(F, B)_n^w$ ve $(F, C)_n^w$ esnek kodlar olsun .

1. $B \subseteq A$ ise $(F, B)_n^w$ esnek koduna $(F, A)_n^w$ esnek kodunun alt kodu denir ve $(F, B)_n^w \subseteq (F, A)_n^w$ şeklinde gösterilir.
2. $A = B$ ise $(F, B)_n^w$ esnek kod yapısı $(F, A)_n^w$ esnek koduna eşittir $(F, B)_n^w = (F, A)_n^w$ şeklinde gösterilir.

Tanım 5.1.5. $(F, A)_n^w, (F, B)_n^w$, $(F, C)_n^w$ U üzerinde esnek kodlar olsun. Buna göre aşağıdaki tanımlar verilebilir.

1. $C = A \cup B$ olmak üzere $(F, C)_n^w$ ne koduna $(F, A)_n^w$ ve $(F, B)_n^w$, iki esnek kodun birleşimi denir.
$$(F, A)_n^w \cup (F, B)_n^w = (F, C)_n^w$$
şeklinde gösterilir.
2. $C = A \cap B$ için, $(F, C)_n^w$ ne koduna $(F, A)_n^w$ ve $(F, B)_n^w$, iki esnek kodun kesişimi denir.
$$(F, A)_n^w \cap (F, B)_n^w = (F, C)_n^w$$
şeklinde gösterilir.
3. U üzerinde $(F, A)_n^w$ nin komplementi $(F, B)_n^w = 1_n$ -$(F, A)_n^w$ şeklinde tanımlanır ve $((F, A)_n^w)^c$ şeklinde gösterilir.
4. $(F, A)_n^w \cap (F, B)_n^w = \emptyset$ ise $(F, A)_n^w$ ve $(F, B)_n^w$ için ayrık esnek kodlar denir.

Önerme 5.1.6. $((F, A)_n^w$ esnek kod olmak üzere aşağıdaki özellikleri sağlanır.

1. $((F, A)_n^w)^c)^c = (F, A)_n^w$,
2. ${0_n}^c = 1_n$.

İspat:

1. $(((F, A)_n^w)^c)^c$ esnek kod yapısının tümleyeninin tümleyeni $(((F, A)_n^w)^c)^c = 1_n - ((F, A)_n^w)^c$şeklinde olur. Şimdi de tümleyeninin yerine yukarıdaki tanım

yazılırsa $((F,A)_n^w)^c)^c = 1_n - (((F,A)_n^w)^c = 1_n - (1_n - ((F,A)_n^w)) =$ $((F,A)_n^w)$ elde edilir.

2. ${0_n}^c$ tanımı yazılırsa ${0_n}^c = 1_n - 0_n$ aynı uzunluğa sahip ve sadece 1 ve 0'dan oluşan 1_n ve 0_n kod kelimeleri ${0_n}^c = 1_n + 0_n = 1_n$ olur.

Önerme 5.1.7. $(F,A)_n^w, (F,B)_n^w, (F,C)_n^w$ esnek kodlar olmak üzere aşağıdaki özellikler sağlanır.

1. $(F,A)_n^w \cup (F,A)_n^w = (F,A)_n^w$,
2. $(F,A)_n^w \cap ((F,A)_n^w)^c = \emptyset$,
3. $(F,A)_n^w \cup (F,B)_n^w = (F,B)_n^w \cup (F,A)_n^w$,
4. $((F,A)_n^w \cup (F,B)_n^w) \cup (F,C)_n^w = (F,A)_n^w \cup ((F,B)_n^w \cup (F,C)_n^w)$.

İspat:

1. $A \cup A = A$ olduğundan $(F,A)_n^w \cup (F,A)_n^w = (F,A)_n^w$ olduğu açıktır.
2. Esnek kod kümesine ait olan bir $F(x)$ elemanı alalım. $F(x) \in (F,A)_n^w \cap ((F,A)_n^w)^c$ olsun. Bu durumda $F(x) \in (F,A)_n^w$ ve $F(x) \in ((F,A)_n^w)^c$ olur. Böylece $F(x) \notin (F,A)_n^w$ olur. Bu da kabulümüzle çelişir. $(F,A)_n^w \cap ((F,A)_n^w)^c = \emptyset$.
3. $A \cup B = B \cup A$ olduğundan $(F,A)_n^w \cup (F,B)_n^w = (F,B)_n^w \cup (F,A)_n^w$ olduğu açıktır.
4. Önerme 5.1.6 nın 3. şıkkına benzer şekilde yapılır.

