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

BAZI CEBİRSEL YAPILAR ÜZERİNDE TANIMLI KODLAR VE UYGULAMALARI

Doktora Tezi

Rabia DERTLİ

Danışman

Prof. Dr. Şenol EREN

SAMSUN
2024

TEZ KABUL VE ONAYI

Rabia DERTLİ tarafından, **Prof. Dr. Şenol EREN** danışmanlığında hazırlanan **"BAZI CEBİRSEL YAPILAR ÜZERİNDE TANIMLI KODLAR VE UYGULAMALARI"** başlıklı bu çalışma, jürimiz tarafından 21.2.2024 tarihinde yapılan sınav sonucunda oy birliği ile başarılı bulunarak Doktora Tezi olarak kabul edilmiştir.

	Unvanı Adı Soyadı **Üniversitesi** **Ana Bilim/Ana Sanat Dalı**	**Sonuç**
Başkan	Prof. Dr. Yasemin ÇENGELLENMİŞ Trakya Üniversitesi Matematik Ana Bilim Dalı	☒ Kabul ☐ Ret
Üye	Prof. Dr. Şenol EREN Ondokuz Mayıs Üniversitesi Matematik Ana Bilim Dalı	☒ Kabul ☐ Ret
Üye	Prof. Dr. Emin KASAP Ondokuz Mayıs Üniversitesi Matematik Ana Bilim Dalı	☒ Kabul ☐ Ret
Üye	Prof. Dr. Hamza ÇALIŞICI Ondokuz Mayıs Üniversitesi Matematik Eğitimi Ana Bilim Dalı	☒ Kabul ☐ Ret
Üye	Dr. Öğr. Üyesi Esra ÖZTÜRK SÖZEN Sinop Üniversitesi Matematik Ana Bilim Dalı	☒ Kabul ☐ Ret

Bu tez, Enstitü Yönetim Kurulunca belirlenen ve yukarıda adları yazılı jüri üyeleri tarafından uygun görülmüştür.

Prof. Dr. Ahmet TABAK
Enstitü Müdürü

BİLİMSEL ETİĞE UYGUNLUK BEYANI

Hazırladığım Doktora 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 ☒

04 / 01 / 2024
Rabia DERTLİ

TEZ ÇALIŞMASI ÖZGÜNLÜK RAPORU BEYANI

Tez Başlığı : BAZI CEBİRSEL YAPILAR ÜZERİNDE TANIMLI KODLAR VE UYGULAMALARI

Yukarıda başlığı belirtilen tez çalışması için şahsım tarafından 04.01.2024 tarihinde intihal tespit programından alınmış olan özgünlük raporu sonucunda;

Benzerlik oranı : % 15

Tek kaynak oranı : % 3 çıkmıştır.

04 / 01 / 2024
Prof. Dr. Şenol EREN

ÖZET

BAZI CEBİRSEL YAPILAR ÜZERİNDE TANIMLI KODLAR VE UYGULAMALARI

Rabia DERTLİ
Ondokuz Mayıs Üniversitesi
Lisansüstü Eğitim Enstitüsü
MATEMATİK ANA BİLİM DALI
Doktora, Şubat/2024
Danışman: Prof. Dr. Şenol EREN

Beş bölümden oluşan bu tezde literatürde yer almayan bir halka ve bu halkayı kullanarak oluşturulan mix alfabe üzerinde tanımlı bazı lineer kodların DNA ve kuantum uygulamaları incelenmiştir.

Birinci bölümünde, kodlama teorisi, DNA kodlar ve kuantum kodlar ile ilgili literatür bilgisi verilmiştir.

İkinci bölümde, cebir ve kodlama teorisi ile ilgili temel tanım ve teoremlere yer verilmiştir.

Üçüncü bölümde, literatürde yer almayan sonlu ve değişmeli bir S_q halkası tanımlanarak Çin Kalan Teoremi yardımıyla bu halkanın parçalı yazılışı elde edilmiştir. Bu yazılışı kullanarak S_q halkası üzerinde devirli kodların yapısı incelenerek üreteç polinomları elde edilmiştir. Ayrıca S_q üzerinde aşikar olmayan bir otomorfizma tanımlanarak skew devirli kodların cebirsel yapısı ifade edilmiştir. S_q halkası üzerinde tanımlanan bu iki tip koddan elde edilen DNA kodlar ve S_q halkası üzerindeki devirli kodlardan elde edilen kuantum kodlar çalışılmış ve bu konular ile ilgili çeşitli örnekler verilmiştir.

Dördüncü bölümde, S_q halkası kullanılarak oluşturulan mix alfabe olarak adlandırılan $R_q = F_q S_q$ halkası üzerinde tanımlı lineer kodların cebirsel yapısı verilmiş ve R_q-devirli, R_q-skew devirli kodlar tanımlanmıştır. R_q-devirli kodlardan elde edilen DNA kodlar, R_q-skew devirli kodlardan elde edilen kuantum kodlar çalışılmış ve bu konular ile ilgili bazı örnekler verilmiştir.

Beşinci bölümde ise sonuçlara yer verilmiştir.

Anahtar Sözcükler: DNA Kodlar, Kuantum Kodlar, Devirli Kodlar, Skew Devirli Kodlar, Sonlu Halkalar, Gray Dönüşümü.

ABSTRACT

CODES OVER SOME ALGEBRAIC STRUCTURES AND THEIR APPLICATIONS

Rabia DERTLİ
Ondokuz Mayıs University
Institute of Graduate Studies
Department of Mathematics
Ph.D., February/2024
Supervisor: Prof. Dr. Şenol EREN

This thesis, consisting of five sections, investigates the DNA and quantum applications of some linear codes defined on a ring not included in the literature and on a mixed alphabet created using this ring.

The first section provides a literature review on coding theory, DNA codes, and quantum codes.

The second section provides fundamental definitions and theorems related to algebra and coding theory.

In the third section, a finite and commutative ring S_q, which is not included in the literature, is defined and the partial representation of this ring is obtained with the help of the Chinese Remainder Theorem. Using this script, the structure of cyclic codes over the ring S_q is examined. In addition, the algebraic structure of skew cyclic codes is expressed by defining a nontrivial automorphism over S_q. DNA codes obtained from these two types of codes defined over the ring S_q and quantum codes obtained from cyclic codes over the ring S_q have been studied and various examples on these subjects have been given.

In the fourth section, the algebraic structure of linear codes defined over the ring $R_q = F_q S_q$, called the mixed alphabet created using the ring S_q, is given and R_q-cyclic and R_q-skew cyclic codes are defined. DNA codes obtained from R_q-cyclic codes and quantum codes obtained from R_q-skew cyclic codes have been studied and some examples on these subjects are provided.

In the fifth section, the results are given.

Keywords: DNA Codes, Quantum Codes, Cyclic Codes, Skew Cyclic Codes, Finite Rings, Gray Map.

ÖN SÖZ VE TEŞEKKÜR

Akademik çalışmalarım süresince beni destekleyen ve yardımlarını esirgemeyen değerli hocam Sayın Prof. Dr. Şenol EREN'e en içten teşekkürlerimi sunarım.

Tecrübeleri ve bilgeliğiyle beni her zaman doğru yönlendiren, insani ve ahlaki değerleriyle örnek olan, tecrübelerinden büyük ölçüde yararlanmama vesile olan kendi bilgi birikimini paylaşmaktan kaçınmayan ve hayatımın birçok alanında bana rehberlik eden değerli hocam Prof. Dr. Yasemin ÇENGELLENMİŞ'e en içten teşekkürlerimi sunarım.

Değerli jüri üyelerine önerilerinden dolayı teşekkür ederim.

Hayatım boyunca her türlü maddi ve manevi desteklerini esirgemeyen sevgili aileme, arkadaşlarıma ve Dr. Savaş KARAAHMETOĞLU'na ve bu süreçte en büyük manevi desteğim olan sevgili eşime sonsuz teşekkürlerimi sunarım.

Rabia DERTLİ

İÇİNDEKİLER

SİMGELER VE KISALTMALAR

$|C|$: C kodunun eleman sayısı

$C^{\perp}$: C kodunun duali

$d(C)$: C kodunun minimum Hamming uzaklığı

$d_L(C)$: C kodunun minimum Lee uzaklığı

$d_G(C)$: C kodunun minimum Gray uzaklığı

der$f(x)$: $f(x)$ polinomunun derecesi

$C = \langle f(x) \rangle$: $f(x)$ polinomu ile üretilen C kodu

F_q : q elemanlı Galois cismi

F_q^n : n uzunluğunda bileşenleri F_q'nun elemanı olan vektörlerin kümesi

$F_q[x]$: Katsayıları F_q cisminin elemanları olan x değişkenine bağlı polinom halkası

$F_q[x, \theta]$: θ otomorfizması ile belirli skew polinom halkası

$|\langle \theta \rangle|$: θ otomorfizmasının mertebesi

(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 lineer kod

$[[n, k, d]]$: n uzunluğunda k boyutlu ve minimum uzaklığı d olan kuantum kod

$w_H(x)$: x'in Hamming ağırlığı

$w_L(x)$: x'in Lee ağırlığı

$w_G(x)$: x'in Gray ağırlığı

$w_H(C)$: C kodunun minimum Hamming ağırlığı

$w_L(C)$: C kodunun minimum Lee ağırlığı

$w_G(C)$: C kodunun minimum Gray ağırlığı

$| \rangle$: Ket vektörü

$\langle |$: Bra vektörü

$\mathbb{C}^q$: q boyutlu karmaşık Hilbert uzayı

$A^{\otimes n}$: A kümesinin n defa tensör çarpımı

δ : S_q^n den F_q^{7n} e tanımlanan Gray dönüşümü

θ : F_q üzerinde tanımlı Frobenius otomorfizması

σ : Devirli öteleme dönüşümü

S_q : $F_q + w_1F_q + w_2F_q + w_3F_q + w_4F_q + w_5F_q + w_1w_2F_q$ halkası

R_q : F_qS_q halkası

ψ : R_q dan F_q^8 e tanımlanan Gray dönüşümü

C_γ : C, R_q-lineer kodunun ilk γ koordinatı

C_μ : C, R_q-lineer kodunun son μ koordinatı

DNA : Deoksiribo Nükleik Asit

A : Adenin

T : Timin

G : Guanin

C : Sitozin

h^R : h vektörünün ters sıralısı

h^C : h vektörünün tamlayanı

h^{RC} : h vektörünün ters sıralı tamlayanı

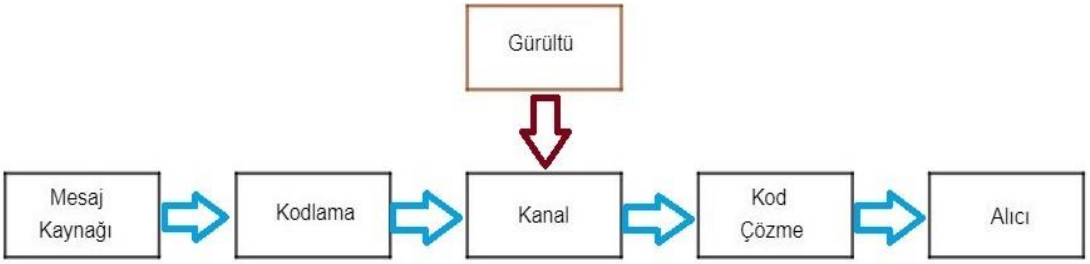
ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

1. GİRİŞ

Claude Shannon'un 1948'de yayımlanan "A Mathematical Theory of Communication" adlı makalesi, kodlama teorisinin temelini oluşturan önemli bir dönemeçtir (Shannon, 1948). Bu etkileyici makalede, iletişim kanallarında (örneğin telefon, radyo, uydu) kodlama ve kod çözme teknikleri kullanılarak belirli bir sınıra kadar güvenilir iletişim sağlanabileceği ortaya konmuştur. Bu makale, kodlama teorisine yönelik bir başlangıç noktası olmuştur ve sonrasında, iletim oranını artırmak, enerji ve zaman tasarrufu sağlamak amacıyla kodlanmış verinin iletimi, bozulmuş mesajların düzeltilmesi gibi konular üzerinde çalışılmıştır (Hill, 1986).

