T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KOD DÖNGÜLERİ

OĞUZHAN SELÇUK

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

DANIŞMAN: PROF. DR. SERKAN SÜTLÜ

HAZİRAN 2025

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KOD DÖNGÜLERİ

OĞUZHAN SELÇUK

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

DANIŞMAN: PROF. DR. SERKAN SÜTLÜ

HAZİRAN 2025

T.R.
GEBZE TECHNICAL UNIVERSITY
GRADUATE SCHOOL

CODE LOOPS

OĞUZHAN SELÇUK

A THESIS OF MASTER OF SCIENCE
DEPARTMENT OF MATHEMATICS

ADVISOR: PROF. DR. SERKAN SÜTLÜ

JUNE 2025

YÜKSEK LİSANS JÜRİ ONAY FORMU

GTÜ Lisansüstü Eğitim Enstitüsü Yönetim Kurulunun 16/06/2025 tarih ve 2025/32 sayılı kararıyla oluşturulan jüri tarafından 20/06/2025 tarihinde tez savunma sınavı yapılan Oğuzhan SELÇUK'un tez çalışması Matematik Anabilim Dalında Matematik Programında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE (TEZ DANIŞMANI)	: Prof. Dr. Serkan SÜTLÜ
ÜYE	: Prof. Dr. Oğul ESEN
ÜYE	: Prof. Dr. Songül ESİN

ONAY

Gebze Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü Yönetim Kurulunun ……/……./...…. tarih ve …..…/…..... sayılı kararı.

İMZA/MÜHÜR

ÖZET

Bu tezde, doğrusal kodlama teorisinin özel bir sınıfı olan *iki katlı çift kodlar* temel alınarak inşa edilen *kod döngüleri* cebirsel ve kohomolojik yönleriyle incelenmiştir. İki katlı çift kodlar, her bir kod sözcüğünün Hamming ağırlığının 4'ün katı olması koşulunu sağlayan $\mathbb{F}_2$-doğrusal kodlardır. Bu kodlar, yalnızca hata düzeltme amacıyla değil, aynı zamanda birleşmeli olmayan cebirsel yapıların inşasında da kullanılabilir niteliktedir.

Kod döngüsü, iki katlı çift kod C üzerinde tanımlanan bir faktör kümesi (koçevrim) $\varphi : C \times C \to \mathbb{F}_2$ aracılığıyla $\mathbb{F}_2 \times C$ kümesi üzerinde oluşturulan yeni bir çarpım yapısıyla elde edilir. Bu çarpım belirli koşulları sağladığında, sonuçta bir *Moufang döngüsü* meydana gelir. Moufang döngüleri, klasik gruplardan farklı olarak birleşmeli olmayan ancak belirli simetri koşullarını karşılayan yapılardır. Tezde, tanımlanan bu çarpımın Moufang özdeşliğini sağladığı, birim ve ters eleman içerdiği gösterilerek yapının döngü olduğu doğrulanmıştır.

Aynı iki kat çift kod için tanımlanabilen farklı koçevrimlerin oluşturduğu döngülerin, aslında birbirine denk (izomorf) yapılar olduğu ve bu denkliğin kodların ikinci dereceden kohomoloji sınıfıyla ilişkili olduğu ispatlanmıştır. Ayrıca, döngülerin *merkez*, *birleşiklikçi*, *iç dönüşüm grupları*, *alt döngü yapıları* gibi çeşitli yapısal bileşenleri detaylı biçimde incelenmiş ve bu döngülerin *ikinci sınıf merkezi nilpotent Moufang döngüleri* olarak sınıflandırılabileceği belirlenmiştir.

Kod döngüleri, yalnızca cebirsel açıdan değil, potansiyel uygulama alanları açısından da önem taşımaktadır. Özellikle doğrusal kodlardan türeyen yapıların cebirsel kontrolünün sağlanabilir olması, bu tür döngüleri bazı kriptografik yapılarda aday gösterilebilir hale getirmektedir. Literatürde, simetrik yapılı ve birleşmeli olmayan sistemlerin şifreleme mekanizmalarında kullanımı giderek artmaktadır. Bu bağlamda, kod döngülerinin barındırdığı cebirsel yapı, gelecekteki kriptolojik modellere katkı sunabilecek bir temel teşkil etmektedir.

Sonuç olarak, bu tezde iki katlı çift kodlara dayalı kod döngülerinin yapısal analizi yapılmış, varlık ve eşdeğerlik koşulları incelenmiş ve literatürdeki bazı sonuçlar genişletilerek daha kapsamlı bir çerçeve sunulmuştur.

Anahtar Kelimeler: İki Kat Çift Kodlar, Döngüler, Moufang Döngüsü, Faktör Kümesi, Birleşiklikçi.

ABSTRACT

This thesis presents an algebraic and cohomological study of *code loops* constructed from a special class of binary linear codes known as *doubly even codes*, in which every codeword has Hamming weight divisible by four. These codes are not only useful in error correction but also serve as a foundation for the construction of certain non-associative algebraic systems.

A code loop is obtained by equipping the set $\mathbb{F}_2 \times C$ with a new multiplication defined via a factor set (cocycle) $\varphi : C \times C \to \mathbb{F}_2$. Under appropriate conditions, this multiplication satisfies the Moufang identity and yields a *Moufang loop*. Moufang loops are non-associative algebraic structures that preserve certain symmetries across triple products. In this work, it is shown that the constructed multiplication admits identity and inverses and satisfies the Moufang property, thereby forming a valid loop structure.

It is proved that all such loops arising from different cocycles over the same code are actually isomorphic, and this equivalence is characterized by the second cohomology class associated with the code. Furthermore, the internal structure of these loops—such as *centers*, *associators*, *subloops*, and *inner mapping groups*—is analyzed in detail. These analyses confirm that the resulting structures belong to the class of *centrally nilpotent Moufang loops of class two*.

Beyond their algebraic interest, code loops have potential relevance in cryptographic applications. The algebraic control afforded by their construction from linear codes makes them plausible candidates for future cryptographic systems. In particular, non-associative and symmetric algebraic systems have recently drawn attention in the development of secure encryption mechanisms. In this context, the structural features of code loops may serve as a mathematical foundation for such applications.

In conclusion, this thesis analyzes the existence, equivalence, and structure of code loops based on doubly even codes, and contributes to the literature by extending and generalizing previous results in a more unified framework.

Keywords: Doubly Even Codes, Loops, Moufang Loops, Factor Set, Associator.

TEŞEKKÜR

Yüksek lisans eğitimim süresince akademik gelişimime yön veren, bilgi ve tecrübesiyle çalışmalarıma rehberlik eden, her zaman yapıcı desteği ve teşvikiyle yanımda olan değerli danışmanım Gebze Teknik Üniversitesi Matematik Bölüm Başkanı Prof. Dr. Serkan SÜTLÜ'ye; tez sürecinde değerlendirmeleri ve kıymetli katkılarıyla çalışmamın bilimsel niteliğini artıran saygıdeğer jüri üyelerim Prof. Dr. Oğul ESEN ve Prof. Dr. Songül ESİN'e en içten teşekkürlerimi sunarım. Eğitim hayatım boyunca bana yol gösteren ve matematik sevgimi pekiştiren tüm hocalarıma da şükranlarımı sunarım.

Bu süreçte desteğini ve ilgisini her zaman hissettiren, sabırları ve özverileriyle bana moral kaynağı olan annem Reyhan SELÇUK'a, fedakarlıklarıyla her zaman yanımda olan babam Muammer SELÇUK'a ve her koşulda desteğini esirgemeyen kardeşim Nisanur SELÇUK'a gönülden teşekkür ederim. Ayrıca, manevi destekleriyle yanımda olan arkadaşlarım Zeynep AKÇALI ve Çağatay ERSİN'e, tüm destekleri için araştırma görevlisi arkadaşlarıma ve TÜBİTAK Bilim İnsanı Destek Programları Başkanlığı (BİDEB) 2211-Yurt İçi Lisansüstü Burs Programı kapsamında bu çalışmanın gerçekleştirilmesine katkı sağlayan destekleri için TÜBİTAK'a teşekkür ederim.

İÇİNDEKİLER

SİMGELER ve KISALTMALAR DİZİNİ

IP	:	ters özellikli
LIP	:	sol ters özellikli
RIP	:	sağ ters özellikli
$\mathbb{F}_q^n$	:	q farklı sembolden oluşan n sıralıların vektör uzayı
$w(x)$	:	x kod kelimesinin Hamming ağırlığı
$Inn(\mathcal{L})$	:	$\mathcal{L}$ döngüsünün iç dönüşüm grubu
$Mlt(\mathcal{L})$	:	$\mathcal{L}$ döngüsünün çarpım grubu
L_a	:	sol öteleme dönüşümü
R_a	:	sağ öteleme dönüşümü
$C(\mathcal{L})$	:	$\mathcal{L}$ döngüsünün komütantı
$N(\mathcal{L})$	:	$\mathcal{L}$ döngüsünün çekirdeği
$Z(\mathcal{L})$	:	$\mathcal{L}$ döngüsünün merkezi
$\mathcal{L}'$	:	$\mathcal{L}$ döngüsünün merkezi türetilmiş alt döngüsü
$\mathcal{L}^*$	:	$\mathcal{L}$ döngüsünün çekirdeksel türetilmiş alt döngüsü

1. GİRİŞ

Soyut cebirde, önemli hedeflerden biri, belirli aksiyomları sağlayan işlemlerle tanımlanan cebirsel yapıları anlamaktır. En temel yapılardan biri, birleşmeli bir ikili işlem, birim elemanın varlığı ve tüm elemanlar için terslerinin bulunmasıyla tanımlanan grup yapısıdır. Ancak, birleşme zengin bir cebirsel yapı için tek seçenek değildir.

*Kuasigrup*lar, grupların birleşme koşulunu genelleştirir: her çift eleman a, b için $a*x = b$ ve $y * a = b$ denklemlerinin tek çözümlerinin bulunduğu, ancak işlemin birleşme zorunluluğu olmadığı kümelerdir [1]. Eğer bir kuasigrup ayrıca birim elemana sahipse, buna *döngü* denir [2, s. 4]. Döngüler, gruplardan en çok birleşme özelliğinin olmaması ile ayrılır; ancak zengin bir iç yapıya sahiptirler ve geometri, kombinatorik ve teorik fizik gibi birçok matematiksel alanda karşımıza çıkarlar [1].

Döngüleri incelemek için genellikle kendileri ile ilişkilendirilen permutasyon grupları ele alınır. Bir döngü $\mathcal{L}$ için *çarpma grubu*, $\mathcal{L}$ üzerindeki simetrik grubun, tüm sol ve sağ ötelemeler tarafından oluşturulan alt grubudur. Bir diğer merkezi kavram ise, birim elemanı sabit tutan ötelemelerin oluşturduğu *iç dönüşüm grubu* Inn($\mathcal{L}$)'dir [2]. Inn($\mathcal{L}$)'nin yapısı, döngünün önemli özelliklerini yansıtır. Örneğin, Inn($\mathcal{L}$)'nin abelyen olması, döngünün merkezi nilpotentlik sınıfı üzerinde kısıtlamalar getirir [2, s. 10]. Bu tür döngülerin merkezi nilpotentlik sınıfının en fazla iki olabileceğini belirten sonuçlar da vardır [2].

En çok incelenen döngü çeşitlerinden biri, iyi tanımlanmış terslere sahip *ters özellikli (IP) döngüler*dir [2]. Özellikle dikkat çeken döngü sınıflarından biri de, $x(y \cdot xz) = (xy \cdot x)z$ gibi çeşitli denk Moufang özelliklerini sağlayan *Moufang döngüleri*dir [3]. Moufang döngüleri, IP döngüler olup, (gruplara ne kadar yakın olduklarını gösteren) dikkat çekici bir özelliğe sahiptirler: herhangi iki elemanları bir grup üretir [2].

Kod döngüleri, iki kat çift ikili kodlardan ve merkezi genişlemelerden doğan, önde gelen Moufang döngü sınıflarını oluşturur. Sonlu basit gruplar, ve özellikle Canavar grubu (Monster group) ile derin bağlantıları nedeniyle büyük ilgi görürler [4, 5, 6, 3]. Bu tez, kod döngülerinin cebirsel (ve kohomolojik) yapısını incelemeyi amaçlamakta olup, özellikle döngü genişlemeleri olarak sınıflandırılmaları üzerinde durmaktadır.

Birleşmeli olmayan yapılar, döngüler dahil olmak üzere, çeşitli alanlarda uygulama bulmaktadır. Bu alanlardan biri, güvenilir veri iletimi için kodların tasarımıyla ilgilenen Kodlama Teorisi'dir [7]. Bu alanda, alfabeler (çoğunlukla sonlu cisimler), kod kelimeleri, kod uzunluğu ve Hamming mesafesi gibi kavramlar kullanılır [7]. Özellikle vektör altuzayları olan doğrusal kodlar önemlidir [7]. Doğrusal kodlar, kod döngülerinin yapısında önemli bir yer tutar ve kodlama teorisi ile yakından ilişkilidir. Bir kod döngüsünün inşası, kodun temel özelliklerini cebirsel bir yapıya dönüştürerek, kodları incelemek ve sınıflandırmak için döngü teorisi araçlarının kullanılmasını sağlar. Bu etkileşim, kodların simetrileri ve genişlemeleri üzerinde de aydınlatıcı olup, kafesler, vörteks operatör cebirleri ve nadir sonlu basit grupların inşasında uygulama alanı bulur [2, 3, 8, 9].

Döngülerin pratik uygulamalar için incelendiği bir diğer yeni alan ise kriptografi, özellikle de simetrik anahtarlı blok şifrelerin tasarımıdır [10, 11]. Modern blok şifreler, örneğin Gelişmiş Şifreleme Standardı (AES), karmaşıklık yaratmak için S-kutuları adı verilen doğrusal olmayan bileşenlere dayanır [10]. Güncel çalışmalar, S-kutuları oluşturmak için Ters Özellikli (IP) döngüler ve Moufang döngülerinin cebirsel yapılarından yararlanarak istenen kriptografik özelliklere ulaşmayı amaçlamaktadır [10, 11].

Sonlu cisimlere dayanan geleneksel yaklaşımlarla karşılaştırıldığında, döngü tabanlı yapılar belirli kriptoanalitik saldırılara karşı potansiyel olarak daha yüksek direnç sunar. Döngü parametrelerinin değiştirilmesiyle S-kutusu aileleri oluşturma veya döngü izotoplarının kullanılması gibi teknikler [10]'te önerilmiştir. Ayrıca, Osborn döngüleri gibi özel döngülerde kriptografik özdeşliklerin incelenmesi, bu uygulamalarda cebirsel sağlamlığın sağlanması açısından dikkate değer bir araştırma yönü olarak değerlendirilmiştir [12].

Son gelişmeler, Moufang yapıları ile bilgi geometrisi arasındaki bağlantıları daha da vurgulamıştır. Sonlu kümelerin olasılık dağılımı uzayları, bilgi geometrisinin kanonik Riemann metriği ile donatıldığında ve değişmeli bir Moufang döngüsünün kodladığı simetriyi kabul ettiğinde bu bağlantı somutlaşır [13]. Ayrıca [14]'de, bir K cismi üzerindeki projeksiyon düzlemi KP^2 içinde yer alan kübik bir eğrinin K-noktalar kümesi E'nin,

$$x * y := u \circ (x \circ y)$$

işlemi ile (değişmeli) bir Moufang döngüsü yapısına sahip olduğu gözlemlenmiştir; burada $u := x + y$, eğrinin KP^2'deki bir projeksiyon doğrusu ile kesişim döngüsüdür. [13]'da ayrıca, bir (sözde-) Riemann manifoldu M üzerinde bir $s_c : M \to M$ *simetrik involüsyonlar* ailesi tanımlanabiliyorsa,

$$c * d := s_c(d)$$

işlemi altında değişmeli Moufang döngüsü yapısına sahip olduğu belirtilmiştir. Belirli bir sonlu kümenin olasılık dağılımı uzayı da [15, 16, 17]'te gözlemlendiği üzere, bu uzaya bağlı kanonik Riemann metriğinin jeodezikleri aracılığıyla böyle involüsyonlarla donatılmıştır.

Öte yandan, daha yakın zamandaki çalışmalar, sonlu cisimler üzerinde tanımlı *neredeyse simplektik vektör uzaylarının* değişmeli olmayan Moufang döngülerini de kapsamaktadır [13, 18]. Bu türden çalışmalar, klasik kodlardan kuantum kodları oluşturan (simplektik) CRSS algoritması [19] ile daha modern benzerlerini içerir [13, 20].

2. KODLAR

2.1. Terminoloji

[7, 3] kaynaklarını takip ederek kodlama teorisine ilişkin temel terminolojiyle başlayacağız.

Tanım: $\mathbb{F}_q = \{\lambda_1, \lambda_2, \ldots, \lambda_q\}$ cismi q farklı sembolden oluşan bir *alfabe* olarak kabul edilirse, n uzunluğunda q-lu bir C *blok kodu*, formal olarak $(\mathbb{F}_q)^n$'nin bir alt kümesi olarak tanımlanır. Burada $(\mathbb{F}_q)^n$, tüm olası n-sıralıların vektör uzayını ifade eder.

Tanım: Bir $C \subseteq (\mathbb{F}_q)^n$ kodunun içindeki elemanlara, C'nin *kod kelimeleri* denir.

Tanım: $(\mathbb{F}_q)^n$ içindeki bir x vektörünün (Hamming) *ağırlığı*, $w(x)$ ile gösterilir ve x'in sıfır olmayan bileşenlerinin sayısı olarak tanımlanır. Yani,

$$w(x) = |\{i \mid x_i \neq 0\}|.$$

Özel olarak, ikili kodlar ($q = 2$) için Hamming ağırlığı, x içindeki 1'lerin sayısına eşittir.

Kod kelimelerinin *toplamı* ve *kesişimi* bileşen bazında tanımlanır. $x, y \in (\mathbb{F}_q)^n$ olmak üzere, $x = x_1x_2 \ldots x_n$ ve $y = y_1y_2 \ldots y_n$ verildiğinde, toplam

$$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n),$$

kesişim ise

$$x \cap y = (x_1y_1, x_2y_2, \ldots, x_ny_n)$$

şeklinde tanımlanır. Buradaki $x_i + y_i$ ve x_iy_i işlemleri ise mod q alınarak hesaplanır.

Tanım: $\mathbb{F}_q$ üzerinde bir *lineer kod*, $(\mathbb{F}_q)^n$'nin bir alt uzayıdır. Öte yandan, $[n, k]$-kod, uzunluğu n ve boyutu k olan bir lineer kodu ifade eder.

$\mathbb{F}_q$ sonlu cismi üzerindeki lineer hata düzeltme kodu, $[n, k, d]$ olmak üzere üç parametreyle tanımlanır; burada (uzunluk) n, her kod kelimesinin bileşen sayısını, (boyut) k, kod kelimelerinin üretildiği lineer bağımsız temel vektörlerin sayısını, ve son olarak (minimum mesafe) d, herhangi iki kod kelimesi arasındaki minimum *Hamming mesafesini* ifade eder. İki kod kelimesi arasındaki Hamming mesafesi bu kod kelimelerinin farklı oldukları pozisyonların sayısı olarak tanımlanır.

Tanım: Bir $C \subseteq \mathbb{F}_q^n$ $[n,k]$-kodu için, *parite kontrol matrisi* H, boyutu $(n-k) \times n$ olan ve sıfır uzayı tam olarak C kodu olan $\mathbb{F}_q$ üzerindeki bir matristir.

Başka bir deyişle,

$$C = \{x \in (\mathbb{F}_q)^n \mid Hx^T = \theta\}$$

olup, burada x^T x vektörünün transpozesini, θ ise boyutu $n-k$ olan sıfır vektörünü ifade eder. Buna göre, H'nin satırları, $C^\perp$ dual kodunun bir bazını oluşturur.

Örnek 1: Bir $[7,4]$-kodu olan $C \subseteq (\mathbb{F}_2)^7$'yi ele alalım. Bu kodun parite kontrol matrisini

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

olarak düşüneceksek, $x \in (\mathbb{F}_2)^7$ olan bir vektör ancak ve ancak $Hx^T = (0,0,0)^T$ olduğunda bir kod kelimesidir.

Örneğin, $x = (1,1,1,0,0,0,0)$ bir kod kelimesidir, çünkü

$$H(1,1,1,0,0,0,0)^T = (0, 1+1, 1+1)^T = (0,0,0)^T,$$

ancak $y = (1,0,1,0,1,1,1) \in (\mathbb{F}_2)^7$ bir kod kelimesi değildir, zira

$$H(1,0,1,0,1,1,1)^T = (1+1+1, 1+1+1, 1+1+1+1)^T = (1,1,0)^T.$$

Tanım: $(\mathbb{F}_q)^n$ içindeki bir C $[n,k]$-kodu için, *üreteç matrisi* $k \times n$ boyutunda ve satırları C için bir baz oluşturan matristir.

Daha açık ifade etmek gerekirse, üreteç matrisi G ile gösterildiğinde,

$$C = \{uG \mid u \in (\mathbb{F}_q)^k\},$$

burada u, k adet *bilgi sembolünden* oluşan bir satır vektörüdür. Üreteç matrisinin standart formu, I_k, $k \times k$ birim matrisi, P ise $k \times (n-k)$ boyutunda bir matris olmak üzere $G = [I_k \mid P]$ şeklindedir.

Örnek 2: Aşağıdaki üreteç matrisi ile oluşturulan $C \subseteq (\mathbb{F}_2)^7$ $[7,4]$-kodunu ele alalım:

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

Bu durumda, 2^4 farklı *bilgi sembolü*ne karşılık gelen kod kelimeleri şu şekilde hesaplanır:

Sembol u	Kod kelimesi $x = uG$
0000	0000000
0001	0001111
0010	0010011
0011	0011100
0100	0100101
0101	0101010
0110	0110110
0111	0111001
1000	1000110
1001	1001001
1010	1010101
1011	1011010
1100	1100011
1101	1101100
1110	1110000
1111	1111111

Bu kodun parite kontrol matrisi ise

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

Bu kod, *Hamming* $[7, 4]$-kodu olarak bilinir.

Hata düzeltme kodları teorisinde önemli bir sınır, *Hamming Sınırı (küre paketleme sınırı)*dır.

Alfabesi $(\mathbb{F}_q)^n$ olan ve minimum Hamming mesafesi d olan kod kelimelerinin sayısını $A(q, n, d)$ ile gösterelim. Hamming mesafesi tanımından şu sonuç çıkar: en fazla

$$t := \left\lfloor \frac{d-1}{2} \right\rfloor$$

hata içeren bir gönderilen kod kelimesi doğru olarak çözümlenebilir. Buna göre, bu $A(q, n, d)$ kadar kod kelimesinin her biri için yarıçapı t olan bir küre içerisindeki her-

hangi bir kod kelimesi de doğru şekilde çözümlenebilir (kürenin merkezi olan kod kelimesi olarak). Her bir böyle kürenin hacmi (küre içindeki kod kelimelerinin sayısı) ise şu şekilde hesaplanır:

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

İki böyle kürenin kesişmeyeceği göz önünde bulundurulduğunda, bu kürelerdeki tüm kod kelimelerinin birleşimi (kürelerin toplam hacmi) şu olur:

$$A(q,n,d) \sum_{k=0}^{t} \binom{n}{k} (q-1)^k.$$

Son olarak, tüm bu kod kelimelerinin hâlâ $(\mathbb{F}_q)^n$ içinde olduğunu ve $|(\mathbb{F}_q)^n| = q^n$ olduğunu göz önüne alırsak, şu eşitsizlik elde edilir:

$$A(q,n,d) \sum_{k=0}^{t} \binom{n}{k} (q-1)^k \leq q^n,$$

veya eşdeğer olarak,

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

bu da küre paketleme sınırı veya Hamming sınırı olarak bilinir. Ayrıca, bir kod eğer Hamming sınırına ulaşırsa (ya da yukarıdaki kürelerin birleşimi $(\mathbb{F}_q)^n$'yi tam olarak kapsıyorsa), bu koda *mükemmel* kod denir.

Örnek 3: Herhangi bir $m \geq 2$ için, $(\mathbb{F}_2)^{2^m-1}$ uzayında yer alan önemli bir ikili (lineer) kod ailesi, *Hamming kodları*dır. Bir Hamming kodu, $[n,k,d] = [2^m-1, 2^m-1-m, 3]$ parametrelerine sahip, mükemmel ve tek hata düzelten bir koddur.

Tanım: $C \subseteq \mathbb{F}_q^n$ bir kod, eğer lineer bir kod olmakla birlikte döngüsel permütasyonlara kapalıysa *döngüsel* (cyclic) olarak adlandırılır. Yani, her $(c_0, c_1, \ldots, c_{n-1}) \in C$ için

$$(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$$

şartı sağlanıyorsa, C döngüsel bir koddur.

Tanım: *Golay kodu*, belirli parametreler için tanımlanmış iki ikili ve iki üçlü kod içeren; küçük fakat önemli bir mükemmel lineer hata düzeltme kodu ailesidir.

