

T.C.
ONDOKUZ MAYIS ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MATEMATİK ANA BİLİM DALI



**BİR HALKA AİLESİ ÜZERİNDE TANIMLI SKEW
CONSTACYCLIC KODLAR**

Yüksek Lisans Tezi

Burakcan KARADENİZ

Danışman
Dr. Öğr. Üyesi Abdullah DERTLİ

SAMSUN

2023

BİLİMSEL ETİĞE UYGUNLUK BEYANI

Hazırladığım Yüksek Lisans tezinin bütün aşamalarında bilimsel etiğe ve akademik kurallara riayet ettiğimi, çalışmada doğrudan veya dolaylı olarak kullandığım her alıntıya kaynak gösterdiğimi ve yararlandığım eserlerin Kaynaklar'da gösterilenlerden oluştuğunu, her unsurun enstitü yazım kılavuzuna uygun yazıldığını ve TÜBİTAK Araştırma ve Yayın Etiği Kurulu Yönetmeliği'nin 3. bölüm 9. maddesinde belirtilen durumlara aykırı davranılmadığını taahhüt ve beyan ederim.

Etik Kurul Gerekli mi ?

Evet ☐

Hayır ☒

21 /06 / 2023

Burakcan KARADENİZ

TEZ ÇALIŞMASI ÖZGÜNLÜK RAPORU BEYANI

Tez Başlığı : BİR HALKA AİLESİ ÜZERİNDE TANIMLI SKEW CONSTACYCLIC KODLAR

Yukarıda başlığı belirtilen tez çalışması için şahsım tarafından 21/06/2023 tarihinde intihal tespit programından alınmış olan özgünlük raporu sonucunda;

Benzerlik oranı : % 14

Tek kaynak oranı : % 4 çıkmıştır.

21 /06/ 2023

Dr. Öğr. Üyesi Abdullah DERTLİ

ÖZET

BİR HALKA AİLESİ ÜZERİNDE TANIMLI SKEW CONSTACYCLIC KODLAR

Burakcan KARADENİZ
Ondokuz Mayıs Üniversitesi
Lisansüstü Eğitim Enstitüsü
Matematik Ana Bilim Dalı
Yüksek Lisans, Haziran/2023
Danışman: Dr. Öğr. Üyesi Abdullah DERTLİ

Bu tez çalışmasında, ilk olarak tanımlanan, $v_i^2 = v_i$, $v_1v_2 = v_2v_1$, $v_iv_j = v_jv_i = 0$ ($i = 1,2,3,4$, $j = 3,4$, $i \neq j$) ve p bir tek asal, m pozitif bir tamsayı, $q = p^m$ olmak üzere $B_q = \mathbb{F}_q + v_1\mathbb{F}_q + v_2\mathbb{F}_q + v_3\mathbb{F}_q + v_4\mathbb{F}_q + v_1v_2\mathbb{F}_q$ sonlu, birimli, değişmeli halka ailesi üzerinde eleman sayısı ve minimum uzaklığı yüksek kod aileleri elde etmek amacıyla aşık olmayan bir θ otomorfizması yardımıyla skew constacyclic kodlar çalışılmış ve bunların polinom temsilleri belirlenmiştir.

İlk bölümde, kodlamanın tarihi kısaca özetlenmiş ve kullanım alanlarına değinilmiştir. Daha sonra kodlama teorisinin ortaya çıkışı ve temel problemlerinden bahsedilmiştir. Son olarak cyclic, skew cyclic, skew constacyclic kodlarla ilgili literatür bilgisi verilmiştir.

İkinci bölümünde cebir, kodlama teorisi ile ilgili temel tanım ve teoremler verilmiştir.

Üçüncü bölümde, $B_q = \mathbb{F}_q + v_1\mathbb{F}_q + v_2\mathbb{F}_q + v_3\mathbb{F}_q + v_4\mathbb{F}_q + v_1v_2\mathbb{F}_q$ halka ailesi tanıtılmıştır. B_q^n den $\mathbb{F}_q^{6n}$ e bir Gray dönüşümü tanımlanıp $\mathbb{F}_q^6$ üzerinde devirli kodlar verilmiştir. Daha sonra B_q üzerinde aşık olmayan bir θ otomorfizması tanımlanıp bu otomorfizma yardımıyla $B_q[x, \theta]$ skew polinom halkası oluşturulmuştur. Son olarak λ birimseliyle birlikte bu halka üzerinde skew λ -constacyclic kodlar tanımlanıp özellikleri incelenmiş ve bazı örnekler verilmiştir.

Anahtar Sözcükler: Sonlu halkalar, Skew constacyclic kod, Multi-twisted kod.

ABSTRACT

SKEW CONSTACYCLIC CODES OVER A FAMILY OF RINGS

Burakcan KARADENİZ
Ondokuz Mayıs University
Institute of Graduate Studies
Department of Matematik Programme
Master, June/2023
Supervisor: Assist. Prof. Dr. Abdullah DERTLİ

In this thesis, skew constacyclic codes are investigated to obtain code families with a high number of elements and minimum distance on a finite, unitary, commutative ring family $B_q = \mathbb{F}_q + v_1\mathbb{F}_q + v_2\mathbb{F}_q + v_3\mathbb{F}_q + v_4\mathbb{F}_q + v_1v_2\mathbb{F}_q$, where $v_i^2 = v_i$, $v_1v_2 = v_2v_1$, $v_iv_j = v_jv_i = 0$ ($i = 1,2,3,4$, $j = 3,4$, $i \neq j$) and p is an odd prime, m is a positive integer and $q = p^m$, using a non-trivial θ -automorphism. Their polynomial representations have been determined.

In the first section, a brief overview of the history of coding is provided, along with discussions on its applications. Subsequently, the emergence of coding theory and its fundamental problems are discussed. Finally, literature information related to cyclic, skew cyclic and skew constacyclic codes is presented.

In the second section, basic definitions and theorems related to algebra and coding theory are provided.

In the third section, the ring family $B_q = \mathbb{F}_q + v_1\mathbb{F}_q + v_2\mathbb{F}_q + v_3\mathbb{F}_q + v_4\mathbb{F}_q + v_1v_2\mathbb{F}_q$ is introduced. A Gray map from B_q^n to $\mathbb{F}_q^{6n}$ is defined and cyclic codes over $\mathbb{F}_q^6$ are given. Then, a non-trivial θ -automorphism is defined over B_q and using this automorphism, the $B_q[x, \theta]$ skew polynomial ring is constructed. Finally, skew λ -constacyclic codes over this ring, along with their properties, are defined and some examples are given.

Keywords: Finite rings, Skew constacyclic code, Multi-twisted code.

ÖN SÖZ VE TEŞEKKÜR

Lisans ve yüksek lisans eğitimim boyunca sabır ve özveriyle benden bilgi birikimini esirgemeyen, bu süreçte geçirdiğimiz pandemi ve 6 Şubat depremlerinde manevi desteğini de her zaman arkamda hissettiğim kıymetli hocam Sayın Dr. Öğr. Üyesi Abdullah DERTLİ'ye teşekkürü borç bilirim.

Eğitim hayatım boyunca hem akademik hem de sosyal anlamda ömür boyu taşıyacağım kazanımlar elde etmemde emeği geçen tüm öğretmenlerime de ayrıca teşekkür ederim.

Ve hayatımın her anında desteklerini her zaman yanımda hissettiğim başta annem olmak üzere tüm ailem ve arkadaşlarıma da çok teşekkür ederim.

Burakcan KARADENİZ

İÇİNDEKİLER

TEZ KABUL VE ONAYI	i
BİLİMSEL ETİĞE UYGUNLUK BEYANI	ii
TEZ ÇALIŞMASI ÖZGÜNLÜK RAPORU BEYANI	ii
ÖZET	iii
ABSTRACT	iv
ÖNSÖZ VE TEŞEKKÜR	v
İÇİNDEKİLER	vi
SİMGELER VE KISALTMALAR	vii
TABLolar DİZİNİ	viii
1. GİRİŞ	1
2. TEMEL KAVRAMLAR	6
3. SKEW CONSTACYCLIC KODLAR	24
3.1. B_q Halkası	24
3.2. Gray Dönüşümü ve Lineer Kodlar	25
3.3. B_q Halkası Üzerinde Tanımı Skew Constacyclic Kodlar	33
4. SONUÇ	56
KAYNAKÇA	57
ÖZ GEÇMİŞ	59

SİMGELER VE KISALTMALAR

$\oplus$	: Direkt toplam
$\otimes$	: Direkt çarpım
$\mathbb{F}_q$	: q elemanlı Galois cismi
$\mathbb{F}_q^n$	: Bileşenleri $\mathbb{F}_q$ cisminin elemanları olan sıralı n 'lilerden oluşan vektörlerin kümesi
$R \cong S$	: R ve S izomorftur
$ C $	: C kodunun eleman sayısı
$C^\perp$	: C kodunun duali
$w_H(x)$	: x vektörünün Hamming ağırlığı
$w_L(x)$	: x vektörünün Lee ağırlığı
$w_H(C)$	: C kodunun minimum Hamming ağırlığı
$w_L(C)$	: C kodunun minimum Lee ağırlığı
$d(C)$	: C kodunun minimum Hamming uzaklığı
$d_L(C)$	: C kodunun minimum Lee uzaklığı
(n, M, d)	: n uzunluğunda M elemanlı ve minimum uzaklığı d olan bir kod
$[n, k, d]$	: n uzunluğunda k boyutlu ve minimum uzaklığı d olan bir lineer kod
$C = \langle g(x) \rangle$	: $g(x)$ polinomu tarafından üretilen C kodu
$\mathbb{F}_q[x]$	: Katsayıları $\mathbb{F}_q$ cisminin elemanı olan x değişkenine bağlı polinom halkası
$der(g)$	: $g(x)$ polinomunun derecesi
B_q	: $\mathbb{F}_q + v_1\mathbb{F}_q + v_2\mathbb{F}_q + v_3\mathbb{F}_q + v_4\mathbb{F}_q + v_1v_2\mathbb{F}_q$ halka ailesi
Ψ	: B_q^n den $\mathbb{F}_q^{6n}$ e tanımlanan Gray dönüşümü
$\Psi(C)$	: B_q üzerinde tanımlı bir C kodunun Gray görüntüsü
θ	: $\mathbb{F}_q$ üzerinde tanımlı Frobenius otomorfizması
Θ	: B_q üzerinde aşıkâr olmayan bir otomorfizma
$B_q[x, \Theta]$	: Skew polinom halka ailesi
$\sigma_{\theta, \lambda}$	: Skew λ -constacyclic shift dönüşümü
$\tau_{Y, s}$	: Multi-twisted shift dönüşümü

TABLÖLAR DİZİNİ

Tablo 3.3.12. $\mathbb{F}_q$ üzerindeki skew cyclic ve skew nega-cyclic kodlardan elde edilen B_q üzerindeki skew constacyclic kodlar.....	43
--	----



1. GİRİŞ

Kodlama kelime anlamıyla, aktarılmak istenilen mesajın çeşitli yöntem ve tekniklerle (sembol, ışık, ses dalgaları vb.) ifade edilmesi anlamına gelmektedir. İlk çağlardan beri kullanılan alfabeler, sayı sistemleri gibi yöntemler kodlamanın ilk örnekleridir. İnsanlığın ilerlemesiyle birlikte bu kodlama yöntem ve teknikleri çeşitlenmiş ve gelişmiştir. Örneğin M.Ö. 58-50 yıllarında Jül Sezar tarafından kullanılan Sezar Şifresi, telgrafın geliştirilmesiyle 1835 yılında S. Morse tarafından oluşturulan Mors Alfabesi, Antik Yunan ve Roma dönemlerinde çeşitli metinleri ve bilgileri kaydetmek ve iletmek için kullanılan nal ve çizgi sistemleri, 2. Dünya savaşında gizli haberleşme için kullanılan Enigma Makinesi gibi yöntemler, kodlamaya birer örnek olarak verilebilirler. Günümüzde gelişen teknoloji ve artan ihtiyaçlarla birlikte bu yöntemler insanlık için olmazsa olmaz hale gelmiş ve varlığını arttırarak sürdürmektedir. Parola ve şifreler, adres numaraları, T.C. kimlik numaraları, araba plakaları, seri numaralar, barkodlar, QR kodlar gibi kodlama yöntemleri sıklıkla kullanılmaktadır. Özellikle insanoğlunun hayatının her alanına giren bilgisayarlar ve makinelerle birlikte kodlamanın önemi daha da artmaktadır. Makine dili, yüksek düzeyli programlama dilleri (C, C++, Java, Python, Ruby, JavaScript vb.), algoritma ve mantıksal akış şemaları, SSL/TLS güvenlik protokolleri, makine ve bilgisayar kodlama yöntemlerine örnek olarak verilebilirler. Bu gelişmelerle birlikte kodlama yöntem ve tekniklerinde kodlanan mesajın tasarruflu, kullanışlı, hatasız iletimi gibi durumları önemli faktörler haline gelmiştir. Veri trafiğinin azaltılması için mesaj içinde bulunan fazlalıkların atılarak sıkıştırılması, aktarım sırasında oluşabilen hataların en aza indirgenip mesajın doğru bir şekilde iletilmesi gibi problemler gün geçtikçe daha çok önemli hale gelmiş ve bu gibi problemlere çözüm arayışları kodlama teorisinin ortaya çıkmasına sebep olmuştur.

Kodlama teorisi genel olarak bilginin iletimi ve depolanmasıyla ilgilenen bir matematiksel disiplindir. Veriyi daha etkin bir şekilde temsil etmek, hata tespiti ve düzeltme yapmak, veri sıkıştırması, veri aktarımı gibi konular kodlama teorisinin bazı temel başlıklarıdır. Bu disiplin; bilgisayar bilminde, iletişim sistemlerinde,

veritabanlarında, kriptografi alanında ve diğer birçok alanda önemli bir rol oynamaktadır. Veri sıkıştırma veya kaynak kodlama; kaynak mesajın kanala uygun hale getirilmesi ve mesajı daha az miktarda veriyle temsil etmek için sıkıştırma algoritmaları ve yöntemlerinin kullanılmasıdır. Bu sayede dosya boyutlarını küçültmek ve veri transferinde daha az bant genişliği kullanmak mümkün olur. Örneğin ZIP veri sıkıştırması, video sıkıştırmaları internet trafiğini azaltmak gibi amaçlarla veri dosyalarını küçültürler. Hata düzeltme veya kanal kodlaması; verinin belirli bir kanal boyunca en az hatayla iletimini sağlamak amacıyla kodlanması, iletim sonrasında oluşan hataların tespit edilmesi ve düzeltilmesini esas alan kodlama yöntemidir. Wi-Fi, bluetooth, 4G/5G gibi kablosuz iletişim protokolleri, telekomünikasyon ağları, radyo yayınları, uydu iletişimi, fiber optik iletişim, CD, DVD, Blu-ray gibi alanlarda hata düzeltme yöntemleri kullanılmaktadır. Kodlama yöntemleri gizli haberleşme ve gizli veri aktarımını konu alan Kriptografi alanında da aktif olarak kullanılmaktadır. Kriptografi; içeriği gizli olan mesajların veya bilgilerin şifrelenip, iletim sırasında güvenliğin sağlanması ve alıcının bu şifrelenmiş bilgiyi orijinal haline geri dönüştürmesi için kullanılan teknikleri içerir. Kriptografinin örnekleri insanlığın ilk dönemlerine kadar dayanmakla birlikte dijitalleşen dünyada bilgi güvenliğinin devletler ve şahıslar açısından hayati öneme sahip olması bu türün önemini arttırmaktadır. Bizim tezimizin konusu ise kodlama teorisinin hata düzeltme kısmı ile ilgilidir.

Kodlama teorisinin temelleri 1948 yılında Claude Shannon tarafından yayımlanan “ A Mathematical Theory of Communication ” adlı makale ile atılmıştır. Bu makalede Shannon eğer doğru kodlama ve kod çözme teknikleri kullanılırsa belirli bir oranda güvenilir iletişimin sağlanabileceğini ortaya koymuştur. Fakat bu yöntemlere somut bir örnek verememiştir (Shannon, 1948). Bu makaleyle uygun kodlama yöntemlerinin bulunmasına yoğunlaşılmasıyla birlikte kodlama teorisi de ortaya çıkmaya başlamıştır. Eşlik kodu, beşin ikisi kodu, tekrar kodu gibi birkaç basit hata düzeltici kodlar bulunsada bu alanda başarılı olan ilk somut örnek 1950 yılında Richard Hamming’in ürettiği tek hata düzeltici kodlardır (Hamming, 1950). Hamming’den kısa bir süre sonra 1954’te Müller çoklu hata düzelten kod sınıflarını tanımlamıştır. Aynı yıl içerisinde Reed’de bu kodları dekodlayan (çözümleyen) algoritmalar vermiştir (Reed, 1954). Fakat bu çalışmalar dahi Shannon’un

makalesinde bahsettiği çok güçlü kodlara nazaran zayıf kalmışlardır. 1950’li yılların sonlarına kadar daha iyi bir kod sınıfı bulunamamıştır. 1960 yılında Bose, Ray-Chaudhuri ve Hocquenghem çoklu hata düzelten BCH kodlarını ve aynı yıl içerisinde Reed, Solomon ve 1961’de bunlardan bağımsız olarak Arimoto’nun iki elemanlı olmayan (nonbinary) kanallar için bir kod sınıfını geliştirmesiyle büyük ilerlemeler katedilmiştir (Bose, vd., 1960; Reed ve Solomon, 1960; Arimoto, 1961). Tüm bu çalışmalar sonlu cisimler üzerinde tanımlanmışlardır.

Halkalar üzerindeki kodlar 1970’lerden itibaren çalışılmaya başlanmıştır. Hammons vd. tarafından 1994 yılında iyi parametrelere sahip kodlar, $\mathbb{Z}_4$ üzerindeki lineer kodların Gray görüntüsü olarak elde edilmiştir. Bu çalışmadan sonra araştırmaların büyük çoğunluğu halkalar üzerine yoğunlaşmıştır (Hammons, vd., 1994).

Bir kod; uzunluğu (n), eleman sayısı (M) ve minimum uzaklığı (d) olmak üzere üç parametreyle ifade edilir. Minimum uzaklığı büyük olan kodların hata düzeltme kapasiteleri daha büyük olduğundan d parametresi büyük kodlar elde etmek kodlama teorisinde önemli bir amaçtır. Bu doğrultuda keşfedilen yöntemlerden biri de sonlu cisimler ve sonlu halkalar üzerinde tanımlanan cyclic (devirli), quasi-cyclic (yarı devirli), nega-cyclic (negatif devirli) ve constacyclic (sabit devirli) kodlardır. Sonlu cisimler ile sonlu halkalar arasında Gray dönüşümü yardımıyla ilişkiler kurularak minimum uzaklığı yüksek kod sınıfları elde edilmiştir.

Cyclic kodlar ilk olarak 1957’de Prange tarafından bulunmuştur. Prange bu çalışmasında $\mathbb{F}_q$ cismi üzerinde n uzunluğundaki her bir cyclic koda denk gelen, $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ halkasının bir idealinin var olduğunu göstermiştir (Prange, 1957). Daha sonra cyclic kodlar genişletilerek; quasi-cyclic, nega-cyclic, constacyclic kodlar tanımlanmıştır.

İlk kez 2007’de D. Boucher, F. Ulmer ve W. Geiselmann skew (değişmeli olmayan) halkalar üzerinde skew cyclic kodları tanımlamışlardır. $\mathbb{F}_q$ sonlu bir cisim, θ aşikar otomorfizmadan farklı bir otomorfizma olmak üzere $\mathbb{F}_q[x; \theta]$ skew cyclic kodlar tanımlanmış ve bunların polinom temsilleri belirlenmiştir. θ otomorfizmasının mertebesi m olmak üzere $m|n$ olduğu durumlarda skew cyclic kodların, $\mathbb{F}_q[x]/$

$\langle x^n - 1 \rangle$ halkasının sol ideallerine karşılık geldiği gösterilmiştir (Boucher, vd., 2007).

Cyclic kodlardan skew cyclic kodlara geçişin başlıca nedeni, skew polinom halkaları tek türlü asal çarpanlara ayrılabilen halkalar olmadıklarından daha fazla bölen dolayısıyla daha fazla kod elde edilebilmesidir. Böylelikle cyclic kodlardan daha geniş bir sınıf ortaya çıkartılarak minimum uzaklığı yüksek olan kodlar elde etme olasılığı arttırılmıştır (Dertli, 2016).

2010 yılında İ. Şiap, T. Abualrub, N. Aydın ve P. Seneviretne tarafından skew cyclic kodların otomorfizmanın mertebesine bağlı olma kısıtlaması kaldırılıp keyfi uzunlukta skew cyclic kodlar tanımlanmıştır. Ayrıca n kodun uzunluğu, m otomorfizmanın mertebesi olmak üzere $(n, m) = 1$ olması durumunda skew cyclic kodun cyclic koda, $(n, m) = d$ olması durumunda quasi-cyclic koda denk olduğu gösterilmiştir (Şiap, vd., 2010).