Kodlama genellikle iki ana gruba ayrılır: kaynak kodlama ve kanal kodlama. Kaynak kodlamada, bilgiyi daha etkin bir şekilde temsil etmek için verinin boyutu azaltılır. Günlük hayatta karşılaştığımız sıkıştırma programları, bu tür bir kodlamanın pratik uygulamalarından biridir; bu işlem, dosyaların boyutunu küçültmek amacıyla gerçekleştirilir. Öte yandan, kanal kodlamada, iletim sırasında oluşabilecek bozulmalara karşı daha güvenli bir iletişim sağlanabilmesi için bilgiye ekstra bitler eklenir. Bu nedenle, bilginin boyutu artar. Örneğin, cep telefonlarında, yüksek frekanslı radyo iletiminden kaynaklanan parazit ve bozulmaları düzeltmek için kanal kodlama kullanılmaktadır. Aynı şekilde, modemlerde ve telefon sinyali iletiminde de kanal kodlama önemli bir rol oynamaktadır.



Şekil 1.1 Dijital bir haberleşme sistemi

Şekil 1.1'de, dijital bir iletişim sisteminde gönderilen bir mesajın, kaynaktan alıcıya ulaşana kadar geçirdiği süreç anlatılmaktadır. Temel iletişim sistemlerinde, gönderilecek mesaj, kaynaktan kanala aktarılır; bu kanalda oluşabilecek hatalardan (ekipman eksikliği, insan hataları, hava koşulları, vb.) korumak için çeşitli matematiksel kodlama yöntemleri uygulanır. Kodlanan mesaj, dekodlama (kod çözme) birimine ulaştığında, mesajın kodlama algoritması ile uyumlu bir dekodlama

yöntemi kullanılarak bozulmuş halleri düzeltilip alıcıya doğru iletimi sağlanmaya çalışılır.

Kodlama teorisinde, ilk araştırmalar F_2 sonlu cisminde gerçekleştirilmiştir. Hamming ve Golay kodları bu sonlu cisim kullanılarak oluşturulmuştur. 1972 yılında Blake tarafından ilk olarak sonlu halkalar üzerinde kodlar ile ilgili çalışmalar yapılmıştır (Blake, 1972). Hammons ve arkadaşlarının 1994'te, Gray dönüşümü kullanarak yaptıkları çalışmalar sonucunda koodlama teorisindeki araştırmaların büyük bir kısmının artık halkalar üzerinde tanımlandığını ortaya koymuştur (Hammons vd., 1994).

Devirli kodlar (cyclic codes), son 50 yıldır pek çok bilim insanı tarafından çalışılmıştır. Kodların bu sınıfı ilk olarak Prange tarafından 1957 yılında tanımlanmıştır (Prange, 1957). Devirli kodlar, kodlama teorisindeki önemli bir sınıf olan hata düzeltici kodlar sınıfını oluşturur. Prange tarafından bir F_q sonlu cismi üzerinde n uzunluğuna sahip bir devirli koda karşılık gelen $F_q[x]/\langle x^n - 1\rangle$ halkasının bir idealinin var olduğu gösterilmiştir. Devirli kod kavramı genelleştirilerek birimsel (sabit) devirli (constacyclic), parçalı devirli (quasi-cyclic) ve negatif devirli (negacyclic) kod kavramları tanımlanmış ve tüm bu çalışmalar, değişmeli halkalar üzerinde tanımlı kodlara taşınmıştır.

Zaman içerisinde, bilim insanları belirli niteliklere sahip klasik hata düzelten kodların çeşitli disiplinlerdeki uygulamalarını inceleyerek önemli bulgular elde etmişlerdir. Bu disiplinler arasında, DNA hesaplaması ve kuantum hesaplaması öne çıkmaktadır. DNA hesaplama kavramı, 1987 yılında Tom Head tarafından öne sürülmüş olup, ilk başarılı deneysel çalışma ise L. Adleman tarafından gerçekleştirilmiştir (Head, 1987). Adleman'ın yaptığı deney, DNA iplikçiklerini kullanarak Hamilton yolu problemine ait bir örneği çözme amacını taşımaktadır (Adleman, 1994). Adleman'ın bu başarılı deneyi, DNA hesaplama alanındaki matematiksel özelliklerin belirlenmesi, DNA nano-yapılarının oluşturulması, DNA dizilerindeki hata düzeltme özelliklerinin araştırılması ve DNA tabanlı veri depolama sistemleri gibi farklı alanlara yönelik çeşitli gelişmelere yol açmıştır.

DNA kodlaması, yüzey tabanlı DNA bilimi, moleküler barkodlarla kimyasal kütüphaneler, DNA Mikroarray teknolojisi, DNA nano-yapıları, veri şifreleme, veri

depolama, DNA nano-araçları, sinyal işleme ve devreleri gibi çeşitli teknolojik alanlarda kullanılmaktadır. Son zamanlarda, DNA kodlarının filogenetik araştırmalarda potansiyeli vurgulanmıştır. Ayrıca, gen düzenleyici ağları ve devirli kodlar aracılığıyla gen yapılarına ilişkin derinlemesine çalışmalara katkı sağlamıştır. Moleküler barkodlar olarak kullanılan DNA kodları, ürünlerin doğrulanmasında biyobelirteç olarak önem kazanmıştır. DNA kodlarının etkili bir şekilde kodlanması, özellikle hedeflenmiş ilaç teslimat sistemleri gibi potansiyel uygulamalarda kullanılan DNA nano-yapılarının tasarımında elde edilecek nano-yapıların yüksek kararlılık ve sağlamlığa sahip olmasında kritik bir rol oynadığı belirtilmiştir (Dixita vd., 2016).

$S = \{A, T, C, G\}$, DNA alfabesi olmak üzere S^n kümesinin herhangi bir alt kümesine DNA kod denir. Bir DNA kodun sağlaması gereken Hamming kısıtlaması, ters sıralı kısıtlama, ters sıralı tamamlayan kısıtlama, GC kısıtlaması gibi kısıtlamalar mevcuttur. Verilen uzunluk, eleman sayısı ve uzunlukta maksimum sayıda kısıtlamayı sağlayan bir DNA kod oluşturmak en zorlayıcı problemlerden biridir. Bu bağlamda ters sıralı tamamlayan kısıtlamayı sağlayan blok kodlara DNA kod adı verilir. Klasik hata düzelten kodlar, DNA kod oluşturmak için geniş ölçüde kullanılmaktadır. Klasik hata düzelten kodlardan DNA kod elde etmek için bilim insanları pek çok yöntem geliştirmiştir. Skew devirli kodlardan DNA kod eldesi, devirli kodlardan DNA kod eldesi sadece bunlardan birkaçıdır. Farklı tipte cebirsel yapılar kullanarak, bu cebirsel yapılar üzerinde tanımlı farklı tipte klasik kodlardan farklı methodlarla arzu edilen nitelikte DNA kod elde etmek önemli problemlerden bir tanesidir.

DNA molekülü, nükleotid adı verilen çift sarmallı bir moleküler yapıya sahiptir. DNA'nın çift sarmal yapısı, genetik bilginin depolanmasını, korunmasını ve aktarılmasını sağlar. Bir nükleotid, bir şeker molekülü, bir fosfat grubu ve bir nükleobaz içerir. DNA'daki dört farklı temel baz G (Guanin), C (Sitozin), A (Adenin), T (Timin)'dir. Bu temel dört baz arasında $G = C$ ve $A = T$ tamlaması vardır ve bu eşleşme hidrojen bağları kullanılarak gerçekleşir. Adenin ve timin arasında iki, guanin ve sitozin arasında üç hidrojen bağı bulunur. DNA, yoğun baz birikimi ve kendi kendini çoğaltma ve tamamlama özellikleri açısından zengin bir hesaplama kaynağıdır. Bu özellikler, DNA molekülünün sonlu cisimler ve sonlu

halkalar üzerinde kodlama teorisine önemli katkılarda bulunmasına neden olmuştur. Bu çalışmalar, ilk olarak 4 elemanlı GF(4) sonlu cismi üzerinde yapılmıştır (Abualrub vd., 2006). Sonra bu çalışmalar 4 ve 4 ün katı eleman sayısına sahip farklı lineer kodlar kullanılarak sonlu halkalar üzerine taşınmıştır (Parakash vd., 2023; Alahmadi vd., 2021; Bathala ve Bhaintwal, 2017; Dinh vd., 2018).

Kuantum bilgi işleme, kuantum teorisinin ifade ettiği fiziksel gerçekliği kullanarak daha önce mümkün görülmeyen görevleri gerçekleştirmeyi amaçlayan bir alandır. Bu tür bilgi işleme görevlerini yerine getiren cihazlar genellikle kuantum bilgisayarlar olarak adlandırılır (Kaye vd., 2006). Klasik bilgisayarlar yetersiz kaldığında, özellikle büyük sayılarla yapılan hesaplamalarda, kuantum bilgisayarlar tercih edilmeye başlanmıştır. Kuantum bilgisayarların temel farkı, kuantum fiziğinin kurallarını kullanmalarıdır.

Kuantum bilgisayarların hesaplama güçleri ve hızları, klasik bilgisayarlarla karşılaştırıldığında önemli ölçüde daha yüksektir. Örneğin, sayıyı çarpanlara ayırma problemi klasik bilgisayarlar için büyük sayılarla zorlu hale gelebilirken, kuantum bilgisayarlar bu tür işlemleri çok daha hızlı bir şekilde gerçekleştirebilirler.

Klasik bilgisayarlar, bitlerden oluşan bellek yapılarına sahiptir ve her bir bit sadece 1 veya 0 değerini alabilir. Kuantum bilgisayarları ise kübitlerden oluşan serilere sahiptir. Süperpozisyon adı verilen bir durumda, tek bir kübit sadece 1 veya 0 değil, bu ikisi arasındaki tüm değerleri alabilir. Bu özellik, kuantum bilgisayarlarının aynı anda birçok durumu işleyebilmesini sağlar. İşlemler sırasında elde edilen sonuçlar daha sonra anlaşılabilir bir formda olması için bitlere dönüştürülür (Dertli, 2016).

Kuantum kodlama, güvenli iletişim ve bilgi saklamak için kuantum mekaniğini kullanan bir kodlama türüdür. Kuantum bilgisayarlarının karşılaştığı zorluklardan biri, kuantum hallerin çevresel etkileşimler nedeniyle bozulma eğiliminde olmalarıdır. Bu durum, hatalı hesaplamalara ve sistem çökmesine yol açabilir. Kuantum bilgisayarlarında bu hassas kuantum hallerini korumak için "Kuantum Hata Düzeltici Kodlar" kullanılır. Bu kodlar, çeşitli hataları tespit etmek ve düzeltmek için tasarlanmıştır (Dertli, 2016).