1. Mükemmel İkili Golay Kodu G_{23}: Parametreleri $[n,k,d] = [23,12,7]$ olan, $\mathbb{F}_2$ üzerinde tanımlı lineer bir koddur ve 3 hatayı düzeltebilen mükemmel bir koddur.
2. Genişletilmiş İkili Golay Kodu G_{24}: Parametreleri $[n,k,d] = [24,12,8]$ olan, $\mathbb{F}_2$ üzerinde tanımlı lineer bir koddur. G_{23}'ten her kod kelimesine bir genel parite

kontrol biti eklenerek elde edilir. G_{24} *kendine dual* bir koddur (aşağıda açıklanan anlamda) ve her kod kelimesinün ağırlığı 4'ün katıdır.

3. Mükemmel Üçlü Golay Kodu G_{11}: Parametreleri $[n, k, d] = [11, 6, 5]$ olan, $\mathbb{F}_3$ üzerinde tanımlı lineer bir koddur ve 2 hatayı düzeltebilen mükemmel bir koddur.

4. Genişletilmiş Üçlü Golay Kodu G_{12}: Parametreleri $[n, k, d] = [12, 6, 6]$ olan, $\mathbb{F}_3$ üzerinde tanımlı lineer bir koddur. $[11, 6, 5]$ koduna sıfır toplamlı bir kontrol basamağı eklenerek elde edilir.

Tanım: $C \subseteq (\mathbb{F}_q)^n$ lineer kodu verildiğinde, *dual kod* (ya da *çift kod*), $C^\perp$ ile gösterilir ve standart iç çarpım altında C'deki her kod kelimesine ortogonal olan $(\mathbb{F}_q)^n$ içindeki tüm vektörlerin kümesi olarak tanımlanır. Daha açık biçimiyle,

$$C^\perp := \{y \in (\mathbb{F}_q)^n \mid x \cdot y = \sum_{i=1}^{n} x_i y_i = 0, \text{ tüm } x \in C \text{ için}\}.$$

Dual kod $C^\perp$, $(\mathbb{F}_q)^n$ içinde bir lineer altuzaydır. Dahası, C'nin boyutu k ise, $C^\perp$'in boyutu $n - k$ olur. Ayrıca, herhangi bir $C \subseteq (\mathbb{F}_q)^n$ kodu *refleksiftir*, yani $(C^\perp)^\perp = C$ eşitliği sağlanır. Üstelik, C'nin bir üreteç matrisi, $C^\perp$ için bir parite kontrol matrisi olarak kullanılabilir ve tersi de geçerlidir.

Buna göre, eğer $G = [I_k \mid P]$ bir kod $C \subseteq (\mathbb{F}_q)^n$'nin sistematik formda bir üreteç matrisi ise, o zaman $H = [-P^T \mid I_{n-k}]$ bu kod için bir parite kontrol matrisi olur.

Özellikle, eğer $C = C^\perp \subseteq (\mathbb{F}_q)^n$ ise (ki bu yalnızca n çift olduğunda mümkündür), o zaman C'ye *kendine dual* kod denir.

Örnek 4: $C \subseteq (\mathbb{F}_2)^4$ kodu aşağıdaki vektörlerle üretilmiş olsun:

$$g_1 = (1, 0, 1, 0) \qquad g_2 = (0, 1, 0, 1).$$

Buna göre, C için üreteç matrisi:

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

Dolayısıyla, C bir $[4, 2]$-kodudur ve kod kelimeleri şunlardır:

$$C = \{(0, 0, 0, 0), (1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1)\}.$$

Ayrıca bu durumda $C^\perp$, bir $[n, n - k] = [4, 2]$-kodudur.

Üreteç matrisini

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} = [I_2 \mid P]$$

şeklinde yazarsak, burada

$$P = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{ve} \quad P^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

olur. Bu durumda, C için bir parite kontrol matrisi şu şekilde verilir:

$$H = [-P^T \mid I_2] = [P^T \mid I_2] = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} = G.$$

Böylece, C kodunun kendine dual olduğu, yani $C = C^{\perp}$ olduğu sonucuna varırız.

2.2. İki Kat Çift Kodlar

Tanım: $C \subset (\mathbb{F}_2)^n$ kodu, eğer

$$w(v) \equiv 0 \quad (\mod 4)$$

her $v \in C$ kod kelimesi için sağlanıyorsa, *iki kat çift* kod olarak adlandırılır.

Buna göre, eğer $C \subset (\mathbb{F}_2)^n$ bir iki kat çift kod ise, o zaman her $u, v \in C$ için $w(u \cap v)$ ifadesi 2 ile tam bölünür. Ayrıca bu durumda, $\frac{1}{4}w(u)$ ve $\frac{1}{2}w(u \cap v)$ ifadeleri de tam sayıdır.

İki kat çift kodun bazı ilave özellikleri aşağıda verilmiştir; örnek olarak [3]'e bakılabilir.

Önerme 2.1: $C \subset (\mathbb{F}_2)^n$ bir iki kat çift kod olsun. O zaman, her $x, y, u, v \in C$ için aşağıdakiler geçerlidir:

$$\frac{1}{4}w(x) + \frac{1}{4}w(x+y) + \frac{1}{4}w(y) \equiv \frac{1}{2}w(x \cap y) \qquad \mod 2 \tag{2.1}$$

$$\frac{1}{4}[w(x) + w(y) + w(z) + w(x+y) + w(y+z) + w(z+x) + w(x+y+z)] \equiv w(x \cap y \cap z) \qquad \mod 2 \tag{2.2}$$

$$w(x \cap u \cap v) + \frac{1}{2}w(x \cap (u+v)) = \frac{1}{2}w(x \cap u) + \frac{1}{2}w(x \cap v); \tag{2.3}$$

$$\frac{1}{2}w(x \cap \sum_{i=1}^{n} u_i) + \sum_{i<j} w(x \cap u_i \cap v_i) \equiv \frac{1}{2}\sum_{i=1}^{n} w(x \cap u_i) \qquad \mod 2$$

$$w((x+y)\cap(u+v)) = w(x\cap u)+w(y\cap u)+w(x\cap v)+w(y\cap v) \qquad (2.4)$$
$$-2[w(x\cap y\cap u)+w(x\cap y\cap v)+$$
$$w(x\cap u\cap v)+w(y\cap u\cap v)]+4w(x\cap y\cap u\cap v)$$

Dahası bir iki kat çift kod için aşağıdaki durumu da ayrıca belirtelim.

Önerme 2.2: $C\subset(\mathbb{F}_2)^n$ bir iki kat çift kod olsun. O zaman, her $x,y,z,u\in C$ için

$$w((x+y)\cap z\cap u) = w(x\cap z\cap u)+w(y\cap z\cap u)$$

eşitliği sağlanır.

İspat.(2.2) ifadesinden doğrudan elde edilir ki:

$$w((x+y)\cap z\cap u) = \frac{1}{4}w(x+y)+\frac{1}{4}w(z)+\frac{1}{4}w(u)+$$
$$\frac{1}{4}w(x+y+z)+\frac{1}{4}w(x+y+u)+\frac{1}{4}w(z+u)+\frac{1}{4}w(x+y+z+u),$$

öte yandan, (2.1) ifadesine göre

$$\frac{1}{4}w(x+y+z+u) = \frac{1}{4}w(x+y+z)+\frac{1}{4}w(u)+\frac{1}{2}w((x+y+z)\cap u)$$

olur. Buna göre, aşağıdaki ifadeyi elde ederiz:

$$\begin{aligned}
&w((x+y)\cap z\cap u) = \\
&\frac{1}{4}w(x+y)+\frac{1}{4}w(z)+\frac{1}{4}w(u)+\frac{1}{4}w(x+y+z)+\frac{1}{4}w(x+y+u)\\
&\quad+\frac{1}{4}w(z+u)+\frac{1}{4}w(x+y+z)+\frac{1}{4}w(u)+\frac{1}{2}w((x+y+z)\cap u)\\
&=\frac{1}{4}w(x+y)+\frac{1}{4}w(z)+\frac{1}{4}w(x+y+u)+\frac{1}{4}w(z+u)\\
&\quad+\frac{1}{2}w((x+y+z)\cap u)\\
&=\frac{1}{4}w(x+y)+\frac{1}{4}w(z)+\frac{1}{4}w(x+y)+\frac{1}{4}w(u)+\frac{1}{2}w((x+y)\cap u)\\
&\quad+\frac{1}{4}w(z+u)+w(x\cap y\cap u)+w(x\cap z\cap u)+w(y\cap z\cap u)\\
&\quad+\frac{1}{2}w(x\cap u)+\frac{1}{2}w(y\cap u)+\frac{1}{2}w(z\cap u)\\
&\quad=\frac{1}{2}w((x+y)\cap u)+w(x\cap y\cap u)+w(x\cap z\cap u)\\
&\quad\quad+w(y\cap z\cap u)+\frac{1}{2}w(x\cap u)+\frac{1}{2}w(y\cap u)\\
&\quad=w(x\cap y\cap u)+\frac{1}{2}w(x\cap u)+\frac{1}{2}w(y\cap u)+w(x\cap y\cap u)\\
&\quad\quad+w(x\cap z\cap u)+w(y\cap z\cap u)+\frac{1}{2}w(x\cap u)+\frac{1}{2}w(y\cap u)\\
&\quad=w(x\cap z\cap u)+w(y\cap z\cap u).
\end{aligned}$$

□

Şimdi de bir iki kat çift kod üzerinde tanımlanan *faktör kümesi* kavramını [3]'dan hatırlayalım.

Tanım: $C \subset (\mathbb{F}_2)^n$ bir iki kat çift kod olsun. Aşağıdaki koşulları her $x, y, z \in C$ için sağlayan bir $\varphi : C \times C \to \mathbb{F}_2$ fonksiyonuna, C üzerinde tanımlı bir *faktör kümesi* (factor set) denir:

$$\varphi(x,x) \equiv \frac{1}{4}w(x) \pmod 2 \tag{2.5}$$

$$\varphi(x,y) + \varphi(y,x) \equiv \frac{1}{2}w(x \cap y) \pmod 2 \tag{2.6}$$

$$\varphi(x,y) + \varphi(x+y,z) + \varphi(y,z) + \varphi(x,y+z) \equiv w(x \cap y \cap z) \pmod 2 \tag{2.7}$$

İki $\varphi, \psi : C \times C \to \mathbb{F}_2$ faktör kümesi, eğer her $x, y \in C$ için

$$\varphi(x,y) - \psi(x,y) = \alpha(x) + \alpha(y) + \alpha(x+y)$$

eşitliğini bir $\alpha : C \to \mathbb{F}_2$ fonksiyonu (ve $\alpha(0) = 0$) için sağlıyorsa, *denk* olarak adlandırılır.

Bir sonraki sonuç, faktör kümelerine ilişkin bazı temel özellikleri derlemektedir, bkz. [3].

Önerme 2.3: Herhangi bir $\varphi : C \times C \to \mathbb{F}_2$ faktör kümesi, her $x, y, z, u \in C$ için aşağıdakileri sağlar:

$$\varphi(0,x) = \varphi(x,0) = 0 \tag{2.8}$$

$$\varphi(x,y) + \varphi(x,x+y) \equiv \frac{1}{4}w(x) \quad (\mod 2) \tag{2.9}$$

$$\varphi(z,x) + \varphi(z,x+u) + \varphi(u,x) + \varphi(u,x+z) \equiv \frac{1}{2}w(z \cap u) \quad (\mod 2) \tag{2.10}$$

İspat. Öncelikle (2.8) ile başlayalım. (2.7) denkleminde $x = 0$ olarak alınırsa,

$$\varphi(0,y) + \varphi(0+y,z) + \varphi(y,z) + \varphi(0,y+z) \equiv w(0 \cap y \cap z).$$

Buradan, $w(0 \cap y) = 0$ olduğu için,

$$\varphi(0,y) + 2\varphi(y,z) + \varphi(0,y+z) \equiv 0,$$

yani,

$$\varphi(0,y) + \varphi(0,y+z) \equiv 0,$$

herhangi $y, z \in C$ için. Burada, kayıp olmadan $z = -y$ alınırsa,

$$\varphi(0, y + z) \equiv 0,$$

ve buradan,

$$\varphi(0, y) \equiv 0$$

sonucuna varılır. Sonra (2.6) denkleminde $x = 0$ olarak alınırsa,

$$\varphi(0, y) + \varphi(y, 0) \equiv \frac{1}{2} w(0 \cap y) = 0,$$

buradan

$$\varphi(y, 0) = \varphi(0, y) \equiv 0$$

sonucu çıkar.

(2.9) için tekrar (2.8) kullanılır. Bu kez $y = x$ olarak alınırsa,

$$\begin{aligned}
&\varphi(x, x) + \varphi(x + x, z) + \varphi(x, z) + \varphi(x, x + z) \equiv w(x \cap x \cap z) \implies \\
&\frac{1}{4} w(x) + \varphi(0, z) + \varphi(x, z) + \varphi(x, x + z) \equiv w(x \cap z) \implies \\
&\frac{1}{4} w(x) + 0 + \varphi(x, z) + \varphi(x, x + z) = w(x \cap z) \implies \\
&\varphi(x, z) + \varphi(x, x + z) \equiv \frac{1}{4} w(x) + w(x \cap z)
\end{aligned}$$

herhangi $x, z \in C$ için, ve C iki kat çift olduğundan dolayı

$$w(x \cap z) \equiv 0,$$

buradan,

$$\varphi(x, z) + \varphi(x, x + z) \equiv \frac{1}{4} w(x).$$

Son olarak (2.10)'ü inceleyelim. Bu kez (2.7)'da $x = z$, $y = x$, $z = u$ olarak alınır:

$$\varphi(z, x) + \varphi(z + x, u) + \varphi(x, u) + \varphi(z, x + u) \equiv w(x \cap z \cap u). \tag{2.11}$$

Sonra, (2.6)'den,

$$\begin{aligned}
&\varphi(z + x, u) + \varphi(u, z + x) \equiv \frac{1}{2} w(u \cap (z + x)) \overset{(2.3)}{\equiv} \\
&\frac{1}{2} w(u \cap z) + \frac{1}{2} w(u \cap x) + w(x \cap z \cap u) \overset{(2.6)}{\equiv} \\
&\frac{1}{2} w(u \cap z) + \varphi(x, u) + \varphi(u, x) + w(x \cap z \cap u)
\end{aligned}$$

buradan,

$$w(x \cap z \cap u) \equiv \varphi(z+x,u) + \varphi(u,z+x) + \frac{1}{2}w(z \cap u) + \varphi(x,u) + \varphi(u,x).$$

Bunu (2.11)'a yerine koyarsak,

$$\varphi(z,x) + \varphi(z+x,u) + \varphi(x,u) + \varphi(z,x+u) \equiv$$
$$\varphi(z+x,u) + \varphi(u,z+x) + \frac{1}{2}w(z \cap u) + \varphi(x,u) + \varphi(u,x).$$

Sadeleştirmeler sonrası geriye,

$$\varphi(z,x) + \varphi(u,x) + \varphi(z,x+u) + \varphi(u,z+x) \equiv \frac{1}{2}w(z \cap u)$$

kalmaktadır. □

Aşağıdaki temel sonuç, bkz. [3], faktör kümelerinin varlığını garanti eder.

Teorem 2.1: $C \subset (\mathbb{F}_2)^n$ herhangi bir iki kat çift kod verildiğinde, $C \times C \to \mathbb{F}_2$ biçiminde bir faktör kümesi φ vardır.

*İspat.*İspatı tümevarımla yapacağız. Bu amaçla,

$$C_0 < C_1 < \ldots < C_n = C$$

şeklinde, $\dim(C_i) = i$ olacak şekilde bir altuzaylar zinciri alalım, ve $k = 0, 1, \ldots, n-1$ için $W_k := C_{k+1} - C_k$ olarak tanımlayalım. Tümevarımla, $\varphi : C_k \times C_k \to \mathbb{F}_2$ fonksiyonu için 2.5, 2.6 ve 2.7 koşullarının sağlandığını varsayarak, bunların $\varphi : C_{k+1} \times C_{k+1} \to \mathbb{F}_2$ için de sağlandığını göstereceğiz.

$k = 1$ için

$$\varphi(x,y) = \begin{cases} 0 & \text{eğer } x = 0 \text{ veya } y = 0, \\ \frac{1}{4}w(x) & \text{eğer } x \in C_1 - \{0\} \end{cases}$$

olarak tanımlayalım ve $0 \leq k \leq n-1$ için φ fonksiyonunun $C_k \times C_k$ üzerinde 2.5, 2.6 ve 2.7 koşullarını sağladığını varsayalım.

Böylece $\varphi : C_{k+1} \times C_{k+1} \to \mathbb{F}_2$ fonksiyonunu, (2.9) ve (2.10) ifadelerine dayanarak aşağıdaki adımlar aracılığıyla inşa edeceğiz.

(D1)$x \in W_k$ verildiğinde, $\varphi : \{x\} \times C_k \to \mathbb{F}_2$ fonksiyonunu keyfi olarak tanımlarız ve ayrıca $\varphi(x, 0) = 0$ olarak belirleriz. Ardından, $y \in C_k$ için 2.6 koşulunu uygularsak:

$$\varphi(x, y) + \varphi(y, x) \equiv \frac{1}{2} w(x \cap y).$$

Buradan $\varphi(x, y)$ ve $\frac{1}{2} w(x \cap y)$ bilindiğinden, $\varphi(y, x)$ hesaplanabilir. Bu şekilde, φ'nın $C_k \times \{x\}$ üzerindeki değerleri elde edilmiş olur.

*(D2)*Sonrasında, (2.9)'yi uygulayarak

$$\varphi(x, y) + \varphi(x, x + y) \equiv \frac{1}{4} w(x)$$

elde ederiz ($y \in W_k$ için). Buradan $\varphi(x, x + y)$ önceki adımdan bilindiği ve $\frac{1}{4} w(x)$ hesaplanabildiği için $\varphi(x, y)$ sonucu çıkar. Böylece, φ'nın $\{x\} \times W_k$ üzerindeki değerleri elde edilir. Aynı şekilde, 2.6 yardımıyla $W_k \times \{x\}$ üzerindeki değerler de bulunabilir.

*(D3)*Şimdi $b \in C_k$ ve $d \in W_k$ olmak üzere $x + d \in C_k$ ve $x + b \in W_k$ olduğunu not edelim. Buna göre, (2.10) koşulunu uygularsak:

$$\varphi(b, x) + \varphi(b, x + d) + \varphi(d, x) + \varphi(d, x + b) \equiv \frac{1}{2} w(b \cap d)$$

elde edilir. Burada, $\varphi(b, x)$ *(D1)*'den, $\varphi(b, x + d)$ tanımdan, $\varphi(d, x)$ *(D2)*'den ve $\varphi(d, x + b)$ ifadesi de $\frac{1}{2} w(b \cap d)$ hesaplanarak elde edilebilir. Böylece, φ'nın $W_k \times W_k$ üzerindeki değerleri de hesaplanmış olur.

*(D4)*Son olarak, $y \in C_k$ ve $x \in W_k$ verilmiş olsun, bu durumda $x + y \in W_k$ olur. Yine (2.9)'yi uygulayarak:

$$\varphi(x, y) + \varphi(x, x + y) \equiv \frac{1}{4} w(x)$$

yazılır. Burada $\varphi(x, x + y)$ *(D3)*'ten elde edilir, $\frac{1}{4} w(x)$ hesaplanabildiği için $\varphi(x, y)$ de elde edilir. Böylece, φ'nın $W_k \times C_k$ üzerindeki değerleri bulunmuş olur. Öte yandan, $C_k \times W_k$ üzerindeki değerler ise 2.6 koşulu yardımıyla *(D1)*'deki gibi hesaplanabilir.

Şimdi ispatın geri kalanında, (2.5), (2.6) ve (2.7) koşullarının gerçekten $\varphi : C_{k+1} \times C_{k+1} \to \mathbb{F}_2$ için sağlandığını göstereceğiz.

Öncelikle (2.5) koşulunu ele alalım.

Herhangi bir $x \in W_k$ için, *(D1)* adımından $\varphi(x,0) = 0$ olduğu ve *(D2)* adımı ile (2.9)'den

$$\varphi(x,0) + \varphi(x,x) \equiv \frac{1}{4}w(x)$$

elde edildiği görülmektedir. Sonuç olarak, $\varphi(x,x) = \frac{1}{4}w(x)$ olur. Diğer yandan, (2.10)'ten şu eşitlik elde edilir:

$$\varphi(b,x) + \varphi(b,x+d) + \varphi(d,x) + \varphi(d,x+b) \equiv \frac{1}{2}w(b \cap d).$$

Burada $b \in C_k$ olmak üzere $d := x + b \in W_k$ alınsın. Bu durumda,

$$\varphi(b,x) + \varphi(b,x+x+b) + \varphi(x+b,x) + \varphi(d,d) \equiv \frac{1}{2}w(b \cap (x+b)) \implies$$
$$\varphi(d,d) \equiv \varphi(b,x) + \varphi(b,b) + \varphi(x+b,x) + \frac{1}{2}w(b \cap (x+b)),$$

olur. Burada

$$\varphi(b,x) + \varphi(x+b,x) \equiv \frac{1}{4}w(x)$$

eşitliği *(D2)* ve (2.9)'den gelir. Öte yandan, $b \in C_k$ olduğundan

$$\varphi(b,b) \equiv \frac{1}{4}w(b)$$

olur (2.5 koşulundan). O halde

$$\varphi(d,d) \equiv \frac{1}{4}w(b) + \frac{1}{4}w(x) + \frac{1}{2}w(b \cap (x+b))$$

elde edilir. Buradan 2.1'e göre

$$\frac{1}{4}w(b) + \frac{1}{4}w(b+d) + \frac{1}{4}w(d) \equiv \frac{1}{2}w(b \cap d) \implies$$
$$\frac{1}{4}w(b) + \frac{1}{4}w(b+x+b) + \frac{1}{4}w(d) \equiv \frac{1}{2}w(b \cap (x+b)) \implies$$
$$\frac{1}{4}w(b) + \frac{1}{4}w(x) + \frac{1}{2}w(b \cap (x+b)) \equiv \frac{1}{4}w(d)$$

olur ki bu da

$$\varphi(d,d) \equiv \frac{1}{4}w(b) + \frac{1}{4}w(x) + \frac{1}{2}w(b \cap (x+b)) = \frac{1}{4}w(d)$$

eşitliğini verir.

$C_{k+1} \times C_{k+1}$ üzerindeki faktör kümesinin (2.6) özelliği ile devam ediyoruz.

Bu kez

$$\varphi(a,b) + \varphi(b,a) \equiv \tfrac{1}{2} w(a \cap b)$$

eşitliğiyle başlıyoruz ki bu, C_k için geçerlidir. Buna göre, $a, b \in W_k$ olmak üzere, *(D3)* ve (2.10)'ü kullanarak, $b + x$ yerine b ve a yerine d koyduğumuzda

$$\varphi(b+x,x) + \varphi(b+x,x+a) + \varphi(a,x) + \varphi(a,b) \equiv \tfrac{1}{2} w((b+x) \cap a) \qquad (2.12)$$

elde edilir. Benzer şekilde, $a + x$ yerine b ve b yerine d konulduğunda

$$\varphi(a+x,x) + \varphi(a+x,x+b) + \varphi(b,x) + \varphi(b,a) \equiv \tfrac{1}{2} w((a+x) \cap b) \qquad (2.13)$$

elde edilir.

(2.12) ve (2.13)'nin toplamı şu şekilde olur:

$$\begin{aligned} &\varphi(b+x,x) + \varphi(b+x,x+a) + \varphi(a,x) + \varphi(a,b) \\ &\quad + \varphi(a+x,x) + \varphi(a+x,x+b) + \varphi(b,x) + \varphi(b,a) \\ &\equiv \tfrac{1}{2} w((b+x) \cap a) + \tfrac{1}{2} w((a+x) \cap b). \end{aligned}$$

(D2), (2.9) ve (2.6) kullanıldığında ise

$$\begin{aligned} &\varphi(b+x,x) + \varphi(b,x) = \varphi(x,b+x) + \tfrac{1}{2} w(x \cap (b+x)) + \varphi(x,b) + \tfrac{1}{2} w(x \cap b) \\ &\equiv \tfrac{1}{4} w(x) + w(x \cap b \cap x) + \tfrac{1}{2} w(x \cap b) + \tfrac{1}{2} w(x \cap x) + \tfrac{1}{2} w(x \cap b) \\ &= \tfrac{1}{4} w(x) \end{aligned}$$

ve dolayısıyla

$$\varphi(c+x,x) + \varphi(c,x) \equiv \tfrac{1}{4} w(x)$$

elde edilir.