2010 yılında T. Abualrub ve P. Seneviratne $v^2 = v$ olmak üzere $R = \mathbb{F}_2[v] / \langle v^2 - v \rangle$ sonlu halkası üzerinde skew cyclic kodları tanımlamışlardır. θ , R üzerinde tanımlı aşikâr otomorfizmadan farklı bir otomorfizma olmak üzere R halkası üzerinde uzunluğu n olan skew cyclic kodun, $R[x, \theta] / \langle x^n - 1 \rangle$ sonlu halkasının bir sol $R[x, \theta]$ -altmodülüne karşılık geldiği gösterilmiştir. Aynı yıl, T. Abualrub, N. Aydın, İ. Şiap ve P. Seneviratne skew-quasi cyclic kodları tanımlanmışlardır (Abualrub, vd., 2010).

2008 yılında D. Boucher, P. Sole ve F. Ulmer tarafından sonlu cisimler yerine Galois halkaları üzerinde tanımlı skew polinom halkaları kullanılarak skew constacyclic kodlar tanımlanmış ve $GR(4,2)$ üzerinde skew constacyclic self-dual kodlar verilmiştir (Boucher, vd., 2008).

2009 yılında S. Jitman, S. Ling ve P. Udomkavanich tarafından sonlu zincir halkaları üzerinde tanımlı skew constacyclic kodlar çalışılmıştır (Jitman, vd., 2009).

2012 yılında T. Abualrub, N. Aydın ve P. Seneviratne $v^2 = v$ olmak üzere $R = \mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, v + 1\}$ halkası üzerinde skew constacyclic kodları tanımlamışlardır (Abualrub, vd., 2012). Daha sonra 2016'da M. AL-Ashker ve M. Abu-Jazar P. bu tanımı p bir asal ve $v^2 = v$ olmak üzere $\mathbb{F}_p + v\mathbb{F}_p$ ye

geniřletmiřlerdir (AL-Ashker ve Abu-Jazar, 2016). 2017’de J. Gao, F. Ma ve F. Fu tarafından $q = p^r$ olmak üzere $\mathbb{F}_q + v\mathbb{F}_q$ halka ailesi üzerinde skew constacyclic kodları tanımlamıřlardır (Gao, vd., 2017).

2017 yılında H. İřlam ve O. Prakash $u^2 = u, v^2 = v$ ve $uv = vu = 0$ olmak üzere $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$ üzerinde skew cyclic ve skew constacyclic kodları vermiřlerdir (İřlam ve Prakash, 2017). 2018’de H. İřlam ve O. Prakash $u^2 = u, v^2 = v$ ve $uv = vu$ olarak bu tanıımı $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$ halka ailesine geniřletmiřlerdir (İřlam ve Prakash 2018).

Bu tez alıřmasında, ilk olarak tanımlanan $v_i^2 = v_i$, $v_1v_2 = v_2v_1$ ve $v_iv_j = v_jv_i = 0$ ($i = 1,2,3,4$, $i \neq j$, $j = 3,4$) olmak üzere sonlu ve deęiřmeli $B_q = \mathbb{F}_q + v_1\mathbb{F}_q + v_2\mathbb{F}_q + v_3\mathbb{F}_q + v_4\mathbb{F}_q + v_1v_2\mathbb{F}_q$ halka ailesinin zellikleri alıřılmıřtır. Daha sonra bu halka ailesi üzerinde ařıkır olmayan bir θ otomorfizması tanımlanmıř ve skew polinom halkası oluřturulmuřtur. Bylece $B_q = \mathbb{F}_q + v_1\mathbb{F}_q + v_2\mathbb{F}_q + v_3\mathbb{F}_q + v_4\mathbb{F}_q + v_1v_2\mathbb{F}_q$ halka ailesi üzerinde skew constacyclic kodlar tanımlanmıř ve zellikleri incelenmiřtir.

2. TEMEL KAVRAMLAR

Bu bölümde cebir ve kodlama teorisi ile ilgili temel bilgiler verilecektir.

Tanım 2.1. $R \neq \emptyset$ bir küme, “+” ve “ $\cdot$ ” R kümesinde ikili işlemler olsunlar

- i) $(R, +)$ değişmeli bir gruptur.
- ii) “ $\cdot$ ” işlemi R de birleşmelidir.
- iii) “ $\cdot$ ” işlemi “+” işlemi üzerine sağdan ve soldan dağılımlıdır. Yani $\forall a, b, c \in R$ için $a \cdot (b + c) = a \cdot b + a \cdot c$ ve $(a + b) \cdot c = a \cdot c + b \cdot c$.

aksiyomları sağlanıyorsa $(R, +, \cdot)$ cebirsel yapısına bir halka denir (Çallıalp, 2018).

“+” işlemine göre etkisiz elemana halkanın sıfırı denir ve 0_R ile gösterilir. Halkanın her zaman “ $\cdot$ ” işlemine göre etkisiz elemanı olmayabilir. Eğer varsa bu elemana birim eleman denir ve 1_R ile gösterilir. Birim elemanı var olan halkaya birimli halka denir. Eğer halkanın “ $\cdot$ ” işlemine göre değişme özelliği varsa yani $\forall a, b \in R$ için $a \cdot b = b \cdot a$ eşitliği sağlanıyorsa bu halkaya değişmeli halka adı verilir (Çallıalp, 2018).

Tanım 2.2. Sonlu sayıda elemana sahip halkaya sonlu halka adı verilir ve R sonlu halka ise eleman sayısı $|R|$ ile gösterilir (Hungerford, 1973).

Tanım 2.3. R halkası birimli bir halka olsun. Herhangi bir $a \in R$ elemanın tersi de R halkasında ise a elemanına birimsel eleman denir (Hungerford, 1973).

Tanım 2.4. R halkasında herhangi bir $0_R \neq a \in R$ elemanı için $a \cdot b = 0_R$ veya $b \cdot a = 0_R$ olacak şekilde $\exists 0_R \neq b \in R$ elemanı varsa a elemanına halkanın bir sıfır böleni denir (Çallıalp, 2018).

Örnek 2.5. $\mathbb{Z}$ tam sayılar halkası birimli, değişmeli ve sıfır böleni olmayan bir halkadır.

Tanım 2.6. Bir R halkasının her $a \in R$ elemanı için, $n \cdot a = 0$ eşitliğini sağlayan $n > 0$ tamsayılarının en küçüğüne R halkasının karakteristiği denir ve $\text{kar}R$

ile gösterilir. Eğer böyle bir n sayısı bulunamazsa halkanın karakteristiği sıfırdır (Hungerford, 1973).

Tanım 2.7. R bir halka ve $\emptyset \neq I \subset R$ olmak üzere

- i) $\forall a, b \in I$ için $a - b \in I$,
- ii) $\forall a \in I$ ve $\forall r \in R$ için $r \cdot a \in I$ (veya $a \cdot r \in I$)

şartları sağlanıyorsa I ya R nin bir sol (veya sağ) ideali denir (Çallıalp, 2018).

Eğer hem sağ hem de sol ideal olma şartı sağlanıyorsa I bir iki taraflı idealdir. İki taraflı ideale kısaca ideal denir.

Örnek 2.8. R herhangi bir halka olmak üzere halkanın sıfırından oluşan küme $\{0_R\}$ ve halkanın kendisi R bu halka üzerinde bir idealdirler. $\{0_R\}$ ve R ye aşık idealer denir. Bunların dışındaki ideallere de öz idealler denir (Çallıalp, 2018).

Tanım 2.9. A , R kümesinin bir alt kümesi olmak üzere R nin A yı içeren bütün ideallerinin kesişimine A nın ürettiği ideal adı verilir ve $\langle A \rangle$ ile gösterilir. Eğer $A = \{a\}$ tek elemandan oluşan bir küme ise A nın ürettiği ideal temel ideal olarak adlandırılır ve $\langle a \rangle$ ile gösterilir. Ve a elemanına A idealinin üretici adı verilir (Hungerford, 1973).

Tanım 2.10. R birimli ve değişmeli bir halka ve I da R nin bir ideali olsun. $I \neq \langle 1 \rangle$ olmak üzere eğer R halkasının I yı kapsayan I ve R nin dışında bir ideali yoksa I idealine R halkasının bir maksimal ideali adı verilir (Hungerford, 1973).

Tanım 2.11. I , R halkasının bir ideali olsun. $\forall r_1, r_2 \in R$ için

$$r_1 \equiv r_2 \pmod{I} \Leftrightarrow r_1 - r_2 \in I$$

bağıntısı bir denklik bağıntısıdır. Bu denklik bağıntısına göre oluşan tüm denklik sınıflarının kümesini R / I ile gösterirsek, R / I ;

$$(r + I) + (s + I) = (r + s) + I,$$

$$(r + I) \cdot (s + I) = (rs) + I$$

işlemleri ile birlikte bir halkadır. Bu halkaya R halkasının I idealine göre bölüm halkası adı verilir (Çallıalp, 2009).

Tanım 2.12. Bir tane maksimal ideali olan halkalara yerel (lokal) halka denir. Maksimal ideali sonlu sayıda olan halkalara ise yarı yerel (semi lokal) halka denir (Jitman, vd., 2010).

Tanım 2.13. R birimli, değişmeli ve sonlu bir halka olmak üzere eğer R deki tüm ideallerden oluşan küme kapsama bağıntısıyla tam sıralı ise R ye sonlu zincir halkası denir (Jitman, vd., 2010).

Tanım 2.14. R ve S iki halka, $f: R \rightarrow S$ bir fonksiyon olsun. $\forall a, b \in R$ için;

- i) $f(a + b) = f(a) + f(b)$
- ii) $f(ab) = f(a)f(b)$

koşulları sağlanıyorsa f fonksiyonuna R den S ye tanımlanan bir halka homomorfizması denir (Çallıalp, 2018).

Tanım 2.15. $f: R \rightarrow S$ homomorfizması birebir ve örten olma şartlarını sağlıyorsa f homomorfizmasına izomorfizma adı verilir. R den S ye bir izomorfizma tanımlanabiliyorsa R ve S halkalarına izomorf halkalar denir ve $R \cong S$ şeklinde gösterilir. Eğer $f: R \rightarrow R$ şeklinde tanımlanan bir izomorfizma ise f ye otomorfizma adı verilir (Fraleigh, 2003).

Tanım 2.16. R bir halka olsun. x bir bilinmeyen, $a_0, a_1, \dots, a_n$ 'ler R nin elemanları olmak üzere,

$$a_0 + a_1x + \dots + a_nx^n$$

şeklindeki ifadelere R den katsayılı polinom adı verilir. R den katsayılı tüm polinomlar kümesi $R[x]$ şeklinde gösterilir (Çallıalp, 2018).

Tanım 2.17. $p(x) = a_0 + a_1x + \dots + a_nx^n, R[x]$ üzerinde bir polinom olsun. $p(x) \neq 0$ ise en büyük dereceli terimin katsayısı a_n ye polinomun baş katsayısı ve en büyük derece n ye de polinomun derecesi denir. Bir $p(x)$ polinomunun derecesi $\deg p(x)$ ile gösterilir (Çallıalp, 2018).

Önerme 2.18. R bir halka olmak üzere

- i) R birimli ise $R[x]$ de birimli,
- ii) R değişmeli ise $R[x]$ de değişmelidir (Çallıalp, 2018).

Teorem 2.19. R değişmeli bir halka ve $f(x), g(x) \in R[x]$ olsun. $g(x) \neq 0$ ve $g(x)$ in baş katsayısı terslenebilir bir eleman ise,

$$f(x) = q(x)g(x) + r(x) \text{ ve } d^0 r < d^0 g$$

olacak şekilde tek türlü $\exists q(x), r(x) \in R[x]$ polinomları bulunabilir (Çallıalp, 2018).

Tanım 2.20. Bir polinomun baş katsayısı 1 ise bu polinoma monik polinom denir (Çallıalp, 2013).

Tanım 2.21. $(M, +)$ bir değişmeli grup, $(R, +, \cdot)$ bir halka olmak üzere,

$$*: R \times M \rightarrow M$$

$$(r, m) \rightarrow r * m \in M$$

fonksiyonu,

- i) $\forall r \in R \text{ ve } \forall m_1, m_2 \in M \text{ için, } r * (m_1 + m_2) = r * m_1 + r * m_2,$
- ii) $\forall r_1, r_2 \in R \text{ ve } \forall m \in M \text{ için, } (r_1 + r_2) * m = r_1 * m + r_2 * m,$
- iii) $\forall r_1, r_2 \in R \text{ ve } \forall m \in M \text{ için, } (r_1 \cdot r_2) * m = r_1 * (r_2 * m)$

koşullarını sağlıyorsa M ye R üzerinde bir sol R -modül denir. Eğer bu fonksiyon R halkası birimli ve birimi 1_R olmak üzere

- iv) $\forall m \in M \text{ için, } 1_R * m = m$

koşulunu da sağlıyorsa, M ye birimli sol R -modül denir (Çallıalp, 2009).

Bu tanıma benzer şekilde sağ R -modül de tanımlanabilir. Eğer M hem sağ hem de sol modül şartlarını sağlıyorsa M ye R -modül denir.

Tanım 2.22. R bir halka, M bir R -modül olmak üzere eğer M nin boştan farklı N altkümesi de bir R -modül oluyorsa N ye, M nin bir altmodülü veya R -altmodül adı verilir (Çallıalp, 2009).

Tanım 2.23. R birimli ve değişmeli bir halka olmak üzere eğer $R^* = R - \{0_R\}$ kümesi de “.” işlemine göre bir grup ise R halkasına cisim adı verilir (Çallıalp, 2018).

Örnek 2.24. $\mathbb{Q}$, $\mathbb{R}$ ve $\mathbb{C}$ kümeleri bir cisimdirler. Fakat $\mathbb{Z}$ bir cisim değildir (Çallıalp, 2018).

Tanım 2.25. Eleman sayısı sonlu olan cisme sonlu cisim adı verilir (Roman, 1992).

Önerme 2.26. p asal ise $\mathbb{Z}_p$, p elemanlı bir cisimdir.

Teorem 2.27. $1 < q \in \mathbb{Z}$ olmak üzere q elemanlı bir cismin var olması için gerek ve yeter koşul $q = p^n$ ($n \in \mathbb{N}$) olacak şekilde bir p asalının var olmasıdır (Roman, 1992).

Tanım 2.28. p bir asal ve $q = p^n$ ($n \in \mathbb{N}$) olsun. q elemanlı bir cisme Galois cismi denir. $\text{GF}(q)$ veya $\mathbb{F}_q$ ile gösterilir (Roman, 1992).

Not 2.29. p asal olmak üzere $\mathbb{F}_q \cong \mathbb{Z}_p$ dir ve $|\mathbb{F}_q^n| = q^n$ dir.

Örnek 2.30. $\mathbb{F}_5 \cong \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

Teorem 2.31. $\mathbb{F}$ sonlu bir cisim ise karakteristiği asal bir sayıdır. Ayrıca $\text{kar}\mathbb{F} = p$ ise $\mathbb{F}$, $q = p^n$ ($n \in \mathbb{Z}$) elemanlıdır (Roman, 1992).

Teorem 2.32. $\mathbb{F}_q[x]$ üzerinde $\text{der}p(x) = d$ olan $p(x)$ asal polinomunu alalım. $\mathbb{F}_q[x]/\langle p(x) \rangle$ bölüm halkası bir cisimdir ve

$$\mathbb{F}_q[x]/\langle p(x) \rangle = \{r(x) + \langle p(x) \rangle : \text{der}[r(x)] < d, r(x) \in \mathbb{F}_q[x]\}$$

şeklindedir (Roman, 1992).

Örnek 2.33. $\text{GF}(16)$ cismi için

$$\text{GF}(16) \cong \text{GF}(2)[x]/\langle x^4 + x^2 + 1 \rangle \cong \mathbb{Z}_2[x]/\langle x^4 + x^2 + 1 \rangle$$

dir.

Tanım 2.34. $\mathbb{F}_q$, karakteristiği p asalı olan bir cisim olsun. $a \in \mathbb{F}_q$ olmak üzere

$$\begin{aligned} \theta: \mathbb{F}_q &\rightarrow \mathbb{F}_q \\ a &\rightarrow \theta(a) = a^p \end{aligned}$$

şeklinde tanımlanan θ otomorfizmasına Frobenius otomorfizması denir (Wan, Z. X., 2003).

Tanım 2.35. $(V, \oplus)$ değişmeli grup ve $(\mathbb{F}_q, +, \cdot)$ bir cisim olsun

$$g: \mathbb{F}_q \times V \rightarrow V$$

$$(a, v) \mapsto g(a, v) = a \odot v$$

şeklindeki g fonksiyonu aşağıdaki özellikleri sağlıyorsa V değişmeli grubuna $\mathbb{F}_q$ cismi üzerinde bir vektör uzayı adı verilir (Çallıalp ve Kuruoğlu, 1996).

- i) Her $a, b \in \mathbb{F}_q$ ve her $u, v \in V$ için $a \odot (u \oplus v) = (a \odot u) \oplus (a \odot v)$ dir
- ii) Her $a, b \in \mathbb{F}_q$ ve her $v \in V$ için $(a + b) \odot v = (a \odot v) \oplus (b \odot v)$ dir
- iii) Her $a, b \in \mathbb{F}_q$ ve her $v \in V$ için $(a \cdot b) \odot v = a \odot (b \odot v)$ dir.
- iv) $1 \in \mathbb{F}$ ve her $v \in V$ için $1 \odot v = v$ dir.

Tanım 2.36. $V, \mathbb{F}_q$ cismi üzerinde tanımlı bir vektör uzayı olmak üzere V nin herhangi bir $\emptyset \neq W \subseteq V$ alt kümesi tanım 2.35. deki özelliklere göre bir vektör uzayı ise W ye V nin bir alt uzayı denir (Çallıalp ve Kuruoğlu, 1996).

Teorem 2.37. $V, \mathbb{F}_q$ cismi üzerinde tanımlı bir vektör uzayı olsun. $\emptyset \neq W \subseteq V$ olmak üzere W kümesinin V vektör uzayının bir alt uzayı olması için gerek ve yeter koşul $\forall w_1, w_2 \in W$ ve $\forall a, b \in \mathbb{F}_q$ için,

$$(a \odot w_1) \oplus (b \odot w_2) \in W$$

olmasıdır (Çallıalp ve Kuruoğlu, 1996).

Tanım 2.38. $V, \mathbb{F}_q$ cismi üzerinde bir vektör uzayı olsun. $v_1, v_2, \dots, v_n \in V$ birbirinden farklı vektörler ve $a_1, a_2, \dots, a_n \in \mathbb{F}_q$ olmak üzere

$$a_1 v_1 + a_2 v_2 + \dots + a_n v_n = 0$$

iken

$$a_1 = a_2 = \dots = a_n = 0$$

oluyorsa $v_1, v_2, \dots, v_n$ vektörleri lineer bağımsızdır denir. $a_1, a_2, \dots, a_n$ katsayılarından en az biri sıfırdan farklıysa bu vektörlere lineer bağımlıdır denir (Ling ve Xing, 2004).

Tanım 2.39. $V, \mathbb{F}_q$ cismi üzerinde bir vektör uzayı olsun. $v_1, v_2, \dots, v_n \in V$ ve $a_1, a_2, \dots, a_n \in \mathbb{F}_q$ olmak üzere her $v \in V$ elemanı $v = a_1 v_1 + a_2 v_2 + \dots + a_n v_n$ şeklinde yazılabiliyorsa, $v_1, v_2, \dots, v_n$ vektörleri V vektör uzayını üretiyor (geriyor) denir (Ling ve Xing, 2004).

Tanım 2.40. $V, \mathbb{F}_q$ cismi üzerinde bir vektör uzayı ve $v_1, v_2, \dots, v_n \in V$ olmak üzere $v_1, v_2, \dots, v_n$ vektörleri lineer bağımsız ve V vektör uzayını geriyorsa $\{v_1, v_2, \dots, v_n\}$ kümesine V vektör uzayının bir tabanı (bazı) denir. Tabandaki toplam vektör sayısına da V vektör uzayının boyutu denir ve $boy(V)$ ile gösterilir (Ling ve Xing, 2004).

Tanım 2.41. V vektör uzayının iki alt uzayı, W_1, W_2 olsun.

- i) $V = W_1 + W_2$
- ii) $W_1 \cap W_2 = \{0_v\}$

yukarıdaki koşullar sağlanıyorsa V vektör uzayına W_1 ve W_2 alt uzaylarının direkt toplamı denir ve $V = W_1 \oplus W_2$ ile gösterilir (Çallıalp ve Kuruoğlu, 1996).

Tanım 2.42. $A = \{a_1, a_2, \dots, a_q\}$, q elemanlı bir küme olsun. Her $i \in \{1, 2, \dots, n\}$ için $u_i \in A$ olmak üzere $u = u_1 u_2 u_3 \dots u_n$ elemanına A kümesi üzerinde uzunluğu n olan bir q -ary (q -lu) sözcüğü denir. Aynı zamanda u , $u = (u_1, u_2, u_3, \dots, u_n)$ şeklinde bir vektör olarak düşünülebilir (Ling ve Xing, 2004).

Tanım 2.43. $\emptyset \neq C \subseteq A^n$ kümesine, A üzerinde uzunluğu n olan bir q -lu blok kod denir. C kodunun elemanlarına kod sözcüğü adı verilir (Ling ve Xing, 2004).