Kuantum hata düzeltici kodlar, bilgi depolama ve iletişim sistemleri gibi bilgi transferi sırasında oluşabilecek hataları fark edip düzeltebilen klasik hata düzeltici kodlama teorisinden farklıdır. Calderbank ve diğerleri, bu iki teori arasında bir geçiş sağlamışlardır (Calderbank ve Shor, 1996). Kuantum hata düzeltici kodlar, ilk olarak P. W. Shor ve Steane tarafından geliştirilmiştir (Shor, 1995; Steane, 1996). Bu kodlar, kuantum bilgisayarlarının matematiksel işlemlerini tanımlamak için kullanılmış ve çeşitli avantajları ortaya konmuştur.

Calderbank ve Shor, klasik kodların dualini içerme ve self-ortogonal olma özelliklerini kullanarak kuantum kodlarını elde etmişlerdir (Calderbank ve Shor, 1996). Ayrıca, Calderbank ve diğerleri, GF(4) sonlu cismi üzerindeki klasik kodlardan faydalanarak kuantum kodları elde etmek için bir yöntem sunmuşlardır (Calderbank vd., 1998). Bu şekilde, farklı cebirsel yapılar üzerinde tanımlı klasik hata düzeltici kodlardan iyi kuantum kodlar elde etmek önemli bir araştırma konusu olarak öne çıkmaktadır.

Bu çalışmalardan sonra sonlu halkalar üzerindeki farklı lineer kodlar kullanılarak kuantum kodların parametreleri elde edilmiştir. İlk olarak J. Qian vd. $F_2 + uF_2,\ u^2 = 0$ halkası üzerinde (Qian vd., 2009) daha sonra X. Kai, S. Zhu $F_4 + uF_4,\ u^2 = 0$ halkası üzerinde (Kai ve Zhu, 2011), X. Yin ve W. Ma $F_2 + uF_2 + u^2F_2,\ u^3 = 0$ halkası üzerinde (Yin ve Ma, 2011), J. Qian $F_2 + vF_2,\ v^2 = v$ halkası üzerinde (Qian, 2013) tanımlı devirli kodlardan kuantum kodların parametrelerini elde etmişlerdir. Klasik lineer kodlardan faydalanılarak kuantum kodlar ile ilgili bir çok çalışma yapılmıştır (Grassl ve Beth, 2004; Sarma, 2012; Ashraf ve Mohammad, 2014; Gao ve Wang, 2018; Li vd., 2018; Islam ve Prakash, 2019; Prakash vd., 2021).

Günümüzde kodlama teorisinde dikkat çeken konulardan biri de farklı cebirsel yapılar bir araya getirilerek oluşturulan ve mix alfabe olarak adlandırılan yeni yapılardır. Bu mix alfabe üzerinde, son zamanlarda farklı lineer kod türleri kullanılarak DNA ve kuantum kodlar ile ilgili çalışmalar yapılmaktadır (Li vd., 2020; Dinh vd., 2020; Benbelkacem vd., 2022; Hebbache ve Sharma, 2022). Bu da kodlama teorisine yeni bir perspektif sunarak parametreleri iyi bir takım kodlar elde etme ihtimalini artırmaktadır.

Zengin cebirsel yapısı ve uygulanabilirliği açısından lineer kodların önemli bir sınıfı olan devirli ve skew devirli kodlar ile ilgili literatürde pek çok çalışma mevcuttur. Bu çalışmanın temel amacı, devirli ve skew devirli kodlarla ilgili bilgi alanına katkı sağlamak ve bu alandaki araştırmalara yeni bir perspektif sunmaktır. Bu bağlamda tezde literatürde yer almayan S_q halkası üzerinde tanımlanan devirli ve skew devirli kodlardan elde edilen DNA kodlar ve S_q halkası üzerindeki devirli kodlardan elde edilen kuantum kodlar çalışılmıştır. S_q halkasını kullanarak oluşturulan $R_q = F_q S_q$ mix alfabe üzerinde R_q-devirli kodlardan elde edilen DNA kodlar, R_q-skew devirli kodlardan elde edilen kuantum kodlar incelenmiştir.

2. TEMEL KAVRAMLAR

Tanım 2.1. G boştan farklı bir küme ve " $*$ ", G üzerinde bir ikili işlem olmak üzere

i) Her $a, b, c \in G$ için $a * (b * c) = (a * b) * c$

ii) En az bir $e \in G$ vardır öyle ki her $a \in G$ için $a * e = e * a = a$

iii) Her $a \in G$ için $a * a^{-1} = a^{-1} * a = e$ olacak şekilde $\exists\ a^{-1} \in G$ vardır

koşulları sağlanıyorsa $(G,*)$ cebirsel yapısına bir grup denir (Çallıalp, 2013).

Tanım 2.2. $(G,*)$ bir grup olmak üzere her $a, b \in G$ için $a * b = b * a$ oluyorsa G grubuna değişmeli grup veya Abel grubu denir (Çallıalp, 2013).

Tanım 2.3. R boştan farklı bir küme, " $+$ " ve " $\cdot$ ", R üzerinde ikili işlemler olmak üzere

i) $(R, +)$ bir değişmeli grup

ii) Her $a, b, c \in R$ için $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

iii) Her $a, b, c \in R$ için $a \cdot (b + c) = a \cdot b + a \cdot c$ ve $(a + b) \cdot c = a \cdot c + b \cdot c$

koşulları sağlanıyorsa $(R, +, \cdot)$ cebirsel yapısına bir halka denir (Hungerford, 1973).

Tanım 2.4. $(R, +, \cdot)$ bir halka olsun. R halkası " $\cdot$ " işlemine göre birim elemana sahipse $(R, +, \cdot)$ halkasına birimli halka denir ve halkanın birimi 1 ile gösterilir (Hungerford, 1973).

Eleman sayısı sonlu olan halkaya sonlu halka denir ve R sonlu bir halka olmak üzere R halkasının eleman sayısı $|R|$ ile gösterilir.

Tanım 2.5. R birimli bir halka olmak üzere R halkasında tersi mevcut olan elemanlara birimsel eleman denir (Hungerford, 1973).

Tanım 2.6. $(R, +, \cdot)$ bir halka olsun. Her $a, b \in R$ için $a \cdot b = b \cdot a$ oluyorsa $(R, +, \cdot)$ halkasına değişmeli halka denir (Hungerford, 1973).

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

i) Her $a, b \in I$ için $a - b \in I$

ii) Her $a \in I$ ve her $r \in R$ için $r \cdot a \in I$ $(a \cdot r \in I)$

koşulları sağlanıyorsa I ya R nin bir sol (sağ) ideali denir (Hungerford, 1973).

Eğer I, hem sol hem de sağ ideal ise I ya kısaca ideal denir. $\{0\}$ ve R, R halkasının idealleridir. Bu ideallere R halkasının aşikar idealeri denir. R halkasının bu ideallerden farklı ideallerine de öz idealleri denir.

Tanım 2.8. A, R halkasının bir alt kümesi olsun. R nin A kümesini kapsayan bütün ideallerinin arakesitine A kümesinin ürettiği ideal denir ve $\langle A\rangle$ ile gösterilir. $A=\{a\}$ tek elemanlı bir küme ise A nın ürettiği ideale temel ideal denir ve $\langle a\rangle$ ile gösterilir. Burada a elemanına da A idealinin bir üreteci denir (Hungerford, 1973).

Tanım 2.9. R bir halka ve $0\neq a\in R$ olmak üzere $ma=0$ eşitliğini sağlayan en küçük pozitif m tam sayısına R halkasının karakteristiği denir ve $karR$ ile gösterilir. Böyle bir m pozitif tam sayısı yoksa halkanın karakteristiği sıfırdır denir (Hungerford, 1973).

Tanım 2.10. R birimli ve değişmeli bir halka ve M de R halkasının $\langle 1\rangle$ den farklı bir ideali olsun. R halkasının M idealini kapsayan M ve R den başka ideali yoksa, M idealine R halkasının bir maksimal ideali denir (Hungerford, 1973).

Tanım 2.11. Tek bir maksimal ideali olan halkaya bir yerel (lokal) halka denir. Sonlu sayıda maksimal ideali olan halkaya ise yarı yerel (semi lokal) halka denir (Jitman vd., 2010).

Tanım 2.12. R birimli, değişmeli ve sonlu bir halka olsun. R halkasının tüm ideallerinin kümesi kapsama bağıntısına göre tam sıralı ise R halkasına sonlu zincir halkası denir (Jitman vd., 2010).

Önerme 2.13. R bir sonlu zincir halkası ise R nin her ideali esas idealdir ve R tek maksimal ideale sahiptir. γ, R halkasının maksimal idealinin bir üreteci olmak üzere R halkasının tüm idealleri

$$R=\langle 1\rangle \supsetneq \langle \gamma\rangle \supsetneq \langle \gamma^2\rangle \supsetneq \cdots \supsetneq \langle \gamma^{e-1}\rangle \supsetneq \langle \gamma^{e}\rangle=\langle 0\rangle$$

şeklinde zincir formundadır (Jitman vd., 2010).

Tanım 2.14. R bir halka ve $(M,+)$ değişmeli grup olmak üzere her $r \in R$ ve her $m \in M$ için

$$f: R \times M \longrightarrow M$$

$$f(r,m) = rm$$

şeklinde tanımlanan ve her $r,s \in R$ ve her $m,n \in M$ için

i) $r(m+n) = rm + rn$

ii) $(r+s)m = rm + sm$

iii) $(sr)m = s(rm)$

özelliklerini sağlayan bir f fonksiyonu varsa M değişmeli grubuna bir sol R-modül denir. Benzer şekilde sağ modül tanımı da yapılabilir (Taşçı, 2007).

Tanım 2.15. M bir R-modül ve $A \subseteq M$ olmak üzere A nın alt modül olması için gerek ve yeter koşul her $a,b \in A$ için $a - b \in A$ ve her $r \in R$, her $a \in A$ için $ra \in A$ olmasıdır (Taşçı, 2007).

Tanım 2.16. $(R,+,\cdot)$ birimli ve değişmeli bir halka olsun. $R - \{0\} = R^*$ olmak üzere $(R^*,\cdot)$ bir grup ise R halkasına cisim denir (Çallıalp, 2013).

Tanım 2.17. Eleman sayısı sonlu olan cisme sonlu cisim denir (Roman, 1992).

Teorem 2.18. $1 < q \in \mathbb{Z}$ olmak üzere q elemanlı bir cismin var olması için gerek ve yeter koşul q sayısının bir asalın kuvveti şeklinde yazılmasıdır (Roman, 1992).

Tanım 2.19. p bir asal sayı $n \epsilon \mathbb{N}$ olmak üzere $q = p^n$ elemanlı cisme Galois cismi denir. $GF(q)$ veya F_q ile gösterilir (Roman, 1992).

Not 2.20. p asal olmak üzere $F_p \cong \mathbb{Z}_p$ dir ve $|F_p| = p$ dir.

Örnek 2.21. $F_5 \cong \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

Teorem 2.22. $\mathbb{F}$ sonlu bir cisim olmak üzere, $\mathbb{F}$ cisminin karakteristiği asal bir sayıdır. Ayrıca $kar\mathbb{F} = p$ ise $n \in \mathbb{Z}^+$ olmak üzere $\mathbb{F}$ cismi $q = p^n$ elemanlıdır (Roman, 1992).

Teorem 2.23. $p(x)$, $F_q[x]$ de $der\big(p(x)\big) = d$ olan asal bir polinom olmak üzere $F_q[x]/\langle p(x)\rangle$ bölüm halkası bir cisimdir ve

$$F_q[x]/\langle p(x)\rangle = \big\{r(x) + \langle p(x)\rangle : der\big(r(x)\big) < d, r(x) \in F_q[x]\big\}$$

şeklindedir (Roman, 1992).