Dolayısıyla,

$$\begin{aligned} &\tfrac{1}{4} w(x) + \tfrac{1}{4} w(x) + \varphi(b+x,x+a) + \varphi(a+x,x+b) \\ &\qquad + \varphi(a,b) + \varphi(b,a) \equiv \tfrac{1}{2} w((b+x) \cap a) + \tfrac{1}{2} w((a+x) \cap b). \end{aligned}$$

Sonraki adımda, (2.6) ifadesini

$$\varphi(b+x,x+a) + \varphi(a+x,x+b) \equiv \tfrac{1}{2} w((a+x) \cap (b+x))$$

şeklinde yorumlarsak, şu sonucu elde ederiz:

$$\tfrac{1}{2}w((a+x)\cap(b+x))+\varphi(a,b)+\varphi(b,a)\equiv\tfrac{1}{2}w((b+x)\cap a)+\tfrac{1}{2}w((a+x)\cap b).$$

Ayrıca, (2.3) ve Önerme 2.2'den şunu da gözlemleriz:

$$\begin{aligned}\tfrac{1}{2}w((b+x)\cap a)&\equiv\tfrac{1}{2}w(a\cap x)+\tfrac{1}{2}w(a\cap b)+w(a\cap b\cap x)\\ \tfrac{1}{2}w((a+x)\cap b)&\equiv\tfrac{1}{2}w(a\cap b)+\tfrac{1}{2}w(b\cap x)+w(a\cap b\cap x)\end{aligned}$$

Sonuç olarak,

$$\begin{aligned}\tfrac{1}{2}w((a+x)\cap(b+x))&\equiv w((a+x)\cap b\cap x)+\tfrac{1}{2}w((a+x)\cap b)\\ &\quad+\tfrac{1}{2}w((a+x)\cap x)\\ &\equiv w(a\cap b\cap x)+w(x\cap b\cap x)+w(a\cap x\cap b)\\ &\quad+\tfrac{1}{2}w(a\cap b)+\tfrac{1}{2}w(x\cap b)+w(a\cap x\cap x)+\tfrac{1}{2}w(a\cap x)\\ &\quad+\tfrac{1}{2}w(x\cap x)\\ &\equiv\tfrac{1}{2}w(a\cap b)+\tfrac{1}{2}w(x\cap b)+\tfrac{1}{2}w(a\cap x),\end{aligned}$$

ve dolayısıyla

$$\begin{aligned}&\tfrac{1}{2}w(a\cap b)+\tfrac{1}{2}w(x\cap b)+\tfrac{1}{2}w(a\cap x)+\varphi(a,b)+\varphi(b,a)\\ &\qquad\equiv\tfrac{1}{2}w(a\cap x)+\tfrac{1}{2}w(a\cap b)+w(a\cap b\cap x)+\tfrac{1}{2}w(a\cap b)\\ &\qquad\quad+\tfrac{1}{2}w(b\cap x)+w(a\cap b\cap x),\end{aligned}$$

buradan

$$\varphi(a,b)+\varphi(b,a)\equiv\tfrac{1}{2}w(a\cap b)$$

sonucunu elde ederiz.

Son olarak (2.7) özelliğine bakalım. Şimdi de

$$A(a,b,c):=\varphi(a,b)+\varphi(a+b,c)+\varphi(b,c)+\varphi(a,b+c)\tag{2.14}$$

fonksiyonunu ele alarak

$$A(a,b,c)=w(a\cap b\cap c)$$

eşitliğini göstereceğiz. Bu eşitlik, $a, b, c \in C_k$ için zaten sağlanmaktadır. Eğer $a, b, c \in C_{k+1}$ ise, o zaman

$$\begin{aligned} A(a,b,c) + A(b,c,a) + A(c,a,b) &= \varphi(a,b) + \varphi(a+b,c) + \varphi(b,c) + \varphi(a,b+c) \\ &\quad + \varphi(b,c) + \varphi(b+c,a) + \varphi(c,a) + \varphi(b,c+a) \\ &\quad + \varphi(c,a) + \varphi(c+a,b) + \varphi(a,b) + \varphi(c,a+b) \\ &= \varphi(a+b,c) + \varphi(b+c,a) + \varphi(c+a,b) \\ &\quad + \varphi(a,b+c) + \varphi(b,c+a) + \varphi(c,a+b). \end{aligned}$$

Buradan, (2.6) kullanılarak

$$\begin{aligned} \varphi(a+b,c) + \varphi(c,a+b) &\equiv \tfrac{1}{2} w((a+b) \cap c), \\ \varphi(b+c,a) + \varphi(a,b+c) &\equiv \tfrac{1}{2} w((b+c) \cap a), \\ \varphi(c+a,b) + \varphi(b,c+a) &\equiv \tfrac{1}{2} w((c+a) \cap b), \end{aligned}$$

elde edilir. Ayrıca (2.3) sayesinde

$$\begin{aligned} \tfrac{1}{2}\, w((a+b) \cap c) &\equiv w(a \cap b \cap c) + \tfrac{1}{2} w(a \cap c) + \tfrac{1}{2} w(b \cap c), \\ \tfrac{1}{2}\, w((b+c) \cap a) &\equiv w(a \cap b \cap c) + \tfrac{1}{2} w(b \cap a) + \tfrac{1}{2} w(c \cap a), \\ \tfrac{1}{2}\, w((c+a) \cap b) &\equiv w(a \cap b \cap c) + \tfrac{1}{2} w(c \cap b) + \tfrac{1}{2} w(a \cap b). \end{aligned}$$

Buna göre,

$$\begin{aligned} A(a,b,c) + A(b,c,a) + A(c,a,b) &\equiv w(a \cap b \cap c) + \frac{1}{2} w(a \cap c) + \frac{1}{2} w(b \cap c) \\ &\quad + w(a \cap b \cap c) + \frac{1}{2} w(b \cap a) + \frac{1}{2} w(c \cap a) \\ &\quad + w(a \cap b \cap c) + \frac{1}{2} w(c \cap b) + \frac{1}{2} w(a \cap b) \end{aligned}$$

eşitliği elde edilir. Buradan da

$$A(a,b,c) + A(b,c,a) + A(c,a,b) \equiv w(a \cap b \cap c) \tag{2.15}$$

sonucuna varılır.

Şimdi, $A(a,b,c) = w(a \cap b \cap c)$ eşitliğini aşağıdaki durumlar için ayrı ayrı inceleyeceğiz:

Durum 1: $a, b, c \in W_k$

Durum 2: $b \in W_k$ ve $a, c \in C_k$

Durum 3: $a \in W_k$ ve $b, c \in C_k$

Durum 4: $c \in W_k$ ve $a, b \in C_k$

Durum 5: $a, b \in W_k$ ve $c \in C_k$

Durum 6: $b, c \in W_k$ ve $a \in C_k$

Durum 7: $a, c \in W_k$ ve $b \in C_k$

Durum 1: Diyelim ki $a, b, c \in W_k$.

(2.14) ifadesiyle başlıyoruz:

$$A(a, b, c) = \varphi(a, b) + \varphi(a + b, c) + \varphi(b, c) + \varphi(a, b + c)$$

burada,

$$\varphi(a, b) + \varphi(b + x, x) + \varphi(b + x, x + a) + \varphi(a, x) \equiv \frac{1}{2} w((b + x) \cap a) \tag{2.16}$$

$$\varphi(b, c) + \varphi(c + x, x) + \varphi(c + x, x + b) + \varphi(b, x) \equiv \frac{1}{2} w((c + x) \cap b) \tag{2.17}$$

ifadeleri *(D3)* ve (2.10)'ten elde edilir.

Bir yandan,

$$\varphi(a + b, c) + \varphi(c, a + b) \equiv \frac{1}{2} w((a + b) \cap c) \implies$$
$$\varphi(a + b, c) \equiv \varphi(c, a + b) + \frac{1}{2} w((a + b) \cap c)$$

ifadesi, şu sonucu verir:

$$\varphi(a + b, c) \equiv \varphi(c, a + b + c) + \frac{1}{4} w(c) + \frac{1}{2} w((a + b) \cap c) \tag{2.18}$$

Diğer yandan ise,

$$\varphi(a, b + c) + \varphi(a, a + b + c) \equiv \frac{1}{4} w(a)$$

eşitliği, (*(D3)*) ve (2.9), *(D4)* ve 2.6 kullanılarak,

$$\varphi(a, b + c) \equiv \varphi(a, a + b + c) + \frac{1}{4} w(a) \tag{2.19}$$

sonucunu verir.

$\varphi(c, a+b+c)$ ifadesi (2.18)'te ve $\varphi(a, a+b+c)$ ifadesi de (2.19)'te geçtiği üzere;

$$\begin{aligned}
&\varphi(a+b+c+x,x)+\varphi(a+b+c+x,x+c)+\varphi(c,x)+\varphi(c,a+b+c)\\
&\qquad\equiv \frac{1}{2}w((a+b+c+x)\cap c)\\
&\qquad\equiv w(c\cap a\cap b)+w(c\cap a\cap c)+w(c\cap a\cap x)\\
&\qquad\quad + w(c\cap b\cap c)+w(c\cap b\cap x)+w(c\cap c\cap x)\\
&\qquad\quad + \frac{1}{2}w(c\cap a)+\frac{1}{2}w(c\cap b)+\frac{1}{2}w(c\cap c)+\frac{1}{2}w(c\cap x)\\
&\qquad\equiv w(c\cap a\cap b)+w(c\cap a\cap x)+w(c\cap b\cap x)\\
&\qquad\quad + \frac{1}{2}w(c\cap a)+\frac{1}{2}w(c\cap b)+\frac{1}{2}w(c\cap x).
\end{aligned}$$

Buradan,

$$\begin{aligned}
\varphi(c,a+b+c) &\equiv \varphi(a+b+c+x,x)+\varphi(a+b+c+x,x+c)+\varphi(c,x)\\
&\quad + w(c\cap a\cap b)+w(c\cap a\cap x)+w(c\cap b\cap x)\\
&\quad + \frac{1}{2}w(c\cap a)+\frac{1}{2}w(c\cap b)+\frac{1}{2}w(c\cap x).
\end{aligned} \tag{2.20}$$

Dolayısıyla,

$$\begin{aligned}
&\varphi(a+b+c+x,x)+\varphi(a+b+c+x,x+a)+\varphi(a,x)+\varphi(a,a+b+c)\\
&\qquad\equiv \frac{1}{2}w((a+b+c+x)\cap a)\\
&\qquad\equiv w(a\cap a\cap b)+w(a\cap a\cap c)+w(a\cap a\cap x)\\
&\qquad\quad + w(a\cap b\cap c)+w(a\cap b\cap x)+w(a\cap c\cap x)\\
&\qquad\quad + \frac{1}{2}w(a\cap a)+\frac{1}{2}w(a\cap b)+\frac{1}{2}w(a\cap c)+\frac{1}{2}w(a\cap x)\\
&\qquad\equiv w(a\cap b\cap c)+w(a\cap b\cap x)+w(a\cap c\cap x)\\
&\qquad\quad + \frac{1}{2}w(a\cap b)+\frac{1}{2}w(a\cap c)+\frac{1}{2}w(a\cap x).
\end{aligned}$$

Buna göre, (*(D3)*) ve (2.10) kullanılarak

$$\begin{aligned}
\varphi(a,a+b+c) &\equiv \varphi(a+b+c+x,x)+\varphi(a+b+c+x,x+a)+\varphi(a,x)\\
&\quad + w(a\cap b\cap c)+w(a\cap b\cap x)+w(a\cap c\cap x)+\frac{1}{2}w(a\cap b)\\
&\quad + \frac{1}{2}w(a\cap c)+\frac{1}{2}w(a\cap x)
\end{aligned} \tag{2.21}$$

eşitliğini elde ederiz.

Dolayısıyla, (2.16), (2.17), (2.18), (2.19), (2.20) ve (2.21) ifadelerini birleştirerek:

$$
\begin{aligned}
A(a,b,c) &\equiv \varphi(b+x,x)+\varphi(b+x,x+a)+\varphi(a,x)+\frac{1}{2}w((b+x)\cap a)\\
&+\varphi(c,a+b+c)+\frac{1}{2}w((a+b)\cap c)+\frac{1}{4}w(c)+\varphi(c+x,x)\\
&+\varphi(c+x,x+b)+\varphi(b,x)+\frac{1}{2}w((c+x)\cap b)+\varphi(a,a+b+c)+\frac{1}{4}w(a)
\end{aligned}
$$

$$
\begin{aligned}
&\equiv \varphi(b+x,x)+\varphi(b+x,x+a)+\varphi(a,x)+\frac{1}{2}w((b+x)\cap a)\\
&\quad+\varphi(a+b+c+x,x)+\varphi(a+b+c+x,c+x)+\varphi(c,x)\\
&\quad+\frac{1}{2}w(c\cap(a+b+x))+\frac{1}{2}w((a+b)\cap c)+\frac{1}{4}w(c)+\varphi(c+x,x)\\
&\quad+\varphi(c+x,x+b)+\varphi(b,x)+\frac{1}{2}w((c+x)\cap b)+\varphi(a+b+c+x,x)\\
&\quad+\varphi(a+b+c+x,x+a)+\varphi(a,x)+\frac{1}{2}w(a\cap(b+c+x))+\frac{1}{4}w(a)
\end{aligned}
$$

$$
\begin{aligned}
&\equiv \varphi(b+x,x+a)+\varphi(a+b+c+x,c+x)+\varphi(c+x,x+b)\\
&\quad+\varphi(a+b+c+x,x+a)+\frac{1}{4}w(x)+\frac{1}{4}w(x)+w(b\cap x\cap a)\\
&\quad+\frac{1}{2}w(a\cap b)+\frac{1}{2}w(a\cap x)+w(a\cap b\cap c)+\frac{1}{2}w(c\cap a)+\frac{1}{2}w(c\cap b)\\
&\quad+w(c\cap a\cap b)+w(c\cap a\cap x)+w(c\cap b\cap x)+\frac{1}{2}w(c\cap a)\\
&\quad+\frac{1}{2}w(c\cap b)+\frac{1}{2}w(c\cap x)+\frac{1}{4}w(c)+w(c\cap x\cap b)+\frac{1}{2}w(b\cap c)\\
&\quad+\frac{1}{2}w(b\cap x)+w(a\cap b\cap c)+w(a\cap b\cap x)+w(a\cap c\cap x)\\
&\quad+\frac{1}{2}w(a\cap b)+\frac{1}{2}w(a\cap c)+\frac{1}{2}w(a\cap x)+\frac{1}{4}w(a)
\end{aligned}
$$

$$
\begin{aligned}
&\equiv \varphi(b+x,x+a)+\varphi(a+b+c+x,c+x)+\varphi(c+x,x+b)\\
&\quad+\varphi(a+b+c+x,x+a)+\frac{1}{2}w(c\cap a)+\frac{1}{2}w(c\cap b)+\frac{1}{2}w(c\cap x)\\
&\quad+\frac{1}{4}w(c)+\frac{1}{2}w(b\cap x)+w(a\cap b\cap c)+\frac{1}{4}w(a)
\end{aligned}
$$

$$
\begin{aligned}
&\equiv \varphi(b+x,x+a)+\varphi(a+x+b+x+c+x,c+x)+\varphi(c+x,x+b)\\
&\quad+\varphi(a+x+b+x+c+x,x+a)+\frac{1}{2}w(c\cap a)+\frac{1}{2}w(c\cap b)\\
&\quad+\frac{1}{2}w(c\cap x)+\frac{1}{4}w(c)+\frac{1}{2}w(b\cap x)+w(a\cap b\cap c)+\frac{1}{4}w(a)
\end{aligned}
$$

elde edilir.

Sonrasında da, $x, a, b, c \in W_k$ olduğundan $a + x = k$, $b + x = m$, $c + x = n \in C_k$ elde ederiz. Böylece, son eşitlikte k, m, n yerlerine yazılırsa

$$\begin{aligned} A(a,b,c) = {} & \varphi(m,k) + \varphi(k+m+n,n) + \varphi(n,m) + \varphi(k+m+n,k) \\ & + \frac{1}{2}w(c \cap a) + \frac{1}{2}w(c \cap b) + \frac{1}{2}w(c \cap x) + \frac{1}{4}w(c) + \frac{1}{2}w(b \cap x) \\ & + w(a \cap b \cap c) + \frac{1}{4}w(a). \end{aligned}$$

Öte yandan, (2.9) ifadesinden

$$\varphi(k+m+n,n) = \varphi(m+k,n) + \frac{1}{4}w(n)$$

ve

$$\varphi(k+m+n,k) \equiv \varphi(m+n,k) + \frac{1}{4}w(k)$$

sonuçları elde edilir.

Bunları da dikkate aldığımızda,

$$\begin{aligned} A(a,b,c) = {} & \varphi(m,k) + \varphi(m+k,n) + \frac{1}{4}w(n) + \varphi(n,m) + \varphi(m+n,k) \\ & + \frac{1}{4}w(k) + \frac{1}{2}w(c \cap a) + \frac{1}{2}w(c \cap b) + \frac{1}{2}w(c \cap x) \\ & + \frac{1}{4}w(c) + \frac{1}{2}w(b \cap x) + w(a \cap b \cap c) + \frac{1}{4}w(a) \end{aligned}$$

sonuca varırız. Ayrıca

$$\begin{aligned} \varphi(m+k,n) \equiv {} & \varphi(n,m+k) + \frac{1}{2}w(n \cap (m+k)) \equiv \\ & \varphi(n,m+k) + w(n \cap m \cap k) + \frac{1}{2}w(n \cap m) + \frac{1}{2}w(n \cap k), \end{aligned}$$

eşitliğini (2.6)'den elde edip kullanarak,

$$\begin{aligned} A(a,b,c) = {} & \varphi(m,k) + \varphi(n,m+k) + w(n \cap m \cap k) + \frac{1}{2}w(n \cap m) + \frac{1}{2}w(n \cap k) \\ & + \frac{1}{4}w(n) + \varphi(n,m) + \varphi(m+n,k) + \frac{1}{4}w(k) + \frac{1}{2}w(c \cap a) + \frac{1}{2}w(c \cap b) \\ & + \frac{1}{2}w(c \cap x) + \frac{1}{4}w(c) + \frac{1}{2}w(b \cap x) + w(a \cap b \cap c) + \frac{1}{4}w(a). \end{aligned}$$

Ardından (2.14) ifadesine başvurarak şu ifadeye ulaşırız:

$$\begin{aligned}A(a,b,c) = A(n,m,k) &+ \frac{1}{4}w(n) + \frac{1}{4}w(k) + w(k\cap m\cap n) + \frac{1}{2}w(n\cap m)\\ &+ \frac{1}{2}w(k\cap n) + \frac{1}{2}w(c\cap a) + \frac{1}{2}w(c\cap b) + \frac{1}{2}w(c\cap x) + \frac{1}{4}w(c)\\ &+ \frac{1}{2}w(b\cap x) + w(a\cap b\cap c) + \frac{1}{4}w(a).\end{aligned}$$

Son olarak, $n, m, k \in C_k$ olduğundan $A(n,m,k) = w(n\cap m\cap k)$ elde edilir ve Önerme 2.2'den

$$\begin{aligned}A(a,b,c) &= w(n\cap m\cap k) + \frac{1}{4}w(c+x) + \frac{1}{4}w(a+x) + w(k\cap m\cap n)\\ &+ \frac{1}{2}w((c+x)\cap(b+x)) + \frac{1}{2}w((a+x)\cap(c+x)) + \frac{1}{2}w(c\cap a)\\ &+ \frac{1}{2}w(c\cap b) + \frac{1}{2}w(c\cap x) + \frac{1}{4}w(c) + \frac{1}{2}w(b\cap x) + w(a\cap b\cap c) + \frac{1}{4}w(a)\\ &\equiv \frac{1}{4}w(x) + \frac{1}{4}w(c) + \frac{1}{2}w(x\cap c) + \frac{1}{4}w(a) + \frac{1}{4}w(x) + \frac{1}{2}w(a\cap x) +\\ &\quad w((c+x)\cap b\cap x) + \frac{1}{2}w((c+x)\cap b) + \frac{1}{2}w((c+x)\cap x)\\ &\quad + w((c+x)\cap a\cap x) + \frac{1}{2}w((c+x)\cap a) + \frac{1}{2}w((c+x)\cap x)\\ &\quad + \frac{1}{2}w(c\cap a) + \frac{1}{2}w(c\cap b) + \frac{1}{2}w(c\cap x) + \frac{1}{4}w(c) + \frac{1}{2}w(b\cap x)\\ &\quad + w(a\cap b\cap c) + \frac{1}{4}w(a)\end{aligned}$$

$$\begin{aligned}&\equiv \frac{1}{2}w(a\cap x) + w(c\cap b\cap x) + w(x\cap b\cap x) + w(c\cap x\cap b) + \frac{1}{2}w(c\cap b)\\ &+ \frac{1}{2}w(x\cap b) + w(c\cap a\cap x) + w(x\cap a\cap x) + w(c\cap x\cap a) + \frac{1}{2}w(c\cap a)\\ &+ \frac{1}{2}w(x\cap a) + \frac{1}{2}w(c\cap a) + \frac{1}{2}w(c\cap b) + \frac{1}{2}w(b\cap x) + w(a\cap b\cap c)\\ &\equiv w(a\cap b\cap c)\end{aligned}$$

sonucu iddia edildiği gibi elde edilir.

Durum 2: $b \in W_k$ ve $a, c \in C_k$ olsun.

İlk olarak, $x := a+b+c$, $y := a+b$, $z := b$ için $x, y, z \in W_k$ olduğunu not edelim. Bu durumda, *Durum 1* ve Önerme 2.2'den

$$A(x,y,z) = A(a+b+c, a+b, b) \equiv w((a+b+c)\cap(a+b)\cap b).$$

Eğer $t = a + b$ olarak alınırsa,

$$\begin{aligned} A(x, y, z) &\equiv w((t + c) \cap t \cap b) = w(t \cap t \cap b) + w(c \cap t \cap b) \\ &\equiv w((a + b) \cap c \cap b) = w(a \cap c \cap b) + w(b \cap c \cap b) \\ &\equiv w(a \cap b \cap c), \end{aligned}$$

ve dolayısıyla

$$A(x, y, z) \equiv w(a \cap b \cap c). \tag{2.22}$$

Bu durumda, (2.14) ifadesinden

$$\begin{aligned} A(x, y, z) &= A(a + b + c, a + b, b) \\ &\equiv \varphi(a + b + c, a + b) + \varphi(c, b) + \varphi(a + b, b) + \varphi(a + b + c, a) \end{aligned} \tag{2.23}$$

elde edilir.

Daha sonra, (2.9) ve (2.6) ifadelerini *(D3)* ve *(D4)* üzerinden kullanarak aşağıdakileri elde ederiz:

$$\begin{aligned} \varphi(a + b + c, a + b) &\equiv \varphi(a + b, a + b + c) + \frac{1}{2} w((a + b + c) \cap (a + b)) \\ &\equiv \varphi(a + b, c) + \frac{1}{4} w(a + b) + \frac{1}{2} w((a + b) \cap c), \end{aligned}$$

ve

$$\begin{aligned} \varphi(a + b, b) &= \varphi(b, a + b) + \frac{1}{2} w((a + b) \cap b) \\ &\equiv \varphi(b, a) + \frac{1}{4} w(b) + \frac{1}{2} w(a \cap b) \\ &\equiv \varphi(a, b) + \frac{1}{2} w(a \cap b) + \frac{1}{4} w(b) + \frac{1}{2} w(a \cap b) \\ &\equiv \varphi(a, b) + \frac{1}{4} w(b), \end{aligned}$$

ve ayrıca

$$\begin{aligned} \varphi(a + b + c, a) &\equiv \varphi(a, a + b + c) + \frac{1}{2} w((a + b + c) \cap a) \\ &\equiv \varphi(a, b + c) + \frac{1}{4} w(a) + \frac{1}{2} w((b + c) \cap a). \end{aligned}$$

Bu ifadeleri (2.23) ifadesine yerine koyarsak, aşağıdakini elde ederiz:

$$\begin{aligned}
A(x,y,z) &\equiv \varphi(a+b,c)+\frac{1}{4}w(a+b)+\frac{1}{2}w((a+b)\cap c)+\varphi(c,b)+\varphi(a,b)\\
&\quad+\frac{1}{4}w(b)+\varphi(a,b+c)+\frac{1}{4}w(a)+\frac{1}{2}w(a\cap(b+c))\\
&\equiv \varphi(a+b,c)+\frac{1}{4}w(a+b)+w(a\cap b\cap c)+\frac{1}{2}w(a\cap c)+\frac{1}{2}w(b\cap c)\\
&\quad+\varphi(b,c)+\frac{1}{2}w(b\cap c)+\varphi(a,b)+\frac{1}{4}w(b)+\varphi(a,b+c)+\frac{1}{4}w(a)\\
&\quad+w(a\cap b\cap c)+\frac{1}{2}w(a\cap b)+\frac{1}{2}w(a\cap c)\\
&\equiv \varphi(a+b,c)+\varphi(b,c)+\varphi(a,b)+\varphi(a,b+c)+\frac{1}{4}w(a)+\frac{1}{4}w(a+b)\\
&\quad+\frac{1}{4}w(b)+\frac{1}{2}w(a\cap b).
\end{aligned}$$

Son olarak, (2.1) göz önüne alındığında

$$\begin{aligned}
A(x,y,z) &\equiv A(a,b,c)+\frac{1}{2}w(a\cap b)+\frac{1}{2}w(a\cap b)\\
&\equiv A(a,b,c)
\end{aligned}$$

elde ederiz. Bu da, aşağıdaki eşitlik yoluyla iddiayı doğrular:

$$A(x,y,z)\equiv w(a\cap b\cap c)\equiv A(a,b,c).$$

Durum 3: $a\in W_k$ ve $b,c\in C_k$ olsun.