Önerme 5.1.8. $(F,A)_n^w, (F,B)_n^w, (F,C)_n^w$ esnek kodlar olmak üzere aşağıdaki gibi verilen bazı özellikler sağlanır.

1. $(F,A)_n^w \cap (F,A)_n^w = (F,A)_n^w$,
2. $(F,A)_n^w \cap (F,B)_n^w = (F,B)_n^w \cap (F,A)_n^w$,
3. $((F,A)_n^w \cap (F,B)_n^w) \cap (F,C)_n^w = (F,A)_n^w \cap ((F,B)_n^w \cap (F,C)_n^w)$

İspat: İspat açıktır.

Önerme 5.1.9. $(F,A)_n^w, (F,B)_n^w$ ve $(F,C)_n^w$ U üzerinde esnek kodlar olsun. Bu durumda De Morgan kanunları geçerlidir.

1. $((F,A)_n^w \cap (F,B)_n^w)^c = ((F,A)_n^w)^c \cap ((F,B)_n^w)^c$,
2. $((F,A)_n^w \cup (F,B)_n^w)^c = ((F,A)_n^w)^c \cup (F,B)_n^w)^c$.

İspat:

1. $$((F,A)_n^w \cap (F,B)_n^w)^c = \mathbf{1}_n - ((F,A)_n^w \cap (F,B)_n^w)$$
$$= (\mathbf{1}_n - (F,A)_n^w) \cap (\mathbf{1}_n - (F,B)_n^w)$$
$$= ((F,A)_n^w)^c \cap ((F,B)_n^w)^c$$
2. $$((F,A)_n^w \cup (F,B)_n^w)^c = \mathbf{1}_n - ((F,A)_n^w \cup (F,B)_n^w))$$
$$= (\mathbf{1}_n - (F,A)_n^w) \cup (\mathbf{1}_n - (F,B)_n^w)$$
$$= ((F,A)_n^w)^c \cup ((F,B)_n^w)^c.$$

Önerme 5.1.10. $(F,A)_n^w, (F,B)_n^w, (F,C)_n^w$ esnek kodlar olmak üzere buna göre aşağıdaki özellikler sağlanır.

1. $((F,A)_n^w \cup (F,B)_n^w)) \cap (F,C)_n^w = ((F,A)_n^w \cap (F,B)_n^w) \cup ((F,A)_n^w) \cap (F,C)_n^w)$,
2. $((F,A)_n^w \cap (F,B)_n^w) \cup (F,C)_n^w = ((F,A)_n^w) \cup (F,C)_n^w) \cap ((F,B)_n^w \cup (F,C)_n^w)$.

İspat:

İspatlar önerme 5.1.7 dekine benzer şekilde ispat edilebilir.

Lineer olmayan esnek kodların temel bazı özellikleri verildikten sonra esnek kodlar üzerinde kodlamanın, kod çözmenin ve hata bulma algoritmasının temelini oluşturacak vektörel çarpım tanımlayalım.

Tanım 5.1.11. Aşağıda gibi tanımlanan çarpıma vektörel çarpım denir. Ayrıca vektörel çarpım sembolü Λ şeklinde gösterilecektir. $a = (a_1 a_2 \dots a_j)$, $d = (d_1 d_2 \dots d_k)$ olmak üzere ;

$(a_1 a_2 \dots a_j) \Lambda (d_1 d_2 \dots d_k) = \{(max\{a_1, d_1\} max\{a_1, d_2\} \dots max\{a_1, d_k\}), (max\{a_2, d_1\} max\{a_2, d_2\} \dots \{max\{a_2, d_k\}) \dots (max\{a_j, d_1\}, max\{a_j, d_2\} \dots max\{a_j, d_k\})$.