Örnek 2.24. $GF(8)$ cismi için

$$GF(8) \cong GF(2)[x]/\langle x^3 + x + 1\rangle \cong \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$$

dir.

Tanım 2.25. $(V,\oplus)$ değişmeli grup, $(F,+,\cdot)$ bir cisim olmak üzere

$$g\colon F \times V \longrightarrow V$$

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

fonksiyonu aşağıdaki özellikleri sağlıyorsa, V ye $(F,+,\cdot)$ cismi üzerinde bir vektör uzayı denir (Çallıalp ve Kuruoğlu, 1996).

i) Her $a,b \in F$ ve her $u,v \in V$ için $a \odot (u \oplus v) = (a \odot u) \oplus (a \odot v)$ dir.

ii) Her $a,b \in F$ ve her $v \in V$ için $(a+b) \odot v = (a \odot v) \oplus (b \odot v)$ dir.

iii) Her $a,b \in F$ 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 2.26. V, F cismi üzerinde bir vektör uzayı ve $\emptyset \neq U \subseteq V$ alt kümesi olsun. U, V vektör uzayındaki işlemlere göre bir vektör uzayı ise U ye V nin bir alt uzayı denir (Çallıalp ve Kuruoğlu, 1996).

Teorem 2.27. V, F cismi üzerinde bir vektör uzayı olsun. $\emptyset \neq U \subseteq V$ kümesinin V nin bir alt uzayı olması için gerek ve yeter koşul her $u_1, u_2 \in U$ ve her $a,b \in \mathbb{F}$ için $(a \odot u_1) \oplus (b \odot u_2) \in U$ olmasıdır (Çallıalp ve Kuruoğlu, 1996).

Tanım 2.28. V, F cismi üzerinde bir vektör uzayı ve $v_1, v_2, \dots, v_n$, V vektör uzayının farklı vektörleri olsun. $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$ iken $a_1 = a_2 = \cdots = a_n = 0$ ise $v_1, v_2, \dots, v_n$ vektörleri lineer bağımsızdır denir. Aksi halde bu vektörlere lineer bağımlıdır denir (Ling ve Xing, 2004).

Tanım 2.29. V, F cismi üzerinde bir vektör uzayı ve $v_1, v_2, \dots, v_n \in V$ ve $a_1, a_2, \dots, a_n \in F$ olmak üzere her $v \in V, v = a_1v_1 + a_2v_2 + \cdots + a_nv_n$ şeklinde yazılabiliyorsa $v_1, v_2, \dots, v_n$ vektörleri V vektör uzayını üretiyor (geriyor) denir (Ling ve Xing, 2004).

Tanım 2.30. V, F 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. V vektör uzayının herhangi bir tabanındaki vektörlerinin sayısına V vektör uzayının boyutu denir ve $boy(V)$ ile gösterilir (Ling ve Xing, 2004).

Tanım 2.31. U_1, U_2, bir V vektör uzayının iki alt uzayı olsun.

i) $V = U_1 + U_2$

ii) $U_1 \cap U_2 = \{0_V\}$

koşulları sağlanıyorsa, V vektör uzayına U_1 ve U_2 alt uzaylarının bir direkt toplamı denir ve $V = U_1 \oplus U_2$ ile gösterilir (Çallıalp ve Kuruoğlu, 1996).

Teorem 2.32. $V = U_1 \oplus U_2$ ise V uzayının her v vektörü, $u_1 \in U_1$ ve $u_2 \in U_2$ olmak üzere, $v = u_1 + u_2$ şeklinde tek türlü yazılır (Çallıalp ve Kuruoğlu, 1996).

Not 2.33. $boy(U + V) = boy(U) + boy(V) - boy(U \cap V)$

$$boy(U \oplus V) = boy(U) + boy(V)$$

Tanım 2.34. $A = \{\alpha_1, \alpha_2, \dots, \alpha_q\}$ sonlu kümesine alfabe denir (Ling ve Xing, 2004).

Tanım 2.35. Bileşenleri A kümesinin elemanlarından oluşan sonlu dizilişlerin kümesine q-lu kod (q-ary kod) denir (Ling ve Xing, 2004).

Tanım 2.36. $\forall\, i \in \{1,2, \dots, q\}$ için $\alpha_i \in A$ olmak üzere $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ elemanına A üzerinde tanımlı n uzunluğunda bir q-lu sözcük denir (Ling ve Xing, 2004).

Tanım 2.37. $\emptyset \neq C \subseteq A^n$ kümesine A üzerinde tanımlı n uzunluğunda q-lu blok kod denir. Kodun elemanlarına da kod sözcükleri denir (Ling ve Xing, 2004).

C kodunun eleman sayısı $|C| = M$ ile gösterilir ve C koduna n uzunluğunda M elemanlı bir kod denir. (n, M) parametreleri ile gösterilir.

Tanım 2.38. F_q sonlu bir cisim olmak üzere

$$F_q^n = \{(a_1, a_2, \dots, a_n) : a_i \in F_q, i = 1,2, \dots, n\}$$

kümesinin elemanlarına vektör ya da sözcük adı verilir (Ling ve Xing, 2004).

Tanım 2.39. S sonlu bir halka ve $n \in \mathbb{Z}^+$ olmak üzere

$$S^n = \{(v_1, v_2, \dots, v_n) : \ v_i \in S, 1 \leq i \leq n\}$$

kümesinin M elemanlı bir C S-alt modülüne, n uzunluğunda, M elemanlı bir lineer kod denir. Kodun herhangi bir elemanına kod sözcüğü, S^n kümesinin herhangi bir elemanına sözcük adı verilir (Huffman ve Pless, 2003).

Tanım 2.40. $F_q^n = \{(a_1, a_2, \dots, a_n) : \ a_i \in F_q, 1 \leq i \leq n\}$ kümesi n boyutlu bir F_q vektör uzayı olmak üzere, F_q^n vektör uzayının bir C alt uzayına lineer kod denir. C, F_q^n vektör uzayının k boyutlu bir alt uzayı ise C ye F_q üzerinde tanımlı bir lineer $[n, k]$-kod ya da kısaca $[n, k]$-kod denir (Hill, 1986).

Tanım 2.41. Her $x = (x_1, x_2, \dots, x_n)$, $y = (y_1, y_2, \dots, y_n) \in F_q^n$ için

$$d : F_q^n \times F_q^n \to \mathbb{N} \cup \{0\}$$

$$(x, y) \mapsto d(x, y) = |\{i : \ x_i \neq y_i\}|$$

şeklinde tanımlanan dönüşüme Hamming uzaklığı denir (Huffman ve Pless, 2003).

Önerme 2.42. Hamming uzaklığı

i) $\forall\, x, y \in F_q^n$ için $d(x, y) \geq 0$, $d(x, y) = 0 \iff x = y$,

ii) $\forall\, x, y \in F_q^n$ için $d(x, y) = d(y, x)$,

iii)$\forall\, x, y, z \in F_q^n$ için $d(x, y) \leq d(x, z) + d(z, y)$

özelliklerini sağlayan bir metriktir (Hill, 1986).

Tanım 2.43. Bir C kodunun birbirinden farklı kod sözcüklerinin Hamming uzaklıklarının en küçüğüne C kodunun minimum uzaklığı denir ve $d(C)$ veya d ile gösterilir (Hill, 1986).

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

Uzunluğu n, eleman sayısı M ve minimum uzaklığı d olan bir C koduna (n, M, d)-kod denir.

Bir $[n,k]$-kodun d minimum uzaklığı da belirtilmek isteniyorsa $[n,k,d]$-kod şeklinde gösterilir.

Tanım 2.44. $a = (a_1, a_2, \dots, a_n) \in F_q^n$ olmak üzere, a elemanının ağırlığı, a elemanında bulunan sıfırdan farklı bileşenlerin sayısı olarak tanımlanır ve $w(a)$ ya da $w_H(a)$ ile gösterilir (Hill, 1986).

$$w(a) = |\{i : a_i \neq 0\}|.$$

Bir C kodunun sıfırdan farklı tüm kod sözcüklerinin ağırlıklarının en küçüğüne C kodunun minimum ağırlığı denir ve $w(C)$ ya da $w_H(C)$ ile gösterilir.

Lemma 2.45. a ve b, F_q^n vektör uzayının herhangi iki elemanı olmak üzere

$$d(a,b) = w(a-b)$$

dir (Roman, 1992).

Teorem 2.46. Bir C lineer kodunun minimum ağırlığı ile minimum uzaklığı eşittir (Roman, 1992).

Tanım 2.47. C, F_q üzerinde tanımlı bir $[n,k]$-kod olsun. Her bir satırı C lineer kodunun taban elemanlarından oluşturulan $k \times n$ mertebeli matrise C kodunun üreteç matrisi denir ve G ile gösterilir. G üreteç matrisi, I_k, $k \times k$ mertebeli birim matris, A, $k \times (n-k)$ mertebeli bir matris olmak üzere $(I_k \mid A)$ şeklinde yazılıyorsa bu matrise G matrisinin standart formu denir (Hill, 1986).

Tanım 2.48. Herhangi iki $a = (a_1, a_2, \dots, a_n)$, $b = (b_1, b_2, \dots, b_n) \in F_q^n$ olmak üzere

$$\cdot : F_q^n \; x \; F_q^n \longrightarrow F_q$$

$$(a, b) \longmapsto a.b = ab = a_1b_1 + a_2b_2 + \cdots + a_nb_n$$

şeklinde tanımlanan dönüşüme iç çarpım adı verilir. $ab = 0$ ise a ile b birbirine diktir denir (Hill, 1986).

Tanım 2.49. C, F_q üzerinde tanımlı bir $[n, k]$-kod olmak üzere

$$C^{\perp} = \{a \in F_q^n : \forall\, b \in C, ab = 0\}$$

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

Teorem 2.50. C, F_q üzerinde tanımlı bir $[n, k]$-kod olmak üzere

i) $|C| = q^k$,

ii) $C^{\perp}$ de lineer bir koddur ve $boy(C) + boy(C^{\perp}) = n$,

iii) $(C^{\perp})^{\perp} = C$

dir (Ling ve Xing, 2004).

Teorem 2.51. C, F_q üzerinde tanımlı bir $[n, k]$-kod ve

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

C kodunun üreteç matrisi olsun. $a = (a_1, a_2, \dots, a_n) \in F_q^n$ olmak üzere $a \in C^{\perp}$ olması için gerek ve yeter koşul $[a_1\ a_2\ \dots\ a_n].G^T = 0$ olmasıdır (Hill, 1986).

Önerme 2.52. C, F_q üzerinde tanımlı bir $[n, k]$-kod ise $C^{\perp}$ de F_q üzerinde tanımlı bir $[n, n-k]$-koddur (Hill, 1986).

Tanım 2.53. C bir $[n, k]$-kod olmak üzere $C^{\perp}$ nin üreteç matrisine C kodunun kontrol (parity-check) matrisi denir ve H ile gösterilir (Hill, 1986).

Teorem 2.54. C bir $[n,k]$-kod olmak üzere C kodunun üreteç matrisinin standart formu $G = (I_k \mid A)$ ise C kodunun kontrol matrisi $H = (-A^T \mid I_{n-k})$ dır (Hill, 1986).