Not 2.44. C kodunun eleman sayısı $|C|$ şeklinde gösterilir (Ling ve Xing, 2004).

Tanım 2.45. $\emptyset \neq C \subseteq A^n$ kümesinin eleman sayısı M ise C koduna n uzunluğunda M elemanlı bir kod denir ve (n, M) -kod şeklinde gösterilir (Ling ve Xing, 2004).

Tanım 2.46. $A = \{a_1, a_2, \dots, a_q\}$ kümesine kod alfabesi denir. A^n kümesinin her bir elemanına da sözcük adı verilir (Ling ve Xing, 2004).

Örnek 2.47. $\mathbb{F}_3 = \{0, 1, 2\}$ kod alfabesi üzerinde tanımlanan bir koda üçlü kod denir.

- i) $C_1 = \{(0,0,0), (0,1,0), (0,1,2)\}$ bir $(3,3)$ -koddur.
- ii) $C_2 = \{(0,0,0,0), (0,1,2,1), (0,0,1,1), (0,2,1,1), (1,1,1,1)\}$ bir $(4,5)$ -koddur.
- iii) $C_3 = \{(0,1,0,2,1), (1,1,1,1,1), (2,1,0,2,1)\}$ bir $(5,3)$ -koddur.

Tanım 2.48. R sonlu bir halka ve $n \in \mathbb{Z}^+$ olmak üzere

$$R^n = \{(u_1, u_2, \dots, u_n) : u_i \in R, i = 1, 2, \dots, n\}$$

kümesinin eleman sayısı M olan bir C , R -altmodülüne uzunluğu n eleman sayısı M olan bir lineer kod denir. C nin elemanlarına kod sözcüğü, R^n kümesinin herhangi bir elemanına sözcük adı verilir (Huffman ve Pless, 2003).

Tanım 2.49.

$$V(n, q) = \mathbb{F}_q^n = \{x = (x_1, x_2, \dots, x_n) : x_i \in \mathbb{F}_q, i = 1, 2, \dots, n\}$$

kümesi $\mathbb{F}_q$ üzerinde boyutu n olan bir vektör uzayı olmak üzere $\emptyset \neq C \subseteq \mathbb{F}_q^n$ alt uzayına bir lineer kod adı verilir. C , $\mathbb{F}_q^n$ vektör uzayının boyutu k olan bir alt uzayı olmak üzere C ye bir $[n, k]$ -kod denir (Hill, 1986).

Tanım 2.50. Her $a = (a_1, a_2, \dots, a_n), b = (b_1, b_2, \dots, b_n) \in \mathbb{F}_q^n$ için

$$d : \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{N} \cup \{0\}$$

$$(a, b) \mapsto d(a, b) = |\{i : a_i \neq b_i\}|$$

dönüşümüne Hamming uzaklığı adı verilir (Huffman ve Pless, 2003).

Lemma 2.51. d , Hamming uzaklığı

- i) $\forall a, b \in \mathbb{F}_q^n$ için $d(a, b) \geq 0$, $d(a, b) = 0 \Leftrightarrow a = b$
- ii) $\forall a, b \in \mathbb{F}_q^n$ için $d(a, b) = d(b, a)$
- iii) $\forall a, b, c \in \mathbb{F}_q^n$ için $d(a, b) \leq d(a, c) + d(c, b)$ (üçgen eşitsizliği)

özellikleriyle birlikte bir metriktir (Hill, 1986).

Tanım 2.52. Bir C kodunun minimum uzaklığı

$$d = d(C) = \min\{d(x, y) : x \neq y, x, y \in C\}$$

şeklinde tanımlanır. n uzunluklu, M elemanlı ve d minimum uzaklığına sahip bir C koduna (n, M, d) -kod denir (Hill, 1986).

Uzunluğu n , boyutu k olan bir lineer kod, d minimum uzaklığıyla birlikte $[n, k, d]$ şeklinde gösterilir.

C , bir $[n, k, d]$ -kod ise eleman sayısı q^k , kodun oranı $\frac{k}{n}$ dir.

Tanım 2.53. Herhangi bir $x \in \mathbb{F}_q^n$ olmak üzere x deki sıfırdan farklı bileşen sayısına x in Hamming ağırlığı denir ve $w(x)$ ya da $w_H(x)$ ile gösterilir (Hill, 1986).

Bir C kodunda sıfırdan farklı olan kod sözcüklerinin Hamming ağırlıklarının en küçük değerine, C kodunun minimum ağırlığı denir ve $w(C)$ ya da $w_H(C)$ ile gösterilir.

Lemma 2.54. $x, y, \mathbb{F}_q^n$ vektör uzayının herhangi iki elemanı olmak üzere

$$d(x, y) = w(x - y)$$

dir (Roman, 1992).

Teorem 2.55. Bir C lineer kodunun minimum uzaklığı ile minimum ağırlığı eşittir (Roman, 1992).

Örnek 2.56. $\mathbb{F}_3$ üzerinde tanımlanan $C = \{(0,1,0,1,2), (0,0,2,2,1), (2,2,0,1,1)\}$, lineer olmayan kodunu alalım

$$d((0,1,0,1,2), (0,0,2,2,1)) = 4$$

$$d((0,1,0,1,2), (2,2,0,1,1)) = 3$$

$$d((0,0,2,2,1), (2,2,0,1,1)) = 4$$

dir. $d = d(C) = \min\{d(x, y) : x \neq y, x, y \in C\}$ olduğundan $d = 3$ dir. O halde C kodu $(5,3,3)$ -koddur.

Tanım 2.57. $C, \mathbb{F}_q$ üzerinde tanımlı lineer bir $[n, k]$ -kod olmak üzere satırları C kodunun taban elemanlarından oluşan $k \times n$ mertebeli matrise C kodunun üreteç matrisi denir ve G ile gösterilir. G üreteç matrisi, I_k birim matris ve A , mertebesi $k \times (n - k)$ olan bir matris olmak üzere $(I_k | A)$ olacak şekilde düzenlenirse, $(I_k | A)$ matrisine G matrisinin standart formu adı verilir (Hill, 1986).

Örnek 2.58. $\mathbb{F}_3$ üzerinde tanımlı

$$C = \{(0,0,0,0), (1,2,0,2), (1,1,2,2), (2,0,2,1)\}$$

kodunun bir tabanı

$$S = \{(1,2,0,2), (1,1,2,2)\}$$

olduğu için $G = \begin{bmatrix} 1202 \\ 1122 \end{bmatrix}_{2 \times 4}$ matrisi, C kodunun üreteç matrisidir. C kodu $\mathbb{F}_3$ üzerinde tanımlı bir $[4,3,2]$ -koddur.

Kodun parametreleri hakkındaki bazı bilgiler aşağıdaki gibidir:

C , bir (n, M, d) -kod olsun. Kodun eleman sayısı ne kadar büyük ise kod o kadar fazla mesajı kodlar, minimum uzaklığı ne kadar büyük ise de o oranda fazla hatayı düzeltebilir. Kodun eleman sayısı ile minimum uzaklığı ters orantılıdır. Yani biri büyüdükçe diğeri küçülmektedir.

C , q elemanlı kod alfabesinin üzerinde tanımlanan n uzunluğunda, d minimum uzaklıklı bir kod olsun. C nin alabileceği en yüksek eleman sayısı $A_q(n, d)$ şeklinde gösterilir.

$\mathbb{F}_q$ üzerinde tanımlı uzunluğu n , boyutu k olan bir lineer kodun alabileceği en yüksek d , minimum uzaklık değeri $d_q(n, k)$ ile, uzunluğu n , minimum uzaklığı d olan bir kodun alabileceği en büyük M , eleman sayısı ise $B_q(n, d)$ ile gösterilir. Kodlama teorisinin en önemli problemlerinden biri de $d_q(n, k)$ ve $B_q(n, d)$ nin belirlenmesidir. Ayrıca $B_q(n, d) \leq A_q(n, d)$ dir (Hill, 1986).

Teorem 2.59. C , d minimum uzaklığa sahip bir kod olsun.

- i) $d \geq k + 1$ ise C kodu herhangi bir kod sözcüğündeki k tane hatayı tespit eder.
- ii) $d \geq 2t + 1$ ise C kodu herhangi bir kod sözcüğündeki t tane hatayı düzeltir (Hill, 1986).

Sonuç 2.60. d minimum uzaklığa sahip olan bir C kodu, herhangi bir kod sözcüğünde $d - 1$ tane hatayı tespit etmekte ya da $\left\lfloor \frac{d-1}{2} \right\rfloor$ tane hatayı düzeltmekte kullanılır (Ling ve Xing, 2004).

Tanım 2.61. Her $u = (u_1, u_2, \dots, u_n)$, $v = (v_1, v_2, \dots, v_n) \in F_q^n$ elemanları için

$$\begin{aligned} \cdot : \mathbb{F}_q^n \times \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q \\ (u, v) &\mapsto u \cdot v = u_1 v_1 + \dots + u_n v_n \end{aligned}$$

biçiminde tanımlanan dönüşüme bir iç çarpım adı verilir. $u \cdot v = 0$ ise u ile v birbirine diktir denir (Hill, 1986).

Tanım 2.62. C , $\mathbb{F}_q$ üzerinde tanımlı bir $[n, k]$ -kod olmak üzere

$$C^\perp = \{v \in \mathbb{F}_q^n : u \cdot v = 0, \forall u \in C\}$$

kümesine C kodunun duali adı verilir. $C^\perp = C$ ise C koduna self-dual kod, $C \subseteq C^\perp$ ise C koduna self-ortogonal kod denir (Ling ve Xing, 2004).

Teorem 2.63. C , $\mathbb{F}_q$ üzerinde tanımlı bir $[n, k]$ -kod olmak üzere

- i) $|C| = q^k$,
- ii) $C^\perp$ de bir lineer koddur ve $\text{boy}(C) + \text{boy}(C^\perp) = n$,
- iii) $(C^\perp)^\perp = C$

dir (Ling ve Xing, 2004).

Teorem 2.64. C , $\mathbb{F}_q$ üzerinde tanımlı bir $[n, k]$ -kod ve

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}_{k \times n}$$

C kodunun üreteç matrisi olsun. $v = (v_1, v_2, \dots, v_n) \in \mathbb{F}_q^n$ olmak üzere $v \in C^\perp$ olması için gerek ve yeter koşul $[v_1 \ v_2 \ \dots \ v_n]_{1 \times n} G_{n \times k}^T = 0$ olmasıdır (Hill, 1986).

Önerme 2.65. C , $\mathbb{F}_q$ üzerinde tanımlı bir $[n, k]$ -kod ise $C^\perp$ de $\mathbb{F}_q$ üzerinde tanımlı bir $[n, n - k]$ -koddur (Hill, 1986).

Tanım 2.66. C bir $[n, k]$ -kod olsun. $C^\perp$ nin üreteç matrisine C kodunun kontrol (parity-check) matrisi adı verilir ve H ile gösterilir (Hill, 1986).

Teorem 2.67. C , $\mathbb{F}_q$ üzerinde tanımlı bir $[n, k]$ -kod olsun C kodunun üreteç matrisi G ve kontrol matrisi H olmak üzere $GH^T = 0$ dır (Hill, 1986).

Not 2.68. C kodu kontrol matrisi H olmak üzere

$$C = \{(v_1, v_2, \dots, v_n) \in \mathbb{F}_q^n : [v_1 \ v_2 \ \dots \ v_n]H^T = 0\}$$

şeklinde de ifade edilebilir (Hill, 1986).

Teorem 2.69. C bir lineer kod ve kontrol matrisi H olsun.

- i) $d(C) \geq d$ olması için gerek ve yeter koşul kontrol matrisi H nin herhangi $d - 1$ sütunun lineer bağımsız olmasıdır.
- ii) $d(C) \leq d$ olması için gerek ve yeter koşul kontrol matrisi H nin herhangi d sütunun lineer bağımlı olmasıdır.
- iii) $d(C) = d$ olması için gerek ve yeter koşul kontrol matrisi H nin herhangi $d - 1$ sütunun lineer bağımsız ve en az d sütunun da lineer bağımlı olmasıdır (Ling ve Xing, 2004).

Teorem 2.70. C bir $[n, k]$ -kod olmak üzere G üreteç matrisinin standart formu $G = (I_k \mid A)$ ise C kodunun kontrol matrisi $H = (-A^T \mid I_{n-k})$ dir (Hill, 1986).

Tanım 2.71. C , $\mathbb{F}_q^n$ vektör uzayının bir alt kümesi olsun. Her $c = (c_0, c_1, \dots, c_{n-1}) \in C$ için $\sigma(c) = (c_{n-1}, c_0, \dots, c_{n-2}) \in C$ ise C kümesine devirli küme adı verilir. C lineer kod iken aynı zamanda devirli bir küme ise bu koda cyclic (devirli) kod denir (Hill, 1986).

Teorem 2.72.

$$\pi: \mathbb{F}_q^n \rightarrow \mathbb{F}_q[x] / \langle x^n - 1 \rangle$$

$a = (a_0, a_1, \dots, a_{n-1}) \mapsto \pi(a) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + \langle x^n - 1 \rangle = \overline{a(x)}$ ile tanımlı π $\mathbb{F}_q$ -vektör uzayı izomorfizması olmak üzere C , $\mathbb{F}_q$ üzerinde tanımlı uzunluğu n olan bir cyclic kod olması için gerekli ve yeterli koşul $\pi(C) = I$ nin $\mathbb{F}_q[x] / \langle x^n - 1 \rangle$ halkasının bir ideali olmasıdır (Ling ve Xing, 2004).

π dönüşümü yardımıyla C kodunun herhangi bir $a = (a_0, a_1, \dots, a_{n-1})$ elemanı $\mathbb{F}_q[x] / \langle x^n - 1 \rangle$ bölüm halkasının bir $\pi(a) = \overline{a(x)} = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + \langle x^n - 1 \rangle$ denklik sınıfına karşılık gelir. Fakat kolay ve sade gösterim için $a_0 + a_1x + \dots + a_{n-1}x^{n-1} + \langle x^n - 1 \rangle$ denklik sınıfı yerine $a(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ polinomu kullanılır. Buradan bir cyclic kodun herhangi bir elemanını ona karşılık gelen polinom gösterimi ile yazmak mümkün olur.

Tanım 2.73. I , $\mathbb{F}_q[x] / \langle x^n - 1 \rangle$ halkasının bir ideali ve $g(x)$ bu idealin en küçük dereceli, sıfırdan farklı ve monik bir polinomu olsun.

- i) $g(x)$ polinomu I nın üreticidir ve tektir.
- ii) $g(x)$ polinomu $x^n - 1$ polinomunu böler (Ling ve Xing, 2004).

Bundan sonraki kısımlarda kolaylık olması için $\pi(C)$ yerine C gösterimini kullanacağız.

Tanım 2.74. $C, \mathbb{F}_q$ üzerinde tanımlı uzunluğu n olan bir cyclic kod ve bu koda karşılık gelen sıfırdan farklı en küçük dereceye sahip monik polinomda $g(x)$ olsun. $g(x)$ polinomuna C kodunun üreteç polinomu denir ve

$$C = \langle g(x) \rangle = \{f(x) \cdot g(x) : f(x) \in \mathbb{F}_q[x]/\langle x^n - 1 \rangle\}$$

şeklinde gösterilir. (Ling ve Xing, 2004).

Teorem 2.75. $\mathbb{F}_q[x]$ halkasında, $x^n - 1$ polinomunun her monik böleni $\mathbb{F}_q$ üzerinde tanımlı bir cyclic kod üretir (Ling ve Xing, 2004).

Teorem 2.76. $\deg(g(x)) = r$ olmak üzere $g(x) = g_0 + g_1x + \dots + g_rx^r$ polinomu n uzunluğundaki C devirli kodunun üreteç polinomu olsun. C kodunun boyutu $\text{boy}(C) = n - r = k$ ve devirli kodun üreteç matrisi

$$G = \begin{bmatrix} g(x) \\ x \cdot g(x) \\ x^2 \cdot g(x) \\ \vdots \\ x^{k-1} \cdot g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & \ddots & & & \vdots \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_r \end{bmatrix}$$

dir (Hill, 1986).

Teorem 2.77. $C_1 = \langle g_1(x) \rangle$ ve $C_2 = \langle g_2(x) \rangle$ iki cyclic kod olmak üzere

- i) $C_1 \subseteq C_2$ olması için gerek ve yeter koşul $g_2(x) | g_1(x)$ olmasıdır.
- ii) $C_1 \cap C_2 = \langle \text{obeb}\{g_1(x), g_2(x)\} \rangle$
- iii) $C_1 + C_2 = \langle \text{okek}\{g_1(x), g_2(x)\} \rangle$ dir (Huffman ve Pless, 2003).

Teorem 2.78. $h(x) = a_0 + a_1x + \dots + a_kx^k$, $\deg(h(x)) = k$ olmak üzere

$$h^*(x) = x^k h(x^{-1}) = a_k + a_{k-1}x + \dots + a_0x^k$$

polinomuna $h(x)$ polinomunun ters sıralı (reciprocal) polinomu denir (Ling ve Xing, 2004).

Teorem 2.79. $C, \mathbb{F}_q$ üzerinde tanımlı bir cyclic $[n, k]$ -kod, $g(x)$ polinomu C kodunun üreteç polinomu, $x^n - 1 = g(x)h(x)$ ve $h(x) = h_0 + h_1x + \dots + h_kx^k$ olsun.

i) $h(x)$, C kodunun kontrol polinomu olmak üzere C kodunun kontrol matrisi

$$H = \begin{bmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & \ddots & & & \vdots \\ 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0 \end{bmatrix}$$

ii) C kodunun duali $C^\perp$ cyclic koddur ve $h_0^{-1}h^*(x)$ polinomu $C^\perp$ nin üreteç polinomudur (Ling ve Xing, 2004).

Teorem 2.80. $C, \mathbb{F}_q$ üzerinde tanımlı n uzunluğunda bir cyclic kod, C kodunun üreteç polinomu $g(x)$ ve kontrol polinomu $h(x)$ olsun. $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ halkasında bir $c(x)$ elemanına karşılık gelen $(c_0, c_1, \dots, c_{n-2}, c_{n-1})$ sıralı n -lisinin C kodunun kod sözcüğü olması için gerek ve yeter koşul $c(x)h(x) = 0$ olmasıdır (Hill, 1986).

Tanım 2.81. $n = s \cdot l$ ve $\emptyset \neq C \subseteq \mathbb{F}_q^n$ olsun.

i) $C, \mathbb{F}_q^n$ kümesinin bir alt uzayı,

ii) Her $c = (c_{0,0}, c_{0,1}, \dots, c_{0,l-1}, c_{1,0}, \dots, c_{1,l-1}, \dots, c_{s-1,0}, \dots, c_{s-1,l-1}) \in C$ için

$$T_{s,l}(c) = (c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,l-1}, c_{0,0}, \dots, c_{0,l-1}, \dots, c_{s-2,0}, \dots, c_{s-2,l-1}) \in C$$

koşulları sağlanıyorsa C ye $n = s \cdot l$ uzunluğunda l indeksli bir quasi-cyclic (yarı-devirli) kod denir (Bhaintwal M., Wasan S. K., 2009).

$l = 1$ alınırsa quasi-cyclic kod tanımı cyclic kod tanımı ile çakışır.

Tanım 2.82. R sonlu bir halka, $\lambda \in R$ bir birimsel bir eleman, C, R üzerinde tanımlı bir lineer kod olsun. σ_λ dönüşümü her $c = (c_0, c_1, \dots, c_{n-1}) \in R^n$ için $\sigma_\lambda(c) = (\lambda c_{n-1}, c_0, \dots, c_{n-2}) \in R^n$ şeklinde constacyclic shift (sabit devirli öteleme) olarak tanımlansın. Eğer $\sigma_\lambda(C) = C$ oluyorsa C koduna R üzerinde tanımlı bir λ -constacyclic (sabit devirli) kod adı verilir (Qian J.i vd., 2006).

Not 2.83. Bu tanım, $\lambda = 1$ ise cyclic kod tanımıyla, $\lambda = -1$ olursa nega-cyclic kod tanımıyla çakışır.

Teorem 2.84. R sonlu bir halka olsun. C , R üzerinde tanımlı n uzunluğa sahip bir lineer kod olmak üzere $c = (c_0, c_1, \dots, c_{n-1}) \in C$ için

$$\pi: R^n \rightarrow R[x] / \langle x^n - 1 \rangle$$

$$c = (c_0, c_1, \dots, c_{n-1}) \mapsto \pi(c) = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1} + \langle x^n - 1 \rangle$$

dönüşümü verilsin. C kodunun cyclic bir kod olması için gerek ve yeter koşul $\pi(C)$ kümesinin $R[x] / \langle x^n - 1 \rangle$ halkasının bir ideali olmasıdır (Ling ve Xing, 2004).