Tanım 5.1.12. $(F,A)_n^w, (F,B)_n^w$ esnek kodlar olmak üzere. Tanım 5.1.10 vektörel çarpım işlemini kullanarak elde edilien esnek kod kümesine kodlanmış esnek kod kümesi denir. Vektörel çarpımın tanımlandığı iki esnek kod kümesinden biri mesaj kümesi olarak

adlandırılırken bir diğeri ise kodlama kümesi olarak adlandırılır. Mesaj kümesi$M$ ile kodlama kümesi ise E ile gösterilir. 1_n herhangi bir kodlama işleminde kullanılmaz.

Örnek 5.1.13. Mesaj kümesi ve kodlama kümesi olarak aşağıdaki iki esnek kod kümesini belirleyelim.

$$(F,A)_4^2 = \{(2,\{1100,1010,1001,0110,0101,0011\},4)\}$$

$$(F,A)_3^0 = (0,\{000\},3)$$

Vektörel çarpımı işlemini uygularsak;

$M\Lambda E =$

$\{(6,\{111111000000,111000111000,000111000111,000111111000,000000111111\},12)\}$ esnek kod kümesi elde edilir. Bu kod $(F,A)_4^2$ mesaj kelimesinin$(F,A)_3^0$ kodlanması ile elde edilen kod kümesidir.

Kod çözme algoritması vektörel çarpım işleminin ters işlemi ugulanırsa esnek kodlarda kod çözme (decoding) işlemi gerçekleştirlir.

Örnek 5.1.14. Örnek 5.1.12 göz önüne alalım. Bu durumda M mesaj kümesinin elemanlarını bulalım. M mesaj kümesinin herhangi bir elemanını $\{xyzt\}$ olarak düşünelim. Eesnek kod kümesi ile vektörel çarpımını kullanırsak $m \in M$için

. $m\Lambda E = \{(6,\{111111000000\},12)\}$ dir. Buna göre

$$\{xyzt\}\Lambda\{000\} = \{111111000000\}$$

$$x\ \Lambda\{000\} = 111 \rightarrow x = 1$$

$$y\ \Lambda\{000\} = 111 \rightarrow y = 1$$

$$z\ \Lambda\{000\} = 000 \rightarrow z = 0$$

$$t\ \Lambda\{000\} = 000 \rightarrow t = 0$$

$$\{xyzt\}\Lambda\{000\} = \{111000111000\}$$

$$x\ \Lambda\{000\} = 111 \rightarrow x = 1$$

$$y\ \Lambda\{000\} = 000 \rightarrow y = 0$$

$$z\ \Lambda\{000\}\ = 111 \rightarrow z\ =\ 1$$

$$t\ \Lambda\{000\}\ =\ 000\ \rightarrow\ t\ =\ 0$$

$$\{xyzt\}\Lambda\{000\} = \{000111000111\}$$

$$x\ \Lambda\{000\}\ = 000 \rightarrow x\ =\ 0$$

$$y\ \Lambda\{000\} = 111 \rightarrow y = 1$$

$$z\ \Lambda\{000\} = 000 \rightarrow z = 0$$

$$t\ \Lambda\{000\}\ =\ 111\ \rightarrow\ t\ =\ 1$$

$$\{xyzt\}\Lambda\{000\} = \{000111111000\}$$

$$x\ \Lambda\{000\}\ = 000 \rightarrow x\ =\ 0$$

$$y\ \Lambda\{000\} = 111 \rightarrow y = 1$$

$$z\ \Lambda\{000\} = 111 \rightarrow z = 1$$

$$t\ \Lambda\{000\}\ =\ 000\ \rightarrow\ t\ =\ 0$$

$$\{xyzt\}\Lambda\{000\} = \{000000111111\}$$

$$x\ \Lambda\{000\}\ = 000 \rightarrow x\ =\ 0$$

$$y\ \Lambda\{000\} = 000 \rightarrow y = 0$$

$$z\ \Lambda\{000\} = 111 \rightarrow z = 1$$

$$t\ \Lambda\{000\}\ =\ 111\ \rightarrow\ t\ =\ 1$$

çözümü elde edilir.