(D4) maddesinden, (2.9) ifadesi kullanılarak

$$\begin{aligned}
\varphi(a,b)+\varphi(a,a+b) &\equiv \frac{1}{4}w(a)\\
\varphi(a,b+c)+\varphi(a,a+b+c) &\equiv \frac{1}{4}w(a)\\
\varphi(a+b,c)+\varphi(a+b,a+b+c) &\equiv \frac{1}{4}w(a+b)
\end{aligned}$$

sonuçlarına ulaşabiliriz. Dolayısıyla

$$\begin{aligned}
A(a,b,c) &\equiv \varphi(a,a+b)+\frac{1}{4}w(a)+\varphi(a+b,a+b+c)+\frac{1}{4}w(a+b)\\
&\quad+\varphi(b,c)+\varphi(a,a+b+c)+\frac{1}{4}w(a)\\
&\equiv \varphi(a,a+b)+\varphi(a+b,a+b+c)+\frac{1}{4}w(a+b)\\
&\quad+\varphi(b,c)+\varphi(a,a+b+c).
\end{aligned}$$

Benzer şekilde, (2.10) ifadesini $b \to b+x$ ve $d \to a$ olarak kullandığımızda

$$\varphi(b+x,x)+\varphi(b+x,x+a)+\varphi(a,x)+\varphi(a,b) \equiv \frac{1}{2}w((b+x)\cap a) \qquad (2.24)$$

elde ederiz. Öte yandan, (2.24) ifadesinde $b \to a+b$ yazıldığında da

$$\varphi(a,a+b) \equiv \varphi(a+b+x,x)+\varphi(a+b+x,x+a)+\varphi(a,x)+\frac{1}{2}w((a+b+x)\cap a)$$

elde edilir.

Aynı şekilde, (2.24) ifadesinde $a \to a+b$ ve $b \to a+b+c$ olarak ayarladığımızda şu sonuca varırız:

$$\begin{aligned}\varphi(a+b,a+b+c) \equiv{}& \varphi(a+b+c+x,x)+\varphi(a+b+c+x,x+a+b)\\ &+\varphi(a+b,x)+\frac{1}{2}w((a+b+c+x)\cap(a+b)).\end{aligned}$$

Son olarak, (2.24) ifadesinde $b \to a+b+c$ olarak ayarladığımızda ise

$$\begin{aligned}\varphi(a,a+b+c) \equiv{}& \varphi(a+b+c+x,x)+\varphi(a+b+c+x,x+a)+\varphi(a,x)\\ &+\frac{1}{2}w((a+b+c+x)\cap a)\end{aligned}$$

elde ederiz.

Şimdi, tüm bunları (2.23) denklemine yerine koyarak

$$\begin{aligned}A(a,b,c) \equiv{}& \varphi(a+b+x,x)+\varphi(a+b+x,x+a)+\\ &\varphi(a,x)+\frac{1}{2}w((a+b+x)\cap a)+\varphi(a+b+c+x,x)+\\ &\varphi(a+b+c+x,a+b+x)+\varphi(a+b,x)+\\ &\frac{1}{2}w((a+b+c+x)\cap(a+b))+\frac{1}{4}w(a+b)+\varphi(b,c)+\\ &\varphi(a+b+c+x,x)+\varphi(a+b+c+x,x+a)+\varphi(a,x)+\\ &\frac{1}{2}w((a+b+c+x)\cap a)\end{aligned}$$

$$\begin{aligned}\equiv{}& \varphi(a+b+x,x)+\varphi(a+b+x,x+a)+\frac{1}{2}w((a+b+x)\cap a)\\ &+\varphi(a+b+c+x,a+b+x)+\varphi(a+b,x)+\\ &\frac{1}{2}w((a+b+c+x)\cap(a+b))+\frac{1}{4}w(a+b)+\varphi(b,c)+\\ &\varphi(a+b+c+x,x+a)+\frac{1}{2}w((a+b+c+x)\cap a).\end{aligned}$$

Buradan,

$$\begin{aligned}\frac{1}{2}w((a+b+x)\cap a) &= w(a\cap a\cap b)+w(a\cap a\cap x)+w(a\cap b\cap x)\\ &\quad+\frac{1}{2}w(a\cap a)+\frac{1}{2}w(a\cap b)+\frac{1}{2}w(a\cap x)\\ &\equiv \frac{1}{2}w((b+x)\cap a)\end{aligned}$$

ve

$$\begin{aligned}\frac{1}{2}w((a+b+c+x)\cap a) &\equiv w(a\cap a\cap b)+w(a\cap a\cap c)+w(a\cap a\cap x)\\ &\quad+w(a\cap b\cap c)+w(a\cap b\cap x)+w(a\cap c\cap x)\\ &\quad+\frac{1}{2}w(a\cap a)+\frac{1}{2}w(a\cap b)+\frac{1}{2}w(a\cap c)+\frac{1}{2}w(a\cap x)\\ &\equiv \frac{1}{2}w((b+c+x)\cap a)\end{aligned}$$

ifadeleri yazabiliriz. Dahası, $\frac{1}{2}w((a+b+c+x)\cap(a+b))$ ifadesinde $a+b=:t$ olarak alırsak

$$\begin{aligned}\frac{1}{2}w((a+b+c+x)\cap(a+b)) &= \frac{1}{2}w((t+c+x)\cap t)\\ &\equiv \frac{1}{2}w((c+x)\cap t)\\ &\equiv \frac{1}{2}w((c+x)\cap(a+b)),\end{aligned}$$

ve sonuç olarak,

$$\begin{aligned}A(a,b,c) &\equiv \varphi(a+b+x,x)+\varphi(a+b+x,x+a)+\frac{1}{2}w((b+x)\cap a)\\ &\quad+\varphi(a+b+c+x,a+b+x)+\varphi(a+b,x)\\ &\quad+\frac{1}{2}w((c+x)\cap(a+b))+\frac{1}{4}w(a+b)+\varphi(b,c)\\ &\quad+\varphi(a+b+c+x,x+a)+\frac{1}{2}w((b+c+x)\cap a)\end{aligned}$$

buluruz.

Şimdi, *(D4)*'ten (2.9) aracılığıyla

$$\varphi(a+b+x,x)+\varphi(a+b,x)=\frac{1}{4}w(x)$$

ilişkisinin dahil edilmesiyle,

$$\begin{aligned}A(a,b,c) \equiv \frac{1}{4}w(x) &+ \varphi(a+b+x, x+a) + \frac{1}{2}w((b+x)\cap a)\\ &+ \varphi(a+b+c+x, a+b+x) + \frac{1}{2}w((c+x)\cap(a+b))\\ &+ \frac{1}{4}w(a+b) + \varphi(b,c) + \varphi(a+b+c+x, x+a)\\ &+ \frac{1}{2}w((b+c+x)\cap a).\end{aligned}$$

Sonraki adımda, $a+b+x=k$ ve $a+x=m$ olarak alıp

$$\varphi(a+b+x, x+a) \equiv \varphi(k,m) = \varphi(m,k) + \frac{1}{2}w(k\cap m)$$
$$\varphi(a+b+c+x, a+b+x) \equiv \varphi(k+c,k) = \varphi(c,k) + \frac{1}{4}w(k)$$
$$\varphi(a+b+c+x, x+a) \equiv \varphi(k+c,m) = \varphi(m,k+c) + \frac{1}{2}w((k+c)\cap m)$$

ifadeleri kullanarak

$$\begin{aligned}A(a,b,c) \equiv \frac{1}{4}w(x) &+ \varphi(m,k) + \frac{1}{2}w(k\cap m) + \frac{1}{2}w((b+x)\cap a) + \varphi(c,k)\\ &+ \frac{1}{4}w(k) + \varphi(m,k+c) + \frac{1}{2}w((k+c)\cap m) + \frac{1}{2}w((b+c+x)\cap a)\\ &+ \frac{1}{2}w((c+x)\cap(a+b)) + \frac{1}{4}w(a+b) + \varphi(b,c)\end{aligned}$$

elde ederiz.

Öte yandan, $k, m, c \in C_k$ olduğundan

$$\varphi(m,k) + \varphi(m,k+c) + \varphi(c,k) + \varphi(c,k+m) \equiv \frac{1}{2}w(m\cap c)$$

eşitliği elde edilir, bu da

$$\varphi(m,k) + \varphi(m,k+c) + \varphi(c,k) \equiv \varphi(c,k+m) + \frac{1}{2}w(m\cap c)$$

sonucunu verir.

Buna göre,

$$\begin{aligned}A(a,b,c) \equiv \frac{1}{4}w(x) &+ \frac{1}{2}w(m\cap c) + \varphi(c,k+m) + \frac{1}{2}w(k\cap m)\\ &+ \frac{1}{2}w((b+x)\cap a) + \frac{1}{4}w(k) + \frac{1}{2}w((k+c)\cap m)\\ &+ \frac{1}{2}w((b+c+x)\cap a) + \frac{1}{2}w((c+x)\cap(a+b))\\ &+ \frac{1}{4}w(a+b) + \varphi(b,c),\end{aligned}$$

buradan

$$\frac{1}{2}w((b+c+x)\cap a) \equiv \frac{1}{2}w(b\cap a)+\frac{1}{2}w((c+x)\cap a)+w((c+x)\cap b\cap a),$$

ve Önerme 2.2'dan da

$$\frac{1}{2}w((c+x)\cap(a+b)) \equiv \frac{1}{2}w((c+x)\cap a)+\frac{1}{2}w((c+x)\cap b)+w((c+x)\cap a\cap b)$$

elde edilir. Böylece,

$$\begin{aligned}A(a,b,c) \equiv{}& \frac{1}{4}w(x)+\frac{1}{2}w(m\cap c)+\varphi(c,k+m)+\frac{1}{2}w(k\cap m)\\ &+\frac{1}{2}w((b+x)\cap a)+\frac{1}{4}w(k)+\frac{1}{2}w((k+c)\cap m)\\ &+\frac{1}{2}w(b\cap a)+\frac{1}{2}w((c+x)\cap a)+w((c+x)\cap b\cap a)\\ &+\frac{1}{2}w((c+x)\cap a)+\frac{1}{2}w((c+x)\cap b)+w((c+x)\cap a\cap b)\\ &+\frac{1}{4}w(a+b)+\varphi(b,c)\end{aligned}$$

$$\begin{aligned}\equiv{}& \frac{1}{4}w(x)+\frac{1}{2}w(m\cap c)+\varphi(c,k+m)+\frac{1}{2}w(k\cap m)+w(b\cap x\cap a)\\ &+\frac{1}{2}w(b\cap a)+\frac{1}{2}w(x\cap a)+\frac{1}{4}w(k)+w(k\cap c\cap m)+\frac{1}{2}w(k\cap m)\\ &+\frac{1}{2}w(c\cap m)+\frac{1}{2}w(b\cap a)+\frac{1}{2}w((c+x)\cap a)+w((c+x)\cap b\cap a)\\ &+\frac{1}{2}w((c+x)\cap a)+\frac{1}{2}w((c+x)\cap b)+w((c+x)\cap a\cap b)\\ &+\frac{1}{4}w(a+b)+\varphi(b,c)\end{aligned}$$

$$\begin{aligned}\equiv{}& \frac{1}{4}w(x)+\varphi(c,k+m)+w(b\cap x\cap a)+\frac{1}{2}w(b\cap a)+\frac{1}{2}w(x\cap a)\\ &+\frac{1}{4}w(k)+w(k\cap c\cap m)+\frac{1}{2}w(b\cap a)+\frac{1}{2}w((c+x)\cap b)\\ &+\frac{1}{4}w(a+b)+\varphi(b,c)\end{aligned}$$

sonuca varılır. Ardından $a+b+x=k$ ve $a+x=m$ yerine konularak

$$\begin{aligned}A(a,b,c) \equiv{}& \frac{1}{4}w(x)+\varphi(c,b)+w(b\cap x\cap a)+\tfrac{1}{2}w(b\cap a)+\tfrac{1}{2}w(x\cap a)\\ &+\tfrac{1}{4}w(a+b+x)+w((a+b+x)\cap c\cap(a+x))+\tfrac{1}{2}w(b\cap a)\\ &+w(c\cap x\cap b)+\tfrac{1}{2}w(b\cap x)+\tfrac{1}{2}w(b\cap c)+\tfrac{1}{4}w(a+b)+\varphi(b,c)\end{aligned}$$

$$\equiv \frac{1}{4}w(x) + \varphi(b,c) + \tfrac{1}{2}w(b\cap c) + w(b\cap x\cap a) + \tfrac{1}{2}w(b\cap a)$$
$$+ \tfrac{1}{2}w(x\cap a) + \tfrac{1}{4}w(a+b+x) + w((a+b+x)\cap c\cap (a+x))$$
$$+ \tfrac{1}{2}w(b\cap a) + w(c\cap x\cap b) + \tfrac{1}{2}w(b\cap x) + \tfrac{1}{2}w(b\cap c)$$
$$+ \tfrac{1}{4}w(a+b) + \varphi(b,c)$$

$$\equiv \frac{1}{4}w(x) + w(b\cap x\cap a) + \tfrac{1}{2}w(x\cap a) + \tfrac{1}{4}w(a+b+x)$$
$$+ w(b\cap c\cap (a+x)) + w(c\cap x\cap b) + \tfrac{1}{2}w(b\cap x) + \tfrac{1}{4}w(a+b).$$

Son olarak,

$$\frac{1}{4}w(x) + \frac{1}{4}w(x+a+b) + \frac{1}{4}w(a+b) \equiv \frac{1}{2}w(x\cap (a+b)),$$

eşitliği nedeniyle, iddia aşağıdaki şekilde elde edilir:

$$\begin{aligned} A(a,b,c) &\equiv \frac{1}{4}w(a+b) + \frac{1}{2}w(x\cap (a+b)) + w(b\cap x\cap a) + \frac{1}{2}w(x\cap a) \\ &\quad + w(b\cap c\cap a) + w(b\cap c\cap x) + w(c\cap x\cap b) \\ &\quad + \frac{1}{2}w(b\cap x) + \frac{1}{4}w(a+b) \\ &\equiv \frac{1}{2}w(x\cap (a+b)) + w(b\cap x\cap a) + \frac{1}{2}w(x\cap a) \\ &\quad + w(b\cap c\cap a) + \frac{1}{2}w(b\cap x) \\ &\equiv w(x\cap a\cap b) + \frac{1}{2}w(x\cap a) + \frac{1}{2}w(x\cap b) + w(b\cap x\cap a) \\ &\quad + \frac{1}{2}w(x\cap a) + w(b\cap c\cap a) + \frac{1}{2}w(b\cap x) \\ &\equiv w(a\cap b\cap c). \end{aligned}$$

Durum 4: $c \in W_k$ ve $a, b \in C_k$ olsun.

(2.15) ifadesinden

$$A(a,b,c) + A(b,c,a) + A(c,a,b) \equiv w(a\cap b\cap c),$$

olduğunu hatırlayalım. Burada

$$A(b,c,a) \equiv w(a\cap b\cap c)$$

Durum 2'den ve

$$A(c,a,b) \equiv w(a\cap b\cap c)$$

Durum 3'ten gelmektedir. Dolayısıyla,

$$A(a,b,c)+A(b,c,a)+A(c,a,b) \equiv A(a,b,c)+w(a\cap b\cap c)$$
$$+w(a\cap b\cap c)\equiv w(a\cap b\cap c)$$

bu da iddia edilen eşitliği verir:

$$A(a,b,c)\equiv w(a\cap b\cap c).$$

Durum 5: $a,b\in W_k$ ve $c\in C_k$ olsun.

$x=a$, $y=a+b+c$ ve $z=c$ alındığında, $y\in C_k$ olur. Buna göre, *Durum 3*'ten

$$\begin{aligned} A(x,y,z)=A(a,a+b+c,c) &\equiv w(a\cap(a+b+c)\cap c)\\ &\equiv w(a\cap(b+c)\cap c)\\ &\equiv w(a\cap b\cap c)\end{aligned}$$

elde edilir. Öte yandan (2.14) ile de

$$\begin{aligned} A(x,y,z)&=A(a,a+b+c,c)\\ &\equiv \varphi(a,a+b+c)+\varphi(b+c,c)+\varphi(a+b+c,c)+\varphi(a,a+b)\end{aligned}$$

elde ederiz.

Daha sonra, *(D4)*'ten (2.9) kullanılarak

$$\begin{aligned} \varphi(a,a+b+c)&\equiv \varphi(a,b+c)+\frac{1}{4}w(a),\\ \varphi(b+c,c)&=\varphi(b+c,b)+\frac{1}{4}w(b+c)\\ &\equiv \varphi(b,b+c)+\frac{1}{2}w(b\cap c)+\frac{1}{4}w(b+c)\\ &\equiv \varphi(b,c)+\frac{1}{4}w(c),\\ \varphi(a,a+b)&\equiv \varphi(a,b)+\frac{1}{4}w(a)\end{aligned}$$

ve

$$\begin{aligned} \varphi(a+b+c,c)&\equiv \varphi(c,a+b+c)+\frac{1}{2}w((a+b)\cap c)\\ &\equiv \varphi(c,a+b)+\frac{1}{4}w(c)+\frac{1}{2}w((a+b)\cap c)\\ &\equiv \varphi(a+b,c)+\frac{1}{4}w(c)\end{aligned}$$

elde ederiz.

Sonuç olarak,

$$\begin{aligned} A(x,y,z) &\equiv \varphi(a,b+c)+\frac{1}{4}w(a)+\varphi(b,c)+\frac{1}{4}w(c)+\varphi(a+b,c) \\ &\quad +\frac{1}{4}w(c)+\varphi(a,b)+\frac{1}{4}w(a) \\ &\equiv A(a,b,c) \end{aligned}$$

bulunur ki, bu da iddia edilen

$$A(a,b,c) \equiv w(a \cap b \cap c)$$

eşitliğini verir.

Durum 6: $b, c \in W_k$ ve $a \in C_k$ olsun.

Durum 5'e benzer şekilde, $x = a$, $y = a+b+c$ ve $z = c$ olarak alıyoruz; böylece $y \in C_k$ olur. Bu durumda *Durum 4*'ten

$$A(x,y,z) = A(a,a+b+c,c) \equiv w(a \cap (a+b+c) \cap c) = w(a \cap b \cap c),$$

ve ardından (2.14)'den

$$\begin{aligned} A(x,y,z) &= A(a,a+b+c,c) \\ &\equiv \varphi(a,a+b+c)+\varphi(b+c,c)+\varphi(a+b+c,c)+\varphi(a,a+b) \end{aligned}$$

bulunur. Şimdi tekrar *(D4)*'ün (2.9) ifadesini kullanarak,

$$\begin{aligned} \varphi(b+c,c) &\equiv \varphi(b,c)+\frac{1}{4}w(c) \\ \varphi(a+b+c,c) &\equiv \varphi(a+b,c)+\frac{1}{4}w(c) \\ \varphi(a,a+b) &\equiv \varphi(a,b)+\frac{1}{4}w(a) \\ \varphi(a,a+b+c) &\equiv \varphi(a,b+c)+\frac{1}{4}w(a). \end{aligned}$$

Buna göre,

$$\begin{aligned} A(x,y,z) &\equiv \varphi(a,b+c)+\frac{1}{4}w(a)+\varphi(b,c)+\frac{1}{4}w(c)+\varphi(a+b,c) \\ &\quad +\frac{1}{4}w(c)+\varphi(a,b)+\frac{1}{4}w(a) \\ &\equiv A(a,b,c) \end{aligned}$$

ve böylece iddia edilen eşitlik elde edilir:

$$A(a,b,c) \equiv w(a \cap b \cap c).$$

Durum 7: $a, c \in W_k$ ve $b \in C_k$ olsun.

Burada tekrar hatırlattığımız (2.15) ifadesine göre

$$A(a,b,c) + A(b,c,a) + A(c,a,b) \equiv w(a \cap b \cap c),$$

olup, *Durum 6*'dan

$$A(b,c,a) \equiv w(a \cap b \cap c)$$

ve *Durum 5*'ten de

$$A(c,a,b) \equiv w(a \cap b \cap c)$$

eşitliği gelir. O halde,

$$\begin{aligned} A(a,b,c) + A(b,c,a) + A(c,a,b) &= A(a,b,c) + w(a \cap b \cap c) \\ &\quad + w(a \cap b \cap c) = w(a \cap b \cap c). \end{aligned}$$

Buradan da, iddia edildiği gibi,

$$A(a,b,c) \equiv w(a \cap b \cap c)$$

sonucu elde edilir. □

Bir sonraki sonuç, [3]'da bulunabileceği üzere, verilen bir iki kat çift kod üzerindeki faktör kümelerinin sayısını verir.

Teorem 2.2: $C \subset (\mathbb{F}_2)^n$ bir iki kat çift kod ve $\dim(C) = t$ olsun. O hâlde C üzerindeki farklı faktör kümelerinin sayısı $2^{2^t - t - 1}$'dir.

*İspat.*İki kat çift kod üzerindeki faktör kümesinin varlığına ilişkin Teorem 2.1 kanıtındaki stratejiyi takip edeceğiz. Daha açık ifade etmek gerekirse, $k = 1, \ldots, t$ için, bir altuzay olan C_{k-1}'den C_k'ye genişletilen faktör kümelerinin sayısını sayacağız.

Bu amaçla, x'i $C_k - C_{k-1}$'den seçilmiş bir eleman olarak alalım.

Farklı faktör kümelerinin sayısı, yapılandırmadaki her k için *(D1)*'de yapılan seçimlerden kaynaklanır. Buna göre, her $y \in C_{k-1}$ için $\varphi(x,y)$ değerleri rastgele tanımlanır; tek şart $\varphi(x,0) = 0$ olmasıdır. Bir taraftan $\dim(C_{k-1}) = k-1$ olduğundan C_{k-1} 2^{k-1}

eleman içerir; diğer taraftan $\varphi(x,0) = 0$ sabittir. Böylece, $y \neq 0$ olan her $y \in C_{k-1}$ için $\varphi(x,y)$ değerlerinde $2^{k-1}-1$ bağımsız seçim yapılabilir.

Bu seçimler $1 \leq k \leq t$ aralığında bağımsız olarak yapıldığından, toplam seçim sayısı

$$\sum_{k=1}^{t}(2^{k-1}-1)$$

şeklindedir. Bu toplam şu şekilde hesaplanabilir:

$$\begin{aligned}\sum_{k=1}^{t}(2^{k-1}-1) &= \left(\sum_{k=1}^{t}2^{k-1}\right) - \left(\sum_{k=1}^{t}1\right)\\ &= (2^0 + 2^1 + \ldots + 2^{t-1}) - t\\ &= (2^t - 1) - t.\end{aligned}$$

Böylece, farklı faktör kümelerinin toplam sayısı tam olarak 2^{2^t-t-1}'dir. □

Bir sonraki sonuç faktör kümelerinin denkliğini gösterir.

Teorem 2.3: $C \subset (\mathbb{F}_2)^n$ iki kat çift bir kod olsun. O hâlde, $\varphi, \psi : C \times C \to \mathbb{F}_2$ biçimindeki herhangi iki faktör kümesi denktir.

*İspat.*İki faktör kümesi $\varphi, \psi : C \times C \to \mathbb{F}_2$ verilsin ve

$$\zeta : C \times C \to \mathbb{F}_2, \quad \zeta(x,y) := \varphi(x,y) + \psi(x,y)$$

olarak tanımlansın. (2.7)'dan şu sonucu gözlemliyoruz:

$$\begin{aligned}&\zeta(x,y) + \zeta(x+y,z) + \zeta(y,z) + \zeta(x,y+z) =\\ &\varphi(x,y) + \psi(x,y) + \varphi(x+y,z) + \psi(x+y,z) + \varphi(y,z) +\\ &\quad \psi(y,z) + \varphi(x,y+z) + \psi(x,y+z)\\ &= \varphi(x,y) + \varphi(x+y,z) + \varphi(y,z) + \varphi(x,y+z) + \psi(x,y)\\ &\quad + \psi(x+y,z) + \psi(y,z) + \psi(x,y+z)\\ &= w(x \cap y \cap z) + w(x \cap y \cap z) = 0,\end{aligned}$$

buradan, her $x, y, z \in C$ için,

$$\begin{aligned}(\delta^2\zeta)(x,y,z) &= x \cdot \zeta(y,z) - \zeta(xy,z) + \zeta(x,yz) - \zeta(x,y)\\ &= \zeta(y,z) - \zeta(x+y,z) + \zeta(x,y+z) - \zeta(x,y) = 0\end{aligned}$$

elde edilir. Başka bir deyişle, $\zeta \in H^2(C, \mathbb{F}_2)$ olup, bu, abelyen grup $(C, +)$ üzerinde trivial C-modülü $\mathbb{F}_2$ katsayıları ile grup kohomolojisi kapsamında (mod 2) bir koçevrimdir. Bu kohomoloji, [21, Cor. 3.4]'de aşağıdaki dönüşümün kokernel'i olarak hesaplanmıştır:

$$\bigoplus_{\substack{2k+\ell+2m=n \\ k\geq 1}} Sym^k(C^\vee) \otimes Sym^\ell(C^\vee) \otimes Sym^m(C^\vee) \to \bigoplus_{i+2j=n} Sym^i(C^\vee) \otimes Sym^k(C^\vee)$$

burada $C^\vee$, dual vektör uzayını temsil etmektedir. Özellikle, $n = 2$ için, ikinci kohomoloji grubu $H^2(C, \mathbb{F}_2)$,

$$Sym^1(C^\vee) \to Sym^2(C^\vee) \otimes Sym^1(C^\vee),$$

dönüşümünün kokernelidir. Bu dönüşüm, birinci bileşende Frobenius otomorfizması ve ikinci bileşende ise birim dönüşüm olarak çalışır. Bu sonuç aslında yine [21, Cor. 3.3]'de verilen

$$W \cong Sym^1(C^\vee), \qquad H^2(C, \mathbb{F}_2)/W \cong \wedge^2 C^\vee$$

olmak üzere,

$$H^2(C, \mathbb{F}_2) \supseteq W \supseteq 0,$$

filtrasyonunun başka bir ifadesidir.