Tanım 2.55. C, F_q^n vektör uzayının bir alt kümesi olsun. $c = (c_0, c_1, \dots, c_{n-1}) \in F_q^n$ olmak üzere

$$\sigma : F_q^n \longrightarrow F_q^n$$

$$\sigma(c_0, c_1, \dots, c_{n-1}) = (c_{n-1}, c_0, c_1, \dots, c_{n-2})$$

şeklinde tanımlanan σ dönüşümü devirli öteleme (cyclic shift) olarak adlandırılır. C bir lineer kod olmak üzere $\sigma(C) = C$ oluyorsa C koduna devirli kod denir (Hill, 1986).

Teorem 2.56. $F_q[x]/\langle x^n - 1\rangle$ polinom halkası bir esas ideal halkasıdır (Hill, 1986).

Teorem 2.57. Her $a = (a_0, a_1, \dots, a_{n-1}) \in F_q^n$ için

$$\Pi: F_q^n \longrightarrow F_q[x]/\langle x^n - 1\rangle$$

$$a = (a_0, a_1, \dots, a_{n-1}) \longrightarrow \Pi(a) = \overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}}$$

$$= a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$$

şeklinde tanımlanan fonksiyon bir F_q-vektör uzayı izomorfizması olmak üzere $C \subseteq F_q^n$ lineer kodunun devirli kod olması için gerek ve yeter koşul $\Pi(C)$ nin $F_q[x]/\langle x^n - 1\rangle$ halkasının bir ideali olmasıdır (Ling ve Xing, 2004).

Teorem 2.58. I, $F_q[x]/\langle x^n - 1\rangle$ halkasının bir ideali ve $g(x)$, I idealinin sıfırdan farklı en küçük dereceli ve monik bir polinomu olsun.

i) $g(x)$ polinomu I idealinin üretecidir ve bu monik polinom tektir.

ii) $g(x)$ polinomu $x^n - 1$ polinomunu böler (Ling ve Xing, 2004).

Tanım 2.59. C, F_q üzerinde tanımlı n uzunluğunda devirli bir kod ve C koduna karşılık gelen $\Pi(C)$ idealindeki sıfırdan farklı en küçük dereceli monik bir polinom $g(x)$ olmak üzere, $g(x)$ polinomuna C kodunun üreteç polinomu denir ve

$$C = \langle g(x) \rangle = \{ f(x).g(x) : f(x) \in F_q[x]/\langle x^n - 1 \rangle \}$$

şeklindedir (Ling ve Xing, 2004).

Teorem 2.60. $F_q[x]$ halkasında $x^n - 1$ polinomunun her monik böleni F_q üzerinde tanımlı bir devirli kod üretir (Ling ve Xing, 2004).

Teorem 2.61. $der(g(x)) = r$ olmak üzere $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ polinomu n uzunluğundaki C devirli kodunun üreteç polinomu olsun. C kodunun boyutu $boy(C) = n - r = k$ ve devirli kodun üreteç matrisi

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

dir (Hill, 1986).

Tanım 2.62. $h(x) = a_0 + a_1 x + \cdots + a_k x^k$, $der(h(x)) = k$ olmak üzere $h_R(x) = h^*(x) = x^k h(x^{-1}) = a_k + a_{k-1} x + \cdots + a_0 x^k$ polinomuna $h(x)$ polinomunun ters sıralı (reciprocal) polinomu denir (Ling ve Xing, 2004).

Teorem 2.63. C, F_q üzerinde tanımlı bir devirli $[n, k]$-kod, $g(x)$ polinomu C kodunun üreteç polinomu, $x^n - 1 = g(x)h(x)$ ve $h(x) = h_0 + h_1 x + \cdots + h_k x^k$ olsun.

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

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

dir.

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

Teorem 2.64. C, F_q üzerinde tanımlı n uzunluğunda bir devirli kod, $g(x)$ ve $h(x)$ sırasıyla C kodunun üreteç ve kontrol polinomları olsun. $F_q[x]/\langle x^n - 1 \rangle$

halkasında bir $c(x)$ elemanına karşılık gelen $(c_0, c_1, \dots, c_{n-1})$ sıralı n-linin C kodunun kod sözcüğü olması için gerek ve yeter koşul $c(x)h(x) = 0$ olmasıdır (Hill, 1986).

Tanım 2.65. θ, F_q üzerinde aşikar olmayan bir otomorfizma olmak üzere

$$F_q[x,\theta] = \{\, a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \,|\forall i \in \{0,1,2,\cdots,n\}, a_i \in F_q \,\}$$

kümesine skew polinomlar kümesi denir.

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

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

kuralı ile belirlidir (McDonald, 1974).

Teorem 2.66. Polinomlardaki standart toplama işlemi ve Tanım 2.65 de verilen çarpma işlemiyle birlikte $F_q[x,\theta]$ kümesi değişmeli olmayan bir halkadır (Boucher vd., 2007).

Tanım 2.67. $F_q[x,\theta]$ halkasına skew polinom halkası denir (Boucher vd., 2007).

Tanım 2.68. θ, F_q üzerinde tanımlı aşikar olmayan bir otomorfizma olsun. C, F_q^n uzayının boştan farklı bir alt kümesi olmak üzere

i) C, F_q^n uzayının bir alt uzayı ve

ii) Herhangi bir $c = (c_0, c_1, \cdots, c_{n-1}) \in C$ için

$$\sigma_\theta(c) = (\theta(c_{n-1}), \theta(c_0), \cdots, \theta(c_{n-2})) \in C$$

oluyorsa C kümesine n uzunluğunda skew devirli (skew cyclic) kod denir. σ_θ dönüşümüne skew devirli shift denir (Boucher vd., 2007).

$$\pi: F_q^n \rightarrow F_q[x,\theta]/\langle x^n - 1\rangle$$

$$c = \left(c_0, c_{1,\dots}, c_{n-1}\right) \rightarrow \pi(c) = c(x) = c_0 + c_1x + \cdots c_{n-1}x^{n-1} + \langle x^n - 1\rangle$$

dönüşümü bir izomorfizmadır. $\sigma_\theta(c)$ elemanının polinom gösterimi

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

şeklindedir.

Teorem 2.69. C, F_q üzerinde tanımlı n uzunluğunda skew devirli kod olması için gerek ve yeter koşul $\pi(C)$ nin $F_q[x,\theta]/\langle x^n - 1\rangle$ halkasının bir sol ideali olmasıdır (Boucher vd., 2007).

Teorem 2.70. C, F_q üzerinde tanımlı n uzunluğunda bir lineer kod olsun. C kodunun skew devirli kod olması için gerek ve yeter koşul $\pi(C)$ nin $F_q[x,\theta]/\langle x^n - 1\rangle$ modülünün bir sol $F_q[x,\theta]$-alt modülü olmasıdır (Şiap vd., 2011).

C, F_q cismi üzerinde tanımlı n uzunluğunda skew devirli kod ve $|\langle\theta\rangle| = m$ olsun. Skew devirli kodlar tanımlanırken iki durum söz konusudur;

i) Eğer $m|n$ ise $F_q[x,\theta]/\langle x^n - 1\rangle$ kümesi bir halkadır ve $\pi(C)$, $F_q[x,\theta]/\langle x^n - 1\rangle$ halkasının bir sol idealidir. Boucher vd. skew devirli kodların tanımını yalnızca $m|n$ olduğu durumda incelemiştir.

ii) Eğer $m \nmid n$ ise $F_q[x,\theta]/\langle x^n - 1\rangle$ kümesi bir halka değildir. Şiap vd. çalışmalarında herhangi bir n değeri için $\pi(C)$ yi $F_q[x,\theta]/\langle x^n - 1\rangle$ in bir sol alt modülü olarak ele almış ve $m|n$ olma kısıtlamasını kaldırmışlardır. Böylece herhangi bir uzunluk için skew devirli kodlar tanımlanmıştır (Şiap, 2011).

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

Teorem 2.71. C, F_q üzerinde tanımlı n uzunluğunda skew devirli kod olmak üzere C kodu $f(x)$ polinomu tarafından üretilsin. Bu durumda $f(x)$ polinomu $x^n - 1$ polinomunun bir sağ bölenidir (Şiap, 2011).

Önerme 2.72. $F_q[x,\theta]$ halkasında $x^n - 1$ polinomunun bir sağ böleni $g(x) = g_r x^r + \cdots + g_1 x + g_0$ olmak üzere $g(x)$ polinomu F_q üzerinde n uzunluğunda boyutu $n - r$ olan bir skew devirli kod üretir ve $g(x)$ polinomuna kodun üreteç polinomu denir. Ayrıca,

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-r-1}g(x) \end{pmatrix}$$

$$= \begin{pmatrix} g_0 & \cdots & g_{r-1} & g_r & 0 & \dots & 0 \\ 0 & \theta(g_0) & \dots & \theta(g_{r-1}) & \theta(g_r) & \dots & 0 \\ \vdots & \ddots & & \vdots & & & \vdots \\ 0 & \cdots & 0 & \theta^{n-r-1}(g_0) & \dots & \theta^{n-r-1}(g_{r-1}) & \theta^{n-r-1}(g_r) \end{pmatrix}$$

dir (Boucher ve Ulmer, 2009).

Tanım 2.73. H sonlu bir halka olsun. Her $h = (h_0, h_1, \dots, h_{n-2}, h_{n-1}) \in H^n$ için $(h_{n-1}, h_{n-2}, \dots, h_1, h_0) \in H^n$ vektörüne h'ın ters sıralısı (reversible) denir ve h^R şeklindede gösterilir. C kodu H üzerinde tanımlı bir lineer kod olmak üzere, eğer her $h \in C$ için $h^R \in C$ oluyorsa C koduna ters sıralı kod denir.

h vektörüne karşılık gelen polinom $h(x) = h_0 + h_1 x + \cdots + h_{n-1}x^{n-1}$ ile temsil edilmek üzere $h(x)$ polinomunun ters sıralısı $h(x)^R = h_{n-1} + h_{n-2}x + \cdots + h_0 x^{n-1}$ şeklinde gösterilir (Dinh vd., 2018).

Tanım 2.73. H sonlu bir halka olsun. Her $h = (h_0, h_1, \dots, h_{n-2}, h_{n-1}) \in H^n$ için $(\bar{h}_0, \bar{h}_1, \dots, \bar{h}_{n-2}, \bar{h}_{n-1}) \in H^n$ vektörüne h'ın tamlayanı (complement) denir ve h^C biçiminde gösterilir. C kodu H üzerinde tanımlı bir lineer kod olmak üzere, eğer her $h \in C$ için $h^C \in C$ oluyorsa C koduna tamlayan kod denir.

h vektörüne karşılık gelen polinom $h(x) = h_0 + h_1 x + \cdots + h_{n-1}x^{n-1}$ ile temsil edilmek üzere $h(x)$ polinomunun tamlayanı $h(x)^C = \bar{h}_0 + \bar{h}_1 x + \cdots + \bar{h}_{n-1}x^{n-1}$ şeklinde gösterilir (Dinh vd., 2018).

Tanım 2.74. H sonlu bir halka olsun. Her $h = (h_0, h_1, \dots, h_{n-2}, h_{n-1}) \in H^n$ için $(\bar{h}_{n-1}, \bar{h}_{n-2}, \dots, \bar{h}_1, \bar{h}_0) \in H^n$ vektörüne h'ın ters sıralı tamlayanı (reversible complement) denir ve h^{RC} biçiminde gösterilir. C kodu H üzerinde tanımlı bir lineer kod olmak üzere, eğer her $h \in C$ için $h^{RC} \in C$ oluyorsa C koduna ters sıralı tamlayan kod denir.

h vektörüne karşılık gelen polinom $h(x) = h_0 + h_1 x + \cdots + h_{n-1}x^{n-1}$ ile temsil edilmek üzere $h(x)$ polinomunun ters sıralısı $h(x)^{RC} = \bar{h}_{n-1} + \bar{h}_{n-2}x + \cdots + \bar{h}_0 x^{n-1}$ şeklinde gösterilir (Dinh vd., 2018).