5.2. $(\frac{n}{2} - 1)$'den Daha Az veya Eşit Tek Sayılarda Hata Doğrulayan Esnek Kodlar

Lineer olmayan esnek kodlarda hata doğrulama algoritmasını vermeden önce hata doğrulama algoritmasında kullanılacak olan bazı teoremleri ifade ve ispat edelim.

Teorem 5.2.1. Aynı uzunluk ve ağırlığa sahip esnek kodların minimum uzaklığı 2'dir.

İspat: x ve y $F(x)$'in birer elemanı olsun. Bu durumda $d(x,y)$ minimum uzaklığı için iki durum vardır. $d(x,y)$ ya çift yada tek olmalıdır.

1. $d(x,y)$ minimum uzaklığı tek olsun. Bu durumda $d(x,y) = 2n+1$ olarak alalım. Fakat bu durum kodların aynı ağırlıkta olması durumu ile çelişir. Yani $w(x) \neq w(y)$ olacaktır. Bu bir çelişkidir. Yani $d(x,y) = 2n+1$ olamaz.
2. $d(x,y)$ minimum uzaklığı çift olsun. Bu durumda $d(x,y) = 2n$ olarak alalım. O zaman kodun minimum uzaklığı bir çift sayıdır. Şunu biliyoruz ki esnek kod kümeleri aynı uzunluğa ve aynı ağırlığa sahip kodlardan oluştuğu bilinmektedir. Yani kod kümesi içerisinde 10… kod kelimesi varken 01… kod kelimesi de bulunmak zorundadır. Minimum uzaklık tanımı gereği kodun en küçük uzaklığı her zaman 2 olmak zorundadır. Böylece kodun her zaman minimum uzaklığı 2'dir.

Teorem 5.2.2. Aynı uzunluk ve ağırlığa sahip tüm kodların toplamı ya 0_n ya da 1_n olur.

İspat: Bu ispatı yapabilmek için aynı ağırlık ve aynı uzunluğa sahip kodların bütün dijitlerine gelen 1 sembolünün aynı sayıda olduğunu göstermek yeterlidir.

1. İlk olarak birinci dijite 1 sembolünün gelme durumunu inceleyelim. Birinci dijite 1 gelme durumu aşağıdaki gibi hesaplanır.

$$\frac{(n-1)!}{(n-1-w+1)!\,(w-1)!}$$

2. Şimdi ikinci dijite bir gelme durumunu inceleyelim. Bu durumda iki seçenek söz konusudur.

a. 01…

↓

$$\frac{(n-2)!}{(n-2-w+1)!\,(w-1)!}$$

b. 11…

↓

$$\frac{(n-2)!}{(n-2-w+2)!\,(w-2)!}$$

Şimdi iki durumu toplarsak

$$\frac{(\mathrm{n}-2)\,!}{(n-2-w+1)!(w-1)!}+\frac{(\mathrm{n}-2)\,!}{(n-2-w+2)!(w-2)!}=\frac{(\mathrm{n}-1)\,!}{(n-1-w+1)!(w-1)!}$$

Görüldüğü gibi ikinci dijitte, birinci dijitte olduğu gibi 1 gelme durumu aynıdır. Şimdi birde son dijite gelme durumunu inceleyelim.

……..

n) …1

↓

$$\frac{(\mathrm{n}-1)\,!}{(n-1-w+1)!\,(w-1)!}$$

Son dijitte 1 gelme durumu diğer dijitlerle aynıdır.

Örnek 5.2.3. C kodunu aşağıdaki gibi belirleyelim ve dijitlerindeki 1'lerin sayısına bakalım.

$$C=\{110,011,101\}$$

Dikkat edecek olursak birinci, ikinci ve üçüncü dijitlerindeki 1'lerin sayısı aynıdır. Yani hepsi 2'dir.

Teorem 5.2.4. Vektörel çarpım sonucu elde edilen esnek kodların elemanları toplamı ya 0_n 'dir ya da 1_n'dir.