Şimdi, (2.6)'dan

$$\begin{aligned} \zeta(x,y) + \zeta(y,x) &= \varphi(x,y) + \psi(x,y) + \varphi(y,x) + \psi(y,x) \\ &= \varphi(x,y) + \varphi(y,x) + \psi(x,y) + \psi(y,x) \\ &= \frac{1}{2}w(x \cap y) + \frac{1}{2}w(x \cap y) = 0, \end{aligned}$$

olduğundan $\zeta \in \wedge^2 C^\vee$'dir. Ancak, (2.5)'e göre,

$$\zeta(x,x) = \varphi(x,x) + \psi(x,x) = \frac{1}{4}w(x) + \frac{1}{4}w(x) = 0$$

olduğu için ζ trivial olmayan bir kohomoloji sınıfını temsil edemez. Yani, bir $\alpha : C \to \mathbb{F}_2$ fonksiyonu için

$$\zeta(x,y) = (\delta\alpha)(x,y) = \alpha(x) + \alpha(x+y) + \alpha(y)$$

eşitliği her $x, y \in C$ için sağlanır.

□

Not: Aynı sonuç [22, Sect. IV]'ten

$$\dim L^1(C, \mathbb{F}_2) = 1$$

gözlemi yapılarak da elde edilebilir. Bir diğer deyişle, $\mathbb{F}_2$ ile C'nin (döngü) genişlemesi tektir.

3. BİRLEŞMELİ OLMAYAN YAPILAR

3.1. Kuasigruplar ve Döngüler

Döngülerle ilgili temel terminoloji tanıtırken [23] kaynağını takip edeceğiz. Ek olarak [1] de incelenebilir.

Tanım: $\mathcal{Q}$, üzerinde ikili işlem tanımlı boş olmayan bir küme olsun:

$$* : \mathcal{Q} \times \mathcal{Q} \to \mathcal{Q}.$$

Eğer $\mathcal{Q}$ kümesi için her $a, b \in \mathcal{Q}$ çifti verildiğinde,

$$ax = b$$

$$ya = b$$

denklemlerinin her ikisinin de $\mathcal{Q}$ içinde birer eşsiz çözümü varsa, bu durumda $\mathcal{Q}$ kümesine bir *kuasigrup* denir.

Örnek 5: p bir asal sayı ve $m, n \in \mathbb{Z}$ olmak üzere, $0 < m, n < p$ koşulunu sağlayacak şekilde seçilmiş olsun. Bu durumda,

$$r \circ s := mr + ns$$

çarpım işlemiyle tanımlanan $\mathbb{Z}_p$ kümesi bir kuasigrup olur.

Kuasigrup tanımı gereği, işlemleri birleşmeli olmak zorunda değildir. Ancak, aşağıdaki durum söz konusu olabilir.

Tanım: $(Q, \cdot)$ bir kuasigrup olmak üzere, her $a, b \in Q$ için

$$\langle a, b \rangle \subseteq Q$$

kümesi birleşmeli olduğunda *iki-birleşmeli* (di-associative) olarak adlandırılır.

Tanım: Birim elemana sahip bir kuasigrup *döngü* olarak adlandırılır.

Örnek 6: Aşağıdaki çarpım tablosu ile verilen $\mathcal{L} := \{1, 2, 3\}$ kümesi

$\cdot$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

birim elemanı $1 \in \mathcal{L}$ olan bir kuasigruptur. Dolayısıyla, $\mathcal{L}$ bir döngüdür.

Not: Örnek 5'deki kuasigrup $\mathbb{Z}_p$'nin, $m = n = 1$ olmadıkça bir döngü olmadığını belirtelim; örneğin bkz. [24, Lemma 2].

Örnek 7: C bir iki kat çift kod olmak üzere $(C, \varphi) := \mathbb{F}_2 \times C$, üzerinde tanımlı

$$(c, x) \circ (d, y) = (c + d + \varphi(x, y), x + y)$$

ikili işlemi ile bir döngüdür. Bu döngüye C'nin *kod döngüsü* adı verilir.

Bir $\mathcal{L}$ döngüsü, diğer yandan, her $a \in \mathcal{L}$ için $a^\ell \in \mathcal{L}$ olacak şekilde

$$a^\ell(ab) = b$$

eşitliğini sağlayan bir eleman varsa *sol ters özellikli (LIP) döngü* olarak adlandırılır. Benzer şekilde, bir $\mathcal{L}$ döngüsü her $a \in \mathcal{L}$ için $a^r \in \mathcal{L}$ olacak şekilde

$$(ba)a^r = b$$

eşitliğini sağlıyorsa *sağ ters özellikli (RIP) döngü* olarak adlandırılır. Son olarak, bir $\mathcal{L}$ döngüsü her $a \in \mathcal{L}$ için $a^{-1} \in \mathcal{L}$ olacak şekilde

$$a^{-1}(ab) = (ba)a^{-1} = b$$

eşitliğini sağlıyorsa, *ters özellikli (IP) döngü* olarak adlandırılır.

Şunu da ayrıca belirtelim ki, bir $\mathcal{L}$ döngüsü ve herhangi bir $a \in \mathcal{L}$ verildiğinde,

$$L_a : \mathcal{L} \to \mathcal{L}, \qquad x \mapsto ax$$

ve

$$R_a : \mathcal{L} \to \mathcal{L}, \qquad x \mapsto xa$$

gösterimleri sırasıyla *sol öteleme* ve *sağ öteleme* olarak adlandırılan birebir ve örten fonksiyonlardır. $\mathcal{L}$'nin tüm sol ve sağ ötelemeleri tarafından üretilen grup, $\mathcal{L}$'nin *çarpım grubu* olarak adlandırılır ve $Mlt(\mathcal{L})$ ile gösterilir.

Öte yandan, $x, y \in \mathcal{L}$ verildiğinde, $L_{(yx)^{-1}}L_yL_x$, $R_xR_yR_{(xy)^{-1}}$ ve $L_xR_{x^{-1}}$ biçimindeki fonksiyonlar tarafından üretilen alt döngü

$$Inn(\mathcal{L}) := \{\varphi \in Mlt(\mathcal{L}) \mid \varphi(1) = 1\}$$

$\mathcal{L}$'nin *iç dönüşüm grubu* olarak adlandırılır ve $Mlt(\mathcal{L})$'nin bir alt döngüsünü oluşturur.

L_a ve R_a, $\mathcal{L}$ kümesinin elemanları üzerinde birer permütasyondur. $Mlt(\mathcal{L})$ ise şu şekilde tanımlanan bir permütasyon grubudur:

$$Mlt(\mathcal{L}) = \langle L_a, R_a \mid a \in \mathcal{L} \rangle.$$

Örnek 8: Aşağıdaki çarpım tablosuyla tanımlanan $\mathcal{L} := \{1, 2, 3, 4, 5\}$ döngüsünü ele alalım:

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	2	3	1

$\mathcal{L}$ döngüsünün sol ötelemeleri şu şekildedir:

a	L_a
1	id
2	$(1\ 2)(3\ 4\ 5)$
3	$(1\ 3)(2\ 5\ 4)$
4	$(1\ 4)(2\ 3\ 5)$
5	$(1\ 5)(2\ 4\ 3)$

Sağ ötelemeler ise aşağıdaki gibidir:

a	R_a
1	id
2	$(1\ 2)(3\ 5\ 4)$
3	$(1\ 3)(2\ 4\ 5)$
4	$(1\ 4)(2\ 5\ 3)$
5	$(1\ 5)(2\ 3\ 4)$

Böylece, $\mathcal{L}$ döngüsünün çarpım grubu

$$Mlt(\mathcal{L}) = \langle L_a, R_a \mid a \in \mathcal{L} \rangle \cong S_5$$

şeklinde verilir.

Sol iç ötelemeler

$$L_{x,y} := L_{(yx)^{-1}} \circ L_y \circ L_x,$$

sağ iç ötelemeler

$$R_{x,y} := R_x \circ R_y \circ R_{(xy)^{-1}},$$

ve orta iç ötelemeler

$$T_x := L_x \circ R_{x^{-1}},$$

hesaplandığında

$$Inn(\mathcal{L}) \cong S_4$$

olduğu görülür.

Tanım: $\mathcal{L}$ döngüsünün bir alt döngüsü olan $\mathcal{N}$, eğer her $\varphi \in Inn(\mathcal{L})$ için

$$\varphi(\mathcal{N}) = \mathcal{N}$$

eşitliği sağlanıyorsa, *normal* olarak adlandırılır.

Tanım: $\mathcal{L}$ bir döngü olmak üzere, herhangi iki $x, y \in \mathcal{L}$ için

$$(yx)[x, y] = xy$$

eşitliğini sağlayan eşsiz $[x, y] \in \mathcal{L}$ elemanına $x, y \in \mathcal{L}$'nin *komütatörü* denir. Benzer şekilde, herhangi üç $x, y, z \in \mathcal{L}$ için

$$(x(yz))[x, y, z] = (xy)z$$

eşitliğini sağlayan eşsiz $[x, y, z] \in \mathcal{L}$ elemanına $x, y, z \in \mathcal{L}$'nin *birleşiklikçisi* denir.

Bir $\mathcal{L}$ döngüsü verildiğinde,

$$C(\mathcal{L}) := \{x \in \mathcal{L} \mid [x, y] = [y, x] = e, \text{ herhangi bir } y \in \mathcal{L} \text{ için}\}$$

kümesine $\mathcal{L}$'nin *komütantı* denir. Benzer şekilde,

$$N(\mathcal{L}) := \{x \in \mathcal{L} \mid [x, y, z] = [y, z, x] = [z, x, y] = e, \text{ herhangi bir } y, z \in \mathcal{L} \text{ için}\}$$

kümesine $\mathcal{L}$'nin *çekirdeği* denir.

Ayrıca $Z(\mathcal{L}) := C(\mathcal{L}) \cap N(\mathcal{L})$ kümesine $\mathcal{L}$'nin *merkezi* denir.

Önerme 3.1: Bir $\mathcal{L}$ döngüsünün merkezi $Z(\mathcal{L})$, her $U \in Inn(\mathcal{L})$ için $U(a) = a$ olacak şekilde $\mathcal{L}$ içinde alınan tüm a öğelerinden oluşan küme olarak verilebilir.

Tersine, eğer her $U \in Inn(\mathcal{L})$ için $U(a) = a$ sağlanıyorsa,

$$T(ax) = aT(x)$$

her $x \in \mathcal{L}$ ve her $T \in Mlt(\mathcal{L})$ için geçerlidir.

*İspat.*Önce ikinci ifadeyi ispatlayalım. $\mathcal{L}$ içinde a, x, y elemanları alalım ve $U(a) = a$ olsun, burada $U \in Inn(\mathcal{L})$. O zaman,

$$R_y(ax) = (ax)y = ((x^{-1}(ax))x)y = R_x R_y(x^{-1}(ax)) = R_x R_y(a).$$

Ayrıca, $Inn(\mathcal{L})$ kümesi $R_{xy}^{-1} R_x R_y$ tarafından üretildiğinden $R_{xy}^{-1} R_x R_y(a) = a$ olur. Buna göre,

$$R_x R_y(a) = R_{xy}(a) = a(xy) = a.R_y(x)$$

ya da

$$R_{y^{-1}}(ax) = R_{y^{-1}}(R_y(a.R_{y^{-1}})) = a.R_{y^{-1}}(x).$$

Benzer şekilde,

$$L_y(ax) = aL_y(x)$$

ve

$$L_{y^{-1}}(ax) = a.L_{y^{-1}}(x).$$

Bu durumda, iddia $Mlt(\mathcal{L})$ kümesinin R_y, L_y ötelemeleri tarafından üretilmesinden dolayı sağlanır.

Şimdi birinci ifadeye bakalım. İlk adımdan şunu elde ederiz:

$$R_y(xa) = (xa)y = (x(yay^{-1})y) = ((x(yay^{-1})x^{-1})x)y = (ax)y.$$

Bundan dolayı, $ax = xa$ her $x \in \mathcal{L}$ için sağlanır ve bu bazı $Inn(\mathcal{L})$ permütasyonları için geçerlidir. Ayrıca aşağıdaki denklemler

$$(ax)y = a(xy), \quad (xa)y = x(ay), \quad (xy)a = x(ya) \tag{3.1}$$

her $x, y \in \mathcal{L}$ için geçerlidir. İkinci ifade ve $ax = xa$ eşitliği sayesinde her iki taraf da $a(xy)$ ile değiştirilebilir. O hâlde (3.1) ifadesi $a \in Z(\mathcal{L})$ sonucunu verir.

Tersine, eğer $a \in \mathcal{L}$ her $x \in \mathcal{L}$ için $ax = xa$ eşitliğini sağlıyorsa, 3.1 ifadesinin ilk denkleminden şunu elde ederiz:

$$\begin{aligned} (ax)y = a(xy) &\implies R_y R_x(a) = R_{xy}(a) \\ &\implies R_{(xy)}^{-1} R_y R_x(a) = a. \end{aligned}$$

Benzer şekilde, 3.1 ifadesinin ikinci denkleminden şunu elde ederiz:

$$\begin{aligned} x(ay) = a(xy) &\implies R_y L_x(a) = R_{xy}(a) \\ &\implies R_{(xy)}^{-1} R_y L_x(a) = a. \end{aligned}$$

Öte yandan, $Inn(\mathcal{L})$ kümesi $R_xR_yR_{(xy)}^{-1}$ ve $R_yL_xR_{(xy)}^{-1}$ tarafından üretildiğinden, her $U \in Inn(\mathcal{L})$ için $U(a) = a$ elde edilir. □

Bir sonraki sonuç, [1] kaynağından alınmış olup, bir döngünün merkezinin her zaman normal bir alt döngü olduğunu gösterir.

Önerme 3.2: Bir $\mathcal{L}$ döngüsü verildiğinde, $Z(\mathcal{L})$ merkezi $\mathcal{L}$'nin normal bir alt döngüsüdür.

*İspat.*Öncelikle $Z(\mathcal{L})$'nin $\mathcal{L}$ içinde bir alt grup olduğunu göstereceğiz. Bunun için, a, b $Z(\mathcal{L})$'nin herhangi iki elemanı olsun. O hâlde, Önerme 3.1'ye göre

$$U(ab) = aU(b) = ab$$

her $U \in Inn(\mathcal{L})$ için geçerlidir, bu da $Inn(\mathcal{L})(ab) = ab$ anlamına gelir. Öte yandan, eğer

$$ax = b = Inn(\mathcal{L})(b) = Inn(\mathcal{L})(ax) = aInn(\mathcal{L})(x)$$

ise, $x = Inn(\mathcal{L})(x) \in Z(\mathcal{L})$ olur. $ax = xa$ olduğundan, $Z(\mathcal{L})$'nin hem değişmeli bir grup hem de $\mathcal{L}$'nin bir alt döngüsü olduğu sonucuna varırız. □

Tanım: Bir $\mathcal{L}$ döngüsü verildiğinde, $\mathcal{L}/\mathcal{L}^*$ ifadesinin birleşmeli olacağı şekilde $\mathcal{L}$ içinde bulunan en küçük normal alt döngü $\mathcal{L}^*$'a *çekirdekten türetilmiş alt döngü* denir.

Aşağıdaki sonuç, bir döngünün çekirdeksel türetilmiş alt döngüsü kavramının iyi tanımlı olduğunu garanti eder, bkz. [9].

Önerme 3.3: Herhangi bir $\mathcal{L}$ döngüsü verildiğinde, çekirdeksel türetilmiş alt döngü $\mathcal{L}^* \subseteq \mathcal{L}$ iyi tanımlıdır.

İspat.$\mathcal{L}^*$'nin, birleşmeli bir bölüm halkasına sahip en küçük normal alt döngü olarak varlığını ve tekilliğini göstereceğiz. Bunun için, birleşmeli bölüm döngüsü $\mathcal{L}/N$ olan tüm normal alt döngülerin kümesi olan

$$\mathcal{S} := \{N \trianglelefteq \mathcal{L} \mid \mathcal{L}/N \text{ birleşmeli}\}$$

kümelerini tanımlayalım.

$\mathcal{L}$ kendisinin normal bir alt döngüsü olduğundan ve $\mathcal{L}/\mathcal{L}$ bariz olarak birleşmeli olduğundan dolayı, $\mathcal{L} \in \mathcal{S}$'dir. Yani, $\mathcal{S}$ boş değildir.

Sonra

$$\mathcal{L}^* := \bigcap_{N \in \mathcal{S}} N$$

kesişimini tanımlayalım. [1, Thm. I.7.6] ve [25, Thm. IV.1.2]'a göre, $\mathcal{L}$ döngüsünün herhangi bir boş olmayan normal alt döngü koleksiyonunun kesişimi yine normal bir alt döngüdür. Dolayısıyla, $\mathcal{L}^*$ $\mathcal{L}$'nin normal bir alt döngüsüdür.

Şimdi, $\mathcal{L}/\mathcal{L}^*$'nin birleşmeli olduğunu göstermemiz gerekiyor. Bunun için, birleşiklikçi

$$[x, y, z] := (x(yz))^{-1}((xy)z)$$

elemanının her $x, y, z \in \mathcal{L}$ için $\mathcal{L}^*$ içinde olduğunu göstermek yeterlidir. Her $N \in \mathcal{S}$ için, tanıma göre $\mathcal{L}/N$ birleşmelidir. Bu yüzden, birleşiklikçi $[x, y, z]$ her x, y, z için N içinde yer alır. Bu, tüm $N \in \mathcal{S}$ için geçerli olduğundan

$$[x, y, z] \in \bigcap_{N \in \mathcal{S}} N = \mathcal{L}^*$$

sonucu çıkar. Yani, $\mathcal{L}/\mathcal{L}^*$ birleşmelidir.

Son olarak, tanımından dolayı $\mathcal{L}^*$ her $N \in \mathcal{S}$ içinde yer alır. Böylece, $\mathcal{L}^*$'nin böyle bir normal alt döngülerin en küçüğü olduğu kanıtlanmış olur. □

Tanım: Bir $\mathcal{L}$ döngüsü verildiğinde, $\mathcal{L}$'nin *merkezi türetilmiş alt döngüsü*, $\mathcal{L}'$ ile gösterilir ve $\mathcal{L}/\mathcal{L}'$ bölüm döngüsünün abelyen bir grup olması koşulunu sağlayan en küçük normal alt döngü olarak tanımlanır.

Önerme 3.4: Herhangi bir $\mathcal{L}$ döngüsü verildiğinde, merkezi türetilmiş alt döngü $\mathcal{L}' \subseteq \mathcal{L}$ iyi tanımlıdır.

*İspat.*Önceki önermenin ispatına uygun olarak, $\mathcal{L}/N$ bölümü bir değişmeli grup olacak şekilde $\mathcal{L}$'nin tüm normal alt döngülerinden oluşan $\mathcal{A}$ kümesini tanımlayalım. $\mathcal{L}/\mathcal{L}$ değişmeli olduğundan, döngünün kendisi $\mathcal{L}$ aşikar olarak $\mathcal{A}$ kümesine aittir. Bu nedenle, $\mathcal{A}$ boş değildir.

Şimdi

$$\mathcal{L}' = \bigcap_{N \in \mathcal{A}} N$$

olarak tanımlayalım. Boş olmayan bir normal alt döngü koleksiyonunun kesişimi olduğundan, [1, Thm. I.7.6] ve [25, Thm. IV.1.2] uyarınca $\mathcal{L}'$ de $\mathcal{L}$'nin bir normal alt döngüsüdür.

Şimdi $\mathcal{L}/\mathcal{L}'$ bölümünün bir abel grup olduğunu gösterelim. Birleşmeli olma için herhangi bir $N \in \mathcal{A}$ seçelim. $\mathcal{L}/N$ abel olduğundan birleşmelidir, dolayısıyla $\mathcal{L}$'nin tüm $[x, y, z]$ birleşiklikçileri N içinde yer almalıdır. Bu durum tüm $N \in \mathcal{A}$ için geçerli olduğundan, tüm birleşiklikçiler $\mathcal{L}' = \bigcap_{N\in\mathcal{A}} N$ kümesinde bulunur. Bu da $\mathcal{L}/\mathcal{L}'$'nin birleşmeli olduğunu gösterir.

Değişmeli olma ise benzer şekilde gösterilir. Herhangi bir $N \in \mathcal{A}$ için, $\mathcal{L}/N$ abel olduğundan, $\mathcal{L}$'nin tüm komütatörleri N içinde yer almalıdır. Bu tüm $N \in \mathcal{A}$ için geçerli olduğundan, tüm komütatörler $\mathcal{L}'$'de bulunur. Dolayısıyla, $\mathcal{L}/\mathcal{L}'$ değişmelidir. Yani, $\mathcal{L}/\mathcal{L}'$ bir abel gruptur.

Son olarak, $\mathcal{L}'$ her $N \in \mathcal{A}$ içinde yer aldığından, bu özelliği sağlayan en küçük normal alt döngüdür. Bu da hem varlığını hem de tekliğini garanti eder. □

Aşağıdaki tanım, ve takip eden sonuç [9] kaynağından alıntılanmıştır.
Tanım: Herhangi bir p asal sayısı için, $\mathcal{L}_p$, $\mathcal{L}$ içindeki, mertebesi p asalının bir kuvveti olan tüm x elemanlarının kümesi olarak tanımlanır.
Teorem 3.1: $\mathcal{L}_p$, $\mathcal{L}$'nin bir alt döngüsüdür.

İspat. $\gamma, \delta \in \mathcal{L}_p$ olsun ve γ ile δ'nın mertebelerinden büyük olanı q ile gösterilsin. Dibirleşmelilik özelliği ile χ fonksiyonunun tanımı kullanıldığında, aşağıdaki ifadeler elde edilir:

$q = 2$ için, $(\gamma\delta)^2 = (\gamma\delta)(\gamma\delta) = \gamma((\gamma\delta)\chi(d,c))\delta = \gamma^2\delta^2\chi(d,c)$

$$\begin{aligned} q = 3 \text{ için, } (\gamma\delta)^3 &= (\gamma\delta)(\gamma\delta)(\gamma\delta) = \gamma((\gamma\delta)\chi(d,c))\delta\gamma\delta = \gamma^2\delta^2\gamma\delta\chi(d,c) \\ &= \gamma^2((\gamma\delta^2)\chi(d^2,c))\delta\chi(d,c) = \gamma^3\delta^3\chi(d,c)^2\chi(d,c) = \gamma^3\delta^3\chi(d,c)^3 \end{aligned}$$

$$\begin{aligned} q = 4 \text{ için, } (\gamma\delta)^4 &= (\gamma\delta)(\gamma\delta)(\gamma\delta)(\gamma\delta) = \gamma((\gamma\delta)\chi(d,c))\delta\gamma\delta\gamma\delta = \gamma^2\delta^2\gamma\delta\gamma\delta\chi(d,c) \\ &= \gamma^2((\gamma\delta^2)\chi(d^2,c))\delta\gamma\delta\chi(d,c) = \gamma^3\delta^3\gamma\delta\chi(d,c)^3 \\ &= \gamma^3((\gamma\delta^3)\chi(d^3,c))\delta\chi(d,c)^3 = \gamma^4\delta^4\chi(d,c)^6 \end{aligned}$$

Genel formda,

$$(\gamma\delta)^q = \gamma^q\delta^q\chi(d,c)^{\left(\frac{q(q-1)}{2}\right)} = \chi(d,c)^{\left(\frac{q(q-1)}{2}\right)} = \chi(d^{\left(\frac{q(q-1)}{2}\right)},c) = \chi(1,c) = 1$$

olup, q bir p asalının kuvveti olduğundan $\gamma\delta \in \mathcal{L}_p$'dir. □

3.2. Moufang Döngüleri

Gruplarla yakın ilişki içinde olan ve oldukça iyi çalışılmış bir döngü sınıfı, ilk olarak R. Moufang tarafından 1935 yılında incelenen Moufang döngüleridir [26]

Tanım: Bir $\mathcal{L}$ döngüsü, eğer her $x, y, z \in \mathcal{L}$ için aşağıdaki *Moufang özdeşliği*

$$(xy)(zx) = (x(yz))x \tag{3.2}$$

sağlanıyorsa, *Moufang döngüsü* olarak adlandırılır.