Teorem 2.85. R sonlu bir halka olsun. C , R üzerinde tanımlı n uzunluğa sahip bir lineer kod olmak üzere $c = (c_0, c_1, \dots, c_{n-1}) \in C$ için

$$\pi: R^n \rightarrow R[x] / \langle x^n - \lambda \rangle$$

$$c = (c_0, c_1, \dots, c_{n-1}) \mapsto \pi(c) = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1} + \langle x^n - \lambda \rangle$$

dönüşümü verilsin. C kodunun λ -constacyclic kod olması için gerek ve yeter koşul $\pi(C)$ kümesinin $R[x] / \langle x^n - \lambda \rangle$ halkasının bir ideali olmasıdır (Ling ve Xing, 2004).

Tanım 2.86. θ , $\mathbb{F}_q$ üzerinde aşık ar olmayan bir otomorfizma olmak üzere

$$\mathbb{F}_q[x, \theta] = \{ a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in \mathbb{F}_q, \forall i \in \{0, 1, 2, \dots, n\} \}$$

kümesine skew polinomlar kümesi denir.

Bu küme üzerinde toplama işlemi polinomlardaki standart toplama işlemi olup, çarpma işlemi ise,

$$(ax^i) * (bx^j) = a\theta^i(b)x^{i+j}$$

kuralı ile belirlidir (McDonald, 1974).

Teorem 2.87. Polinomlardaki standart toplama işlemi ve Tanım 2.86 da tanımlanan çarpma işlemiyle birlikte $\mathbb{F}_q[x, \theta]$ kümesi bir halkadır. Ayrıca $\mathbb{F}_q[x, \theta]$ değişmeli olmayan bir halkadır.

Bu halkaya skew polinom halkası denir.

Tanım 2.88. θ , $\mathbb{F}_q$ üzerinde tanımlı aşık ar olmayan bir otomorfizma olsun. C , $\mathbb{F}_q^n$ uzayının boştan farklı bir alt kümesi olmak üzere

i) C , $\mathbb{F}_q^n$ uzayının bir alt uzayı ve

ii) $\forall c = (c_0, c_1, \dots, c_{n-1}) \in C$ için $\sigma(c) = (\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})) \in C$

oluyorsa C kümesine n uzunluğunda skew cyclic (devirli) kod denir. σ dönüşümüne skew cyclic shift (skew devirsel öteleme) denir.

$$\pi: \mathbb{F}_q^n \rightarrow \mathbb{F}_q[x, \theta]/\langle x^n - 1 \rangle$$

$$c = (c_0, c_1, \dots, c_{n-1}) \rightarrow \pi(c) = c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$$

dönüşümü bir izomorfizmadır. $\sigma(c)$ skew cyclic shift ötelemesi polinom yazılımında

$$x * c(x) = \theta(c_{n-1}) + \theta(c_0)x + \dots + \theta(c_{n-2})x^{n-2}$$

ifadesine karşılık gelir.

C , $\mathbb{F}_q$ üzerinde tanımlı n uzunluğunda skew cyclic kod iken $\pi(C)$ $\mathbb{F}_q[x, \theta]/\langle x^n - 1 \rangle$ halkasının bir sol idealidir.

C , $\mathbb{F}_q$ cismi üzerinde tanımlı n uzunluğunda skew cyclic kod ve $|\langle \theta \rangle| = m$ olsun. Skew cyclic kodlar tanımlanırken iki durum söz konusudur;

- i) Eğer $m|n$ ise $\mathbb{F}_q[x, \theta]/\langle x^n - 1 \rangle$ kümesi bir halkadır ve $\pi(C)$, $\mathbb{F}_q[x, \theta]/\langle x^n - 1 \rangle$ halkasının bir sol idealidir. Boucher vd. skew cyclic kodların tanımını yalnızca $m|n$ olduğu durumlara kısıtlamışlardır.
- ii) Eğer $m \nmid n$ ise $\mathbb{F}_q[x, \theta]/\langle x^n - 1 \rangle$ kümesi bir halka değildir. Şiap vd. çalışmalarında herhangi bir n değeri için $\pi(C)$ yi $\mathbb{F}_q[x, \theta]/\langle x^n - 1 \rangle$ in bir sol altmodülü olarak ele almış ve $m|n$ olma kısıtlamasını kaldırmışlardır. Böylelikle herhangi bir uzunluk için skew cyclic kodlar tanımlanabilmiştir (Şiap, 2011).

Bundan sonra kolaylık olması açısından $\pi(C)$ yerine C gösterimi kullanılacaktır.

Teorem 2.89. C , $\mathbb{F}_q$ üzerinde tanımlı uzunluğu n olan bir lineer kod olsun. C kodunun skew cyclic kod olması için gerek ve yeter koşul C nin $\mathbb{F}_q[x, \theta]/\langle x^n - 1 \rangle$ modülünün bir sol $\mathbb{F}_q[x, \theta]$ -altmodülü olmasıdır (Şiap, 2011).

Teorem 2.90. $C, \mathbb{F}_q[x, \theta]/\langle x^n - 1 \rangle$ modülünün bir sol $\mathbb{F}_q[x, \theta]$ -altmodülü olsun ve C kodu $f(x)$ polinomu tarafından üretilsin. Bu durumda $f(x)$ polinomu $x^n - 1$ in sağ bölenidir (Şiap, 2011).

Önerme 2.91. $\mathbb{F}_q[x, \theta]$ halkasında $x^n - 1$ in bir sağ böleni $g(x) = g_r x^r + \dots + g_1 x + g_0$ olsun. $g(x)$ polinomu $\mathbb{F}_q$ üzerinde n uzunluğunda boyutu $n - 1$ olan bir skew cyclic kod üretir ve bu polinoma bu kodun üreteç polinomu denir. Ayrıca,

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-r-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & \dots & g_{r-1} & g_r & 0 & \dots & 0 \\ 0 & \theta(g_0) & \dots & \theta(g_{r-1}) & \theta(g_r) & \dots & 0 \\ \vdots & \ddots & & \vdots & & & \vdots \\ 0 & \dots & 0 & \theta^{n-r-1}(g_0) & \dots & \theta^{n-r-1}(g_{r-1}) & \theta^{n-r-1}(g_r) \end{bmatrix}$$

matrisi bu kodun üreteç matrisidir (Boucher vd., 2009).

Örnek 2.92. $\mathbb{F}_4$ üzerinde $[4,2]$ parametrelerine sahip skew cyclic kod bulmak için öncelikle $x^4 - 1 \in \mathbb{F}_4[x, \theta]$ polinomunun derecesi 2 olan sağ böleni bulunmalıdır. $x^4 - 1$ in derecesi 2 olan tüm sağ bölenleri aşağıdaki gibidir (Boucher vd., 2007).

$$\begin{aligned} x^4 - 1 &= (x^2 + 1)(x^2 + 1) \\ &= (x^2 + \alpha x + \alpha)(x^2 + \alpha x + \alpha) \\ &= (x^2 + \alpha^2 x + \alpha^2)(x^2 + \alpha^2 x + \alpha) \\ &= (x^2 + \alpha^2 x + \alpha)(x^2 + \alpha^2 x + \alpha) \\ &= (x^2 + x + \alpha^2)(x^2 + x + \alpha) \\ &= (x^2 + x + \alpha)(x^2 + x + \alpha) \\ &= (x^2 + \alpha x + \alpha^2)(x^2 + \alpha x + \alpha) \end{aligned}$$

$g = x^2 + \alpha x + \alpha^2$ polinomu $[4,2,3]$ parametrelerine sahip, üreteç matrisi

$$G = \begin{pmatrix} \alpha^2 & \alpha & 1 & 0 \\ 0 & \alpha & \alpha^2 & 1 \end{pmatrix}$$

olan skew cyclic kod üretir. $\mathbb{F}_4[x]/\langle x^4 - 1 \rangle$ değişmeli polinom halkasında $x^4 - 1$ polinomunun derecesi 2 olan böleni $g_2 = x^2 + 1$ dir. g_2 tarafından üretilen ideal $\mathbb{F}_4$ üzerinde $[4,2,2]$ parametrelerine sahip cyclic bir koda karşılık gelir. $\mathbb{F}_4[x]/\langle x^4 - 1 \rangle$

halkasında $x^4 - 1$ polinomunun ikinci dereceden başka çarpanı yoktur dolayısıyla parametreleri $[4,2]$ olan başka bir cyclic kod da yoktur. Brouwer'in tablosuna göre $\mathbb{F}_4$ üzerinde $[4,2,3]$ parametrelerine sahip kodlar optimaldir. Bu örnekte skew cyclic kod ailesinin cyclic kodlar ailesine göre daha iyi parametrelere sahip olduğu görülebilir (Grassl, 2013).



3. SKEW CONSTACYCLIC KODLAR

3.1. B_q Halkası

p bir tek asal sayı, m bir pozitif tamsayı, $q = p^m$ olmak üzere $\mathbb{F}_q$, q elemanlı sonlu bir cisim ve

- a) $i = 1, 2, 3, 4$ için $v_i^2 = v_i$,
- b) $v_1 v_2 = v_2 v_1$,
- c) $i = 1, 2, 3, 4, j = 3, 4$ ve $i \neq j$ için $v_i v_j = v_j v_i = 0$ olmak üzere

$$B_q = \mathbb{F}_q + v_1 \mathbb{F}_q + v_2 \mathbb{F}_q + v_3 \mathbb{F}_q + v_4 \mathbb{F}_q + v_1 v_2 \mathbb{F}_q = \{ b = b_0 + b_1 v_1 + b_2 v_2 + b_3 v_3 + b_4 v_4 + b_5 v_1 v_2 : b_i \in \mathbb{F}_q, i = 0, 1, 2, 3, 4, 5 \}$$

kümesi toplama (+) ve çarpma ($\cdot$) işlemlerine göre sonlu, değişmeli, birimli bir halkadır. Ayrıca $i = 1, 2, 3, 4, j = 3, 4, i \neq j$ için B_q halkası $\mathbb{F}_q[v_1, v_2, v_3, v_4] / \langle v_i^2 = v_i, v_1 v_2 = v_2 v_1, v_i v_j = v_j v_i = 0 \rangle$ halkasına izomorftur.

$$\eta_1 = 1 - v_1 - v_2 - v_3 - v_4 + v_1 v_2$$

$$\eta_2 = v_1 v_2$$

$$\eta_3 = v_1 - v_1 v_2$$

$$\eta_4 = v_2 - v_1 v_2$$

$$\eta_5 = v_3$$

$$\eta_6 = v_4$$

seçilirse $i, j = 1, 2, 3, 4, 5, 6$, için,

$$\eta_i \eta_j = \begin{cases} \eta_i, & i = j \\ 0, & i \neq j \end{cases}$$

ve $\sum_{i=1}^6 \eta_i = 1$ olup decomposition özellikleri sağlanır. Buradan,

$$B_q = \eta_1 B_q \oplus \eta_2 B_q \oplus \eta_3 B_q \oplus \eta_4 B_q \oplus \eta_5 B_q \oplus \eta_6 B_q$$

şeklinde yazılabilir.

3.2. Gray Dönüşümü ve Lineer Kodlar

Tanım 3.2.1. Herhangi bir $b = b_0 + b_1v_1 + b_2v_2 + b_3v_3 + b_4v_4 + b_5v_1v_2 \in B_q$ için

$$\Psi: B_q \rightarrow \mathbb{F}_q^6$$

$$\Psi(b) = (b_0, b_0 + b_1 + b_2 + b_5, b_0 + b_1, b_0 + b_2, b_0 + b_3, b_0 + b_4)$$

şeklinde tanımlanan dönüşüme Gray dönüşümü denir. $i = 0, 1, \dots, n-1$, $b^i = b_0^i + b_1^i v_1 + b_2^i v_2 + b_3^i v_3 + b_4^i v_4 + b_5^i v_1 v_2 \in B_q$ olmak üzere

$$\Psi: B_q^n \rightarrow \mathbb{F}_q^{6n}$$

$$\begin{aligned} \Psi(b^0, b^1, b^2, \dots, b^{n-1}) = & (b_0^0, b_0^1, \dots, b_0^{n-1}, b_0^0 + b_1^0 + b_2^0 + b_5^0, b_0^1 + b_1^1 + b_2^1 + \\ & b_5^1, \dots, b_0^{n-1} + b_1^{n-1} + b_2^{n-1} + b_5^{n-1}, b_0^0 + b_1^0, b_0^1 + b_1^1, \dots, b_0^{n-1} + b_1^{n-1}, b_0^0 + \\ & b_2^0, b_0^1 + b_2^1, \dots, b_0^{n-1} + b_2^{n-1}, b_0^0 + b_3^0, b_0^1 + b_3^1, \dots, b_0^{n-1} + b_3^{n-1}, b_0^0 + b_4^0, b_0^1 + \\ & b_4^1, \dots, b_0^{n-1} + b_4^{n-1}) \end{aligned}$$

dönüşümüyle Gray dönüşümü B_q^n den $\mathbb{F}_q^{6n}$ e genelleştirilebilir.

Teorem 3.2.2. Ψ dönüşümü B_q^n (d_L Lee uzaklığı) den $\mathbb{F}_q^{6n}$ (d_H Hamming uzaklığı) e uzaklık koruyan bir dönüşümdür.

İspat: $\forall a_1, a_2 \in \mathbb{F}_q$ ve $\forall x, y \in B_q$ için,

$$\Psi(a_1x + a_2y) = a_1\Psi(x) + a_2\Psi(y)$$

olup Ψ bir lineer dönüşümdür.

$$\begin{aligned} d_L(x, y) &= w_L(x - y) \\ &= w_H(\Psi(x - y)) \\ &= w_H(\Psi(x) - \Psi(y)) \\ &= d_H(\Psi(x), \Psi(y)) \end{aligned}$$

elde edilir. Dolayısıyla Gray dönüşümü uzaklık koruyan bir dönüşümdür.

Teorem 3.2.3. C , B_q üzerinde tanımlı minimum uzaklıklığı d_L , eleman sayısı M ve uzunluğu n olan bir lineer kod olsun. O zaman $\Psi(C)$ de $\mathbb{F}_q$ üzerinde tanımlı bir $(6n, M, d_H)$ -koddur. Ayrıca $d_H = d_L$ dir.

İspat: Ψ nin tanımından ve Teorem 3.2.2. den $\Psi(C)$, $6n$ uzunluğundadır ve $d_H = d_L$ dir. Ψ , 1-1 ve örten olup $|C| = |\Psi(C)|$ dir. Dolayısıyla $\Psi(C)$ bir $(6n, M, d_L)$ -koddur.

Teorem 3.2.4. C , B_q üzerinde bir lineer kod olsun. C kodu self-ortogonal kod ise $\Psi(C)$ de self-ortogonal koddur.

İspat: $\forall b^i, b^j \in B_q$ için,

$$\begin{aligned} b^i b^j &= (b_0^i + b_1^i v_1 + b_2^i v_2 + b_3^i v_3 + b_4^i v_4 + b_5^i v_1 v_2)(b_0^j + b_1^j v_1 + b_2^j v_2 + b_3^j v_3 \\ &+ b_4^j v_4 + b_5^j v_1 v_2) = b_0^i b_0^j + (b_0^i b_1^j + b_1^i b_0^j + b_1^i b_1^j) v_1 + (b_0^i b_2^j + b_1^i b_2^j + b_1^i b_1^j) v_1 \\ &+ (b_0^i b_3^j + b_1^i b_3^j + b_1^i b_1^j) v_1 + (b_0^i b_2^j + b_2^i b_0^j + b_2^i b_2^j) v_2 + (b_0^i b_3^j + b_3^i b_0^j + b_3^i b_3^j) v_3 \\ &+ (b_0^i b_4^j + b_4^i b_0^j + b_4^i b_4^j) v_4 + (b_0^i b_5^j + b_1^i b_2^j + b_1^i b_5^j + b_2^i b_1^j + b_2^i b_5^j + b_5^i b_0^j \\ &+ b_5^i b_2^j + b_5^i b_5^j) v_1 v_2 \end{aligned}$$

C self-ortogonal olduğundan,

$$b_0^i b_0^j = 0$$

$$b_0^i b_1^j + b_1^i b_0^j + b_1^i b_1^j = 0$$

$$b_0^i b_2^j + b_2^i b_0^j + b_2^i b_2^j = 0$$

$$b_0^i b_3^j + b_3^i b_0^j + b_3^i b_3^j = 0$$

$$b_0^i b_4^j + b_4^i b_0^j + b_4^i b_4^j = 0$$

$$b_0^i b_5^j + b_1^i b_2^j + b_1^i b_5^j + b_2^i b_1^j + b_2^i b_5^j + b_5^i b_0^j + b_5^i b_1^j + b_5^i b_2^j + b_5^i b_5^j = 0$$

olmalıdır.

$$\begin{aligned} \Psi(b^i) \Psi(b^j) &= (b_0^i, b_0^i + b_1^i + b_2^i + b_5^i, b_0^i + b_2^i, b_0^i + b_3^i, b_0^i + b_4^i)(b_0^j, b_0^j + b_1^j + b_2^j + \\ &b_5^j, b_0^j + b_2^j, b_0^j + b_3^j, b_0^j + b_4^j) = 0 \end{aligned}$$

bulunur. O halde $\Psi(C)$ de self-ortogonaldir.

C , B_q üzerinde tanımlanan n uzunluğunda bir lineer kod olmak üzere $i = 1, 2, 3, 4, 5, 6$ için $\mathbb{F}_q$ üzerindeki C_i kodlarını

$$\begin{aligned}
C_1 &= \left\{ b_0 \in \mathbb{F}_q^n : \exists b_1, b_2, b_3, b_4, b_5 \in \mathbb{F}_q^n \text{ için } \sum_{i=1}^6 \eta_i b_i \in C \right\} \\
C_2 &= \left\{ b_0 + b_1 + b_2 + b_5 \in \mathbb{F}_q^n : \exists b_3, b_4 \in \mathbb{F}_q^n \text{ için } \sum_{i=1}^6 \eta_i b_i \in C \right\} \\
C_3 &= \left\{ b_0 + b_1 \in \mathbb{F}_q^n : \exists b_2, b_3, b_4, b_5 \in \mathbb{F}_q^n \text{ için } \sum_{i=1}^6 \eta_i b_i \in C \right\} \\
C_4 &= \left\{ b_0 + b_2 \in \mathbb{F}_q^n : \exists b_1, b_3, b_4, b_5 \in \mathbb{F}_q^n \text{ için } \sum_{i=1}^6 \eta_i b_i \in C \right\} \\
C_5 &= \left\{ b_0 + b_3 \in \mathbb{F}_q^n : \exists b_1, b_2, b_4, b_5 \in \mathbb{F}_q^n \text{ için } \sum_{i=1}^6 \eta_i b_i \in C \right\} \\
C_6 &= \left\{ b_0 + b_4 \in \mathbb{F}_q^n : \exists b_1, b_2, b_3, b_5 \in \mathbb{F}_q^n \text{ için } \sum_{i=1}^6 \eta_i b_i \in C \right\}
\end{aligned}$$

şeklinde tanımlayabiliriz.

Teorem 3.2.5. C, B_q üzerinde tanımlı n uzunluğunda bir lineer kod olmak üzere $\Psi(C) = \bigotimes_{1 \leq i \leq 6} C_i, |C| = \prod_{i=1}^6 |C_i|$ ve $d_L(C) = \min\{d_H(C_i) : 1 \leq i \leq 6\}$ dir.

İspat: Ψ 1-1 ve örten olduğundan

$$\begin{aligned}
b' &= (b_0^0, b_0^1, \dots, b_0^{n-1}, b_0^0 + b_1^0 + b_2^0 + b_5^0, b_0^1 + b_1^1 + b_2^1 + b_5^1, \dots, b_0^{n-1} + b_1^{n-1} + \\
&b_2^{n-1} + b_5^{n-1}, b_0^0 + b_1^0, b_0^1 + b_1^1, \dots, b_0^{n-1} + b_1^{n-1}, b_0^0 + b_2^0, b_0^1 + b_2^1, \dots, b_0^{n-1} + \\
&b_2^{n-1}, b_0^0 + b_3^0, b_0^1 + b_3^1, \dots, b_0^{n-1} + b_3^{n-1}, b_0^0 + b_4^0, b_0^1 + b_4^1, \dots, b_0^{n-1} + b_4^{n-1}) \in \Psi(C)
\end{aligned}$$

ve $\Psi(t) = b'$ olacak şekilde $t_i = b_0^i + v_1 b_1^i + v_2 b_2^i + v_3 b_3^i + v_4 b_4^i + v_1 v_2 b_5^i$ olmak üzere $t = (t_0, t_1, \dots, t_{n-1}) \in C$ vardır. C_i lerin tanımından

$$(b_0^0, b_0^1, \dots, b_0^{n-1}) \in C_1,$$

$$(b_0^0 + b_1^0 + b_2^0 + b_5^0, b_0^1 + b_1^1 + b_2^1 + b_5^1, \dots, b_0^{n-1} + b_1^{n-1} + b_2^{n-1} + b_5^{n-1}) \in C_2,$$

$$(b_0^0 + b_1^0, b_0^1 + b_1^1, \dots, b_0^{n-1} + b_1^{n-1}) \in C_3,$$

$$(b_0^0 + b_2^0, b_0^1 + b_2^1, \dots, b_0^{n-1} + b_2^{n-1}) \in C_4,$$

$$(b_0^0 + b_3^0, b_0^1 + b_3^1, \dots, b_0^{n-1} + b_3^{n-1}) \in C_5,$$

$$(b_0^0 + b_4^0, b_0^1 + b_4^1, \dots, b_0^{n-1} + b_4^{n-1}) \in C_6$$

dır. Buradan

$$(b_0^0, b_0^1, \dots, b_0^{n-1}, b_0^0 + b_1^0 + b_2^0 + b_5^0, b_0^1 + b_1^1 + b_2^1 + b_5^1, \dots, b_0^{n-1} + b_1^{n-1} + b_2^{n-1} + b_5^{n-1}, b_0^0 + b_1^0, b_0^1 + b_1^1, \dots, b_0^{n-1} + b_1^{n-1}, b_0^0 + b_2^0, b_0^1 + b_2^1, \dots, b_0^{n-1} + b_2^{n-1}, b_0^0 + b_3^0, b_0^1 + b_3^1, \dots, b_0^{n-1} + b_3^{n-1}, b_0^0 + b_4^0, b_0^1 + b_4^1, \dots, b_0^{n-1} + b_4^{n-1}) \in \bigotimes_{1 \leq i \leq 6} C_i$$

olduğu elde edilir. Böylece $\Psi(C) \subseteq \bigotimes_{1 \leq i \leq 6} C_i$ dir.