Tanım 2.75. H sonlu bir halka olsun. $g^*(x)$, $g(x) = c_0 + c_1 x + \cdots + c_t x^t \in H[x]$ polinomunun reciprocal polinomu olmak üzere, bir m birimsel elemanı için $g^*(x) = mg(x)$ oluyorsa, $g(x)$ polinomuna self-reciprocal polinom denir (Dinh vd., 2018).

Tanım 2.76. C, H halkası üzerinde tanımlı n uzunluğunda devirli bir kod olsun. Bu durumda, her $h = (h_0, h_1, \dots, h_{n-2}, h_{n-1}) \in C$ için

$$h^{RC} = \left(\bar{h}_{n-1}, \bar{h}_{n-2}, \dots, \bar{h}_1, \bar{h}_0\right) \in C$$

oluyorsa C koduna devirli DNA kod denir (Dinh vd., 2018).

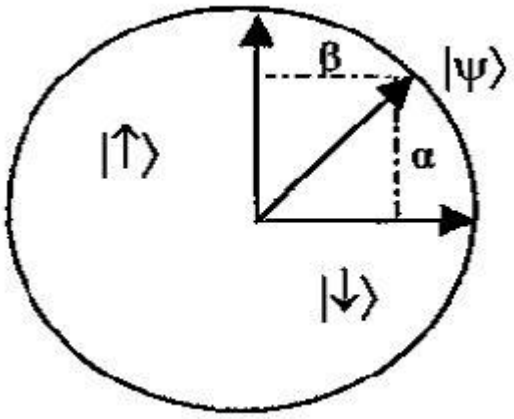
Kuantum hesaplamada kullanılan vektör uzayı, kompleks sayılar üzerinde sonlu boyutlu bir uzaydır. Bu tip bir vektör uzayı için genellikle Hilbert vektör uzayı terimi kullanılır. Dolayısıyla, kuantum kodları sonlu boyutlu Hilbert uzayı üzerinde tanımlanır. Bir n uzunluğundaki kuantum kodu, 2^n boyutlu Hilbert uzayının bir alt uzayını oluşturur.

Klasik hesaplamalarda bilgi birimi olarak "bit" kullanılırken, kuantum hesaplamalarında kullanılan bilgi birimine "kuantum bit" ya da kısaca "kübit" (qubit) denir. Bir kübitin durumu, iki boyutlu Hilbert uzayındaki bir vektör olarak düşünülebilir. Klasik bir bit sadece 0 veya 1 değerini alabilirken, kübitlerin durumu çok daha karmaşıktır. İki boyutlu bir kuantum uzayında bir kübit $|0\rangle$, $|1\rangle$ ya da bu durumların lineer kombinasyonu olabilir.Yani;

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}$$

halinde olabilir. Kübitin bu özelliğine süperpozisyon denir (Güzeltepe, 2014).

Kuantum bilgisayarlarının klasik bilgisayarlara üstün olma sebeplerinden biri, kübitlerin böyle bir özelliğe sahip olmalarıdır.



Şekil 2.1. Süperpozisyon durumundaki kübitin şematik gösterimi

$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \alpha, \beta \in \mathbb{C}$ halindeki bir kuantum bitin (kübit) ölçüm sonucu elde edilen değeri $|\alpha|^2$ olasılığı ile $|0\rangle$, $|\beta|^2$ olasılığı ile $|1\rangle$ dir. Bütün olasılıklar toplamı 1 olduğundan $|\alpha|^2 + |\beta|^2 = 1$ elde edilir.

Bu durum, benzer biçimde n kübit için genellenebilir. Bir n kübitli kuantum durumu, 2^n boyutlu Hilbert uzayındaki normu 1'e eşit olan bir vektördür.

$(\mathbb{C}^2)^{\otimes n}$, uzunluğu n olan kuantum sözcüklerinin uzayını temsil eder.. $(\mathbb{C}^2)^{\otimes n}$, n tane $\mathbb{C}^2$ uzayının tensör çarpımıdır.

Tanım 2.77. $(\mathbb{C}^2)^{\otimes n}$ uzayının k boyutlu bir C alt uzayına kuantum kod denir ve bir C kuantum kodu $[[n,k]]$-kod biçiminde ifade edilir. C kuantum kodu d hata düzeltici kod ise C koduna bir $[[n,k,d]]$-kod denir. Buradaki çift parantez kuantum kodlarını klasik kodlardan ayırmak için kullanılır (Dertli, 2016).

CSS kodları olarak bilinen kuantum kodları, Calderbank, Shor ve Steane tarafından geliştirilen bir kuantum kod yapısıdır. Bu kuantum kodları, iki klasik lineer kodun yardımıyla inşa edilir. Bu kod yapısı, klasik lineer kodlar ile kuantum kodları arasında bir bağlantı kurmuş ve kuantum kod bulma problemini dualini içeren lineer kodu bulma problemine dönüştürmüştür.

Teorem 2.78. C, F_q üzerinde tanımlı bir kod ve $l(x)$, C kodunun üreteç polinomu olmak üzere C kodunun dualini içermesi için gerek ve yeter koşul $l^*(x)$, $l(x)$ polinomunun ters sıralı polinomu ve $\lambda = \pm 1$ olmak üzere

$$x^n - \lambda \equiv 0\big(mod\ l(x)l^*(x)\big)$$

olmasıdır (Gao ve Wang, 2018).

Teorem 2.79. C_1 ve C_2, F_q üzerinde tanımlı sırasıyla $[n, k_1, d_1]$ ve $[n, k_2, d_2]$ kod olmak üzere $C_2^{\perp} \subseteq C_1$, $d = min\{w(v): v \in (C_1 \backslash C_2^{\perp}) \cup (C_2 \backslash C_1^{\perp})\} \geq \min\{d_1, d_2\}$ olsun. Bu durumda $\big[[n, k_1 + k_2 - n, d]\big]$ parametreli kuantum kodu vardır.

Özel olarak $C_1 = C_2$ ise kuantum kodun parametreleri $\big[[n, 2k_1 - n, d]\big]$ olur (Calderbank vd., 1998).

Teorem 2.80. C, F_q üzerinde tanımlı self-ortogonal $[n, k]$-kod olmak üzere $d = min\{w(v): v \in C^{\perp} \backslash C\}$ olsun. Bu durumda $\big[[n, n - 2k, d]\big]$ parametreli kuantum kodu vardır (Calderbank vd., 1998).

Teorem 2.81. C, F_q üzerinde $[n, k, d]$-kod olsun. $C^{\perp} \subseteq C$ ise $\big[[n, 2k - n, \geq d]\big]$ parametreli bir kuantum kod elde edilebilir (Li vd., 2018).

3. S_q HALKASI ÜZERİNDEKİ DNA VE KUANTUM KODLAR

Bu bölümde, S_q halkası üzerinde devirli ve skew devirli kodlar tanımlanarak devirli ve skew devirli kodlardan DNA kodlar, devirli kodlardan kuantum kodlar incelendi.

3.1. S_q Halkası

$i = 1,2,3,4,5, j = 3,4,5,\ i \neq j$ olmak üzere

$$F_q[w_i]/\langle w_i^2 = w_i, w_1w_2 - w_2w_1, w_iw_j = 0\rangle$$

halkası, değişmeli, q^7 elemalı bir halkadır.

Bu halka $S_q = F_q + w_1F_q + w_2F_q + w_3F_q + w_4F_q + w_5F_q + w_1w_2F_q$ ya izomorftur.

$$S_q = \{s_0 + w_1s_1 + w_2s_2 + w_3s_3 + w_4s_4 + w_5s_5 + w_1w_2s_6 : s_i \in F_q, 0 \leq i \leq 6\}$$

dir.

$$\alpha_1 = 1 - w_1 - w_2 - w_3 - w_4 - w_5 + w_1w_2$$
$$\alpha_2 = w_1 - w_1w_2$$
$$\alpha_3 = w_2 - w_1w_2$$
$$\alpha_4 = w_3$$
$$\alpha_5 = w_4$$
$$\alpha_6 = w_5$$
$$\alpha_7 = w_1w_2$$

olmak üzere $1 \leq i, j \leq 7$ ve $i \neq j$ için

$$\alpha_i^2 = \alpha_i,$$
$$\alpha_i\alpha_j = 0,$$
$$\sum_{i=1}^{7} \alpha_i = 1$$

şeklindedir. Dolayısıyla

$$S_q = \bigoplus_{1 \leq k \leq 7} \alpha_k S_q$$

elde edililir.

3.2. S_q Halkası Üzerinde Tanımlı Devirli Kodlar

Tanım 3.2.1. S_q^n, S_q-modülünün bir alt modülüne n uzunluğunda bir lineer kod denir.

Tanım 3.2.2. Her $v' = \sum_{k=1}^{7} \alpha_k v_k \in S_q$ için

$$\delta: S_q \longrightarrow F_q^7$$

$$\delta(v') = (v_1, v_2, v_3, v_4, v_5, v_6, v_7)$$

şeklinde tanımlı δ lineer dönüşümüne S_q üzerinde tanımlı Gray dönüşümü denir. Buna denk olarak δ Gray dönüşümü her $s = s_0 + \sum_{k=1}^{5} w_k s_k + w_1 w_2 s_6 \in S_q$ için

$$\delta(s) = (s_0, s_0 + s_1, s_0 + s_2, s_0 + s_3, s_0 + s_4, s_0 + s_5, s_0 + s_1 + s_2 + s_6)$$

şeklinde de tanımlanır. Bu Gray dönüşümü S_q^n den F_q^{7n} e genelleştirilebilir.

w_H, F_q^7 vektör uzayı üzerinde tanımlı Hamming ağırlığı olmak üzere $s = s_0 + \sum_{k=1}^{5} w_k s_k + w_1 w_2 s_6 \in S_q$ için $w_L(s) = w_H(s_0, s_0 + s_1, s_0 + s_2, s_0 + s_3, s_0 + s_4, s_0 + s_5, s_0 + s_1 + s_2 + s_6)$ şeklinde tanımlanan w_L fonksiyonuna s elemanının Lee ağırlığı denir.

Herhangi bir $c = (c_0, c_1, \dots, c_{n-1})$ kod sözcüğünün Lee ağırlığı $0 \leq i \leq n-1$ olmak üzere $w_L(c) = \sum_{i=0}^{n-1} w_L(c_i)$ şeklindedir.

Her $c, \dot{c} \in C$ için $d_L(c, \dot{c}) = w_L(c - \dot{c})$ şeklinde tanımlanan d_L fonksiyonuna Lee uzaklığı denir. C kodunun minimum Lee uzaklığı ise $d_L(C) = min\{d_L(c, \dot{c}) : \forall\, c \in C, c \neq \dot{c}\}$ şeklinde tanımlanır.

Teorem 3.2.3. δ Gray dönüşümü $\left(S_q^n, d_L\right)$ den $\left(F_q^{7n}, d_H\right)$ e uzaklık koruyan lineer bir dönüşümdür.