Not: (3.2)'deki Moufang özdeşliğinin aşağıdaki özdeşliklerden her biriyle denk olduğunu not edelim:

$$x(y(xz)) = ((xy)x)z, \tag{3.3}$$

$$y(x(zx)) = ((yx)z)x, \tag{3.4}$$

$$(xy)(zx) = x((yz)x). \tag{3.5}$$

Aşağıdaki sonuç, Moufang döngüsünün tanımından oldukça açık bir şekilde çıkarılabilir, bkz. örneğin [1].

Önerme 3.5: Her Moufang döngüsü iki-birleşmelidir (di-associative).

Bir Moufang döngüsünde birleşiklikçinin teknik özelliklerini elde etmek amacıyla aşağıdaki sonuçları vereceğiz.

İlk olarak [25, Lemma VII.5.4]'te yer alan bir sonucu alıntılayalım.

Lemma 3.2: Bir $\mathcal{M}$ Moufang döngüsü verildiğinde, her $\gamma, \delta, \epsilon \in \mathcal{M}$ için aşağıdakiler sağlanır.

$$R_{\gamma^{-1},\delta^{-1}} = L_{\gamma,\delta} = L^{-1}_{\delta,\gamma}, \tag{3.6}$$

$$L_{\gamma,\delta} = L_{\gamma\delta,\delta}, \qquad L_{\gamma,\delta} = L_{\gamma,\delta\gamma}, \tag{3.7}$$

$$L_{\gamma^{-1},\delta^{-1}} \circ L_{\gamma^{-1},\delta} = L_{[\gamma,\delta],\delta}, \tag{3.8}$$

$$L_{\epsilon,\delta}(\gamma) = \gamma[\gamma, \delta, \epsilon]^{-1}, \tag{3.9}$$

$$[\gamma, \delta, \epsilon] = [\gamma, \delta\epsilon, \epsilon] = [\gamma, \delta, \epsilon\delta], \tag{3.10}$$

$$[\gamma, \delta, \epsilon] = [\gamma\delta, \epsilon, \delta]^{-1}, \tag{3.11}$$

$$[\gamma, \delta, \epsilon] = [\gamma, \delta, \epsilon\gamma], \tag{3.12}$$

$$[\delta(\gamma[\gamma, \delta, \epsilon]^{-1}]) = (\delta\gamma)[\delta, \gamma, \epsilon]. \tag{3.13}$$

Aşağıdaki sonuç, Moufang döngüsünde birleşiklikçisi aşikar olan elemanlarla ilgilidir, bkz. [1].

Lemma 3.3: Bir $\mathcal{M}$ Moufang döngüsü ve $\gamma, \delta, \epsilon \in \mathcal{M}$ verildiğinde

$$[\gamma, \delta, \epsilon] = 1.$$

eşitliği, birleşiklikçinin argümanlarının herhangi bir permütasyonu için ya da argümanlardan birinin tersi ile değiştirilmesi durumunda da geçerliliğini korur.

Moufang döngüsünün birleşiklikçisiyle ilgili olarak, son olarak [1] kaynağından aşağıdaki ifadeyi not ediyoruz.

Lemma 3.4: $\mathcal{M}$ bir Moufang döngüsü ve $\gamma, \delta, \epsilon, \lambda \in \mathcal{M}$ olsun. Eğer

$$[x, y, z] = 1$$

eşitliği $\{\gamma, \delta, \epsilon, \lambda\}$ kümesinden seçilen herhangi üç farklı x, y, z elemanı için sağlanıyorsa, aşağıdaki ifadeler birbirine denktir.

$$[\gamma\delta, \epsilon, \lambda] = 1$$
$$[(\gamma\delta)^2, \epsilon, \lambda] = 1$$
$$[[\gamma, \delta], \epsilon, \lambda] = 1$$
$$[\epsilon\lambda, \gamma, \delta] = 1$$
$$[\delta\epsilon, \lambda, \gamma] = 1$$

Şimdi de bu sonuçları kullanarak bir Moufang döngüsü içerisindeki birleşiklikçilerin bazı başka özelliklerini gözlemleyelim.

Önerme 3.6: Bir Moufang döngüsü $\mathcal{M}$ ve $\gamma, \delta, \epsilon \in \mathcal{M}$ verildiğinde, aşağıdaki eşitliklerin ya hepsi sağlanır ya da hiçbiri sağlanmaz.

$$[[\gamma, \delta, \epsilon], \gamma] = 1 \tag{3.14}$$
$$[\gamma, \delta, [\delta, \epsilon]] = 1 \tag{3.15}$$
$$[\gamma, \delta, \epsilon]^{-1} = [\gamma^{-1}, \delta, \epsilon] \tag{3.16}$$
$$[\gamma, \delta, \epsilon]^{-1} = [\gamma^{-1}, \delta^{-1}, \epsilon^{-1}] \tag{3.17}$$
$$[\gamma, \delta, \epsilon] = [\gamma, \epsilon\delta, \epsilon] \tag{3.18}$$
$$[\gamma, \delta, \epsilon] = [\gamma, \epsilon, \delta^{-1}] \tag{3.19}$$
$$[\gamma, \delta, \epsilon] = [\gamma, \gamma\delta, \epsilon] \tag{3.20}$$

Eğer (3.14) - (3.20) ifadelerinin tümü, tüm $\gamma, \delta, \epsilon \in \mathcal{M}$ için sağlanıyorsa, o zaman $[\gamma, \delta, \epsilon] \in \mathcal{M}$, $\langle \gamma, \delta, \epsilon \rangle \subseteq \mathcal{M}$ içinde merkezde yer alır ve aşağıdaki ifadeler her $n \in \mathbb{Z}$ için geçerlidir.

$$[\gamma, \delta, \epsilon] = [\delta, \epsilon, \gamma] = [\delta, \gamma, \epsilon]^{-1} \tag{3.21}$$

$$[\gamma^n, \delta, \epsilon] = [\gamma, \delta, \epsilon]^n \tag{3.22}$$

$$[\gamma\delta, \epsilon] = [\gamma, \epsilon][[\gamma, \epsilon], \delta][\delta, \epsilon][\gamma, \delta, \epsilon]^3 \tag{3.23}$$

İspat. $\mathcal{M}$ bir Moufang döngüsü olsun. [25, (VII.5.16)] kaynağına göre, her $\gamma, \delta, \epsilon \in \mathcal{L}$ için

$$\theta_{\delta,\epsilon} : w \to w[w, \delta, \epsilon]^{-1}$$

şeklindeki dönüşüm bir sözde-otomorfizmadır ve [25, (VII.3.2)] uyarınca yarı-endomorfizma gibi davranır. Buna göre, [25, (VII.4.1)] dikkate alındığında

$$\theta_{\delta,\epsilon}(\gamma^n) = (\theta_{\delta,\epsilon}(\gamma))^n,$$

yani

$$\gamma^n[\gamma^n, \delta, \epsilon]^{-1} = (\gamma[\gamma, \delta, \epsilon]^{-1})^n \tag{3.24}$$

her $n \in \mathbb{Z}$ için geçerlidir.

Öncelikle, (3.14) ifadesinin (3.16) ifadesine denk olduğunu ve (3.22) ifadesinin (3.14) den elde edildiğini göstereceğiz.

Bu amaçla, $n = -1$ için (3.24) ifadesini ele alalım, yani

$$\gamma^{-1}[\gamma^{-1}, \delta, \epsilon]^{-1} = (\gamma[\gamma, \delta, \epsilon]^{-1})^{-1}.$$

Ters eleman özelliğini kullanarak sağ tarafı şu şekilde sadeleştiririz:

$$([\gamma, \delta, \epsilon]^{-1})^{-1}\gamma^{-1} = [\gamma, \delta, \epsilon]\gamma^{-1}.$$

Böylece,

$$\gamma^{-1}[\gamma^{-1}, \delta, \epsilon]^{-1} = [\gamma, \delta, \epsilon]\gamma^{-1},$$

bu da şu sonucu verir:

$$[\gamma^{-1}, \delta, \epsilon]^{-1} = \gamma[\gamma, \delta, \epsilon]\gamma^{-1}. \tag{3.25}$$

Öte yandan, eğer (3.14) sağlanıyorsa

$$\gamma[\gamma, \delta, \epsilon]\gamma^{-1} = [\gamma, \delta, \epsilon]$$

olur. Bu durumda denklem

$$[\gamma^{-1}, \delta, \epsilon]^{-1} = [\gamma, \delta, \epsilon]$$

şeklini alır, bu da şu ifadeye denktir:

$$[\gamma, \delta, \epsilon]^{-1} = [\gamma^{-1}, \delta, \epsilon].$$

Başka bir deyişle, (3.16) sağlanır.

Tersine, eğer (3.16) sağlanıyorsa

$$[\gamma, \delta, \epsilon] = [\gamma^{-1}, \delta, \epsilon]^{-1}$$

olur ve bu ifadeyi (3.25) denklemine yerine koyarsak

$$[\gamma, \delta, \epsilon] = \gamma[\gamma, \delta, \epsilon]\gamma^{-1}$$

elde edilir. Bu da $[\gamma, \delta, \epsilon]$ ifadesinin γ ile değişmeli olduğunu gösterir. Buna göre, (3.14) ve (3.16) birbirine denktir.

Şimdi (3.14)'in sağlandığını, yani $[\gamma, \delta, \epsilon]$ ifadesinin γ ile değişmeli olduğunu varsayalım. Bu durumda, aynı ifade γ^n ile de değişmelidir. O hâlde, (3.24) özdeşliği şu şekle dönüşür:

$$\gamma^n[\gamma^n, \delta, \epsilon]^{-1} = (\gamma[\gamma, \delta, \epsilon]^{-1})^n = \gamma^n([\gamma, \delta, \epsilon]^{-1})^n = \gamma^n[\gamma, \delta, \epsilon]^{-n}.$$

Terimleri karşılaştırdığımızda

$$[\gamma^n, \delta, \epsilon]^{-1} = [\gamma, \delta, \epsilon]^{-n}$$

elde edilir ki bu da (3.22)'yi verir.

Şimdi (3.15) ifadesine geçelim; bu ifade $[\gamma, \delta, [\delta, \epsilon]] = 1$ olduğunu belirtmektedir. $C := [\delta, \epsilon]$ şeklinde tanımlayarak (3.15) ifadesini $[\gamma, \delta, C] = 1$ biçiminde yeniden yazabiliriz. Bu durumda, (3.9)'dan elde edilen

$$L_{C,\delta}(\gamma) = \gamma[\gamma, \delta, C]^{-1}$$

özdeşliği, (3.15)'den gelen $[\gamma, \delta, C]^{-1} = 1$ sonucu sayesinde

$$L_{C,\delta}(\gamma) = \gamma 1^{-1} = \gamma$$

biçiminde sadeleşir. Diğer bir deyişle, $L_{[\delta,\epsilon],\delta}$ özdeşlik dönüşümü olur. Öte yandan, (3.8) ifadesinden de

$$L_{\delta^{-1},\epsilon^{-1}} L_{\delta^{-1},\epsilon} = L_{[\delta,\epsilon],\epsilon}$$

eşitliği bilinir.

Şimdi (3.7), (3.8) ve (3.9) ifadelerini kullanarak $L_{[\delta,\epsilon],\delta} = I$ eşitliğinden $L_{[\delta,\epsilon],\epsilon} = I$ sonucuna ulaşabiliriz; bu konuda ayrıca bkz. [25, Lemma 5.4 & Lemma 5.5]. Buna göre,

$$L_{\delta^{-1},\epsilon^{-1}} L_{\delta^{-1},\epsilon} = I \implies L_{\delta^{-1},\epsilon^{-1}} = L^{-1}_{\delta^{-1},\epsilon},$$

ki bu da (3.6) ifadesi aracılığıyla şu sonucu verir:

$$L^{-1}_{\delta^{-1},\epsilon} = L_{\epsilon,\delta^{-1}} \implies L_{\delta^{-1},\epsilon^{-1}} = L_{\epsilon,\delta^{-1}}.$$

Şimdi $\delta^{-1} = \epsilon$ olarak alırsak,

$$L_{\epsilon,\delta} = L_{\delta^{-1},\epsilon}$$

eşitliği geçerlidir. Buna göre, (3.9) ifadesi kullanılarak,

$$L_{\epsilon,\delta}(\gamma) = \gamma[\gamma,\delta,\epsilon]^{-1}$$

ve

$$L_{\delta^{-1},\epsilon}(\gamma) = \gamma[\gamma,\epsilon,\delta^{-1}]^{-1}$$

elde edilir. Buna bağlı olarak,

$$\begin{aligned} \gamma[\gamma,\delta,\epsilon]^{-1} &= \gamma[\gamma,\epsilon,\delta^{-1}]^{-1} \\ \implies [\gamma,\delta,\epsilon]^{-1} &= [\gamma,\epsilon,\delta^{-1}]^{-1} \\ \implies [\gamma,\delta,\epsilon] &= [\gamma,\epsilon,\delta^{-1}]. \end{aligned}$$

Yani, (3.15) ifadesi (3.19) ile denktir. Bu durumda,

$$\begin{aligned} [\gamma,\delta,\epsilon] &\overset{3.11}{=} [\gamma\delta,\epsilon,\delta]^{-1} \overset{3.16}{=} [\delta^{-1}\gamma^{-1},\epsilon,\delta] \\ &\overset{3.10}{=} [\delta^{-1}\gamma^{-1},\epsilon,\gamma^{-1}] \overset{3.11}{=} [\delta^{-1},\gamma^{-1},\epsilon]^{-1} \end{aligned} \tag{3.26}$$

ve

$$\begin{aligned} [\gamma,\delta,\epsilon] &\overset{3.11}{=} [\gamma\delta,\epsilon,\delta]^{-1} \overset{3.26}{=} [\epsilon^{-1},\delta^{-1}\gamma^{-1},\delta] \overset{3.10}{=} [\epsilon^{-1},\delta^{-1}\gamma^{-1},\gamma^{-1}] \\ &\overset{3.10}{=} [\epsilon^{-1},\delta^{-1},\gamma^{-1}] \overset{3.26}{=} [\delta,\epsilon,\gamma^{-1}]^{-1}. \end{aligned} \tag{3.27}$$

(3.27) ifadesinin $[\gamma, \delta, \epsilon]$ üzerine tekrarlı uygulanması, aşağıdaki yolla (3.17) ifadesini verir:

$$[\gamma, \delta, \epsilon] \overset{3.27}{=} [\delta, \epsilon, \gamma^{-1}]^{-1} \overset{3.27}{=} [\epsilon, \gamma^{-1}, \delta^{-1}] \overset{3.27}{=} [\gamma^{-1}, \delta^{-1}, \epsilon^{-1}]^{-1}.$$

Sonrasında, (3.17) kullanılarak (3.18) aşağıdaki şekilde elde edilir:

$$[\gamma, \epsilon\delta, \epsilon] \overset{3.17}{=} [\gamma^{-1}, \delta^{-1}\epsilon^{-1}, \epsilon^{-1}]^{-1} \overset{3.10}{=} [\gamma^{-1}, \delta^{-1}, \epsilon^{-1}]^{-1} \overset{3.17}{=} [\gamma, \delta, \epsilon].$$

(3.18) ifadesi göz önünde bulundurulduğunda, aşağıdaki eşitlik elde edilir:

$$\begin{aligned}
[\gamma, \epsilon, \delta^{-1}] \overset{3.18}{=} [\gamma, \delta^{-1}\epsilon, \delta^{-1}] &\overset{3.26}{=} [\epsilon^{-1}\delta, \gamma^{-1}, \delta^{-1}]^{-1} \\
&\overset{3.12}{=} [\epsilon^{-1}\delta, \gamma^{-1}, \epsilon^{-1}\delta\delta^{-1}]^{-1} = [\epsilon^{-1}\delta, \gamma^{-1}, \epsilon^{-1}]^{-1} \\
&\overset{3.26}{=} [\gamma, \delta^{-1}\epsilon, \epsilon^{-1}] \overset{3.10}{=} [\gamma, \delta^{-1}\epsilon\epsilon^{-1}, \epsilon^{-1}] = [\gamma, \delta^{-1}, \epsilon^{-1}] \\
&\overset{3.17}{=} [\gamma^{-1}, \delta, \epsilon]^{-1} \overset{3.16}{=} [\gamma, \delta, \epsilon],
\end{aligned}$$

yani (3.19) doğrulanmış olur.

Benzer şekilde, (3.20) ifadesi (3.19) ifadesinden şu şekilde elde edilir:

$$\begin{aligned}
[\gamma, \gamma\delta, \epsilon] \overset{3.19}{=} [\gamma, \epsilon, \delta^{-1}\gamma^{-1}] &\overset{3.12}{=} [\gamma, \epsilon, \delta^{-1}\gamma^{-1}\gamma] \\
&= [\gamma, \epsilon, \delta^{-1}] \\
&\overset{3.19}{=} [\gamma, \delta, \epsilon].
\end{aligned}$$

Şimdi (3.20) ifadesini kullanarak

$$\begin{aligned}
[\gamma, \delta, \epsilon] &\overset{(3.16)}{=} [\gamma^{-1}, \delta, \epsilon]^{-1} \overset{(3.20)}{=} [\gamma^{-1}, \gamma^{-1}\delta, \epsilon]^{-1} \\
&\overset{3.16}{=} [\gamma, \gamma^{-1}\delta, \epsilon] \overset{(3.11)}{=} [\gamma\gamma^{-1}\delta, \epsilon, \gamma^{-1}\delta]^{-1} = [\delta, \epsilon, \gamma^{-1}\delta]^{-1} \\
&\overset{(3.16)}{=} [\delta^{-1}, \epsilon, \gamma^{-1}\delta] \overset{(3.12)}{=} [\delta^{-1}, \epsilon, \gamma^{-1}\delta\delta^{-1}] = [\delta^{-1}, \epsilon, \gamma^{-1}] \\
&\overset{(3.20)}{=} [\delta^{-1}, \delta^{-1}\epsilon, \gamma^{-1}] \overset{(3.16)}{=} [\delta, \delta^{-1}\epsilon, \gamma^{-1}]^{-1} \overset{(3.11)}{=} [\delta\delta^{-1}\epsilon, \gamma^{-1}, \delta^{-1}\epsilon] \\
&= [\epsilon, \gamma^{-1}, \delta^{-1}\epsilon] \overset{(3.16)}{=} [\epsilon^{-1}, \gamma^{-1}, \delta^{-1}\epsilon]^{-1} \overset{(3.12)}{=} [\epsilon^{-1}, \gamma^{-1}, \delta^{-1}\epsilon\epsilon^{-1}]^{-1} \\
&= [\epsilon^{-1}, \gamma^{-1}, \delta^{-1}] \overset{(3.20)}{=} [\epsilon^{-1}, \epsilon^{-1}\gamma^{-1}, \delta^{-1}] \overset{(3.16)}{=} [\epsilon, \epsilon^{-1}\gamma^{-1}, \delta^{-1}]^{-1} \\
&\overset{(3.11)}{=} [\epsilon\epsilon^{-1}\gamma^{-1}, \delta^{-1}, \epsilon^{-1}\gamma^{-1}] = [\gamma^{-1}, \delta^{-1}, \epsilon^{-1}\gamma^{-1}] \overset{(3.16)}{=} [\gamma, \delta^{-1}, \epsilon^{-1}\gamma^{-1}] \\
&\overset{(3.12)}{=} [\gamma, \delta^{-1}, \epsilon^{-1}\gamma^{-1}\gamma] = [\gamma, \delta^{-1}, \epsilon^{-1}] \overset{(3.16)}{=} [\gamma^{-1}, \delta^{-1}, \epsilon^{-1}]^{-1},
\end{aligned}$$

yani (3.17), ve dolayısıyla (3.19) eşitliğini elde ederiz.

Öte yandan, (3.17) ve (3.19) ifadeleri göz önüne alındığında,

$$[\gamma,\delta,\epsilon]^{-1} \overset{(3.17)}{=} [\gamma^{-1},\delta^{-1},\epsilon^{-1}] \overset{(3.19)}{=} [\gamma^{-1},\epsilon^{-1},\delta] \overset{(3.19)}{=} [\gamma^{-1},\delta,\epsilon]$$

elde edilir ve böylece (3.16) sonucu elde edilir.

Sonuç olarak, bu yedi özdeşliğin hepsi birbirine denktir ve bunlar (3.22) ifadesini sağlar.

Sonraki adımda, (3.16) ifadesinden şu sonuç elde edilir:

$$\begin{aligned}
[\gamma,\delta,\epsilon] &\overset{(3.16)}{=} [\gamma^{-1},\delta,\epsilon]^{-1} \overset{(3.11)}{=} [\gamma^{-1}\delta,\epsilon,\delta] \\
&\overset{(3.16)}{=} [\delta^{-1}\gamma,\epsilon,\delta]^{-1} \\
&\overset{(3.12)}{=} [\delta^{-1}\gamma,\epsilon,\delta\delta^{-1}\gamma]^{-1} \\
&= [\delta^{-1}\gamma,\epsilon,\gamma]^{-1} \\
&\overset{(3.11)}{=} [\delta^{-1},\gamma,\epsilon] \\
&\overset{(3.16)}{=} [\delta,\gamma,\epsilon]^{-1},
\end{aligned} \tag{3.28}$$

ve ardından (3.19) ifadesinden şu sonuç elde edilir:

$$\begin{aligned}
[\gamma,\delta,\epsilon] &\overset{(3.19)}{=} [\gamma,\epsilon,\delta^{-1}] \overset{3.28}{=} [\epsilon,\gamma,\delta^{-1}]^{-1} \\
&\overset{(3.27)}{=} [\gamma,\delta^{-1},\epsilon^{-1}] \\
&\overset{(3.27)}{=} [\delta^{-1},\epsilon^{-1},\gamma^{-1}]^{-1} \\
&\overset{(3.17)}{=} [\delta,\epsilon,\gamma].
\end{aligned} \tag{3.29}$$

Böylece (3.28) ve (3.29) ifadelerinden (3.21) sonucunu elde ederiz.

Şimdi (3.13) ifadesini ele alalım; bu ifade şu şekilde yazılabilir:

$$\delta(\gamma[\gamma,\delta,\epsilon]^{-1}) = (\delta\gamma)[\delta,\gamma,\epsilon].$$

Bu eşitliği (3.21) kullanarak yeniden düzenlersek, şu ifadeyi elde ederiz:

$$\delta(\gamma[\gamma,\delta,\epsilon]^{-1}) = (\delta\gamma)[\gamma,\delta,\epsilon]^{-1},$$

bu da şu anlama gelir:

$$[\gamma,\delta,[\gamma,\delta,\epsilon]^{-1}] = 1.$$

Dolayısıyla [25, Lemma 4.1] ifadesinden şu sonucu çıkarırız:

$$[\gamma,\delta,[\gamma,\delta,\epsilon]] = 1. \tag{3.30}$$

Şimdi $a := [\gamma, \delta, \epsilon]$ ve $H := \langle \gamma, \delta, \epsilon \rangle$ olarak tanımlayalım; (3.14) ifadesine göre $[a, \gamma] = 1$ elde edilir. Ayrıca [25, Lemma VII.2.2] sonucundan $R_{a,\gamma}$ ifadesinin $\mathcal{M}$ üzerinde bir otomorfizma olduğu sonucuna da varabiliriz.

Sonra $S := \{s \in H \mid [s, a, \gamma] = 1\}$ olarak tanımlansın, burada

$$[s, a, \gamma] = 1 \implies (sa)\gamma = s(a\gamma)$$

olur. Bunun ardından, birleşiklikçi tanımından şu sonuç çıkar:

$$\begin{aligned}(1a)\gamma = (1(a\gamma))[1, a, \gamma] &\implies a\gamma = (a\gamma)[1, a, \gamma] \\ &\implies [1, a, \gamma] = 1 \\ &\implies 1 \in S.\end{aligned}$$

Ayrıca, herhangi bir $s \in S$ için,

$$[s, a, \gamma] = 1 \implies [s, a, \gamma]^{-1} = 1 \overset{(3.16)}{\implies} [s^{-1}, a, \gamma] = 1 \implies s^{-1} \in S.$$

Sonra $s_1, s_2 \in S$ olsun, yani $[s_1, a, \gamma] = 1$ ve $[s_2, a, \gamma] = 1$. $R_{a,\gamma}(s) = ((sa)\gamma)(a\gamma)^{-1}$ olduğunu hatırlarsak,

$$[s, a, \gamma] = 1 \implies R_{a,\gamma}(s) = (s(a\gamma))(a\gamma)^{-1} = s$$

Yani, $s \in S$ olmak, $R_{a,\gamma}(s) = s$ olmakla eşdeğerdir. Bu yüzden

$$R_{a,\gamma}(s_1) = s_1, \qquad R_{a,\gamma}(s_2) = s_2,$$

ve dolayısıyla

$$R_{a,\gamma}(s_1 s_2) = R_{a,\gamma}(s_1) R_{a,\gamma}(s_2) = s_1 s_2 \implies s_1 s_2 \in S.$$

Sonuç olarak, S kümesi H'nin bir alt döngüsüdür.