İspat: M ve E sırasıyla bir mesaj kümesi ve kodlama kümesi olsun. M ve E esnek kod kümeleri $M=\{x_1 \dots x_n, y_1 \dots y_n\}$ ve $E=\{a_1 \dots a_n, b_1 \dots b_n\}$ şeklinde alınsın. Şimdi M esnek kod kümesini yukarıdaki vektörel çarpım işlemini kullanarak E kodlayıcı kümesi ile kodlayalım.

$M\Lambda E=\{x_1 \dots x_n \Lambda a_1 \dots a_n, x_1 \dots x_n \Lambda b_1 \dots b_n, y_1 \dots y_n \Lambda a_1 \dots a_n, y_1 \dots y_n \Lambda b_1 \dots b_n\}$.
Şimdi bu elemanların toplamını aşağıdaki gibi yazalım.

$= \{x_1 \dots x_n \Lambda a_1 \dots a_n + x_1 \dots x_n \Lambda b_1 \dots b_n + y_1 \dots y_n \Lambda a_1 \dots a_n + y_1 \dots y_n \Lambda b_1 \dots b_n\}$ olur.

$$= \{(x_1 \dots x_n + y_1 \dots y_n) \Lambda a_1 \dots a_n + (x_1 \dots x_n + y_1 \dots y_n) \Lambda b_1 \dots b_n\}$$

Şunu biliyoruz ki Teorem 5.2.2 den aynı ağırlık ve uzunluğa sahip kodların toplamı ya 0_n ya da 1_n olduğu bilinmektedir. Bu durumda yukarıdaki ifadeyi aşağıdaki gibi yazabiliriz. $(x_1 \dots x_n + y_1 \dots y_n) = 0_n$ yada 1_n olacaktır. Diğer taraftan $(x_1 \dots x_n + y_1 \dots y_n) = 0_n$ olsun. Böylece

$$= \{(x_1 \dots x_n + y_1 \dots y_n) \Lambda a_1 \dots a_n + (x_1 \dots x_n + y_1 \dots y_n) \Lambda b_1 \dots b_n\}$$

elde edilir.

Bu ifadenin sonucu 0_n ya da 1_n şeklinde olacaktır. $(x_1 \dots x_n + y_1 \dots y_n) = 1_n$ olsun. Bu durumda yukarıdaki ifadenin sonucu 0_n olmak zorundadır. Buda ispatı tamamlar.

Örnek 5.2.5. Şimdi iki esnek kod seçelim ve yukarıdaki gibi bir vektörel çarpımı tanımlayalım.

$\{100,010,001\} \Lambda \{110,011,101\}$ aşağıdaki gibi çarpımını hesaplayalım.

$100 \Lambda \{110,101,011\} = \{111110110,111101101,111011011\}$ kod kelimelerinin toplamını yazalım. $\{111\ 000\ 000\} = 1_3 0_3 0_3$

$010 \Lambda \{110,101,011\} = \{110111110, 101111101, 011111011\}$ bunlarında toplamı yazılırsa

$\{000\ 111\ 000\} = 0_3 1_3 0_3$

$001 \Lambda \{110,101,011\} = \{110110111, 101101111, 011011111\}$ bunlarında toplamı yazılırsa

$\{000\ 000\ 111\} = 0_3 0_3 1_3$

Bu üç toplamı aşağıdaki gibi yazarsak

$$\{1_3 0_3 0_3,\ 0_3 1_3 0_3,\ 0_3 0_3 1_3\}$$

şeklinde elde edilir.

Kodların toplamının 1_9 olduğu açıktır.

Bu tanım ve teoremler yardımı ile hata bulma algoritmasını şu şekilde ifade edilir.

5.3. Esnek Kümelerde Hata Bulma Algoritması

Aşağıdaki adımlar izlenerek bir algoritma verilecektir.

1. Esnek kodun her $F(x)$ elemanın içindeki tüm elemanlar toplanır.
2. Bu toplam hatalı ise 0_n ya da 1_n' den farklı olacaktır.
3. Bu toplam ile 0_n ya da 1_n arasındaki minimum uzaklığa bakılır.
4. Bu toplamın minimum uzaklığının 0_n ya da 1_n nin hangisine yakın olduğu belirlenir.
5. Hatalı olan eleman, elde edilen toplamın yani 0_n ya da 1_n'nin uzaklığından farklıdır.
6. Hatalı eleman bulunduktan sonra hatalı olmayan tüm elemanlar toplanır.
7. Hatalı olmayan elemanların toplamından elde edilen sonuç ile 0_n ya da 1_n toplanır hatalı eleman doğrulanır.