Tersine $i = 1, 2, 3, 4, 5, 6$ için

$$a = (b_0^0, b_0^1, \dots, b_0^{n-1}) \in C_1,$$

$$b = (b_0^0 + b_1^0 + b_2^0 + b_5^0, b_0^1 + b_1^1 + b_2^1 + b_5^1, \dots, b_0^{n-1} + b_1^{n-1} + b_2^{n-1} + b_5^{n-1}) \in C_2,$$

$$c = (b_0^0 + b_1^0, b_0^1 + b_1^1, \dots, b_0^{n-1} + b_1^{n-1}) \in C_3,$$

$$d = (b_0^0 + b_2^0, b_0^1 + b_2^1, \dots, b_0^{n-1} + b_2^{n-1}) \in C_4,$$

$$e = (b_0^0 + b_3^0, b_0^1 + b_3^1, \dots, b_0^{n-1} + b_3^{n-1}) \in C_5,$$

$$f = (b_0^0 + b_4^0, b_0^1 + b_4^1, \dots, b_0^{n-1} + b_4^{n-1}) \in C_6,$$

olmak üzere $(a, b, c, d, e, f, g) \in \bigotimes_{1 \leq i \leq 6} C_i$ olsun.

$$t = a + (c - a)v_1 + (d - a)v_2 + (e - a)v_3 + (f - a)v_4 + (a - c - d + b)v_1v_2 \in C$$

elemanı vardır ve $\Psi(t) = (a, b, c, d, e, f, g)$ dir. Buradan $\bigotimes_{1 \leq i \leq 6} C_i \subseteq \Psi(C)$ elde edilir.

Bu durumda $\Psi(C) = \bigotimes_{1 \leq i \leq 6} C_i$ bulunur.

Ψ , 1-1 ve örten olduğundan

$$|C| = \left| \bigotimes_{1 \leq i \leq 6} C_i \right| = \prod_{i=1}^6 |C_i|$$

olur.

Ayrıca Ψ uzaklık koruyan lineer bir dönüşüm olduğundan

$$d_L(C) = d_H(\Psi(C)) = d_H\left(\bigotimes_{1 \leq i \leq 7} C_i\right) = \min\{d_H(C_i) : 1 \leq i \leq 6\}$$

elde edilir.

Sonuç 3.2.6. B_q üzerinde tanımlanan herhangi bir C kodu

$$C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$$

şeklinde tek türlü ifade edilebilir.

Sonuç 3.2.7. $i = 1, 2, 3, 4, 5, 6$ için $\mathbb{F}_q$ üzerinde tanımlanan C_i kodlarının üreteç matrisleri G_i matrisleri, C kodunun üreteç matrisi G

$$G = \begin{pmatrix} \eta_1 G_1 \\ \eta_2 G_2 \\ \vdots \\ \eta_6 G_6 \end{pmatrix}$$

ve $\Psi(C)$ nin üreteç matrisi G'

$$G' = \begin{pmatrix} \Psi(\eta_1 G_1) \\ \Psi(\eta_2 G_2) \\ \vdots \\ \Psi(\eta_6 G_6) \end{pmatrix}$$

şeklindedir.

Teorem 3.2.8. $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$ kodu B_q üzerinde tanımlı n uzunluğunda bir lineer kod olsun. C kodunun bir cyclic kod olması için gerek ve yeter koşul $i = 1, 2, 3, 4, 5, 6$ için C_i kodlarının $\mathbb{F}_q$ üzerinde cyclic kod olmasıdır.

İspat: C, B_q üzerinde tanımlı bir cyclic kod ve

$$a = (a_0, a_1, \dots, a_{n-1}) \in C_1,$$

$$b = (b_0, b_1, \dots, b_{n-1}) \in C_2,$$

$$c = (c_0, c_1, \dots, c_{n-1}) \in C_3,$$

$$d = (d_0, d_1, \dots, d_{n-1}) \in C_4,$$

$$e = (e_0, e_1, \dots, e_{n-1}) \in C_5,$$

$$f = (f_0, f_1, \dots, f_{n-1}) \in C_6$$

olsun. $i = 0, 1, \dots, n-1$ için $t_i = \eta_1 a_i + \eta_2 b_i + \eta_3 c_i + \eta_4 d_i + \eta_5 e_i + \eta_6 f_i$ ve $t = (t_0, t_1, \dots, t_{n-1}) \in C$ olmak üzere C cyclic kod olduğundan $(t_{n-1}, t_0, \dots, t_{n-2}) \in C$ dir. Yani

$$(t_{n-1}, t_0, \dots, t_{n-2}) = \eta_1(a_{n-1}, a_0, \dots, a_{n-2}) + \eta_2(b_{n-1}, b_0, \dots, b_{n-2}) + \\ \eta_3(c_{n-1}, c_0, \dots, c_{n-2}) + \eta_4(d_{n-1}, d_0, \dots, d_{n-2}) + \eta_5(e_{n-1}, e_0, \dots, e_{n-2}) + \\ \eta_6(f_{n-1}, f_0, \dots, f_{n-2})$$

dir. Böylece

$$(a_{n-1}, a_0, \dots, a_{n-2}) \in C_1,$$

$$(b_{n-1}, b_0, \dots, b_{n-2}) \in C_2,$$

$$(c_{n-1}, c_0, \dots, c_{n-2}) \in C_3,$$

$$(d_{n-1}, d_0, \dots, d_{n-2}) \in C_4,$$

$$(e_{n-1}, e_0, \dots, e_{n-2}) \in C_5,$$

$$(f_{n-1}, f_0, \dots, f_{n-2}) \in C_6$$

elde edilir. O halde $i = 1, 2, \dots, 6$ için C_i kodları $\mathbb{F}_q$ üzerinde tanımlı cyclic kodlardır.

Tersine $i = 1, 2, \dots, 6$ için C_i kodları $\mathbb{F}_q$ üzerinde tanımlı cyclic kod olsunlar. $i = 0, 1, \dots, n-1$ için $t_i = \eta_1 a_i + \eta_2 b_i + \eta_3 c_i + \eta_4 d_i + \eta_5 e_i + \eta_6 f_i$ ve $t = (t_0, t_1, \dots, t_{n-1}) \in C$ dir. O zaman

$$a = (a_0, a_1, \dots, a_{n-1}) \in C_1,$$

$$b = (b_0, b_1, \dots, b_{n-1}) \in C_2,$$

$$c = (c_0, c_1, \dots, c_{n-1}) \in C_3,$$

$$d = (d_0, d_1, \dots, d_{n-1}) \in C_4,$$

$$e = (e_0, e_1, \dots, e_{n-1}) \in C_5,$$

$$f = (f_0, f_1, \dots, f_{n-1}) \in C_6$$

olur. C_i kodları cyclic kodlar olduğundan

$$(t_{n-1}, t_0, \dots, t_{n-2}) = \eta_1(a_{n-1}, a_0, \dots, a_{n-2}) + \eta_2(b_{n-1}, b_0, \dots, b_{n-2}) + \\ \eta_3(c_{n-1}, c_0, \dots, c_{n-2}) + \eta_4(d_{n-1}, d_0, \dots, d_{n-2}) + \eta_5(e_{n-1}, e_0, \dots, e_{n-2}) + \\ \eta_6(f_{n-1}, f_0, \dots, f_{n-2}) \in C$$

dir. O halde C, B_q üzerinde tanımlı cyclic bir koddur.

Teorem 3.2.9. $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$ kodu B_q üzerinde tanımlı bir cyclic kod olsun. $\rho_1(x), \rho_2(x), \rho_3(x), \rho_4(x), \rho_5(x)$ ve $\rho_6(x)$ sırasıyla C_1, C_2, C_3, C_4, C_5 ve C_6 kodlarının üreteç polinomları olmak üzere

$$C = \langle \eta_1 \rho_1(x), \eta_2 \rho_2(x), \eta_3 \rho_3(x), \eta_4 \rho_4(x), \eta_5 \rho_5(x), \eta_6 \rho_6(x) \rangle$$

ve

$$|C| = q^{6n - (\text{der} \rho_1(x) + \text{der} \rho_2(x) + \dots + \text{der} \rho_6(x))}$$

dir.

İspat: $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$ olsun. $i = 1, 2, \dots, 6$ için $C_i = \langle \rho_i(x) \rangle \subseteq \mathbb{F}_q[x] / \langle x^n - 1 \rangle$ olduğundan

$$C = \left\{ t(x) : t(x) = \sum_{i=1}^6 \eta_i m_i(x) \rho_i(x), m_i(x) \in \mathbb{F}_q[x], i = 1, 2, \dots, 6 \right\}$$

şeklindedir. O halde

$$C \subseteq \langle \eta_1 \rho_1(x), \eta_2 \rho_2(x), \eta_3 \rho_3(x), \eta_4 \rho_4(x), \eta_5 \rho_5(x), \eta_6 \rho_6(x) \rangle \subseteq B_q[x] / \langle x^n - 1 \rangle$$

dir.

$k_1(x), k_2(x), \dots, k_6(x) \in \mathbb{F}_q[x] / \langle x^n - 1 \rangle$ olmak üzere herhangi bir

$$\sum_{i=1}^6 \eta_i k_i(x) \rho_i(x) \in \langle \eta_1 \rho_1(x), \eta_2 \rho_2(x), \eta_3 \rho_3(x), \eta_4 \rho_4(x), \eta_5 \rho_5(x), \eta_6 \rho_6(x) \rangle$$

için,

$$(1 - v_1 - v_2 - v_3 - v_4 + v_1 v_2) k_1(x) = (1 - v_1 - v_2 - v_3 - v_4 + v_1 v_2) r_1(x)$$

$$(v_1 v_2) k_2(x) = (v_1 v_2) r_2(x)$$

⋮

$$v_4 k_6(x) = v_4 r_6(x)$$

olacak şekilde $r_1(x), r_2(x), \dots, r_6(x) \in B_q[x]$ vardır. Bu durumda

$$\langle \eta_1 \rho_1(x), \eta_2 \rho_2(x), \eta_3 \rho_3(x), \eta_4 \rho_4(x), \eta_5 \rho_5(x), \eta_6 \rho_6(x) \rangle \subseteq C$$

elde edilir. O halde

$$C = \langle \eta_1 \rho_1(x), \eta_2 \rho_2(x), \eta_3 \rho_3(x), \eta_4 \rho_4(x), \eta_5 \rho_5(x), \eta_6 \rho_6(x) \rangle$$

dir. Ayrıca $|C| = |C_1| \cdot |C_2| \cdots |C_6|$ olduğundan

$$|C| = q^{6n - (\text{der}\rho_1(x) + \text{der}\rho_2(x) + \dots + \text{der}\rho_6(x))}$$

dir.

Teorem 3.2.10. C , B_q üzerinde tanımlı bir cyclic kod, $i = 1, 2, \dots, 6$ için $\rho_i(x), C_i$ kodlarının üreteç polinomları olsun. $C = \langle \rho(x) \rangle$ olacak şekilde bir tek

$$\rho(x) = \eta_1\rho_1(x) + \eta_2\rho_2(x) + \eta_3\rho_3(x) + \eta_4\rho_4(x) + \eta_5\rho_5(x) + \eta_6\rho_6(x)$$

polinomu vardır ve $\rho(x) | x^n - 1$ dir.

İspat: Teorem 3.2.9. dan

$$C = \langle \eta_1\rho_1(x), \eta_2\rho_2(x), \eta_3\rho_3(x), \eta_4\rho_4(x), \eta_5\rho_5(x), \eta_6\rho_6(x) \rangle$$

dir. $\rho(x) = \eta_1\rho_1(x) + \eta_2\rho_2(x) + \eta_3\rho_3(x) + \eta_4\rho_4(x) + \eta_5\rho_5(x) + \eta_6\rho_6(x)$ şeklinde yazılabildiğinden $\langle \rho(x) \rangle \subseteq C$ olur. Ayrıca

$$\eta_1\rho_1(x) = \eta_1\rho(x),$$

$$\eta_2\rho_2(x) = \eta_2\rho(x),$$

$$\eta_3\rho_3(x) = \eta_3\rho(x),$$

$$\eta_4\rho_4(x) = \eta_4\rho(x),$$

$$\eta_5\rho_5(x) = \eta_5\rho(x),$$

$$\eta_6\rho_6(x) = \eta_6\rho(x)$$

dir. Bu durumda $C \subseteq \langle \rho(x) \rangle$ elde edilir. O halde $C = \langle \rho(x) \rangle$ dir.

$i = 1, 2, \dots, 6$ için $\rho_i(x)$ polinomları $x^n - 1$ polinomunun bölenleri olduğundan $x^n - 1 = \rho_i(x)k_i(x)$ olacak şekilde $k_i(x) \in \mathbb{F}_q[x]$ vardır. Bu durumda

$$\begin{aligned} (\sum_{i=1}^6 \eta_i k_i(x)) \rho(x) &= \sum_{i=1}^6 \eta_i k_i(x) \sum_{i=1}^6 \eta_i \rho_i(x) \\ &= \sum_{i=1}^6 \eta_i k_i(x) \rho_i(x) \\ &= \sum_{i=1}^6 \eta_i (x^n - 1) = x^n - 1 \end{aligned}$$

elde edilir. O halde $k(x), x^n - 1$ polinomunun bölenidir.

3.3. B_q Halkası Üzerinde Tanımlı Skew Constacyclic Kodlar

$$i = 1, 2, 3, 4, j = 3, 4, i \neq j \text{ için } v_i^2 = v_i, v_1 v_2 = v_2 v_1, v_i v_j = v_j v_i = 0$$

özellikleriyle birlikte B_q halka ailesinin birimsel elemanı

$$\lambda = \lambda_0 + \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 + \lambda_4 v_4 + \lambda_5 v_1 v_2$$

ve

$$\eta_1 = 1 - v_1 - v_2 - v_3 - v_4 + v_1 v_2$$

$$\eta_2 = v_1 v_2$$

$$\eta_3 = v_1 - v_1 v_2$$

$$\eta_4 = v_2 - v_1 v_2$$

$$\eta_5 = v_3$$

$$\eta_6 = v_4$$

olmak üzere $\lambda_0 = \beta_1$, $(\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5) = \beta_2$, $(\lambda_0 + \lambda_1) = \beta_3$, $(\lambda_0 + \lambda_2) = \beta_4$, $(\lambda_0 + \lambda_3) = \beta_5$, $\lambda_0 + \lambda_4 = \beta_6$ olarak alınırsa,

$$\begin{aligned} \lambda \eta_1 &= (\lambda_0 + \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 + \lambda_4 v_4 + \lambda_5 v_1 v_2)(1 - v_1 - v_2 - v_3 - v_4 + v_1 v_2) \\ &= \lambda_0 - \lambda_0 v_1 - \lambda_0 v_2 - \lambda_0 v_3 - \lambda_0 v_4 + \lambda_0 v_1 v_2 + \lambda_1 v_1 - \lambda_1 v_1 v_1 - \lambda_1 v_1 v_2 + \\ &\quad \lambda_1 v_1 v_2 + \lambda_2 v_2 - \lambda_2 v_1 v_2 - \lambda_2 v_2 v_2 + \lambda_2 v_1 v_2 + \lambda_3 v_3 - \lambda_3 v_3 v_3 + \lambda_4 v_4 - \lambda_4 v_4 v_4 + \\ &\quad \lambda_5 v_1 v_2 - \lambda_5 v_1 v_2 v_2 - \lambda_5 v_1 v_2 v_2 + \lambda_5 v_1 v_2 = (1 - v_1 - v_2 - v_3 - v_4 + v_1 v_2) \lambda_0 = \eta_1 \lambda_0 \end{aligned}$$

buradan

$$\lambda \eta_1 = \eta_1 \beta_1$$

bulunur. Benzer şekilde

$$\lambda \eta_2 = \eta_2 \beta_2$$

$$\lambda \eta_3 = \eta_3 \beta_3$$

$$\lambda \eta_4 = \eta_4 \beta_4$$

$$\lambda \eta_5 = \eta_5 \beta_5$$

$$\lambda \eta_6 = \eta_6 \beta_6$$

elde edilir. Böylelikle $\lambda \in B_q$ birimsel elemanı

$$\lambda = \lambda \left(\sum_{i=1}^6 \eta_i \right)$$

$$= \eta_1 \beta_1 + \eta_2 \beta_2 + \eta_3 \beta_3 + \eta_4 \beta_4 + \eta_5 \beta_5 + \eta_6 \beta_6$$

şeklinde yazılabilir.

Lemma 3.3.1. $\lambda_i \in \mathbb{F}_q$ olmak üzere $\lambda = \lambda_0 + \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 + \lambda_4 v_4 + \lambda_5 v_1 v_2 \in B_q$ elemanının birimsel eleman olması için gerek ve yeter koşul $\lambda_0, \lambda_0 + \lambda_1 + \lambda_2 + \lambda_5, \lambda_0 + \lambda_1, \lambda_0 + \lambda_2, \lambda_0 + \lambda_3, \lambda_0 + \lambda_4$ elemanlarının $\mathbb{F}_q$ da birimsel olmasıdır.

İspat: $\lambda_i \in F_q$ olmak üzere $\lambda = \lambda_0 + \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 + \lambda_4 v_4 + \lambda_5 v_1 v_2 \in B_q$ birimsel eleman olsun. O zaman $\lambda \cdot \gamma = 1$ olacak şekilde bir $\gamma = \gamma_0 + \gamma_1 v_1 + \gamma_2 v_2 + \gamma_3 v_3 + \gamma_4 v_4 + \gamma_5 v_1 v_2 \neq 0 \in B_q$ elemanı vardır.

$$\begin{aligned} \lambda \cdot \gamma &= \lambda_0 \gamma_0 + \lambda_0 \gamma_1 v_1 + \lambda_0 \gamma_2 v_2 + \lambda_0 \gamma_3 v_3 + \lambda_0 \gamma_4 v_4 + \lambda_0 \gamma_5 v_1 v_2 + \lambda_1 \gamma_0 v_1 + \\ &\lambda_1 \gamma_1 v_1 + \lambda_1 \gamma_2 v_1 v_2 + \lambda_1 \gamma_5 v_1 v_2 + \lambda_2 \gamma_0 v_2 + \lambda_2 \gamma_1 v_1 v_2 + \lambda_2 \gamma_2 v_2 + \lambda_2 \gamma_5 v_1 v_2 + \\ &\lambda_3 \gamma_0 v_3 + \lambda_3 \gamma_3 v_3 + \lambda_4 \gamma_0 v_4 + \lambda_4 \gamma_4 v_4 + \lambda_5 \gamma_0 v_1 v_2 + \lambda_5 \gamma_1 v_1 v_2 + \lambda_5 \gamma_2 v_1 v_2 + \\ &\lambda_5 \gamma_5 v_1 v_2 \\ &= \lambda_0 \gamma_0 + (\lambda_0 \gamma_1 + \lambda_1 \gamma_0 + \lambda_1 \gamma_1) v_1 + (\lambda_0 \gamma_2 + \lambda_2 \gamma_0 + \lambda_2 \gamma_2) v_2 + (\lambda_0 \gamma_3 + \lambda_3 \gamma_0 + \\ &\lambda_3 \gamma_3) v_3 + (\lambda_0 \gamma_4 + \lambda_4 \gamma_0 + \lambda_4 \gamma_4) v_4 + (\lambda_0 \gamma_5 + \lambda_1 \gamma_2 + \lambda_1 \gamma_5 + \lambda_2 \gamma_1 + \lambda_2 \gamma_5 + \\ &\lambda_5 \gamma_0 + \lambda_5 \gamma_1 + \lambda_5 \gamma_2 + \lambda_5 \gamma_5) v_1 v_2 = 1 \end{aligned}$$

Bu durumda

$$\lambda_0 \gamma_0 = 1,$$

$$(\lambda_0 \gamma_1 + \lambda_1 \gamma_0 + \lambda_1 \gamma_1) = 0,$$

$$(\lambda_0 \gamma_2 + \lambda_2 \gamma_0 + \lambda_2 \gamma_2) = 0,$$

$$(\lambda_0 \gamma_3 + \lambda_3 \gamma_0 + \lambda_3 \gamma_3) = 0,$$

$$(\lambda_0 \gamma_4 + \lambda_4 \gamma_0 + \lambda_4 \gamma_4) = 0,$$

$$(\lambda_0 \gamma_5 + \lambda_1 \gamma_2 + \lambda_1 \gamma_5 + \lambda_2 \gamma_1 + \lambda_2 \gamma_5 + \lambda_5 \gamma_0 + \lambda_5 \gamma_1 + \lambda_5 \gamma_2 + \lambda_5 \gamma_5) = 0$$

O halde

$$\lambda_0 \neq 0,$$

$$(\lambda_0 + \lambda_1) \neq 0,$$

$$(\lambda_0 + \lambda_2) \neq 0, \quad (\lambda_0 + \lambda_3) \neq 0,$$

$$(\lambda_0 + \lambda_4) \neq 0, \quad (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5) \neq 0$$

olmalıdır.