Sonra (3.30) ve $[a, \gamma] = 1$'den birleşiklikçi $a := [\gamma, \delta, \epsilon]$'nin γ ile değişmeli olduğu görülür. Böylece, herhangi bir $s \in S$ için $[a, \gamma, s] = 1$, $[\gamma, a, s] = 1$ ve $[\gamma, s, a] = 1$ olur. Özellikle $s = \gamma$ için $[\gamma, a, s] = 1$ ifadesinden

$$[\gamma, a, \gamma] = 1 \implies \gamma \in S.$$

Ayrıca, (3.30) ve (3.21)'den şu sonuç çıkar:

$$[\gamma, \delta, a] = 1 \overset{(3.21)}{\implies} [\delta, a, \gamma] = 1 \Rightarrow \delta \in S.$$

Tekrar, (3.30)'e göre $[\epsilon, \gamma, [\epsilon, \gamma, \delta]] = 1$ olduğundan,

$$[\epsilon, \gamma, \delta] \overset{(3.16)}{=} [\epsilon^{-1}, \gamma, \delta]^{-1} \overset{(3.27)}{=} ([\gamma, \delta, \epsilon]^{-1})^{-1} = [\gamma, \delta, \epsilon] = a.$$

Böylece,

$$[\epsilon, \gamma, a] = 1 \overset{(3.21)}{\Longrightarrow} [\gamma, \epsilon, a]^{-1} = 1 \implies$$
$$[\gamma, \epsilon, a] = 1 \overset{(3.21)}{\Longrightarrow} [\epsilon, a, \gamma] = 1 \implies \epsilon \in S.$$

Sonuç olarak, S kümesi H'nin üreteçlerini içerir ve bundan $S = H$ sonucu çıkar. Başka bir deyişle, her $h \in H$ için

$$[h, a, \gamma] = 1$$

doğrudur.

Argümanın simetrikliği nedeniyle, özellik (3.14) aynı zamanda a açısından δ ve ϵ için de geçerlidir. Böylece

$$[h, a, \delta] = 1$$

ve

$$[h, a, \epsilon] = 1$$

her $h \in H$ için sağlanır. Buna göre, (3.16) ve (3.21)'den

$$[a, \gamma, h] = 1$$

ve

$$[\gamma, h, a] = 1$$

denkliği elde edilir. Bu denklemler, a'nın γ ve herhangi bir $h \in H$ ile ilişkili olarak sol, sağ ve orta çekirdek elemanı gibi davrandığını gösterir. Ayrıca, benzer sonucun γ yerine δ veya ϵ konması durumunda da geçerli olduğunu belirtelim. Yani herhangi bir $h_1 \in H$ ve herhangi bir üreteç $g \in \{\gamma, \delta, \epsilon\}$ için, a'nın birleşiklikçi içindeki konumundan bağımsız olarak,

$$[h_1, a, g] = 1$$

denkliği sağlanır.

Öte yandan, (3.3) ve (3.4)'ten, her $h_1, h_2 \in H$ için

$$[h_1, a, h_2] = 1$$

denkliği çıkar. Sonuç olarak, (3.16) ve (3.21)'den $a \in N(H)$ olduğu sonucuna varılır.

Şimdi, a'nın H'deki herhangi bir eleman ile değişmeli olduğunu göstereceğiz. Bunun için,

$$P := \{p \in H \mid [p, a] = 1\},$$

ve

$$F := \{f \in H \mid fP \subseteq P\},$$

olarak tanımlayalım; burada fP ile

$$\{fp \mid p \in P\}$$

kümesi kastedilmektedir. [25, Lemma 3.4]'a göre F, H'nin bir alt döngüsüdür ve dolayısıyla her $\gamma \in F$ için $\gamma P \subseteq P$ geçerlidir. Öte yandan, herhangi bir $p \in P$ için $[p, a] = 1$ olduğundan, $[\gamma p, a] = 1$ olduğunu göstermek yeterlidir.

Şimdi, [25, Lemma VII 2.2] vasıtasıyla

$$T_a(s) = L_a^{-1} \circ R_a(s) = a^{-1}(sa)$$

bir eş-otomorfizma olup, eşlikçisi a^{-3}'tür. Dolayısıyla,

$$T_a(uv)a^{-3} = T_a(u)(T_a(v)a^{-3})$$

ve bundan,

$$T_a(p) = a^{-1}(pa) = a^{-1}(ap) = p$$

her $p \in P$ için geçerlidir. Böylece (3.22)'den $[\gamma, p, a^{-3}] = 1$ olduğu görülür ve

$$\gamma^{-1}T_a(\gamma) = \gamma^{-1}(a^{-1}(\gamma a)) = \gamma^{-1}(a^{-1}(a\gamma)) = \gamma^{-1}((aa^{-1})\gamma) = 1.$$

Buradan $T_a(\gamma) = \gamma$ sonucuna varılır. Buna göre,

$$T_a(\gamma p)a^{-3} = T_a(\gamma)(T_a(p)a^{-3}) = \gamma(pa^{-3}) = (\gamma p)a^{-3}$$
$$\Longrightarrow\ T_a(\gamma p) = \gamma p \ \Longrightarrow\ \gamma p \in P \ \Longrightarrow\ \gamma \in F.$$

Sonra, (3.14) ve (3.21)'den δ ve ϵ'in de F'de olduğu çıkar, yani $F = H$ olur. Böylece, her $h \in H$ için

$$[h, a] = 1$$

geçerlidir.

Sonra şunu not edelim ki

$$[\gamma, a, h] = [\delta, a, h] = [\epsilon, a, h] = [a, h] = 1,$$

ve her $h_1, h_2 \in H$ için

$$[h_1, a, h_2] = 1$$

denkliği sağlanır. Bundan dolayı, $a \in N(H)$ ve dolayısıyla $a \in C(H)$ olması, a'nın $Z(H)$'de olduğunu gösterir.

Şimdi, ϵ ile eşlikçisi ϵ^{-3} olan bir eş-otomorfizma T_ϵ tanımlansın. [25]'den şu sonuç çıkar:

$$T_\epsilon(\gamma) = s[s, \epsilon]. \tag{3.31}$$

Böylece,

$$T_\epsilon(\gamma\delta) = (\gamma\delta)[\gamma\delta, \epsilon],$$

ve ayrıca

$$T_\epsilon(\gamma\delta)\epsilon^{-3} = T_\epsilon(\gamma)(T_\epsilon(\delta)\epsilon^{-3}).$$

Buna göre,

$$\begin{aligned}
T_\epsilon(\gamma\delta) = (T_\epsilon(\gamma)(T_\epsilon(\delta)\epsilon^{-3}))\epsilon^3 &= T_\epsilon(\gamma)(T_\epsilon(\delta)\epsilon^{-3}\epsilon^3)[T_\epsilon(\gamma), T_\epsilon(\delta)\epsilon^{-3}, \epsilon^3] \\
&= T_\epsilon(\gamma)T_\epsilon(\delta)[T_\epsilon(\gamma), T_\epsilon(\delta)\epsilon^{-3}, \epsilon^3] \\
&= T_\epsilon(\gamma)T_\epsilon(\delta)[\epsilon^{-1}\gamma\epsilon, \epsilon^{-1}\delta\epsilon, \epsilon^3] \\
&\overset{(3.21)}{=} T_\epsilon(\gamma)T_\epsilon(\delta)[\delta\epsilon^{-3}, \gamma, \epsilon^3]^{-1} \\
&\overset{(3.16)}{=} T_\epsilon(\gamma)T_\epsilon(\delta)[\epsilon^3\delta^{-1}, \gamma, \epsilon^3] \\
&\overset{(3.21)}{=} T_\epsilon(\gamma)T_\epsilon(\delta)[\gamma, \epsilon^3\delta^{-1}, \epsilon^3]^{-1} \\
&\overset{(3.18)}{=} T_\epsilon(\gamma)T_\epsilon(\delta)[\gamma, \delta^{-1}, \epsilon^3]^{-1} \\
&\overset{(3.21)}{=} T_\epsilon(\gamma)T_\epsilon(\delta)[\delta^{-1}, \gamma, \epsilon^3] \\
&\overset{(3.16)}{=} T_\epsilon(\gamma)T_\epsilon(\delta)[\delta, \gamma, \epsilon^3]^{-1} \\
&\overset{(3.21)}{=} T_\epsilon(\gamma)T_\epsilon(\delta)[\gamma, \delta, \epsilon^3] \\
&\overset{(3.22)}{=} T_\epsilon(\gamma)T_\epsilon(\delta)[\gamma, \delta, \epsilon]^3.
\end{aligned}$$

Böylece,

$$\begin{aligned}
&(\gamma\delta)[\gamma\delta, \epsilon] = T_\epsilon(\gamma\delta) = T_\epsilon(\gamma)T_\epsilon(\delta)[\gamma, \delta, \epsilon]^3 \\
&\implies ((\gamma\delta)[\gamma\delta, \epsilon])[\gamma, \delta, \epsilon]^{-3} = T_\epsilon(\gamma)T_\epsilon(\delta).
\end{aligned}$$

Öte yandan, $[\gamma, \delta, \epsilon] \in Z(H)$ olduğundan,

$$\begin{aligned}(\gamma\delta)([\gamma\delta, \epsilon][\gamma, \delta, \epsilon]^{-3}) &= T_\epsilon(\gamma)T_\epsilon(\delta) \\ &\overset{3.31}{=} (\gamma[\gamma, \epsilon])(\delta[\delta, \epsilon]) \\ &= \gamma([\gamma, \epsilon](\delta[\delta, \epsilon])) \\ &= \gamma((\delta[\gamma, \epsilon][[\gamma, \epsilon], \delta])[\delta, \epsilon]) \\ &= \gamma((\delta T_\delta([\gamma, \epsilon]))[\delta, \epsilon]) \\ &= \gamma(\delta(T_\delta([\gamma, \epsilon]))[\delta, \epsilon]),\end{aligned}$$

ve bundan dolayı,

$$\begin{aligned}(\gamma\delta)([\gamma\delta, \epsilon][\gamma, \delta, \epsilon]^{-3}) &= (\gamma\delta)^{-1}(\gamma(\delta(T_\delta([\gamma, \epsilon])[\delta, \epsilon]))) \\ &= (\gamma\delta)^{-1}((\gamma\delta)(T_\delta([\gamma, \epsilon])[\delta, \epsilon]))[\gamma, \delta, T_\delta([\gamma, \epsilon])[\delta, \epsilon]]^{-1}.\end{aligned}$$

Bu denklemin sağ tarafında,

$$\begin{aligned}[\gamma, \delta, T_\delta([\gamma, \epsilon])[\delta, \epsilon]]^{-1} &\overset{(3.10)}{=} [\gamma, \delta, (T_\delta([\gamma, \epsilon])[\delta, \epsilon])\delta]^{-1} \\ &= [\gamma, \delta, \delta(T_\delta([\gamma, \epsilon])[\delta, \epsilon])]^{-1} \\ &= [\gamma, \delta, (\delta T_\delta([\gamma, \epsilon]))[\delta, \epsilon]]^{-1} \\ &= [\gamma, \delta, (\delta(\delta^{-1}([\gamma, \epsilon]\delta)))[\delta, \epsilon]]^{-1} \\ &= [\gamma, \delta, [\gamma, \epsilon]\delta[\delta, \epsilon]]^{-1} \\ &= [\gamma, \delta, \gamma[\gamma, \epsilon]\delta[\delta, \epsilon]]^{-1} \\ &= [\gamma, \delta, T_\epsilon(\gamma)T_\delta(\delta)]^{-1} \\ &= [\gamma, \delta, T_\epsilon(\gamma\delta)]^{-1} \\ &= [\gamma, \delta, (\gamma\delta)[\gamma\delta, \epsilon]]^{-1} \\ &= [\gamma, \gamma\delta, (\gamma\delta)[\gamma\delta, \epsilon]]^{-1} \\ &= [\gamma, \gamma\delta, [\gamma\delta, \epsilon]]^{-1} \\ &\overset{(3.15)}{=} 1^{-1} = 1.\end{aligned}$$

Böylece, (3.23)'ü şu şekilde sonuçlandırırız:

$$\begin{aligned}&[\gamma\delta, \epsilon][\gamma, \delta, \epsilon]^{-3} = T_\delta([\gamma, \epsilon])[\delta, \epsilon] = [\gamma, \epsilon][[\gamma, \epsilon], \delta][\delta, \epsilon] \\ &\Rightarrow [\gamma\delta, \epsilon] = [\gamma, \epsilon][[\gamma, \epsilon], \delta][\delta, \epsilon][\gamma, \delta, \epsilon]^3.\end{aligned}$$

□

4. BİRLEŞMELİ OLMAYAN YAPILARIN GENİŞLEMELERİ

4.1. 2. Sınıftan Merkezi Nilpotent Moufang Döngüleri

Bu alt bölümün amacı, Moufang döngülerinin birleşme özelliğine ne kadar yakın olduğuna dair bir sezgi kazandırmaktır. Ayrıca, ikinci sınıfa ait merkezi nilpotent Moufang döngülerinin yapısal özellikleri, merkezi genişlemeler ve kod döngüleri ile yakından ilişkilidir.

Tanım: Bir $\mathcal{L}$ döngüsü verilsin, aşağıdaki

$$\{1\} = Z_0(\mathcal{L}) \leq Z_1(\mathcal{L}) \leq \ldots \leq Z_n(\mathcal{L})$$

alt döngüler zinciri,

$$Z_{i+1}(\mathcal{L})/Z_i(\mathcal{L}) = Z(\mathcal{L}/Z_i(\mathcal{L}))$$

koşulunu sağlıyorsa, buna $\mathcal{L}$'nin *üst merkezi serisi* denir.

Bir $\mathcal{L}$ döngüsü, $Z_n(\mathcal{L}) = \mathcal{L}$ ve $Z_{n-1}(\mathcal{L}) \neq \mathcal{L}$ koşullarını sağlıyorsa, *merkezi nilpotent* ve sınıfı n olarak adlandırılır.

Özellikle, bir $\mathcal{L}$ döngüsü, $Z_2(\mathcal{L}) = \mathcal{L}$ ve $Z_1(\mathcal{L}) \neq \mathcal{L}$ ise, sınıfı 2 olan merkezi nilpotent olarak adlandırılır; burada $Z_0(\mathcal{L}) = \{1\}$ olduğundan

$$Z_1(\mathcal{L}) = Z_1(\mathcal{L})/Z_0(\mathcal{L}) = Z(\mathcal{L}/Z_0(\mathcal{L})) = Z(\mathcal{L})$$

dir. Ayrıca, bu durumda,

$$\mathcal{L}/Z(\mathcal{L}) = Z_2(\mathcal{L})/Z_1(\mathcal{L}) = Z(\mathcal{L}/Z_1(\mathcal{L})) = Z(\mathcal{L}/Z(\mathcal{L})),$$

yani, $\mathcal{L}/Z(\mathcal{L})$ bir değişmeli gruptur.

Sınıfı 2 olan merkezi nilpotent bir Moufang döngüsü $\mathcal{L}$'de, $\mathcal{L}'$ merkezi türetilmiş alt döngüsü merkezin içinde yer alır, bkz. [9]. Bu, böyle bir döngü için tüm komütatörlerin ve birleşiklikçilerin merkezi olduğu anlamına gelir. Buna bağlı olarak, komütatörler ve birleşiklikçiler için $\mathcal{L}/Z(\mathcal{L})$'den $Z(\mathcal{L})$'ye iyi tanımlı fonksiyonlar yazılabilir. Gerçekten de, herhangi $x, y, z \in \mathcal{L}$ için, komütatör $[x, y]$ sadece $xZ(\mathcal{L})$ ve $yZ(\mathcal{L})$ kosetlerine

bağlıdır. Bazı $z_1, z_2 \in Z(\mathcal{L})$ için $x' = xz_1$ ve $y' = yz_2$ olarak tanımlarsak, şunu görürüz:

$$\begin{aligned}[x', y'] = [xz_1, yz_2] &= ((yz_2)(xz_1))^{-1}((xz_1)(yz_2)) \\ &= ((yx)(z_2z_1))^{-1}((xy)(z_1z_2)) \\ &= (z_1z_2)^{-1}(yx)^{-1}(xy)(z_1z_2) \\ &= (z_1z_2)^{-1}(z_1z_2)(yx)^{-1}(xy) \\ &= (yx)^{-1}(xy) = [x, y].\end{aligned}$$

Böylece, $C := \mathcal{L}/Z(\mathcal{L})$ için,

$$\chi : C \times C \to Z, \qquad \chi(c, d) := [\gamma, \delta]$$

ve

$$\alpha : C \times C \times C \to Z, \qquad \alpha(c, d, e) := [\gamma, \delta, \epsilon]$$

her ikisi de iyi tanımlıdır, bkz. örneğin [9].

Bir 2. sınıftan merkezi nilpotent Moufang döngüsünün soyutlaması olarak, bundan sonra $\mathcal{L}$'nin sabit bir merkezi alt grup Z içeren ve $C := \mathcal{L}/Z$'nin değişmeli grup olduğu bir Moufang döngüsü olduğunu varsayacağız.

Yukarıdaki χ ve α dönüşümlerinin temel özelliklerine ilişkin aşağıdaki sonuç [9]'te verilmiştir.

Teorem 4.1: Her $c, d, e, f \in C$, ve her $n \in \mathbb{Z}$ için,

$$\chi(c, c) = 1, \tag{4.1}$$

$$\chi(c, d) = \chi(d, c)^{-1}, \tag{4.2}$$

$$\chi(c^n, d) = \chi(c, d)^n, \tag{4.3}$$

$$\chi(cd, e) = \chi(c, e)\chi(d, e)\alpha(c, d, e)^3, \tag{4.4}$$

$$\alpha(c, d, d) = \alpha(d, c, d) = \alpha(d, d, c) = 1, \tag{4.5}$$

$$\alpha(c, d, e) = \alpha(d, c, e)^{-1} = \alpha(d, e, c), \tag{4.6}$$

$$\alpha(c^n, d, e) = \alpha(c, d, e)^n, \tag{4.7}$$

$$\alpha(cd, e, f) = \alpha(c, e, f)\alpha(d, e, f) \tag{4.8}$$

eşitlikleri sağlanır.

*İspat.*İlk özdeşlik olan (4.1),

$$\chi(c,c) = [\gamma,\gamma] = (\gamma\gamma)^{-1}(\gamma\gamma) = 1$$

gözleminden doğrudan çıkar. (4.2) için ise,

$$\begin{aligned}&\chi(d,c) = [\delta,\gamma] = (\gamma\delta)^{-1}(\delta\gamma)\\ &\implies \chi(d,c)^{-1} = [\delta,\gamma]^{-1} = ((\gamma\delta)^{-1}(\delta\gamma))^{-1} = (\delta\gamma)^{-1}(\gamma\delta) = \chi(c,d)\end{aligned}$$

olduğunu görmek yeterlidir. Sonra, (4.3) için de

$$[\gamma,\delta] = \gamma^{-1}\delta^{-1}\gamma\delta \quad \text{ve} \quad \delta^{-1}\gamma\delta = \gamma[\gamma,\delta].$$

olduğunu not ederek, [25, Lemma 5.1] ve $\gamma\delta = (\delta\gamma)[\gamma,\delta]$ ifadelerini kullanırız. Böylece,

$$\gamma^n[\gamma^n,\delta] = \delta^{-1}\gamma^n\delta = (\delta^{-1}\gamma\delta)^n \quad \text{veya} \quad \gamma^n[\gamma^n,\delta] = (\gamma[\gamma,\delta])^n$$

her $n \in \mathbb{Z}$ için geçerlidir. Son olarak,

$$\gamma^n[\gamma^n,\delta] = (\gamma[\gamma,\delta])^n = (\delta^{-1}\gamma\delta)^n = \underbrace{\delta^{-1}\gamma\delta\cdot\delta^{-1}\gamma\delta\cdot\delta^{-1}\gamma\delta\ldots\delta^{-1}\gamma\delta}_{n \text{ defa}} = \gamma^n[\gamma,\delta]^n.$$

Böylece,

$$[\gamma^n,\delta] = [\gamma,\delta]^n$$

veya eşdeğer olarak,

$$\chi(c^n,d) = \chi(c,d)^n$$

buluruz. Bir sonraki aşamada (4.4)'ü ele alalım. (3.23)'ten

$$[\gamma\delta,\epsilon] = [\gamma,\epsilon][[\gamma,\epsilon],\delta][\delta,\epsilon][\gamma,\delta,\epsilon]^3,$$

ve buradan da, $\mathcal{L}'$ merkezde olduğundan,

$$[[\gamma,\epsilon],\delta] = 1$$

olduğu görülür.

Şimdi (4.6) ile devam edelim. Öncelikle, α'nın tanımından

$$[\gamma,\delta,\epsilon] = [\delta,\gamma,\epsilon]^{-1} = [\delta,\epsilon,\gamma]$$

olup, [25, Lemma 5.4 & Lemma 5.5]'ten de şu ifadeleri biliyoruz:

$$[\gamma,\delta,\epsilon]^{-1} = [\gamma^{-1},\delta,\epsilon],$$
$$[\gamma,\delta,\epsilon] = [\gamma\delta,\epsilon,\delta]^{-1},$$
$$[\gamma,\delta,\epsilon] = [\gamma,\delta,\epsilon\gamma],$$
$$[\gamma,\delta,\epsilon] = [\gamma,\epsilon,\delta^{-1}].$$

Buna göre,

$$\begin{aligned}[\gamma,\delta,\epsilon] &= [\gamma^{-1},\delta,\epsilon]^{-1} = [\gamma^{-1}\delta,\epsilon,\delta],\\ &= [\delta^{-1}\gamma,\epsilon,\delta]^{-1} = [\delta^{-1}\gamma,\epsilon,\gamma]^{-1},\\ &= [\delta^{-1},\gamma,\epsilon] = [\delta,\gamma,\epsilon]^{-1},\end{aligned}$$

ve

$$\begin{aligned}[\gamma,\delta,\epsilon] &= [\gamma,\epsilon,\delta^{-1}] = [\epsilon,\gamma,\delta^{-1}]^{-1},\\ &= [\epsilon,\delta,\gamma]^{-1} = [\delta,\epsilon,\gamma].\end{aligned}$$

Böylece (4.6) elde edilir.

(4.5) için,

$$\alpha(c,d,d) = [\gamma,\delta,\delta],$$

burada $\gamma,\delta \in \mathcal{L}$ sırasıyla $c,d \in C$'nin ön görüntüleridir. Öte yandan, (3.5) göz önüne alındığında, $\mathcal{L}$ bir Moufang döngüsü olduğundan di-birleşmelidir. Başka bir deyişle, $\mathcal{L}$'nin iki eleman tarafından üretilen herhangi bir alt döngüsü birleşmelidir. Buna bağlı olarak, δ tarafından üretilen alt döngü birleşmelidir. Benzer şekilde, δ ve γ tarafından üretilen alt döngü de birleşmelidir. Sonuç olarak,

$$\gamma(\delta\delta) = (\gamma\delta)\delta.$$

Böylece,

$$\alpha(c,d,d) = 1.$$

Kalan

$$\alpha(d,c,d) = \alpha(d,d,c) = 1$$

eşitliklerini ise (4.6)'dan çıkarırız.

(4.7) özdeşliği de hemen gösterilebilir. (3.22)'den

$$[\gamma^n,\delta,\epsilon] = [\gamma,\delta,\epsilon]^n \tag{4.9}$$

olup, buna bağlı olarak (4.7) özdeşliği (4.9)'den gelir.

Son olarak, (4.8)'i inceleyelim. α tanımından

$$\begin{aligned}\alpha(cd,e,f) &= ((\gamma\delta)(\epsilon\varphi))^{-1}(((\delta\gamma)\epsilon)\varphi)\\ &= ((\gamma\delta)(\epsilon\varphi))^{-1}((\gamma(\delta\epsilon))\varphi)\alpha(c,d,e)\\ &= ((\gamma\delta)(\epsilon\varphi))^{-1}(\gamma((\delta\epsilon)\varphi))\alpha(c,d,e)\alpha(c,de,f)\\ &= ((\gamma\delta)(\epsilon\varphi))^{-1}(\gamma(\delta(\epsilon\varphi)))\alpha(c,d,e)\alpha(c,de,f)\alpha(d,e,f)\end{aligned}$$

olmak üzere,

$$(\gamma\delta)(\epsilon\varphi) = (\gamma(\delta(\epsilon\varphi)))\alpha(c,d,ef),$$

ve dolayısıyla

$$\begin{aligned}\alpha(cd,e,f) &= ((\gamma\delta)(\epsilon\varphi))^{-1}((\gamma\delta)(\epsilon\varphi))\alpha(c,d,ef)^{-1}\alpha(c,d,e)\alpha(c,de,f)\alpha(d,e,f)\\ &= \alpha(c,d,ef)^{-1}\alpha(c,d,e)\alpha(c,de,f)\alpha(d,e,f).\end{aligned} \tag{4.10}$$

Böylece,

$$\alpha(cd,e,f) = \alpha(c,d,e)\alpha(c,de,f)\alpha(d,e,f)\alpha(c,d,ef)^{-1} \tag{4.11}$$

denkliği elde edilir. Buradan da

$$\alpha(de,f,c) = \alpha(d,e,f)\alpha(d,ef,c)\alpha(e,f,c)\alpha(d,e,fc)^{-1} \tag{4.12}$$

sonucu çıkar.