Örnek 5.3.1. Şimdi aşağıdaki gibi esnek kod kümelerinin vektörel çarpımını yazalım. Bozuk eleman aşağıdaki gibi **010001011** bir eleman olsun.

{111110110, 111011011, 111101101, 110111110, **010001011**, 101111101, 110110111, 011011111, 101101111}

1. Önce elemanları toplayalım. Elde edilen sonuç $\{110001111\}$.
2. Kodun 0_n ya da 1_n 'e yakın olduğuna bakalım.

$$d(110001111, 111111111) = 3$$

$$d(110001111,000000000) = 6$$

3. Kod elemanlarının toplamı 111111111 olmak zorundadır
4. Şimdi kod elemanlarını tek tek 111111111 ile karşılaştıralım.

$$d(111111111, 111110110) = 2$$

$$d(111111111111011011) = 2$$

$$d(111111111, 111101101) = 2$$

$$d(111111111, 110111110) = 2$$

$$d(111111111, 101111101) = 2$$

$$d(111111111, 110110111) = 2$$

$$d(111111111, 011011111) = 2$$

$$d(111111111, 101101111) = 2$$

$d(111111111, \mathbf{010001011}) = 4$ (hatalı kod kelimesi)

5. Hatalı olmayan kod kelimelerini hepsini toplarsak 100000100 elde edilir.
6. Şimdi tüm kod kelimelerinin toplamını yazarsak doğru kod kelimesini 111111111+100000100 = 011111011 şeklinde bulunur.

6.BÖLÜM

SONUÇ VE ÖNERİLER

Hata doğrulama kod teorisi 1948 yılında Claude Shannon'un "A Mathematical Theory of Communication" makalesi ile birlikte cebirsel yapıları içeren matematiksel teorilerde kullanılmaya başlanmıştır. 1948 yılında ortaya atılan bu teori günümüzde birçok bilgisayar sisteminin yapısında iletişim araçlarında kullanılmaya başlanmıştır. Bir gürültülü kanal üzerinde bilginin daha güvenilir iletimi için yapılan kodlama ve kod çözme teknikleri bugün hayatımızda çok büyük önem teşkil etmektedir.

Bu tezde, esnek kümeler kullanılarak devirli esnek gruplar inşa edilmiş ve bu gruplarla devirli esnek kodlar tanımlanarak çeşitli sonuçlar elde edilmiştir. Bir, iki ve üçüncü bölümlerde esnek kümeler, esnek cebirsel yapılar, kodlar ve devirli kodlarla ilgili literatür çalışması yapılmıştır.

Dördüncü bölümde bir esnek kümenin kuvveti, mertebesi, esnek grubun mertebesi, devirli esnek gruplar ve esnek kümeler üzerinde inşa edilen devirli esnek kodlar oluşturulmuş bu kavramlara ait sonuçlar elde edilmiştir.

Devirli esnek kodların tanımı kullanılarak yeni bir üreteç matrisi elde edilmiş ve bu matrisin hamming kodlarla arasındaki ilişkiler incelenmiştir.

Beşinci bölümde ise, esnek kümeler üzerinde vektörel çarpım tanımlanmış ve bu çarpım kullanılarak lineer olmayan kodlar elde edilmiştir. Ayrıca bu metot için kodlama ve kod çözme algoritması geliştirilmiştir. Özellikle kurulan algoritmanın bilgisayar programları üzerinde uygulanabilirliği gözetilmiştir.

Sonuç olarak esnek kümeler yardımı ile elde edilen esnek devirli kodlardan Hamming kodların elde ediliş yöntemi ile golay kodlar gibi devirli kodlarında elde edilebileceği düşünülmektedir.