Tersine

$$\lambda_0 \neq 0,$$

$$(\lambda_0 + \lambda_1) \neq 0,$$

$$(\lambda_0 + \lambda_2) \neq 0, \quad (\lambda_0 + \lambda_3) \neq 0,$$

$$(\lambda_0 + \lambda_4) \neq 0, \quad (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5) \neq 0$$

olsun.

$$\begin{aligned} \gamma = \lambda^{-1} = & \lambda_0^{-1}(1 - v_1 - v_2 - v_3 - v_4 + v_1v_2) + (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)^{-1}(v_1v_2) + \\ & (\lambda_0 + \lambda_1)^{-1}(v_1 - v_1v_2) + (\lambda_0 + \lambda_2)^{-1}(v_2 - v_1v_2) + (\lambda_0 + \lambda_3)^{-1}v_3 + \\ & (\lambda_0 + \lambda_4)^{-1}v_4 \end{aligned}$$

alınırsa $\lambda \cdot \gamma = \lambda \cdot \lambda^{-1} = 1$ elde edilir. O halde λ birimsel elemandır.

Tanım 3.3.2. $\text{Aut}(\mathbb{F}_q)$, $\mathbb{F}_q$ üzerindeki otomorfizmalar kümesi ve $\theta \in \text{Aut}(\mathbb{F}_q)$ aşıkâr olmayan bir otomorfizma olsun. Her $b = b_0 + b_1v_1 + b_2v_2 + b_3v_3 + b_4v_4 + b_5v_1v_2 \in B_q$ için

$$\theta: B_q \rightarrow B_q$$

$$b \mapsto \theta(b) = \theta(b_0) + \theta(b_1)v_1 + \theta(b_2)v_2 + \theta(b_3)v_3 + \theta(b_4)v_4 + \theta(b_5)v_1v_2$$

şeklinde tanımlı θ dönüşümü B_q üzerinde tanımlı aşıkâr olmayan bir otomorfizma olmak üzere

$$B_q[x, \theta] = \{b_0 + b_1x + \cdots + b_{n-1}x^{n-1} : b_i \in B_q, n \in \mathbb{N}\}$$

şeklinde tanımlı kümeye skew polinom kümesi denir. Polinomlardaki klasik toplama işlemi ve çarpma işlemin

$$\alpha x^i \beta x^j = \alpha \theta^i(\beta) x^{i+j}$$

şeklinde tanımlandığı kümeye skew polinom halkası denir.

$\forall b \in B_q$ için $\theta^2(b) = b$ olduğundan θ otomorfizmasının mertebesi 2 dir.

Tanım 3.3.3. $\lambda \in B_q$ birimsel bir eleman olmak üzere

$$\sigma_{\theta, \lambda}: B_q^n \rightarrow B_q^n$$

bir skew λ -constacyclic shift dönüşümü olsun.

- i) C, B_q^n nin bir B_q -altmodülü
- ii) Her $t = (t_0, t_1, \dots, t_{n-1}) \in C$ için

$$\sigma_{\theta, \lambda}(t) = (\lambda\theta(t_{n-1}), \theta(t_0), \dots, \theta(t_{n-2})) \in C$$

koşulları sağlanıyorsa C kümesine B_q üzerinde n uzunluğunda skew λ -constacyclic kod denir.

Burada, $\lambda = 1$ seçilirse skew λ -constacyclic kod skew cyclic koda, $\lambda = -1$ seçilirse skew λ -constacyclic kod skew nega-cyclic koda karşılık gelir.

θ otomorfizması aşikar otomorfizma seçilirse skew λ -constacyclic kod, λ -constacyclic koda, θ aşikar otomorfizma, $\lambda = 1$ seçilirse cyclic koda ve θ aşikar otomorfizma, $\lambda = -1$ seçilirse nega-cyclic koda karşılık gelir.

Önerme 3.3.4.

$$\varphi: B_q^n \rightarrow B_q[x, \theta]/\langle x^n - \lambda \rangle$$

$$\ell = (\ell_0, \ell_1, \dots, \ell_{n-1}) \mapsto \varphi(\ell) = \ell_0 + \ell_1 x + \dots + \ell_{n-1} x^{n-1} + \langle x^n - \lambda \rangle$$

şeklinde tanımlanan fonksiyon bir izomorfizmadır. Bu dönüşüm yardımıyla $\ell = (\ell_0, \ell_1, \dots, \ell_{n-1})$ vektörünü kısaca;

$$\varphi(\ell) = \ell(x) = \ell_0 + \ell_1 x + \dots + \ell_{n-1} x^{n-1} \in B_q[x, \theta]/\langle x^n - \lambda \rangle$$

ile göstereceğiz.

Kolaylık olması açısından bu tezde $\varphi(C)$ gösterimi yerine C yi kullanacağız.

Teorem 3.3.5. Her $\ell(x) + \langle x^n - \lambda \rangle \in B_q[x, \theta]/\langle x^n - \lambda \rangle$ ve $f(x) \in B_q[x, \theta]$ için

$$: B_q[x, \theta] \times B_q[x, \theta]/\langle x^n - \lambda \rangle \rightarrow B_q[x, \theta]/\langle x^n - \lambda \rangle$$

$$f(x)(\ell(x) + \langle x^n - \lambda \rangle) = f(x)\ell(x) + \langle x^n - \lambda \rangle$$

şeklindeki soldan çarpma işlemi ve polinomlardaki toplama işlemine göre $B_q[x, \theta]/\langle x^n - \lambda \rangle$ bir sol $B_q[x, \theta]$ -modüldür.

Teorem 3.3.6. Bir C kodunun skew λ -constacyclic kod olması için gerek ve yeter koşul C nin $B_q[x, \theta]/\langle x^n - \lambda \rangle$ 'nın bir sol $B_q[x, \theta]$ -altmodülü olmasıdır.

İspat: C , B_q üzerinde skew λ -constacyclic kod ve $\ell = (\ell_0, \ell_1, \dots, \ell_{n-1}) \in C$ olsun. ℓ kod sözcüğüne karşılık gelen polinom $\ell(x) = \ell_0 + \ell_1 x + \dots + \ell_{n-1} x^{n-1}$ olmak üzere

$$\begin{aligned} x \cdot \ell(x) &= x(\ell_0 + \ell_1 x + \dots + \ell_{n-1} x^{n-1}) \\ &= \theta(\ell_0)x + \theta(\ell_1)x^2 + \dots + \theta(\ell_{n-1})x^n \end{aligned}$$

dir. $x^n = \lambda$ olduğundan

$$\begin{aligned} x \cdot \ell(x) &= \lambda\theta(\ell_{n-1}) + \theta(\ell_0)x + \dots + \theta(\ell_{n-2})x^{n-1} \\ &= \sigma_{\theta, \lambda}(\ell) \in C \end{aligned}$$

elde edilir. Benzer şekilde $i \geq 2$ için $x^i \ell(x) \in C$ olur. C bir lineer kod olduğundan $r(x) \in B_q[x, \theta]$ için $r(x) \ell(x) \in C$ dir. Bu durumda C , $B_q[x, \theta]/\langle x^n - \lambda \rangle$ nin bir sol $B_q[x, \theta]$ -altmodülü olur.

Tersine C , $B_q[x, \theta]$ nin bir sol $B_q[x, \theta]$ -altmodülü olsun. Böylece $\ell = (\ell_0, \ell_1, \dots, \ell_{n-1}) \in C$ için,

$$\sigma_{\theta, \lambda}(\ell) = x\ell(x) \in C$$

elde edilir. Bu durumda C , B_q üzerinde n uzunluğunda skew λ -constacyclic kod olur.

Teorem 3.3.7. n pozitif bir tamsayı ve $\lambda^{n+1} = 1$ olmak üzere,

$$\omega: B_q[x, \theta]/\langle x^n - 1 \rangle \rightarrow B_q[x, \theta]/\langle x^n - \lambda \rangle$$

dönüşümü

$$\ell(x) \mapsto \omega(\ell(x)) = \ell(\lambda x)$$

şeklinde tanımlansın. O halde ω dönüşümü sol $B_q[x, \theta]$ modül izomorfizmasıdır.

İspat: Her $\ell_1(x), \ell_2(x) \in B_q[x, \theta]/\langle x^n - 1 \rangle$ için

$$\ell_1(x) \equiv \ell_2(x) \pmod{x^n - 1}$$

dir. Bu denklikte x yerine λx yazılırsa

$$\ell_1(\lambda x) - \ell_2(\lambda x) \equiv 0 \pmod{\lambda^n x^n - 1}$$

denkliği elde edilir. $\lambda^{n+1} = 1$ olduğundan

$$\ell_1(\lambda x) - \ell_2(\lambda x) \equiv 0 \lambda^n \pmod{x^n - \lambda}$$

bulunur. O halde

$$\omega(\ell_1(x)) = \omega(\ell_2(x))$$

dir.

Sonuç olarak ω , 1-1 ve iyi tanımlı bir dönüşüm olur. Ayrıca ω dönüşümü örten ve sol $B_q[x, \theta]$ modül homomorfizmasıdır. O halde ω dönüşümü bir sol $B_q[x, \theta]$ modül izomorfizmasıdır.

Sonuç 3.3.8. n pozitif bir tamsayı ve $\lambda^{n+1} = 1$ olsun. C skew cyclic kod ise $\omega(C)$ skew λ -constacyclic kod olur.

Teorem 3.3.9. $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$ lineer kodunun B_q üzerinde tanımlı bir skew $\lambda = \lambda_0 + \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 + \lambda_4 v_4 + \lambda_5 v_1 v_2$ -constacyclic kod olması için gerek ve yeter koşul $\mathbb{F}_q$ üzerinde tanımlanan otomorfizmayla birlikte, $C_1, C_2, C_3, C_4, C_5, C_6$ kodlarının $\mathbb{F}_q$ üzerinde sırasıyla, skew

$$\lambda_0\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_1)\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_2)\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_3)\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_4)\text{-constacyclic}$$

kod olmasıdır.

İspat: $t = (t_0, t_1, \dots, t_{n-1}) \in C$ ve $i = 0, 1, \dots, n-1$ olmak üzere $t_i = \eta_1 a_i + \eta_2 b_i + \eta_3 c_i + \eta_4 d_i + \eta_5 e_i + \eta_6 f_i$ olsun. Burada

$$a = (a_0, a_1, \dots, a_{n-1}) \in C_1,$$

$$b = (b_0, b_1, \dots, b_{n-1}) \in C_2,$$

$$c = (c_0, c_1, \dots, c_{n-1}) \in C_3,$$

$$d = (d_0, d_1, \dots, d_{n-1}) \in C_4,$$

$$e = (e_0, e_1, \dots, e_{n-1}) \in C_5,$$

$$f = (f_0, f_1, \dots, f_{n-1}) \in C_6$$

dır. $\mathbb{F}_q$ üzerinde tanımlanan Frobenius otomorfizması yardımıyla, $C_1, C_2, C_3, C_4, C_5, C_6$ kodları sırasıyla, skew

λ_0 -constacyclic,

$(\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)$ -constacyclic,

$(\lambda_0 + \lambda_1)$ -constacyclic,

$(\lambda_0 + \lambda_2)$ -constacyclic,

$(\lambda_0 + \lambda_3)$ -constacyclic,

$(\lambda_0 + \lambda_4)$ -constacyclic

kod olsun. Bu durumda,

$$\sigma_{\theta, \lambda_0}(a) \in C_1,$$

$$\sigma_{\theta, (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)}(b) \in C_2,$$

$$\sigma_{\theta, (\lambda_0 + \lambda_1)}(c) \in C_3,$$

$$\sigma_{\theta, (\lambda_0 + \lambda_2)}(d) \in C_4,$$

$$\sigma_{\theta, (\lambda_0 + \lambda_3)}(e) \in C_5,$$

$$\sigma_{\theta, (\lambda_0 + \lambda_4)}(f) \in C_6$$

dir. Buradan

$$\begin{aligned} \sigma_{\theta, (\lambda_0 + \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 + \lambda_4 v_4 + \lambda_5 v_1 v_2)}(t) &= \eta_1 \sigma_{\theta, \lambda_0}(a) + \eta_2 \sigma_{\theta, (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)}(b) + \\ \eta_3 \sigma_{\theta, (\lambda_0 + \lambda_1)}(c) + \eta_4 \sigma_{\theta, (\lambda_0 + \lambda_2)}(d) + \eta_5 \sigma_{\theta, (\lambda_0 + \lambda_3)}(e) + \eta_6 \sigma_{\theta, (\lambda_0 + \lambda_4)}(f) &\in \eta_1 C_1 \oplus \\ \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6 &= C \end{aligned}$$

olduğundan C bir skew $\lambda = \lambda_0 + \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 + \lambda_4 v_4 + \lambda_5 v_1 v_2$ -constacyclic koddur.

Diğer taraftan C nin bir skew λ -constacyclic kod olduğunu kabul edelim.

$$a = (a_0, a_1, \dots, a_{n-1}) \in C_1,$$

$$b = (b_0, b_1, \dots, b_{n-1}) \in C_2,$$

$$c = (c_0, c_1, \dots, c_{n-1}) \in C_3,$$

$$d = (d_0, d_1, \dots, d_{n-1}) \in C_4,$$

$$e = (e_0, e_1, \dots, e_{n-1}) \in C_5,$$

$$f = (f_0, f_1, \dots, f_{n-1}) \in C_6$$

olsun. $i = 0, 1, \dots, n-1$ için $t_i = \eta_1 a_i + \eta_2 b_i + \eta_3 c_i + \eta_4 d_i + \eta_5 e_i + \eta_6 f_i$ olmak üzere $t = (t_0, t_1, \dots, t_{n-1}) \in C$ dir. C bir skew λ -constacyclic kod olduğundan $\sigma_{\theta, \lambda}(t) \in C$ dir.

$$\begin{aligned} \sigma_{\theta, \lambda}(t) = & \eta_1 \sigma_{\theta, \lambda_0}(a) + \eta_2 \sigma_{\theta, (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)}(b) + \eta_3 \sigma_{\theta, (\lambda_0 + \lambda_1)}(c) + \eta_4 \sigma_{\theta, (\lambda_0 + \lambda_2)}(d) + \\ & \eta_5 \sigma_{\theta, (\lambda_0 + \lambda_3)}(e) + \eta_6 \sigma_{\theta, (\lambda_0 + \lambda_4)}(f) \in C \end{aligned}$$

dir. Böylece

$$\sigma_{\theta, \lambda_0}(a) \in C_1,$$

$$\sigma_{\theta, (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)}(b) \in C_2,$$

$$\sigma_{\theta, (\lambda_0 + \lambda_1)}(c) \in C_3,$$

$$\sigma_{\theta, (\lambda_0 + \lambda_2)}(d) \in C_4,$$

$$\sigma_{\theta, (\lambda_0 + \lambda_3)}(e) \in C_5,$$

$$\sigma_{\theta, (\lambda_0 + \lambda_4)}(f) \in C_6$$

elde edilir. O halde $C_1, C_2, C_3, C_4, C_5, C_6$ kodları $\mathbb{F}_q$ üzerinde sırasıyla, skew

λ_0 -constacyclic,

$(\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)$ -constacyclic,

$(\lambda_0 + \lambda_1)$ -constacyclic,

$(\lambda_0 + \lambda_2)$ -constacyclic,

$(\lambda_0 + \lambda_3)$ -constacyclic,

$(\lambda_0 + \lambda_4)$ -constacyclic

koddur.

Teorem 3.3.10. $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$, B_q üzerinde tanımlı bir skew λ -constacyclic kod olsun. Bu durumda $C^\perp = \eta_1 C_1^\perp \oplus \eta_2 C_2^\perp \oplus \eta_3 C_3^\perp \oplus \eta_4 C_4^\perp \oplus \eta_5 C_5^\perp \oplus \eta_6 C_6^\perp$, B_q da bir skew $\lambda^{-1} = (\lambda_0 + \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 + \lambda_4 v_4 + \lambda_5 v_1 v_2)^{-1}$ -constacyclic koddur. Ayrıca $C_1^\perp, C_2^\perp, C_3^\perp, C_4^\perp, C_5^\perp, C_6^\perp$ kodları $\mathbb{F}_q$ üzerinde sırasıyla, skew

$$\lambda_0^{-1}\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)^{-1}\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_1)^{-1}\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_2)^{-1}\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_3)^{-1}\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_4)^{-1}\text{-constacyclic}$$

koddur.

İspat: Teorem 3.3.9. dan C, B_q üzerinde tanımlı bir skew λ -constacyclic kod ise $C_1, C_2, C_3, C_4, C_5, C_6$ kodları da $\mathbb{F}_q$ üzerinde sırasıyla, skew

$$\lambda_0\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_1)\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_2)\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_3)\text{-constacyclic,}$$

$$(\lambda_0 + \lambda_4)\text{-constacyclic}$$

koddur. (Jitman, vd., 2010, Lemma 3.1)'den $C_1^\perp$ kodu, skew λ_0^{-1} -constacyclic, $C_2^\perp$ kodu, skew $(\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)^{-1}$ -constacyclic, $C_3^\perp$ kodu, skew $(\lambda_0 + \lambda_1)^{-1}$ -constacyclic, $C_4^\perp$ kodu, skew $(\lambda_0 + \lambda_2)^{-1}$ -constacyclic, $C_5^\perp$ kodu, skew $(\lambda_0 + \lambda_3)^{-1}$ -constacyclic, $C_6^\perp$ kodu, skew $(\lambda_0 + \lambda_4)^{-1}$ -constacyclic koddur. Bu durumda Teorem 3.3.9. dan dolayı $C^\perp, B_q$ üzerinde bir skew λ^{-1} -constacyclic kod olur.

Sonuç 3.3.11. $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$, B_q üzerinde tanımlı skew λ -constacyclic kod olmak üzere C nin self-dual kod olması için gerek ve yeter koşul $i = 1, 2, \dots, 6$ için C_i kodlarının sırasıyla skew λ_0 -constacyclic, $(\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)$ -constacyclic, $(\lambda_0 + \lambda_1)$ -constacyclic, $(\lambda_0 + \lambda_2)$ -constacyclic, $(\lambda_0 + \lambda_3)$ -constacyclic, $(\lambda_0 + \lambda_4)$ -constacyclic self-dual kod olmasıdır.