(4.11) ifadesindeki ikinci terimde (4.10) kullanıp, (4.6) ile yer değiştirdiğimizde,

$$\begin{aligned}\alpha(cd,e,f) &= \alpha(c,d,e)\alpha(de,f,c)\alpha(d,e,f)\alpha(c,d,ef)^{-1}\\ &= \alpha(c,d,e)\alpha(d,e,f)\alpha(d,ef,c)\alpha(e,f,c)\\ &\quad \alpha(d,e,fc)^{-1}\alpha(d,e,f)\alpha(c,d,ef)^{-1}\\ &= \alpha(c,d,e)\alpha(d,e,f)^2\alpha(d,ef,c)\alpha(c,e,f)\alpha(e,d,fc)\alpha(d,ef,c)^{-1}\\ &= \alpha(c,d,e)\alpha(d,e,f)^2\alpha(c,e,f)\alpha(cf,e,d).\end{aligned}$$

Bu son özdeşliği, (4.11) içindeki $\alpha(c,de,f)$ ve $\alpha(c,d,ef)^{-1}$ ifadelerine uyguladığımızda ise

$$\begin{aligned}\alpha(c,de,f) &= \alpha(de,f,c)\\ &= \alpha(dc,f,e)\alpha(d,e,f)\alpha(d,f,c)\alpha(e,f,c)^2\\ &= \alpha(cd,e,f)^{-1}\alpha(d,e,f)\alpha(c,d,f)\alpha(c,e,f)^2\end{aligned}$$

ve

$$\begin{aligned}
\alpha(c,d,ef)^{-1} &= \alpha(ef,d,c) \\
&= \alpha(ec,d,f)\alpha(e,f,d)\alpha(e,d,c)\alpha(f,d,c)^2 \\
&= \alpha(ce,f,d)^{-1}\alpha(d,e,f)\alpha(c,d,e)^{-1}\alpha(c,d,f)^{-2} \\
&= \alpha(cd,f,e)^{-1}\alpha(c,e,f)^{-1}\alpha(c,f,d)^{-1}\alpha(e,f,d)^{-2} \\
&\quad \alpha(d,e,f)\alpha(c,d,e)^{-1}\alpha(c,d,f)^{-2} \\
&= \alpha(cd,e,f)\alpha(c,e,f)^{-1}\alpha(c,d,f)\alpha(e,f,d)^{-2}\alpha(e,f,d) \\
&\quad \alpha(c,d,e)^{-1}\alpha(c,d,f)^{-2} \\
&= \alpha(cd,e,f)\alpha(c,e,f)^{-1}\alpha(e,f,d)^{-1}\alpha(c,d,e)^{-1}\alpha(c,d,f)^{-1} \\
&= \alpha(cd,e,f)\alpha(c,e,f)^{-1}\alpha(d,e,f)^{-1}\alpha(c,d,e)^{-1}\alpha(c,d,f)^{-1}
\end{aligned}$$

elde ederiz.

Bitirirken, son iki ifadeyi (4.11) içine yerleştirdiğimizde,

$$\begin{aligned}
\alpha(cd,e,f) &= \alpha(c,d,e)\alpha(c,de,f)\alpha(d,e,f)\alpha(c,d,ef)^{-1} \\
&= \alpha(c,d,e)\alpha(cd,e,f)^{-1}\alpha(d,e,f)\alpha(c,d,f)\alpha(c,e,f)^2\alpha(d,e,f) \\
&\quad \alpha(cd,e,f)\alpha(c,e,f)^{-1}\alpha(d,e,f)^{-1}\alpha(c,d,e)^{-1}\alpha(c,d,f)^{-1} \\
&= \alpha(c,e,f)\alpha(d,e,f)
\end{aligned}$$

olup, bu da ispatı tamamlar.

□

χ ve α'nın ek özellikleri aşağıda verilmiştir, bkz. [9].

Önerme 4.1: $c,d,e \in C$ olsun ve $c^k = d^m = e^n = 1$ koşulları sağlansın. O halde $\chi(c,d)$'nin mertebesi $gcd(k,m)$'yi, $\alpha(c,d,e)$'nin mertebesi ise $gcd(k,m,n)$'yi böler.

İspat.(4.3) ve (4.7)'den hemen şu sonuçlar çıkar:

$$\begin{aligned}
&\chi(c,d)^k = \chi(c^k,d) = \chi(1,d) = 1 \implies \\
&\chi(c,d)^m = \chi(d,c)^m = \chi(d^m,c) = \chi(1,c) = 1
\end{aligned}$$

komütatörler için, ve

$$\alpha(c,d,e)^k = \alpha(c^k,d,e) = \alpha(1,d,e) = 1 \implies$$
$$\alpha(c,d,e)^m = \alpha(d,e,c)^m = \alpha(d^m,e,c) = \alpha(1,e,c) = 1 \implies$$
$$\alpha(c,d,e)^n = \alpha(d,e,c)^n = \alpha(e,c,d)^n = \alpha(e^n,c,d) = \alpha(1,c,d) = 1$$

birleşiklikçiler için geçerlidir. □

Bu alt bölümün son sonucu da [9]'ten alınmıştır.

Önerme 4.2: $\mathcal{L}$ sınıfı 2 olan merkezi nilpotent bir Moufang döngüsü olsun. O halde, $\mathcal{L}^*$'nin kuvveti 6'yı böler. Özel olarak, $p > 3$ için $\mathcal{L}$'de mertebesi p'nin bir kuvvetine eşit olan elemanların kümesi olan $\mathcal{L}_p$ gruptur.

*İspat.*Öncelikle, (4.8)'den birleşiklikçilerin değişmeli olduğunu not edelim. Böylece, $\mathcal{L}^*$, tüm $c,d,e \in C$ için $\alpha(c,d,e)$ tarafından üretilen değişmeli bir gruptur. Buna göre, tüm $c,d,e \in C$ için $\alpha(c,d,e)^6 = 1$ olduğunu göstermek yeterlidir.

Bunun için, (4.4)'ten

$$\chi(c,e)\chi(d,e)\alpha(c,d,e)^3 = \chi(cd,e) = \chi(dc,e) = \chi(d,e)\chi(c,e)\alpha(d,c,e)^3,$$

olduğunu hatırladıktan sonra, önermenin iddiası (4.6) vasıtasıyla,

$$\alpha(c,d,e)^3 = \alpha(d,c,e)^3 = \alpha(c,d,e)^3 \implies \alpha(c,d,e)^6 = 1$$

olmasından elde edilir. □

4.2. İki Kat Çift Kodların Kod Döngüleri

Son olarak, kod döngülerine geri dönerek belirtelim ki bunlar özel bir Moufang döngü ailesi oluştururlar.

C bir iki katlı çift kod ve $\varphi : C \times C \to \mathbb{F}_2$ de bir faktör kümesi olsun. Bu durumda, $\mathbb{F}_2 \times C$ üzerinde şu işlemi tanımlayalım:

$$(a,x)(b,y) := (a+b+\varphi(x,y), x+y).$$

Daha önce de işaret edildiği gibi $(C,\varphi) := \mathbb{F}_2 \times C$ yukarıdaki işlem altında bir döngü yapısına sahiptir. Bu döngünün bir Moufang döngüsü olduğunu iddia eden, ve bu alt bölümün ana sonucu olan aşağıdaki önerme [3, Prop. 9]'te verilmiştir.

Önerme 4.3: Bir kod döngüsü bir Moufang döngüsüdür.

İspat. $(a,x),(b,y),(c,z) \in \mathbb{F}_2 \times C$ için, Moufang özdeşlikleri göz önüne alındığında,

$$((a,x)\circ(b,y))\circ((c,z)\circ(a,x)) = ((a,x)\circ((b,y)\circ(c,z)))\circ(a,x) \implies$$

$$(a+b+\varphi(x,y), x+y)\circ(c+a+\varphi(z,x), z+x) =$$

$$((a,x)\circ(b+c+\varphi(y,z), y+z))\circ(a,x) \implies$$

$$(a+b+\varphi(x,y)+c+a+\varphi(z,x)+\varphi(x+y,z+x), x+y+z+x) =$$

$$(a+b+c+\varphi(y,z)+\varphi(x,y+z), x+y+z)\circ(a,x) \implies$$

$$(b+c+\varphi(x,y)+\varphi(z,x)+\varphi(x+y,z+x), y+z) =$$

$$(a+a+b+c+\varphi(y,z)+\varphi(x,y+z)+\varphi(x+y+z,x), x+x+y+z) \implies$$

$$(b+c+\varphi(x,y)+\varphi(z,x)+\varphi(x+y,z+x), y+z) =$$

$$(b+c+\varphi(y,z)+\varphi(x,y+z)+\varphi(x+y+z,x), y+z).$$

Böylece, $\mathbb{F}_2 \times C$'nin bir Moufang döngüsüdür olması için gerek ve yeter şart

$$\varphi(x,y)+\varphi(z,x)+\varphi(x+y,z+x) = \varphi(y,z)+\varphi(x,y+z)+\varphi(x+y+z,x)$$

eşitliğinin sağlanmasıdır.

Şimdi faktör kümesi $\varphi : C\times C \to \mathbb{F}_2$'nin bu özdeşliği sağladığını göstereceğiz. Bunun için, (2.7)'de $z := z+x$ olarak alırsak,

$$\varphi(x,y)+\varphi(x+y,z+x)+\varphi(y,z+x)+\varphi(x,x+y+z) = w(x\cap y\cap(x+z)),$$

yani

$$\varphi(x,y)+\varphi(x+y,z+x) = \varphi(y,z+x)+\varphi(x,x+y+z)+w(x\cap y\cap(x+z))$$

buluruz.

Böylece,

$$\varphi(x,y)+\varphi(z,x)+\varphi(x+y,z+x) =$$

$$\varphi(z,x)+\varphi(y,z+x)+\varphi(x,x+y+z)+w(x\cap y\cap(x+z)),$$

ve buradan da

$$\varphi(x,y)+\varphi(x+y,z+x) = \varphi(z,x)+\varphi(y,z+x)+\varphi(x+y+z,x)+$$
$$\frac{1}{2}w(x\cap y)+\frac{1}{2}w(x\cap z)+w(x\cap y\cap z)+w(x\cap y\cap(x+z))$$

sonucunu çıkarırız. Şimdi, (2.7)'de $y \leftrightarrow z$ yer değiştirmesi ile,

$$\varphi(x,z)+\varphi(x+z,y)+\varphi(z,y)+\varphi(x,y+z)=w(x\cap y\cap z),$$

ve (2.6)'yi iki kere uygulayarak,

$$\varphi(z,x)+\frac{1}{2}w(x\cap z)+\varphi(y,x+z)+\frac{1}{2}w(y\cap(x+z))+\varphi(z,y)+\varphi(x,y+z)=$$
$$w(x\cap y\cap z)\implies$$
$$\varphi(z,x)+\varphi(y,x+z)=$$
$$w(x\cap y\cap z)+\frac{1}{2}w(x\cap z)+\frac{1}{2}w(y\cap(x+z))+\varphi(z,y)+\varphi(x,y+z)$$

elde edilir.

Sonuç olarak,

$$\begin{aligned}
&\varphi(x,y)+\varphi(z,x)+\varphi(x+y,z+x)=\\
&w(x\cap y\cap z)+\frac{1}{2}w(x\cap z)+\frac{1}{2}w(y\cap(x+z))+\varphi(z,y)+\varphi(x,y+z)+\\
&\varphi(x+y+z,x)+\frac{1}{2}w(x\cap y)+\frac{1}{2}w(x\cap z)+\\
&\qquad w(x\cap y\cap z)+w(x\cap y\cap(x+z))=\\
&w(x\cap y\cap z)+\frac{1}{2}w(x\cap z)+\frac{1}{2}w(y\cap x)+\\
&\quad\frac{1}{2}w(y\cap z)+w(x\cap y\cap z)+\varphi(y,z)+\frac{1}{2}w(y\cap z)+\\
&\varphi(x,y+z)+\varphi(x+y+z,x)+\frac{1}{2}w(x\cap y)+\\
&\qquad\frac{1}{2}w(x\cap z)+w(x\cap y\cap z)+w(x\cap y\cap z)=\\
&4w(x\cap y\cap z)+w(y\cap z)+w(x\cap z)+\\
&\qquad w(x\cap y)+\varphi(y,z)+\varphi(x,y+z)+\varphi(x+y+z,x)=\\
&\varphi(y,z)+\varphi(x,y+z)+\varphi(x+y+z,x).
\end{aligned}$$

□

Şimdi somut bir kod döngüsü üzerinde Moufang döngü yapısını inceleyelim.

Örnek 9: Aşağıdaki

$$C:=\text{span}\begin{cases}100000001000111000111000\\100000000100101000010111\\011011000001111011111111\end{cases}$$

ve

$$\varphi : C \times C \to \mathbb{F}_2$$

faktör kümesi, tabloyla verilmiştir:

	u_0	u_1	u_2	u_3	u_4	u_5	u_6	u_7
u_0	0	0	0	0	0	0	0	0
u_1	0	0	0	0	1	1	1	1
u_2	0	0	0	0	1	1	1	1
u_3	0	0	0	0	1	1	1	1
u_4	0	0	0	0	0	0	0	0
u_5	0	0	1	1	1	1	0	0
u_6	0	1	0	1	1	0	1	0
u_7	0	1	1	0	1	0	0	1

burada

$$u_0 = 000000000000000000000000,$$
$$u_1 = 100000001000111000111000,$$
$$u_2 = 100000000100101000010111,$$
$$u_3 = 011011000001111011111111,$$
$$u_4 = 000000001100010000101111,$$
$$u_5 = 111011001001000011000111,$$
$$u_6 = 111011000101010011101000,$$
$$u_7 = 011011001101101011010000$$

olup,

$$((0, u_4) \circ (1, u_5)) \circ ((1, u_1) \circ (0, u_4)) = ((0, u_4) \circ ((1, u_5) \circ (1, u_1))) \circ (0, u_4)$$

eşitliğini Moufang özdeşliklerine bir örnek olarak gözlemleyebiliriz

Böyle yapılar aslında *Parker döngüsü* olarak bilinen bir yapıdan esinlenilmiş, ancak ayrıntıları yaygın olarak paylaşılmamıştır [3]. Bu özel döngü, $\mathbb{F}_2$ cismi üzerinde sonlu boyutlu bir vektör uzayı V'nin bir *Parker fonksiyonu*

$$p : V \times V \to \mathbb{F}_2$$

ile genişlemesi olarak tanıtılmıştır. Bu inşaada kullanılan Parker fonksiyonunun

$$p(x,x) = |x \cap \mathscr{D}|,$$
$$p(x,y) + p(y,x) = \sum_{i,j \in \mathbb{F}_2} |(ix + jy) \cap \mathscr{D}|,$$
$$p(x,y) + p(x+y,z) + p(y,z) + p(x,y+z) = \sum_{i,j,k \in \mathbb{F}_2} |(ix + jy + kz) \cap \mathscr{D}|,$$

koşullarına tabi olduğu farz edilir; burada $\mathscr{D} \subseteq V \setminus \{0\}$ bir alt kümedir. Böylece, yukarıdaki gibi tanımlanan $(V,p) := \mathbb{F}_2 \times V$ döngüsüne Parker döngüsü denir.

Parker döngüsü ile kod döngüleri arasındaki ilişki, aşağıdaki sonuçta ortaya konmuştur, bkz. [3, Teorem 14].

Teorem 4.2: Eğer sonlu boyutlu bir $\mathbb{F}_2$ vektör uzayı V, *Parker koşulu*nu sağlarsa; yani 4-boyutlu her $U \subseteq V$ altuzayı için

$$\sum_{x \in U} p(x) = 0$$

olursa, Parker döngüsü $(V,p) = \mathbb{F}_2 \times V$ bir kod döngüsüdür. Başka bir ifadeyle, bu durumda, bir iki kat çift kod W ve buna bağlı bir faktör kümesi $\varphi : W \times W \to \mathbb{F}_2$ için

$$\mathbb{F}_2 \times V =: (V,p) \cong (W,\varphi) := \mathbb{F}_2 \times W$$

dir. Tersine, her kod döngüsü bir Parker döngüsüdür ve faktör kümesi Parker koşulunu sağlar.

Bir $\mathcal{L}$ döngüsü verildiğinde, eğer bir iki katlı çift kod V üzerine tanımlı bir faktör kümesi $\varphi : V \times V \to \mathbb{F}_2$ için $\mathcal{L} \cong (V,\varphi)$ ise, $\mathcal{L}$ bir kod tarafından *sağlanmış* olarak adlandırılır, [3, Def. 12].

Son olarak belirtmek gerekir ki, verilen bir döngü için ona karşılık gelen (izomorf olmayan) birden fazla kod olabilir.

Gerçekten de, [3]'de belirtildiği gibi, bir Parker döngüsü (V,p) verildiğinde, ona karşılık gelen çift katlı kod $C \subseteq \mathscr{P}(\Omega)$ olsun. Ayrıca, $|\Gamma| \equiv 0 \pmod 8$ olacak şekilde Γ adlı bir küme ve $\Gamma \cap \Omega = \emptyset$ olsun. Ayrıca, $f : C \to \mathbb{F}_2$ sıfır olmayan doğrusal bir fonksiyon olsun ve

$$C' \subseteq \mathscr{P}(\Omega \cup \Gamma) := \{x + f(x)\Gamma \mid x \in C\}$$

olarak tanımlansın. Bu durumda, C' de (V,p)'yi sağlar ancak $C' \ncong C$ olur.

5. SONUÇLAR

Bu tez çalışmasında, iki katlı çift kodlara dayalı olarak tanımlanan kod döngüleri incelenmiş ve bu yapıların çeşitli cebirsel özellikleri ele alınmıştır. Kod döngüleri, doğrusal kodların üzerine tanımlanan faktör kümeleri aracılığıyla oluşturulan birleşmeli olmayan döngü yapılarıdır. Çalışmada, bu çarpım yapısının Moufang özdeşliğini sağladığı ve bu sayede ortaya çıkan yapının bir Moufang döngüsü oluşturduğu gösterilmiştir.

Ayrıca, aynı iki katlı çift koddan türeyebilecek farklı faktör kümelerinin oluşturduğu döngülerin izomorf olduğu ve bu durumun kohomolojik bir açıklamaya sahip olduğu gözlemlenmiştir. Döngülerin merkezleri, birleşiklikçileri, iç dönüşüm grupları gibi yapısal bileşenleri de incelenmiş ve bunların belirli sınıflara dâhil edilebileceği belirtilmiştir. Özellikle ikinci sınıf merkezi nilpotent Moufang döngülerinin bu çerçevede önemli bir rol oynadığı değerlendirilmiştir.

Kod döngülerinin, Parker döngüleriyle olan ilişkisi de ayrıca ele alınmıştır. Parker koşulunu sağlayan vektör uzaylarının oluşturduğu döngülerin, bir kod döngüsü ile izomorf olduğu ve tersine her kod döngüsünün de bir Parker döngüsü olduğu bilinmektedir. Bu ilişkinin tez kapsamında göz önünde bulundurulması, kodların cebirsel yapıların inşasındaki yerini netleştirmeye yardımcı olmuştur.

Aslında, verilen bir döngüyü sağlayan (iki katlı çift) kodların sınıflandırılması [13]'te açık bir soru olarak belirtilmiştir; bu da gelecekteki araştırmalar için potansiyel bir çalışma alanı olarak not edilmiştir.

Tez kapsamında incelenen kod döngüleri doğrudan uygulamaya yönelik olarak ele alınmamış olsa da, bu yapıların sahip olduğu birleşmeli olmayan ve düzenli özellikler, bazı kriptografik sistemlerin matematiksel temeli açısından ilgi çekici olabilir. Özellikle doğrusal kodlar üzerinden inşa edilen bu döngülerin, cebirsel olarak kontrol edilebilir olmaları, güvenlik gereksinimlerine cevap verebilecek yapıların tasarımında potansiyel oluşturabilir. Bu bağlamda, ileride yapılacak çalışmalarda kod döngülerinin homomorfik şifreleme, kuantum sonrası kriptografi ya da doğrusal olmayan anahtar değişim protokolleri gibi alanlarda nasıl değerlendirilebileceği araştırılabilir. Kod döngülerinin cebirsel yapılarının daha sistematik biçimde analiz edilmesi, bu tür uygulamalara katkı sağlayabilecek yeni modellerin geliştirilmesine zemin hazırlayabilir.

KAYNAKLAR

[1] Pflugfelder, H. O., (1990), "'Quasigroups and loops: introduction'", c. 7 of Sigma Series in Pure Mathematics, Heldermann Verlag, Berlin.

[2] Bruck, R. H., (1946). "Contributions to the theory of loops". *Trans. Amer. Math. Soc.* 60, 245–354.

[3] Griess Jr., R. L., (1986). "Code loops". *J. Algebra*, 100(1), 224–234.

[4] Conway, J. H., (1985). "A simple construction for the Fischer-Griess monster group". *Invent. Math.* 79(3), 513–540.

[5] Griess Jr., R. L., (1982). "The friendly giant". *Invent. Math.* 69(1), 1–102.

[6] Griess Jr., R. L., (1985), "The Monster and its nonassociative algebra", in "'Finite groups—coming of age (Montreal, Que., 1982)'", c. 45 of Contemp. Math. Amer. Math. Soc., Providence, RI, 121–157.

[7] Hill, R., (1986), "'A first course in coding theory'", Oxford Applied Mathematics and Computing Science Series, The Clarendon Press, Oxford University Press, New York.

[8] Griess Jr., R. L., (1987), "Sporadic groups, code loops and nonvanishing cohomology", in "*Proceedings of the Northwestern conference on cohomology of groups (Evanston, Ill., 1985)*", Vol. C. 44, 191–214.

[9] Hsu, T., (2000). "Moufang loops of class 2 and cubic forms". *Math. Proc. Cambridge Philos. Soc.* 128(2), 197–222.

[10] Hussain, S., Shah, T. ve Javeed, A., (2023). "Modified advanced encryption standard (MAES) based on non-associative inverse property loop". *Multimed. Tools Appl.* 82(11), 16237–16256.

[11] Hussain, T. ve diğ., (2022). "Designing of nonlinear component of block cipher by a Moufang loop and its application in image encryption". *(Preprint))*.

[12] Jaiyedola, T. G. ve Adeniran, J. O., (2010). "On another two cryptographic identities in universal Osborn loops". *Surv. Math. Appl.* 5, 17–34.

[13] Combe, N., Manin, Y. I. ve Marcolli, M., (2023). "Moufang patterns and geometry of information". *Pure Appl. Math. Q.* 19(1), 149–189.

[14] Manin, Y. I., (1986), "'Cubic forms'", c. 4 of North-Holland Mathematical Library, Second Edition, North-Holland Publishing Co., Amsterdam. Algebra, geometry, arithmetic, Translated from the Russian by M. Hazewinkel.

[15] Combe, N. ve Manin, Y. I., (2020). "F-manifolds and geometry of information". *Bull. Lond. Math. Soc.* 52(5), 777–792.

[16] Combe, N., Manin, Y. I. ve Marcolli, M., (2022). "Geometry of information: classical and quantum aspects". *Theoret. Comput. Sci.* 908, 2–27.

[17] Vinberg, E. B., (1963). "The theory of homogeneous convex cones". *Trudy Moskov. Mat. Obšč.* 12, 303–358.

[18] Grishkov, A. ve Miguel Pires, R., (2018). "Variety of loops generated by code loops". *Internat. J. Algebra Comput.* 28(1), 163–177.

[19] Calderbank, A. R. ve diğ., (1997). "Quantum error correction and orthogonal geometry". *Phys. Rev. Lett.* 78(3), 405–408.

[20] Heydeman, M. ve diğ., (2021). "Nonarchimedean holographic entropy from networks of perfect tensors". *Adv. Theor. Math. Phys.* 25(3), 591–721.

[21] Ivanov, S. O. ve Zaikovskii, A. A., (2019). "Mod-2 (co)homology of an abelian group". *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 484, 72–85.

[22] Johnson, K. W., (1990). "Loop Cohomology". *Czech. Math. J.* 40(2), 182–194.

[23] Nagy, G. P. ve Vojtvechovsky, P., (2003). "Octonions, simple Moufang loops and triality". *Quasigroups Related Systems*, 10, 65–94.

[24] Kunen, K., (1996). "Quasigroups, loops, and associative laws". *J. Algebra*, 185(1), 194–204.

[25] Bruck, R. H., (1958), "'A survey of binary systems'", Reihe: Gruppentheorie, Springer-Verlag, Berlin-Göttingen-Heidelberg. Ergebnisse der Mathematik und ihrer Grenzgebiete, (N.F.), Heft 20.

[26] Moufang, R., (1935). "Zur Struktur von Alternativkörpern". *Math. Ann.* 110(1), 416–430.

ÖZGEÇMİŞ

İlk, orta ve lise öğrenimini Balıkesir'de tamamladı. 2017 yılında Balıkesir Üniversitesi Matematik Öğretmenliği bölümünde lisans eğitimine başladı ve 2021 yılında bölümünü dereceyle tamamladı. 2022 yılında Ankara Üniversitesi Matematik Bölümü'nde yüksek lisans eğitimine başladı. 2024 yılında araştırma görevlisi kadrosuna kabul edilmesinin ardından Gebze Teknik Üniversitesi Matematik Bölümü'ne yatay geçiş yaptı. Hâlen yüksek lisans eğitimine Gebze Teknik Üniversitesi'nde devam etmektedir.