KAYNAKLAR

1. Shannon, C. E., "A mathematical theory of communication", *Bell System Tech. J.,* pp. 379-423, 623-656, 27 (1948).
2. Hoffman, D. G.,Leonard, D. A., Lidner,C. C., Phelps, K. T.,Rodger, C. A., Wal, J. R., "Coding Theory: The Essentials", *Marcel Dekker Inc*, s. 277, New York City, 1991.
3. R. Hill, "A First Course in Coding Theory", *Clarendon Press*, s. 264, Oxford, 1986.
4. Hamming, R. W., "Error detecting and error-correcting codes", *Bell Syst. T.J.,*29(2),147-60, 1950.
5. Pellikaan, R. And Wu, X.W., "*Code Constructions and Bounds",* (1994) 49-57.
6. Peterson,W. W.,"Error-correcting codes", *The M.I.T. Press*, s. 572, Cambridge, 1961.
7. Williams, F. M. And Sloane,N.,"The Theory of Error Correcting Codes", North-Hollard Publishing Company, s.788, Amsterdam, 1977.
8. Şarkbülbülü, G., "Kodlama Kuramında Lineer Proğramlama Sınırı", *İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü* Yüksek Lisans Tezi, İstanbul, 2007.
9. Roman, S., "Coding and Information Theory", *Springer*, s.488, Verlag Groduate Text in Mathematics, 1992.
10. Pless, V.," Introduction to theTheory of Error-Correcting Codes", Wiley, New York, 2nd edition, s.205, 1989.
11. Hill, R., "A first course in coding theory", *Oxford Press*, s.264, NewYork 1990.
12. Harmancı, A. ve Güngöroğlu, G.,",Soyut Cebire Giriş Dersleri", *Hacettepe Üniversitesi Basımevi* s.272, Ankara:,1999.
13. VanLint, J. H, "Introduction to coding theory", *Springer-Verlag*, Berlin, third ed., s.234, 1999.
14. Reed, S., Solomon, G.,"Polynomial Codes Over Certain Finite Fields", *Journal of the Society for Industrial and Applied Mathematics* 8(2), 300-304,1960.
15. Babithaand K., Sunil ,V., J.J., "Soft set relation sand functions", *Computers and Mathematics with Applications* 1840-1849, 60 (2010).
16. Ahmatand, B., Kharal A.," On fuzzy soft sets", *Hindawi Publishing Corporation Advances in Fuzzy Systems* Article *ID 586507*, 6 pages (2009).

17. Herewan, T. ,Deris, M., “Soft Set Theoretic Approach for Dimensionality Reduction” *İnternational Journal of Database Theory and Application*, 47-59, (2010).
18. Pawlak, Z., “Rough sets”, I*nternational Journal of Information and Computer Science* 341 – 356,11 (1982).
19. Mushrif, M., M., Sengupta, S., Ray, A. K,” Texture classification using a novel soft set theory based classification algorithm”, *Springer,* LNCS 3851(2006) 254.
20. Peng, Y.,,Xu, X., “The dual composition of fuzzy relation sand its applications to transitivity properties”, *Fuzzy Systems and Mathematics* 19(2005), 54–59.
21. Inan, E., Ozturk, M.A., “Fuzzy Soft Rings and Fuzzy Soft Ideals”, *Neural Computing and Applications,* (2011), 1-8.
22. Manemaran, S.V. “On Fuzzy Soft Groups” ,*International Journal of Computer Applications* (0975 – 8887) Volume 15, (2011).
23. Ghosh, J., Dinda, B., Samanta, T.K., “Fuzzy Soft Rings and Fuzzy Soft Ideals”, *Int. J. P. App. Sc. Tech*. 2(2) 66-74,(2011).
24. Dubois, D. and Prade, H.,Editorial, “FuzzySets andSyst” . Volume 270., 122 (2001).
25. Sezgin, A., Atagun, A.O., “Soft Groups and Normalistic Soft Groups”, *Computers and Mathematics with Applications*, 685-698, 62 (2011).
26. Molodtsov, D. “Soft set theory-first results”. *Computers and Mathematics with Applications*., 19–31, 37(1999).
27. Maji, P. K., Biswas, R., ve Roy, A. R., “Soft set theory” *Computers and Mathematics with Applications,* 555-562, 45 (2003).
28. Aktaş, H., ve Çağman, N.. “Soft set and soft groups” *Information Sciences*, 2726-2735 Volume.177,(2007).
29. Aygünoğlu, A., ve Aygün, H., “Introduction to fuzzy soft groups”, *Computers and Mathematics with Applications*, 1279-1286, 58 (2009).
30. Feng, F., Jun ,Y.B., ve Zhao, X.. “Soft semirings”, *Computers and Mathematics with Applications,* 2621-2628, 56 (2008).
31. Sun, Q. M., Zhangand, Z. L., Liu, J., “Soft sets and soft modules”, In Wang, G., Li, T., Grzymala-Busse, J. W., Miao, D., Skowron, A., Yao, Y., eds.,”Rough Sets and Knowledge Technology”,RSKT-08, Proceedings, Springer, 403-409, (2008).