Ayrıca C nin self-dual kod olması için gerek ve yeter koşul $\lambda^2 = 1$ olmasıdır. Bu durumu sağlayan λ elemanları,

$$\begin{aligned}
& -1, 1, 1 - 2v_1, 1 - 2v_2, 1 - 2v_3, 1 - 2v_4, 1 - 2v_1v_2, \\
& -1 + 2v_1, -1 + 2v_2, -1 + 2v_3, -1 + 2v_4, -1 + 2v_1v_2, 1 - 2v_1 + 2v_1v_2, \\
& 1 - 2v_2 + 2v_1v_2, 1 - 2v_3 - 2v_1v_2, 1 - 2v_4 - 2v_1v_2, 1 - 2v_3 - 2v_4, \\
& 1 - 2v_3 - 2v_2, 1 - 2v_4 - 2v_2, 1 - 2v_3 - 2v_1, 1 - 2v_4 - 2v_1, \\
& -1 + 2v_2 - 2v_1v_2, -1 + 2v_1 - 2v_1v_2, -1 + 2v_3 + 2v_4, \\
& -1 + 2v_3 + 2v_1v_2, -1 + 2v_2 + 2v_3, -1 + 2v_4 + 2v_1v_2, \\
& -1 + 2v_2 + 2v_4, -1 + 2v_1 + 2v_3, -1 + 2v_1 + 2v_4, \\
& 1 - 2v_1 - 2v_2 + 4v_1v_2, 1 - 2v_1 - 2v_2 + 2v_1v_2, 1 - 2v_3 - 2v_4 - 2v_1v_2, \\
& 1 - 2v_3 - 2v_4 - 2v_2, 1 - 2v_2 - 2v_3 + 2v_1v_2, 1 - 2v_2 - 2v_4 + 2v_1v_2, \\
& 1 - 2v_3 - 2v_4 - 2v_1, 1 - 2v_1 - 2v_3 + 2v_1v_2, 1 - 2v_1 - 2v_4 + 2v_1v_2, \\
& -1 + 2v_1 + 2v_2 - 2v_1v_2, -1 + 2v_1 + 2v_2 - 4v_1v_2, \\
& -1 + 2v_3 + 2v_4 + 2v_1v_2, -1 + 2v_2 + 2v_3 + 2v_4, \\
& -1 + 2v_2 + 2v_3 - 2v_1v_2, -1 + 2v_2 + 2v_4 - 2v_1v_2, \\
& -1 + 2v_1 + 2v_3 + 2v_4, -1 + 2v_1 + 2v_3 - 2v_1v_2, \\
& -1 + 2v_1 + 2v_4 - 2v_1v_2, 1 - 2v_1 - 2v_2 - 2v_3 + 4v_1v_2, \\
& 1 - 2v_1 - 2v_2 - 2v_4 + 4v_1v_2, 1 - 2v_1 - 2v_2 - 2v_3 + 2v_1v_2, \\
& 1 - 2v_1 - 2v_2 - 2v_4 + 2v_1v_2, 1 - 2v_2 - 2v_3 - 2v_4 + 2v_1v_2, \\
& 1 - 2v_1 - 2v_3 - 2v_4 + 2v_1v_2, -1 + 2v_1 + 2v_2 + 2v_3 - 2v_1v_2, \\
& -1 + 2v_1 + 2v_2 + 2v_4 - 2v_1v_2, -1 + 2v_1 + 2v_2 + 2v_3 - 4v_1v_2,
\end{aligned}$$

$$\begin{aligned}
& -1 + 2v_1 + 2v_2 + 2v_4 - 4v_1v_2, -1 + 2v_2 + 2v_3 + 2v_4 - 2v_1v_2, \\
& -1 + 2v_1 + 2v_3 + 2v_4 - 2v_1v_2, 1 - 2v_1 - 2v_2 - 2v_3 - 2v_4 + 4v_1v_2, \\
& 1 - 2v_1 - 2v_2 - 2v_3 - 2v_4 + 2v_1v_2, \\
& -1 + 2v_1 + 2v_2 + 2v_3 + 2v_4 - 2v_1v_2, \\
& -1 + 2v_1 + 2v_2 + 2v_3 + 2v_4 - 4v_1v_2
\end{aligned}$$

şeklindedir.

Tablo 3.3.12. B_q üzerindeki skew cyclic ve skew nega-cyclic kodlardan elde edilen skew constacyclic kodlar

C	C_1	C_2	C_3	C_4	C_5	C_6
Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic
Skew $(1 - 2v_1 - 2v_2 - 2v_3 - 2v_4 - 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_1 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_2 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_3)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_4)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(1 - 2v_1 - 2v_2 - 2v_3 - 2v_4 + 4v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(1 - 2v_2 - 2v_3 - 2v_4)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(1 - 2v_1 - 2v_3 - 2v_4)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic

Tablo 3.3.12. B_q üzerindeki skew cyclic ve skew nega-cyclic kodlardan elde edilen skew constacyclic kodlar (Devamı)

Skew $(1 - 2v_1 - 2v_2 - 2v_4 + 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(1 - 2v_1 - 2v_2 - 2v_3 + 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(-1 + 2v_1)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_2)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_3 + 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_4 + 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(-1 + 2v_1 + 2v_2 - 4v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_1 + 2v_3 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_1 + 2v_4 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(-1 + 2v_2 + 2v_3 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_2 + 2v_4 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(-1 + 2v_3 + 2v_4)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic
Skew $(1 - 2v_2 - 2v_3 - 2v_4 + 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(1 - 2v_1 - 2v_3 - 2v_4 + 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic

Tablo 3.3.12. B_q üzerindeki skew cyclic ve skew nega-cyclic kodlardan elde edilen skew constacyclic kodlar (Devamı)

Skew $(1 - 2v_1 - 2v_2 - 2v_4 + 4v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(1 - 2v_1 - 2v_2 - 2v_3 + 4v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(1 - 2v_3 - 2v_4 - 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(1 - 2v_2 - 2v_4)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(1 - 2v_2 - 2v_3)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(1 - 2v_1 - 2v_4)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(1 - 2v_1 - 2v_3)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(1 - 2v_1 - 2v_2 + 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic
Skew $(-1 + 2v_1 + 2v_2 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_1 + 2v_3)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_1 + 2v_4)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(-1 + 2v_2 + 2v_3)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_2 + 2v_4)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(-1 + 2v_3 + 2v_4 + 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic

Tablo 3.3.12. B_q üzerindeki skew cyclic ve skew nega-cyclic kodlardan elde edilen skew constacyclic kodlar (Devamı)

Skew $(-1 + 2v_1 + 2v_2 + 2v_3 - 4v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_1 + 2v_2 + 2v_4 - 4v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(-1 + 2v_2 + 2v_3 + 2v_4 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic
Skew $(-1 + 2v_1 + 2v_3 + 2v_4 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic
Skew $(1 - 2v_3 - 2v_4)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic
Skew $(1 - 2v_2 - 2v_4 + 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(1 - 2v_2 - 2v_3 + 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(1 - 2v_1 - 2v_4 + 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(1 - 2v_1 - 2v_3 + 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(1 - 2v_1 - 2v_2 + 4v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic
Skew $(1 - 2v_4 - 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(1 - 2v_3 - 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(1 - 2v_2)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic
Skew $(1 - 2v_1)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic

Tablo 3.3.12. B_q üzerindeki skew cyclic ve skew nega-cyclic kodlardan elde edilen skew constacyclic kodlar (Devamı)

Skew $(-1 + 2v_1 + 2v_2 + 2v_3 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(-1 + 2v_1 + 2v_2 + 2v_4 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(-1 + 2v_1 + 2v_3 + 2v_4)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic
Skew $(-1 + 2v_2 + 2v_3 + 2v_4)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic
Skew $(-1 + 2v_1 + 2v_2 + 2v_3 + 2v_4 - 4v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic
Skew $(1 - 2v_4)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic
Skew $(1 - 2v_3)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic
Skew $(1 - 2v_2 + 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic
Skew $(1 - 2v_1 + 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic
Skew $(1 - 2v_1v_2)$ -constacyclic	Skew Cyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic
Skew $(-1 + 2v_1 + 2v_2 + 2v_3 + 2v_4 - 2v_1v_2)$ -constacyclic	Skew Nega-cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic	Skew Cyclic
Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic	Skew Nega-cyclic

Teorem 3.3.13. $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$, B_q üzerinde tanımlı skew λ -constacyclic kod ve $\rho_1(x), \rho_2(x), \rho_3(x), \rho_4(x), \rho_5(x), \rho_6(x)$ sırasıyla C_1, C_2, C_3, C_4, C_5 ve C_6 kodlarının üreteç polinomları olmak üzere

$$C = \langle \eta_1 \rho_1(x), \eta_2 \rho_2(x), \eta_3 \rho_3(x), \eta_4 \rho_4(x), \eta_5 \rho_5(x), \eta_6 \rho_6(x) \rangle$$

ve

$$|C| = q^{6n - (der\rho_1(x) + der\rho_2(x) + \dots + der\rho_6(x))}$$

dir.

$$\text{İspat: } C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6 \text{ ve}$$

$$C_1 = \langle \rho_1(x) \rangle,$$

$$C_2 = \langle \rho_2(x) \rangle,$$

$$C_3 = \langle \rho_3(x) \rangle,$$

$$C_4 = \langle \rho_4(x) \rangle,$$

$$C_5 = \langle \rho_5(x) \rangle,$$

$$C_6 = \langle \rho_6(x) \rangle$$

olmak üzere

$$C = \{c(x) : c(x) = \eta_1 m_1(x) \rho_1(x) + \eta_2 m_2(x) \rho_2(x) + \eta_3 m_3(x) \rho_3(x) + \eta_4 m_4(x) \rho_4(x) + \eta_5 m_5(x) \rho_5(x) + \eta_6 m_6(x) \rho_6(x), m_i(x) \in B_q[x, \theta], i = 1, 2, \dots, 6\}$$

dir. Dolayısıyla

$$C \subseteq \langle \eta_1 \rho_1(x), \eta_2 \rho_2(x), \eta_3 \rho_3(x), \eta_4 \rho_4(x), \eta_5 \rho_5(x), \eta_6 \rho_6(x) \rangle$$

elde edilir. $k_1(x), k_2(x), \dots, k_6(x) \in B_q[x, \theta] / \langle x^n - \lambda \rangle$ olmak üzere herhangi bir

$$\eta_1 k_1(x) \rho_1(x) + \eta_2 k_2(x) \rho_2(x) + \dots + \eta_6 k_6(x) \rho_6(x) \in \langle \eta_1 \rho_1(x), \eta_2 \rho_2(x), \eta_3 \rho_3(x), \eta_4 \rho_4(x), \eta_5 \rho_5(x), \eta_6 \rho_6(x) \rangle$$

için,

$$(1 - v_1 - v_2 - v_3 - v_4 + v_1 v_2) k_1(x) = (1 - v_1 - v_2 - v_3 - v_4 + v_1 v_2) r_1(x)$$

$$(v_1 v_2) k_2(x) = (v_1 v_2) r_2(x)$$

$\vdots$

$$v_4 k_6(x) = v_4 r_6(x)$$

olacak şekilde $r_1(x), r_2(x), \dots, r_6(x) \in B_q[x, \theta]$ vardır. Bu durumda

$$\langle \eta_1 \rho_1(x), \eta_2 \rho_2(x), \eta_3 \rho_3(x), \eta_4 \rho_4(x), \eta_5 \rho_5(x), \eta_6 \rho_6(x) \rangle \subseteq C$$

elde edilir. O halde

$$C = \langle \eta_1 \rho_1(x), \eta_2 \rho_2(x), \eta_3 \rho_3(x), \eta_4 \rho_4(x), \eta_5 \rho_5(x), \eta_6 \rho_6(x) \rangle$$

dir.

Ayrıca $|C| = |C_1| \cdot |C_2| \cdots |C_6|$ olduğundan

$$|C| = q^{6n - (\text{der} \rho_1(x) + \text{der} \rho_2(x) + \cdots + \text{der} \rho_6(x))}$$

dir.

Theorem 3.3.14. $C_1, C_2, \dots, C_6$, $\mathbb{F}_q$ üzerinde tanımlı sırasıyla skew, λ_0 -constacyclic, $(\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)$ -constacyclic, $(\lambda_0 + \lambda_1)$ -constacyclic, $(\lambda_0 + \lambda_2)$ -constacyclic, $(\lambda_0 + \lambda_3)$ -constacyclic, $(\lambda_0 + \lambda_4)$ -constacyclic kodlar ve $\rho_1(x), \rho_2(x), \rho_3(x), \rho_4(x), \rho_5(x)$ ve $\rho_6(x)$ sırasıyla bu kodların üreteç polinomları olsun. $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$, B_q üzerinde tanımlı n uzunluğunda bir skew λ -constacyclic kod ise $C = \langle \rho(x) \rangle$ olacak şekilde bir tek

$$\rho(x) = \eta_1 \rho_1(x) + \eta_2 \rho_2(x) + \eta_3 \rho_3(x) + \eta_4 \rho_4(x) + \eta_5 \rho_5(x) + \eta_6 \rho_6(x)$$

polinomu vardır ve $\rho(x)$, $x^n - \lambda$ nın sağ bölenidir.

İspat: Theorem 3.3.13. den

$$C = \langle \eta_1 \rho_1(x), \eta_2 \rho_2(x), \eta_3 \rho_3(x), \eta_4 \rho_4(x), \eta_5 \rho_5(x), \eta_6 \rho_6(x) \rangle$$

olduğunu biliyoruz. $\rho(x) = \eta_1 \rho_1(x) + \eta_2 \rho_2(x) + \eta_3 \rho_3(x) + \eta_4 \rho_4(x) + \eta_5 \rho_5(x) + \eta_6 \rho_6(x)$ olarak alınırsa $\langle \rho(x) \rangle \subseteq C$ elde edilir. Diğer taraftan $i = 1, 2, 3, 4, 5, 6$ için

$$\eta_1 \rho_1(x) = \eta_1 \rho(x),$$

$$\eta_2 \rho_2(x) = \eta_2 \rho(x),$$

$$\eta_3 \rho_3(x) = \eta_3 \rho(x),$$

$$\eta_4 \rho_4(x) = \eta_4 \rho(x),$$

$$\eta_5 \rho_5(x) = \eta_5 \rho(x),$$

$$\eta_6 \rho_6(x) = \eta_6 \rho(x)$$

şeklindedir. Böylece $C \subseteq \langle \rho(x) \rangle$ dir. O halde $C = \langle \rho(x) \rangle$ bulunur.

$i = 1, 2, 3, 4, 5, 6$ için $\rho_i(x)$ ler $x^n - \lambda$ polinomunun sağ bölenleri olduğundan $x^n - \lambda = k_i(x) \rho_i(x)$ olacak şekilde $k_i(x) \in B_q[x, \theta]$ vardır. Bu durumda

$$(\sum_{i=1}^6 \eta_i k_i(x)) \rho(x) = \sum_{i=1}^6 \eta_i k_i(x) \sum_{i=1}^6 \eta_i \rho_i(x)$$

$$\begin{aligned}
&= \sum_{i=1}^6 \eta_i k_i(x) \rho_i(x) \\
&= \sum_{i=1}^6 \eta_i (x^n - \lambda) = x^n - \lambda
\end{aligned}$$

elde edilir. O halde $\rho(x)$, $x^n - \lambda$ polinomunun sağ bölenidir.

Not 3.3.15. $h(x) = \sum_{i=0}^k h_i x^i \in B_q[x, \theta]$ bir polinom olsun. $\overline{h(x)} = \sum_{i=0}^k \theta^i (h_{k-i}) x^i$ polinomuna $h(x)$ polinomunun skew reciprocal polinomu denir.

Sonuç 3.3.16. $\mathbb{F}_q$ üzerinde tanımlı $C_1, C_2, C_3, C_4, C_5, C_6$ kodları sırasıyla, $\rho_1(x), \rho_2(x), \rho_3(x), \rho_4(x), \rho_5(x), \rho_6(x)$ üreteç polinomlarıyla üretilen skew λ_0 -constacyclic, $(\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)$ -constacyclic, $(\lambda_0 + \lambda_1)$ -constacyclic, $(\lambda_0 + \lambda_2)$ -constacyclic, $(\lambda_0 + \lambda_3)$ -constacyclic, $(\lambda_0 + \lambda_4)$ -constacyclic kodlar olsun.

$$x^n - \lambda_0 = \rho_1(x) h_1(x) \in B_q[x, \theta],$$

$$x^n - (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5) = \rho_2(x) h_2(x) \in B_q[x, \theta],$$

$$x^n - (\lambda_0 + \lambda_1) = \rho_3(x) h_3(x) \in B_q[x, \theta],$$

$$x^n - (\lambda_0 + \lambda_2) = \rho_4(x) h_4(x) \in B_q[x, \theta],$$

$$x^n - (\lambda_0 + \lambda_3) = \rho_5(x) h_5(x) \in B_q[x, \theta],$$

$$x^n - (\lambda_0 + \lambda_4) = \rho_6(x) h_6(x) \in B_q[x, \theta]$$

olmak üzere $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3 \oplus \eta_4 C_4 \oplus \eta_5 C_5 \oplus \eta_6 C_6$ ise

$$C^\perp = \langle \eta_1 \bar{h}_1(x) + \eta_2 \bar{h}_2(x) + \eta_3 \bar{h}_3(x) + \eta_4 \bar{h}_4(x) + \eta_5 \bar{h}_5(x) + \eta_6 \bar{h}_6(x) \rangle$$

ve

$$|C^\perp| = q^{\text{der}\rho_1(x) + \text{der}\rho_2(x) + \dots + \text{der}\rho_6(x)}$$

dir.

Tanım 3.3.17. C , $\mathbb{F}_q$ üzerinde tanımlı $6n$ uzunluğunda bir kod olsun. $i = 1, 2, \dots, 6$ olmak üzere $a^{(i)} \in \mathbb{F}_q^n$ ve $a = (a_1, a_2, \dots, a_{6n-1}) = (a^{(1)} | a^{(2)} | a^{(3)} | a^{(4)} | a^{(5)} | a^{(6)}) \in \mathbb{F}_q^{6n}$ olsun. Her $t = (t_0, t_1, \dots, t_{n-1}) \in \mathbb{F}_q^n$ için $\sigma(t) = (t_{n-1}, t_0, \dots, t_{n-2}) \in \mathbb{F}_q^n$ olmak üzere

$$\sigma^{\otimes 6}: \mathbb{F}_q^{6n} \rightarrow \mathbb{F}_q^{6n}$$

$$a \mapsto \sigma^{\otimes 6}(a) = (\sigma(a^{(1)})|\sigma(a^{(2)})|\sigma(a^{(3)})|\sigma(a^{(4)})|\sigma(a^{(5)})|\sigma(a^{(6)}))$$

dönüşümü tanımlansın. $\sigma^{\otimes 6}(C) = C$ ise C koduna indeksi 6 olan quasi-cyclic kod denir.

Tanım 3.3.18. $\delta = (\lambda_i: \lambda_i \in \mathbb{F}_q^*, 1 \leq i \leq s)$, $n = ms$, $a^i \in \mathbb{F}_q^n$ olmak üzere $\tau_{\delta,s}$ dönüşümü

$$\tau_{\delta,s}: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$$

$$\tau_{\delta,s}(a^1|a^2|\dots|a^s) = (\sigma_{\theta,\lambda_1}(a^1)|\sigma_{\theta,\lambda_2}(a^2)|\dots|\sigma_{\theta,\lambda_s}(a^s))$$

şeklinde tanımlansın. $\tau_{\delta,s}(C) = C$ oluyorsa, $\mathbb{F}_q$ üzerinde tanımlı n uzunluğunda lineer C koduna indeksi s olan skew multi-twisted kod denir.

Önerme 3.3.19. $\delta = (\lambda_0, \lambda_0 + \lambda_1 + \lambda_2 + \lambda_5, \lambda_0 + \lambda_1, \lambda_0 + \lambda_2, \lambda_0 + \lambda_3, \lambda_0 + \lambda_4)$ olmak üzere $\Psi\sigma_{\theta,\lambda} = \tau_{\delta,6}\Psi$ dir.