İspat: $\forall\, r, r' \in F_q, \forall\, s', s'' \in S_q^n$ için

$$\delta(rs' + r's'') = r\delta(s') + r'\delta(s'')$$

olduğundan δ lineer bir dönüşümdür. Ayrıca $\delta(s' - s'') = \delta(s') - \delta(s'')$ olduğu kolaylıkla görülebilir. Buradan

$$d_L(s', s'') = w_L(s' - s'')$$
$$= w_H\big(\delta(s' - s'')\big)$$
$$= w_H\big(\delta(s') - \delta(s'')\big)$$
$$= d_H\big(\delta(s'), \delta(s'')\big)$$

elde edilir. O halde Gray dönüşümü uzaklık koruyan bir dönüşümdür.

Teorem 3.2.4. C, S_q üzerinde tanımlı d_L minimum uzaklıklı, M elemanlı, n uzunluğunda lineer bir kod olmak üzere $\delta(C), F_q$ üzerinde tanımlı bir $(7n, M, d_H)$ koddur. Ayrıca $d_H = d_L$ dir.

İspat: Teorem 3.2.3 ve δ dönüşümünün tanımından $\delta(C), 7n$ uzunluğunda ve $d_H = d_L$ dir. δ, 1-1 ve örten olduğundan $|C| = |\delta(C)|$ dir. Dolayısıyla $\delta(C)$ bir $(7n, M, d_L)$-koddur.

Teorem 3.2.5. C, S_q üzerinde bir lineer kod olsun. C kodu self-ortogonal kod ise $\delta(C)$ de self-ortogonal koddur.

İspat: Herhangi bir $v' = \sum_{k=1}^{7} \alpha_k v_k$, $v'' = \sum_{k=1}^{7} \alpha_k v_k' \in S_q$ için,

$$v'v'' = \left(\sum_{k=1}^{7} \alpha_k v_k\right)\left(\sum_{k=1}^{7} \alpha_k v_k'\right)$$
$$= \sum_{k=1}^{7} \alpha_k v_k v_k'$$

olur. C self-ortogonal olduğundan $\sum_{k=1}^{7} \alpha_k v_k v_k' = 0$ dir. O halde $1 \leq k \leq 7$ için $v_k v_k' = 0$ olur.

$$\delta(v') = (v_1, v_2, v_3, v_4, v_5, v_6, v_7),\ \ \delta(v'') = (v_1', v_2', v_3', v_4', v_5', v_6', v_7')$$

olmak üzere

$$\delta(v')\delta(v'') = v_1 v_1' + v_2 v_2' + \cdots + v_7 v_7'$$
$$= \sum_{k=1}^{7} v_k v_k' = 0$$

bulunur. O halde $\delta(C)$ self-ortogonal koddur.

C, S_q üzerinde tanımlı n uzunluğunda lineer bir kod olmak üzere $1 \leq k \leq 7$ için F_q üzerindeki lineer C_k kodları

$$C_k = \left\{ v_k \in F_q^n : \exists\, v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_7 \in F_q^n, \sum_{k=1}^{7} \alpha_k v_k \in C \right\}$$

şeklinde tanımlansın. Ayrıca bu C_k kodlarını

$$\mathrm{C}_1 = \left\{ \mathrm{s}_0 \in F_q^n : \exists\, \mathrm{s}_1, \mathrm{s}_2, \mathrm{s}_3, \mathrm{s}_4, \mathrm{s}_5, \mathrm{s}_6 \in F_q^n, \mathrm{s}_0 + \sum_{\mathrm{k}=1}^{5} w_k s_k + \mathrm{w}_1 \mathrm{w}_2 \mathrm{s}_6 \in \mathrm{C} \right\},$$

$$\mathrm{C}_2 = \left\{ \mathrm{s}_0 + \mathrm{s}_1 \in F_q^n : \exists\, \mathrm{s}_2, \mathrm{s}_3, \mathrm{s}_4, \mathrm{s}_5, \mathrm{s}_6 \in F_q^n, \mathrm{s}_0 + \sum_{\mathrm{k}=1}^{5} w_k s_k + \mathrm{w}_1 \mathrm{w}_2 \mathrm{s}_6 \in \mathrm{C} \right\},$$

$$\mathrm{C}_3 = \left\{ \mathrm{s}_0 + \mathrm{s}_2 \in F_q^n : \exists\, \mathrm{s}_1, \mathrm{s}_3, \mathrm{s}_4, \mathrm{s}_5, \mathrm{s}_6 \in F_q^n, \mathrm{s}_0 + \sum_{\mathrm{k}=1}^{5} w_k s_k + \mathrm{w}_1 \mathrm{w}_2 \mathrm{s}_6 \in \mathrm{C} \right\},$$

$$\mathrm{C}_4 = \left\{ \mathrm{s}_0 + \mathrm{s}_3 \in F_q^n : \exists\, \mathrm{s}_1, \mathrm{s}_2, \mathrm{s}_4, \mathrm{s}_5, \mathrm{s}_6 \in F_q^n, \mathrm{s}_0 + \sum_{\mathrm{k}=1}^{5} w_k s_k + \mathrm{w}_1 \mathrm{w}_2 \mathrm{s}_6 \in \mathrm{C} \right\},$$

$$\mathrm{C}_5 = \left\{ \mathrm{s}_0 + \mathrm{s}_4 \in F_q^n : \exists\, \mathrm{s}_1, \mathrm{s}_2, \mathrm{s}_3, \mathrm{s}_5, \mathrm{s}_6 \in F_q^n, \mathrm{s}_0 + \sum_{\mathrm{k}=1}^{5} w_k s_k + \mathrm{w}_1 \mathrm{w}_2 \mathrm{s}_6 \in \mathrm{C} \right\},$$

$$C_6 = \left\{ s_0 + s_5 \in F_q^n : \exists\, s_1, s_2, s_3, s_4, s_6 \in F_q^n, s_0 + \sum_{k=1}^{5} w_k s_k + w_1 w_2 s_6 \in \mathrm{C} \right\},$$

$$C_7 = \left\{ s_0 + s_1 + s_2 + s_6 \in F_q^n : \exists\, s_3, s_4, s_5 \in F_q^n, s_0 + \sum_{k=1}^{5} w_k s_k + w_1 w_2 s_6 \in \mathrm{C} \right\}$$

şeklinde de tanımlayabiliriz.

Teorem 3.2.6. $C \subseteq S_q^n$ bir lineer kod olmak üzere

$$\delta(C) = \bigotimes_{1 \leq k \leq 7} C_k, \quad |C| = \prod_{k=1}^{7} |C_k|$$

ve

$$d_L(C) = \min\{d_H(C_k) : 1 \leq k \leq 7\}$$

dir.

İspat: δ, 1-1 ve örten olduğundan

$$s' = (s_0^0, s_0^1, \dots, s_0^{n-1}, s_0^0 + s_1^0, \dots, s_0^{n-1} + s_1^{n-1}, s_0^0 + s_2^0, \dots, s_0^{n-1} + s_2^{n-1}, s_0^0 + s_3^0, \dots, s_0^{n-1} + s_3^{n-1}, s_0^0 + s_4^0, \dots, s_0^{n-1} + s_4^{n-1}, s_0^0 + s_5^0, \dots, s_0^{n-1} + s_5^{n-1}, s_0^0 + s_1^0 + s_2^0 + s_6^0, \dots, s_0^{n-1} + s_1^{n-1} + s_2^{n-1} + s_6^{n-1}) \in \delta(C)$$

olacak şekilde $v_i = s_0^i + \sum_{k=1}^{5} w_k s_k^i + w_1 w_2 s_6^i \in S_q$ olmak üzere $v = (v_0, v_1, \dots, v_{n-1}) \in C$ vardır ve $\delta(v) = s'$ dir.

$1 \le k \le 7$ için C_k kodlarının tanımından

$$(s_0^0, s_0^1, \dots, s_0^{n-1}) \in C_1,$$

$$(s_0^0 + s_1^0, \dots, s_0^{n-1} + s_1^{n-1}) \in C_2,$$

$$(s_0^0 + s_2^0, \dots, s_0^{n-1} + s_2^{n-1}) \in C_3,$$

$$(s_0^0 + s_3^0, \dots, s_0^{n-1} + s_3^{n-1}) \in C_4,$$

$$(s_0^0 + s_4^0, \dots, s_0^{n-1} + s_4^{n-1}) \in C_5,$$

$$(s_0^0 + s_5^0, \dots, s_0^{n-1} + s_5^{n-1}) \in C_6,$$

$$(s_0^0 + s_1^0 + s_2^0 + s_6^0, \dots, s_0^{n-1} + s_1^{n-1} + s_2^{n-1} + s_6^{n-1}) \in C_7$$

olur. Dolayısıyla

$$(s_0^0, s_0^1, \dots, s_0^{n-1}, s_0^0 + s_1^0, \dots, s_0^{n-1} + s_1^{n-1}, s_0^0 + s_2^0, \dots, s_0^{n-1} + s_2^{n-1}, s_0^0 + s_3^0, \dots, s_0^{n-1} + s_3^{n-1}, s_0^0 + s_4^0, \dots, s_0^{n-1} + s_4^{n-1}, s_0^0 + s_5^0, \dots, s_0^{n-1} + s_5^{n-1}, s_0^0 + s_1^0 + s_2^0 + s_6^0, \dots, s_0^{n-1} + s_1^{n-1} + s_2^{n-1} + s_6^{n-1}) \in \bigotimes_{1 \le k \le 7} C_k$$

elde edilir. Böylece $\delta(C) \subseteq \bigotimes_{1 \le k \le 7} C_k$ olur.

Tersine,

$$a = (s_0^0, s_0^1, \dots, s_0^{n-1}) \in C_1,$$

$$b = (s_0^0 + s_1^0, \dots, s_0^{n-1} + s_1^{n-1}) \in C_2,$$

$$c = (s_0^0 + s_2^0, \dots, s_0^{n-1} + s_2^{n-1}) \in C_3,$$

$$d = (s_0^0 + s_3^0, \dots, s_0^{n-1} + s_3^{n-1}) \in C_4,$$

$$e = (s_0^0 + s_4^0, \dots, s_0^{n-1} + s_4^{n-1}) \in C_5,$$

$$f = (s_0^0 + s_5^0, \dots, s_0^{n-1} + s_5^{n-1}) \in C_6,$$

$$g = (s_0^0 + s_1^0 + s_2^0 + s_6^0, \dots, s_0^{n-1} + s_1^{n-1} + s_2^{n-1} + s_6^{n-1}) \in C_7$$

olmak üzere $(a, b, c, d, e, f, g) \in \bigotimes_{1 \le k \le 7} C_k$ olsun. Lineer C kodunun tanımından

$$t = a + w_1(b - a) + w_2(c - a) + w_3(d - a) + w_4(e - a) + w_4(f - a) + w_1 w_2(a - b - c + g) \in C$$

vardır ve $\delta(t) = (a, b, c, d, e, f, g)$ dir. Böylece $\bigotimes_{1 \le k \le 7} C_k \subseteq \delta(C)$ olur. O halde $\bigotimes_{1 \le k \le 7} C_k = \delta(C)$ elde edilir.

δ, 1-1 ve örten olduğundan $|C| = \left| \bigotimes_{1 \le k \le 7} C_k \right| = \prod_{k=1}^{7} |C_k|$ olur. Ayrıca δ uzaklık koruyan lineer bir dönüşüm olduğundan

$$d_L(C) = d_H\big(\delta(C)\big) = d_H\left(\bigotimes_{1 \le k \le 7} C_k\right)$$

$$= \min\{d_H(C_k) : 1 \le k \le 7\}$$

elde edilir.

Sonuç 3.2.7. S_q üzerinde tanımlı bir C kodu

$$C = \bigoplus_{1 \le k \le 7} \alpha_k C_k$$

şeklinde tek türlü yazılır.