32. Xiao, Z., Gongand, K. Zou, Y., "A combined for ecasting approach based on fuzzy soft sets", *Journal of Computational and Applied Mathematics*, 326-333, 228(2009).
33. Pei, D., ve Miano, D., "From soft sets to information systems" *Granular Computing, 2005 IEEE International Conference on (2).* 617-621, 2005.
34. Peiand, D., Miao, D., "From soft sets to information systems", In: Hu, X., Liu, Q., Skowron, A., Lin, T. Y., Yager, R. R., Zhang, B. ,eds.,*Proceedings of Granular Computing, IEEE*, 617-621,2 (2005).
35. Jun, Y.B., ve Park, C.H.. "Applications of softsets in ideal theory of BCK/BCIalgebras, "*Information Sciences",* 2466-2475,178 (2008).
36. Feng, F., Jun, Y. B., ve Zhao, X. Z.. "Soft semirings" *Computers and Mathematics with Applications,* 2621–2628,56 (2008).
37. Jun, Y.B., Lee, K.J., Park, C.H., "Soft set theory applied to ideals in d-algebras", *Comput. Math. Appl*., 367-378, 2009(57).
38. Park, C. H., Junand, Y. B., Öztürk, M. A., "Soft WS-algebras", *Commun. Korean Math. Soc.*, 313-324, 23(3) (2008).
39. Sun, Q.M., Zhang, Z.L, Liu, J., "Soft sets and soft modules, Proceedings of Rough Sets and Knowledge Technology", *Third International Conference*, RSKT 2008, 17-19 May, Chengdu, China, pp. 403-409, 2008.
40. Maji, P.K., Roy, A.R., and Biswas, R., "An application of soft sets in a decision making problem", *Computur and Mathematics with Application*, (44), 2002.
41. Som, T., "On the theory of soft sets, soft relation and fuzzy soft relation", *Proc. Of the National Conference on Uncertainty: A Mathematical Approach*, UAMA-06, Burdwan, 1-9 (2006).
42. Ali, M.I., Feng, F., Liuand, X. Shabir, W.K.M., "On some new operations in soft set theory", *Computers and Mathematics with Applications*, 1547-1553, 57 (2009).
43. Rose, J.S., "A Course in Group Theory", s.320, *Cambridge Unıversity Press, New York: Dover*, 1994.
44. Chen, W. W. L., "Matrix Codes and Polynomial Codes", lecturer notes, 190, (1981).
45. Aktaş, H., Özlü, Ş., " Cyclic Soft Groups and Their Aplications on Groups", *Scientific World Journal,* 2004.

ÖZGEÇMİŞ

Şerif ÖZLÜ 1985 yılında Gaziantep'te doğdu. İlk ve orta öğrenimini Gaziantep'te tamamladı. Afyon Kocatepe Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümünden 2008 yılında mezun oldu. 2011 yılında Gaziantep Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalında Yüksek Lisans eğitimini tamamladı. Aynı yıl Nevşehir Hacı Bektaş Veli Üniversitesi Fen Bilimleri Enstitüsünde doktora yapmaya hak kazandı. Kilis 7 Aralık Üniversitesi'nde memuriyeti devam etmektedir.

Adres: Oğuzlar mah. Karayılan cad. no: 124

27300 - Gaziantep

Telefon: 0 506 479 31 17

E-posta : serif.ozlu@hotmail.com