İspat: C, B_q üzerinde tanımlı bir kod, $t = (t_0, t_1, \dots, t_{n-1}) \in C$ ve $t_i = b_0^i + b_1^i v_1 + b_2^i v_2 + b_3^i v_3 + b_4^i v_4 + b_5^i v_1 v_2$ olmak üzere

$$\begin{aligned} \sigma_{\theta,\lambda}(t) &= (\lambda\theta(t_{n-1}), \theta(t_0), \dots, \theta(t_{n-2})) \\ &= (\lambda_0\theta(b_0^{n-1}) + (\lambda_0\theta(b_1^{n-1}) + \lambda_1\theta(b_0^{n-1}) + \lambda_1\theta(b_1^{n-1}))v_1 + (\lambda_0\theta(b_2^{n-1}) + \lambda_2\theta(b_0^{n-1}) + \lambda_2\theta(b_2^{n-1}))v_2 + (\lambda_0\theta(b_3^{n-1}) + \lambda_3\theta(b_0^{n-1}) + \lambda_3\theta(b_3^{n-1}))v_3 + \\ &\quad (\lambda_0\theta(b_4^{n-1}) + \lambda_4\theta(b_0^{n-1}) + \lambda_4\theta(b_4^{n-1}))v_4 + (\lambda_0\theta(b_5^{n-1}) + \lambda_1\theta(b_2^{n-1}) + \lambda_1\theta(b_5^{n-1}) + \lambda_2\theta(b_1^{n-1}) + \lambda_2\theta(b_5^{n-1}) + \lambda_5\theta(b_0^{n-1}) + \lambda_5\theta(b_1^{n-1}) + \lambda_5\theta(b_2^{n-1}) + \\ &\quad \lambda_5\theta(b_5^{n-1}))v_1 v_2, \theta(b_0^0) + \theta(b_1^0)v_1 + \theta(b_2^0)v_2 + \theta(b_3^0)v_3 + \theta(b_4^0)v_4 + \\ &\quad \theta(b_5^0)v_1 v_2, \dots, \theta(b_0^{n-2}) + \theta(b_1^{n-2})v_1 + \theta(b_2^{n-2})v_2 + \theta(b_3^{n-2})v_3 + \theta(b_4^{n-2})v_4 + \\ &\quad \theta(b_5^{n-2})v_1 v_2) \end{aligned}$$

dir. Buradan,

$$\begin{aligned} \Psi(\sigma_{\theta,\lambda}(t)) &= (\lambda_0\theta(b_0^{n-1}), \theta(b_0^0), \dots, \theta(b_0^{n-2}), (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)(\theta(b_0^{n-1}) + \\ &\quad \theta(b_1^{n-1}) + \theta(b_2^{n-1}) + \theta(b_5^{n-1})), \theta(b_0^0) + \theta(b_1^0) + \theta(b_2^0) + \theta(b_5^0), \dots, \theta(b_0^{n-2}) + \\ &\quad \theta(b_1^{n-2}) + \theta(b_2^{n-2}) + \theta(b_5^{n-2}), (\lambda_0 + \lambda_1)(\theta(b_0^{n-1}) + \theta(b_1^{n-1})), \theta(b_0^0) + \\ &\quad \theta(b_1^0), \dots, \theta(b_0^{n-2}) + \theta(b_1^{n-2}), (\lambda_0 + \lambda_2)(\theta(b_0^{n-1}) + \theta(b_2^{n-1})), \theta(b_0^0) + \\ &\quad \theta(b_2^0), \dots, (b_0^{n-2}) + \theta(b_2^{n-2}), (\lambda_0 + \lambda_3)(\theta(b_0^{n-1}) + \theta(b_3^{n-1})), \theta(b_0^0) + \end{aligned}$$

$$\theta(b_3^0), \dots, \theta(b_0^{n-2}) + \theta(b_3^{n-2}), (\lambda_0 + \lambda_4)(\theta(b_0^{n-1}) + \theta(b_4^{n-1})), \theta(b_0^0) + \theta(b_4^0), \dots, \theta(b_0^{n-2}) + \theta(b_4^{n-2}))$$

elde edilir. Diğer taraftan,

$$\Psi(t) = (b_0^0, b_0^1, \dots, b_0^{n-1}, b_0^0 + b_1^0 + b_2^0 + b_5^0, b_0^1 + b_1^1 + b_2^1 + b_5^1, \dots, b_0^{n-1} + b_1^{n-1} + b_2^{n-1} + b_5^{n-1}, b_0^0 + b_1^0, b_0^1 + b_1^1, \dots, b_0^{n-1} + b_1^{n-1}, b_0^0 + b_2^0, b_0^1 + b_2^1, \dots, b_0^{n-1} + b_2^{n-1}, b_0^0 + b_3^0, b_0^1 + b_3^1, \dots, b_0^{n-1} + b_3^{n-1}, b_0^0 + b_4^0, b_0^1 + b_4^1, \dots, b_0^{n-1} + b_4^{n-1})$$

dir, $\delta = (\lambda_0, \lambda_0 + \lambda_1 + \lambda_2 + \lambda_5, \lambda_0 + \lambda_1, \lambda_0 + \lambda_2, \lambda_0 + \lambda_3, \lambda_0 + \lambda_4)$ olmak üzere

$$\begin{aligned} \tau_{\delta,6}(\Psi(t)) = & (\lambda_0 \theta(b_0^{n-1}), \theta(b_0^0), \dots, \theta(b_0^{n-2}), (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_5)(\theta(b_0^{n-1}) + \\ & \theta(b_1^{n-1}) + \theta(b_2^{n-1}) + \theta(b_5^{n-1})), \theta(b_0^0) + \theta(b_1^0) + \theta(b_2^0) + \theta(b_5^0), \dots, \theta(b_0^{n-2}) + \\ & \theta(b_1^{n-2}) + \theta(b_2^{n-2}) + \theta(b_5^{n-2}), (\lambda_0 + \lambda_1)(\theta(b_0^{n-1}) + \theta(b_1^{n-1})), \theta(b_0^0) + \\ & \theta(b_1^0), \dots, \theta(b_0^{n-2}) + \theta(b_1^{n-2}), (\lambda_0 + \lambda_2)(\theta(b_0^{n-1}) + \theta(b_2^{n-1})), \theta(b_0^0) + \\ & \theta(b_2^0), \dots, \theta(b_0^{n-2}) + \theta(b_2^{n-2}), (\lambda_0 + \lambda_3)(\theta(b_0^{n-1}) + \theta(b_3^{n-1})), \theta(b_0^0) + \\ & \theta(b_3^0), \dots, \theta(b_0^{n-2}) + \theta(b_3^{n-2}), (\lambda_0 + \lambda_4)(\theta(b_0^{n-1}) + \theta(b_4^{n-1})), \theta(b_0^0) + \\ & \theta(b_4^0), \dots, \theta(b_0^{n-2}) + \theta(b_4^{n-2})) \end{aligned}$$

bulunur. Buradan,

$$\Psi \sigma_{\theta,\lambda} = \tau_{\delta,6} \Psi$$

eşitliği ispatlanmış olur.

Teorem 3.3.20. C, B_q üzerinde tanımlı n uzunluğunda bir skew λ -constacyclic kod olması için gerek ve yeter koşul $\Psi(C)$ nin $\mathbb{F}_q$ üzerinde tanımlı $6n$ uzunluğunda indeksi 6 olan bir skew multi-twisted kod olmasıdır.

İspat: C bir skew λ -constacyclic kod olsun. Bu durumda $\sigma_{\theta,\lambda}(C) = C$ dir. Ψ Gray dönüşümü uygulanırsa $\Psi(\sigma_{\theta,\lambda}(C)) = \Psi(C)$ elde edilir. Önerme 3.3.19. dan $\tau_{\delta,6}(\Psi(C)) = \Psi(C)$ dir. O halde $\Psi(C)$ indeksi 6 olan skew multi-twisted koddur.

Tersine $\Psi(C)$ indeksi 6 olan bir skew multi-twisted kod olsun. Bu durumda $\tau_{\delta,6}(\Psi(C)) = \Psi(C)$ dir. Önerme 3.3.19. dan $\tau_{\delta,6}(\Psi(C)) = \Psi(\sigma_{\theta,\lambda}(C)) = \Psi(C)$ elde edilir. Ψ , 1-1 olduğundan $\sigma_{\theta,\lambda}(C) = C$ dir. O halde C bir skew λ -constacyclic koddur.

Örnek 3.3.21. $q = 9, \gamma^2 = \gamma + 1$ olmak üzere

$$\begin{aligned}\mathbb{F}_9 &= \mathbb{F}_3[\gamma] = \{0, 1, \gamma, \gamma^2, \gamma^3, \gamma^4, \gamma^5, \gamma^6, \gamma^7\} \\ &= \{0, 1, \gamma, \gamma + 1, 2\gamma + 1, 2, 2\gamma, 2\gamma + 2, \gamma + 2\}\end{aligned}$$

şeklindedir. $a \in \mathbb{F}_9$ için $\theta(a) = a^3$ olacak şekilde Frobenius otomorfizmasını alalım.

$$x^6 - 1 = (x + \gamma^2)^2(x + \gamma^6)^2(x - 2)(x - 1) \in \mathbb{F}_9[x, \theta]$$

$$x^6 + 1 = (2x^5 + \gamma^7x^4 + x^3 + (2\gamma + 1)x^2 - x + \gamma + 2)(\gamma - x) \in \mathbb{F}_9[x, \theta]$$

$$\rho_1(x) = \rho_2(x) = \rho_3(x) = x^2 + \gamma^7x + 1$$

alınırsa,

$$C_1 = C_2 = C_3 = \langle x^2 + \gamma^7x + 1 \rangle$$

kodları $\mathbb{F}_9$ üzerinde 6 uzunluğunda skew cyclic kod olur.

$$\rho_4(x) = \rho_5(x) = \rho_6(x) = \gamma - x$$

alınırsa,

$$C_4 = C_5 = C_6 = \langle \gamma - x \rangle$$

kodları $\mathbb{F}_9$ üzerinde 6 uzunluğunda skew nega-cyclic kod olur. Bu durumda

$$\begin{aligned}C &= \langle \eta_1\rho_1(x) + \eta_2\rho_2(x) + \eta_3\rho_3(x) + \eta_4\rho_4(x) + \eta_5\rho_5(x) + \eta_6\rho_6(x) \rangle \\ &= \langle -x^2 + \gamma^7 + 1 + (v_2 + v_3 + v_4 - v_1v_2)(-x^2 - \gamma^7 - 1 + \gamma - x) \rangle\end{aligned}$$

kodu B_9 üzerinde 6 uzunluğunda skew $\lambda = (1 - 2v_2 - 2v_3 - 2v_4 + 2v_1v_2)$ -constacyclic kod olur.

Ayrıca $i = 1, 2, \dots, 6$ için $\lambda_i^2 = (\mp 1)^2 = 1$ olduğundan $\lambda^2 = 1$ olur. Bu durumda C bir self-dual kod olur. O halde $\Psi(C)$, $\mathbb{F}_9$ üzerinde $[36, 27, 3]$ self-dual koddur. Aynı zamanda $\delta = (1, 1, 1, -1, -1, -1)$ seçilirse $\Psi(C)$ skew multi-twisted kod olur.

Örnek 3.3.22. $q = 25$, $\mathbb{F}_{25} = \mathbb{F}_5[\gamma]$ ve $\gamma^2 = \gamma + 3$ olmak üzere $a \in \mathbb{F}_{25}$ için $\theta(a) = a^5$ olacak şekilde Frobenius otomorfizmasını alalım.

$$x^6 - 1 = (x^2 + \gamma^4)(x + 1)(x - 1)(x^2 + \gamma^{20}) \in \mathbb{F}_{25}[x, \theta]$$

$$x^6 + 1 = (x^2 + \gamma^8)(x - 3)(x - 2)(x^2 + \gamma^{16}) \in \mathbb{F}_{25}[x, \theta]$$

$$\rho_1(x) = (x - 1)(x^2 + \gamma^{20}) = x^3 - x^2 + \gamma^4x - \gamma^{20}$$

alınırsa

$$C_1 = \langle x^3 - x^2 + \gamma^4 x - \gamma^{20} \rangle$$

kodu $\mathbb{F}_{25}$ üzerinde 6 uzunluğunda skew cyclic kod olur.

$$\begin{aligned} \rho_2(x) = \rho_3(x) = \rho_4(x) = \rho_5(x) = \rho_6(x) &= (x - 2)(x^2 + \gamma^{16}) \\ &= x^3 - 2x^2 + \gamma^8 x - 2\gamma^{16} \end{aligned}$$

alınırsa

$$C_2 = C_3 = C_4 = C_5 = C_6 = \langle x^3 - 2x^2 + \gamma^8 x - 2\gamma^{16} \rangle$$

kodları $\mathbb{F}_{25}$ üzerinde 6 uzunluğunda skew nega-cyclic kod olur. Bu durumda

$$\begin{aligned} C &= \langle x^3 - x^2 + \gamma^4 x - \gamma^{20} \\ &\quad + (v_1 + v_2 + v_3 + v_4 - v_1 v_2)(x^2 - x\gamma^4 + \gamma^{20} - 2x^2 + \gamma^8 x \\ &\quad - 2\gamma^{16}) \rangle \end{aligned}$$

kodu B_{25} üzerinde 6 uzunluğunda skew $(1 - 2v_1 - 2v_2 - 2v_3 - 2v_4 - 2v_1 v_2) -$ constacyclic kod olur.

Ayrıca $\lambda_i^2 = 1$ olduğundan $\lambda^2 = 1$ olur. Buradan C bir self-dual koddur. O halde $\Psi(C)$, $\mathbb{F}_{25}$ üzerinde $[36, 18, 3]$ self-dual koddur. Aynı zamanda $\delta = (1, -1, -1, -1, -1, -1)$ seçilirse $\Psi(C)$ skew multi-twisted kod olur.

Örnek 3.3.23. $q = 25$, $\mathbb{F}_{25} = \mathbb{F}_5[\gamma]$, $\gamma^2 = \gamma + 3$ ve $n = 12$ olmak üzere

$a \in \mathbb{F}_{25}$ için $\theta(a) = a^5$ olacak şekilde Frobenius otomorfizmasını alalım.

$$\rho_1(x) = \rho_4(x) = x^2 + (2\gamma + 3)x - 2\gamma - 2 \in \mathbb{F}_{25}[x, \theta],$$

$$\begin{aligned} \rho_2(x) = \rho_3(x) = \rho_5(x) = \rho_6(x) &= x^5 + \gamma x^4 + \gamma^8 x^3 + \gamma^{21} x^2 + \gamma^{21} x + \gamma^{11} \in \\ &\mathbb{F}_{25}[x, \theta] \end{aligned}$$

seçilirse,

$$C_1 = C_4 = \langle x^2 + (2\gamma + 3)x - 2\gamma - 2 \rangle$$

$$C_2 = C_3 = C_5 = C_6 = \langle x^5 + \gamma x^4 + \gamma^8 x^3 + \gamma^{21} x^2 + \gamma^{21} x + \gamma^{11} \rangle$$

olmak üzere C_1, C_4 kodları $\mathbb{F}_{25}$ üzerinde 12 uzunluğunda skew cyclic kodlar, C_2, C_3, C_5, C_6 kodları $\mathbb{F}_{25}$ üzerinde 12 uzunluğunda skew nega-cyclic kodlar olur.

Bu durumda,

$$C = x^2 + (2\gamma + 3)x - 2\gamma - 2 + (v_1 + v_3 + v_4)\gamma x^4 + (1 + \gamma^8)x^3 + (\gamma^{21} - 1)x^2 + (\gamma^{21} - 2\gamma - 3)x + 2\gamma + 2 + \gamma^{11}$$

kode B_{25} üzerinde 12 uzunluğunda skew $(1 - 2v_1 - 2v_3 - 2v_4) - \text{constacyclic}$ kod olur.

Ayrıca $\lambda_i^2 = 1$ olduğundan $\lambda^2 = 1$ olur. Buradan C bir self-dual koddur. O halde $\Psi(C)$, $\mathbb{F}_{25}$ üzerinde $[72, 48, 4]$ self-dual koddur. Aynı zamanda $\delta = (1, -1, -1, 1, -1, -1)$ seçilirse $\Psi(C)$ skew multi-twisted kod olur.

Not 3.3.24. Her $b = b_0 + b_1v_1 + b_2v_2 + b_3v_3 + b_4v_4 + b_5v_1v_2 \in B_q$ için θ otomorfizması,

$$\theta(b) = \theta(b_0) + \theta(b_2)v_1 + \theta(b_1)v_2 + \theta(b_3)v_3 + \theta(b_4)v_4 + \theta(b_5)v_1v_2$$

şeklinde tanımlanarak benzer teori ve sonuçlar elde edilebilir.

4. SONUÇ

Bu tezde, $v_1^2 = v_1$, $v_2^2 = v_2$, $v_3^2 = v_3$, $v_4^2 = v_4$, $v_1v_2 = v_2v_1$, $v_1v_3 = 0$, $v_1v_4 = 0$, $v_2v_4 = 0$, $v_3v_4 = 0$ ve $q = p^m$, p bir tek asal, m pozitif bir tamsayı olmak üzere $B_q = \mathbb{F}_q + v_1\mathbb{F}_q + v_2\mathbb{F}_q + v_3\mathbb{F}_q + v_4\mathbb{F}_q + v_1v_2\mathbb{F}_q$ sonlu, birimli, değişmeli halka ailesi tanımlanarak bu halkanın özellikleri incelendi. B_q^n den $\mathbb{F}_q^{6n}$ e bir Gray dönüşümü verildi. B_q halka ailesi üzerinde aşikar olmayan bir θ otomorfizması tanımlanarak bu otomorfizmayla yardımıyla $B_q[x, \theta]$ polinom halkası oluşturuldu. Daha sonra bu halka üzerinde λ birimsel elemanı yardımıyla skew λ -constacyclic kodların cebirsel özellikleri incelendi ve bu kodların Gray görüntülerinin $\mathbb{F}_q$ üzerinde skew multi-twisted kodlar olduğu gösterildi. Son olarak B_q üzerinde skew λ -constacyclic kodlara bazı örnekler verildi. Böylelikle minimum uzaklığı yüksek ve daha geniş kod aileleri elde edebilmek amacıyla B_q üzerinde skew λ -constacyclic kodlar tanımlandı.

B_q halka ailesi üzerinde tanımlanan skew constacyclic kodlardan quantum kodlar ve $\lambda = 1$ alınarak skew cyclic kodlardan DNA kodlar elde edilebilir. Ayrıca B_q halkası k parçaya genelleştirilerek benzer çalışmalar yapılabilir ve parametreleri daha iyi olan farklı kodlar bulunabilir.

KAYNAKLAR

- Abualrub, T., Ghayeb A., Aydın N. and Siap I. (2010). "On the construction of skew quasi-cyclic codes". *IEEE Transactions on Information Theory*, 56 (5), 2081-2090.
- Abualrub, T, Seneviratne P. (2010). "Skew cyclic Codes over $\mathbb{F}_2 + v\mathbb{F}_2$ ". Proceeding of the International Multi Conference Of Engineers and Computer Scientists, Hong Kong, March 17-19.
- Abualrub, T., Aydın N. and Seneviratne P., (2012). "On θ -cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$ ". *Australasian Journal of Combinatorics* 54. 115-126.
- Arimoto, S. (1961). "Encoding and decoding of p-ary group codes and the correction system". *Information Processing in Japan* 2 , 320–325.
- AL-Ashker, M.M., Abu-Jazar, A.Q.M. (2016). "Skew constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ ". *Palestine Journal of Mathematics*, 5(2), 96–103.
- Bhaintwal, M., Wasan S. K. (2009). "On quasi-cyclic codes over $\mathbb{Z}_q$ ". *Applicable Algebra in Engineering, Communication and Computing*, 20 (5-6), 459-480.
- Bose, R. C., Ray-Chaudhuri D. K. (1960). "On A Class of Error Correcting Binary Group Codes". *Information and Control*, 3 (1), 68–79.
- Boucher, D., Geiselmann, W. ve Ulmer, F. (2007). "Skew Cyclic Codes". *Applicable Algebra in Eng. Comm. and Computing*, 18, 379-389.
- Boucher, D. ve Ulmer, F. (2009). "Coding with skew polynomial rings", *Journal of Symbolic Computation*, 44, 1644-1656.
- Çallıalp, F. (2013). "Örneklerle soyut cebir". İstanbul: Birsen Yayınevi.
- Çallıalp, F. ve Kuruoğlu, N. (1996). "Lineer cebir". Samsun: Ondokuz Mayıs Üniversitesi Yayınları.
- Çallıalp, F. (2018). "Örneklerle soyut cebir". İstanbul: Birsen Yayınevi.
- Dertli, A. (2016). "Halkalar üzerinde tanımlı kodlar hakkında bazı araştırmalar". Doktora Tezi. Ondokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı, Samsun.
- Fraleigh, J. B. (2003). "A First Course in Abstract Algebra". Pearson Education, Boston.
- Gao, J., Ma, F., & Fu, F. (2017). Skew constacyclic codes over the rin $\mathbb{F}_q + v\mathbb{F}_q$ g. *Appl. Comput. Math*, 6(3), 286-295.
- Grassl, M. (2013). "Bounds on the Minimum Distance of Linear Codes and Quantum Codes", <http://www.codetables.de>.
- Hamming, R. W. (1950). Error detecting and error correcting codes. *The Bell system technical journal*, 29(2), 147-160.
- Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J., & Solé, P. (1994). The $\mathbb{Z}/4\mathbb{Z}$ -linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2), 301-319.
- Hill, R. (1986). "A first course in coding theory". Oxford: The Oxford University Press.
- Huffman, W. C. and Pless, V. (2003). "Fundamentals of error correcting codes". New York: Cambridge University Press.
- Hungerford, T. W. (1973). *Algebra*. New York: Springer.

- Hocquenghem, A. (1959), "Codes correcteurs d'erreurs". Chiffres (in French), Paris, 2, 147–156.
- Islam, H., Prakash, O. (2018). "Skew cyclic and skew $(\alpha_1 + u\alpha_2 + v\alpha_3 + uv\alpha_4)$ -constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$ ". International Journal of Information and Coding Theory, 5(2), 101-116.
- Islam, H., Prakash, O. (2017). Skew constacyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$. arXiv preprint arXiv:1710.07789.
- Jitman, S., Ling, S. and Udamkavanich, P. (2010). "Skew constacyclic codes over finite chain rings". Advances in Mathematics of Communications, 6(1), 39-63.
- Ling, S. and Xing, C. (2004). "Coding theory a first course". New York: Cambridge University Press.
- McDonald, B.R. (1974). "Finite Rings With Identity". Marcel Dekker Inc., New York.
- Qian, J., Zhang L. N., Zhu S. X., 2006. " $(1 + u)$ -constacyclic and cyclic codes over $\mathbb{F}_{2^u} + u\mathbb{F}_2$ ". Appl. Math. Letters, 19, 820-823.
- Parange, E., (1957). "Cyclic error-correcting codes in two symbols". Air Force Cambridge Research Center-TN-57-103.
- Reed, I. S. (1953). A class of multiple-error-correcting codes and the decoding scheme. Massachusetts Inst of Tech Lexington Lincoln Lab.
- Reed, I. S., Solomon, G. (1960). Polynomial codes over certain finite fields. Journal of the society for industrial and applied mathematics, 8(2), 300-304.
- Roman, S. (1992). "Coding and Information Theory", Graduate Texts in Mathematics, Springer Verlag.
- Shannon, C., (1948). "A Mathematical Theory of Communication". The Bell System Technical Journal, 27, 379-423, 623-656.
- Siap, I., Abualrub, T., Aydin, N. and Seneviratne P. (2011). "Skew Cyclic Codes of Arbitrary Length", Int. J. Inform. Coding Theory, 2, 10-20.
- Wan, Z. X. (2003). Lectures on finite fields and Galois rings. World Scientific Publishing Company.