Sonuç 3.2.8. $1 \le k \le 7$ için G_k matrisleri C_k kodlarının üreteç matrisleri olmak üzere C kodunun üreteç matrisi

$$G = \begin{pmatrix} \alpha_1 G_1 \\ \alpha_2 G_2 \\ \vdots \\ \alpha_7 G_7 \end{pmatrix}$$

ve $\delta(C)$ nin üreteç matrisi

$$G' = \begin{pmatrix} \delta(\alpha_1 G_1) \\ \delta(\alpha_2 G_2) \\ \vdots \\ \delta(\alpha_7 G_7) \end{pmatrix}$$

dir.

Teorem 3.2.9. $C = \bigoplus_{1 \le k \le 7} \alpha_k C_k$, S_q üzerinde tanımlı lineer bir kod olmak üzere C kodunun devirli bir kod olması için gerek ve yeter koşul, $1 \le k \le 7$ için C_k kodlarının F_q üzerinde devirli kod olmasıdır.

İspat: C, S_q üzerinde tanımlı devirli bir kod ve $1 \le k \le 7$ için $v^k = \left(v_1^k, v_2^k, \dots, v_n^k\right) \in C_k$ olsun. $1 \le i \le n$ için $c_i = \sum_{k=1}^{7} \alpha_k v_i^k$ olmak üzere $(c_1, c_2, \dots, c_n) \in C$ dir. C devirli kod olduğundan $(c_n, c_1, \dots, c_{n-1}) \in C$ olur. Bu durumda $(c_n, c_1, \dots, c_{n-1}) = \sum_{k=1}^{7} \alpha_k \left(v_n^k, v_1^k, \dots, v_{n-1}^k\right)$ dir. Böylece $1 \le k \le 7$ için $\left(v_n^k, v_1^k, \dots, v_{n-1}^k\right) \in C_k$ elde edilir. O halde $1 \le k \le 7$ için C_k kodları F_q üzerinde tanımlı devirli kodlardır.

Tersine, $1 \le k \le 7$ için C_k kodları F_q üzerinde tanımlı devirli kodlar ve $1 \le i \le n$ için $c_i = \sum_{k=1}^{7} \alpha_k v_i^k$ olmak üzere $(c_1, c_2, \dots, c_n) \in C$ olsun. O zaman $1 \le k \le 7$ için $v^k = \left(v_1^k, v_2^k, \dots, v_n^k\right) \in C_k$ olur. $1 \le k \le 7$ için C_k kodları devirli kodlar olduğundan $(c_n, c_1, \dots, c_{n-1}) = \sum_{k=1}^{7} \alpha_k \left(v_n^k, v_1^k, \dots, v_{n-1}^k\right) \in C$ olur. O halde C, S_q üzerinde tanımlı devirli bir koddur.

Teorem 3.2.10. $C = \bigoplus_{1 \le k \le 7} \alpha_k C_k$, S_q üzerinde tanımlı devirli kod olsun. $1 \le k \le 7$ için $\mathrm{r}_k(x)$, C_k kodlarının üreteç polinomları olmak üzere

$$C = \langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x) \rangle$$

ve $|C| = q^{7n - \left(\sum_{k=1}^{7} \mathrm{der}(r_k(x))\right)}$ dir.

İspat: $C = \bigoplus_{1 \le k \le 7} \alpha_k C_k$ olsun. $1 \le k \le 7$ için $C_k = \langle r_k(x) \rangle \subseteq F_q[x]/\langle x^n - 1 \rangle$ olduğundan

$$C = \left\{ a(x) : \ a(x) = \sum_{k=1}^{7} \alpha_k r_k(x) g_k(x) \, , g_k(x) \in F_q[x], 1 \le k \le 7 \right\}$$

şeklindedir. O halde $C \subseteq \langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x) \rangle \subseteq F_q[x]/\langle x^n - 1 \rangle$ dir.

$1 \leq k \leq 7$ için $h_k(x) \in F_q[x]/\langle x^n - 1\rangle$ olmak üzere herhangi bir eleman

$$\sum_{k=1}^{7} \alpha_k r_k(x) h_k(x) \in \langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x)\rangle$$

olsun. Bu durumda $1 \leq k \leq 7$ için $\alpha_k h_k(x) = \alpha_k f_k(x)$ olacak şekilde $f_k(x) \in F_q[x]$ elemanları vardır. Böylece

$$\langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x)\rangle \subseteq C$$

dir. O halde

$$C = \langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x)\rangle$$

elde edilir. Ayrıca $C = \prod_{k=1}^{7} |C_k|$ olduğundan

$$|C| = q^{7n - \left(\sum_{k=1}^{7} \mathrm{der}(r_k(x))\right)}$$

dir.

Teorem 3.2.11. C, S_q üzerinde tanımlı devirli bir kod, $1 \leq k \leq 7$ için $r_k(x), C_k$ kodlarının üreteç polinomları olsun. $C = \langle r(x)\rangle$ olacak sekilde bir tek $r(x) = \sum_{k=1}^{7} \alpha_k r_k(x)$ vardır ve $r(x) \mid x^n - 1$ dir.

İspat: Teorem 3.2.10 dan $C = \langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x)\rangle$ dir. $r(x) = \sum_{k=1}^{7} \alpha_k r_k(x)$ olarak alınırsa $\langle r(x)\rangle \subseteq C$ olur. Ayrıca $1 \leq k \leq 7$ için $\alpha_k r_k(x) = \alpha_k r(x)$ dir. Bu durumda $C \subseteq \langle r(x)\rangle$ elde edilir. O halde $C = \langle r(x)\rangle$ dir.

$1 \leq k \leq 7$ için $r_k(x)$ polinomları $x^n - 1$ polinomunun bölenleri olduğundan $x^n - 1 = t_k(x) r_k(x)$ olacak şekilde $t_k(x) \in F_q[x]$ vardır. Bu durumda

$$\left(\sum_{k=1}^{7} \alpha_k t_k(x)\right) r(x) = \sum_{k=1}^{7} \alpha_k t_k(x) \sum_{k=1}^{7} \alpha_k r_k(x)$$

$$= \sum_{k=1}^{7} \alpha_k t_k(x)\, r_k(x)$$

$$= \sum_{k=1}^{7} \alpha_k (x^n - 1)$$

$$= x^n - 1$$

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

Teorem 3.2.12. $C = \bigoplus_{1 \le k \le 7} \alpha_k C_k, S_q$ üzerinde n uzunluğunda devirli bir kod olmak üzere

$$C^{\perp} = \bigoplus_{1 \le k \le 7} \alpha_k C_k^{\perp}$$

dir. Ayrıca C kodunun S_q üzerinde self-dual olması için gerek ve yeter koşul $1 \le k \le 7$ için C_k kodlarının F_q üzerinde self-dual olmasıdır.

Sonuç 3.2.13. $C = \bigoplus_{1 \le k \le 7} \alpha_k C_k, S_q$ üzerinde tanımlı n uzunluğunda bir devirli kod ve $C^{\perp}$, C kodunun duali olsun. $1 \le k \le 7$ için $h_k(x) = (x^n - 1)/r_k(x)$ polinomlarının ters sıralı polinomları $h_k^*(x) = x^{der(h_k(x))} h_k(x^{-1})$ olmak üzere

$$C^{\perp} = \langle \alpha_1 h_1^*(x), \alpha_1 h_2^*(x), \alpha_3 h_3^*(x), \alpha_4 h_4^*(x), \alpha_5 h_5^*(x), \alpha_6 h_6^*(x), \alpha_7 h_7^*(x) \rangle$$

ve

$$|C^{\perp}| = q^{\sum_{k=1}^{7} der(r_k(x))}$$

dir.

Tanım 3.2.14. C, F_q üzerinde tanımlı $7n$ uzunluğunda bir kod, $0 \le i \le 6$ olmak üzere $a^{(i)} \in F_q^n$ ve

$$a = (a_0, a_1, \dots, a_{7n-1}) = \left(a^{(0)} | a^{(1)} | a^{(2)} | a^{(3)} | a^{(4)} | a^{(5)} | a^{(6)}\right) \in F_q^{7n}$$

olsun. Her $c = (c_0, c_1, \dots, c_{n-1}) \in F_q^n$ için $\sigma(c) = (c_{n-1}, c_0, \dots, c_{n-2}) \in F_q^n$ olmak üzere

$$\sigma^{\otimes 7} : F_q^{7n} \to F_q^{7n}$$

$$a \mapsto \sigma^{\otimes 7}(a) = \left(\sigma\left(a^{(0)}\right) | \sigma\left(a^{(1)}\right) | \sigma\left(a^{(2)}\right) | \sigma\left(a^{(3)}\right) | \sigma\left(a^{(4)}\right) | \sigma\left(a^{(5)}\right) | \sigma\left(a^{(6)}\right)\right)$$

şeklinde tanımlanan dönüşüm verilsin. $\sigma^{\otimes 7}(C) = C$ ise C koduna indeksi 7 olan quasi-devirli kod denir.

Önerme 3.2.15. δ, S_q üzerinde Gray dönüşümü olmak üzere $\delta\sigma = \sigma^{\otimes 7}\delta$ dir.

İspat: $0 \le i \le n-1$, $r_i = s_0^i + \sum_{k=1}^{5} w_k s_k^i + w_1 w_2 s_6^i \in S_q$ olsun.

$\sigma(r_0, r_1, \dots, r_{n-1}) = (r_{n-1}, r_0, \dots, r_{n-2})$ ifadesine δ dönüşümü uygulanırsa

$$\begin{aligned}\delta\big(\sigma(r_0, r_1, \dots, r_{n-1})\big) = \delta(r_{n-1}, r_0, \dots, r_{n-2})\\ = (s_0^{n-1}, s_0^0, \dots, s_0^{n-2}, s_0^{n-1} + s_1^{n-1}, \dots, s_0^{n-2} + s_1^{n-2}, s_0^{n-1}\\ + s_2^{n-1}, \dots, s_0^{n-2} + s_2^{n-2}, s_0^{n-1} + s_3^{n-1}, \dots, s_0^{n-2}\\ + s_3^{n-2}, s_0^{n-1} + s_4^{n-1}, \dots, s_0^{n-2} + s_4^{n-2}, s_0^{n-1}\\ + s_5^{n-1}, \dots, s_0^{n-2} + s_5^{n-2}, s_0^{n-1} + s_1^{n-1} + s_2^{n-1}\\ + s_6^{n-1}, \dots, s_0^{n-2} + s_1^{n-2} + s_2^{n-2} + s_6^{n-2})\end{aligned}$$

elde edilir.

Diğer yandan

$$\begin{aligned}\delta(r_0, \dots, r_{n-1}) = (s_0^0, s_0^1, \dots, s_0^{n-1}, s_0^0 + s_1^0, \dots, s_0^{n-1} + s_1^{n-1}, s_0^0 + s_2^0, \dots, s_0^{n-1}\\ + s_2^{n-1}, s_0^0 + s_3^0, \dots, s_0^{n-1} + s_3^{n-1}, s_0^0 + s_4^0, \dots, s_0^{n-1} + s_4^{n-1}, s_0^0\\ + s_5^0, \dots, s_0^{n-1} + s_5^{n-1}, s_0^0 + s_1^0 + s_2^0 + s_6^0, \dots, s_0^{n-1} + s_1^{n-1} + s_2^{n-1}\\ + s_6^{n-1})\end{aligned}$$

ifadesine $\sigma^{\otimes 7}$ dönüşümü uygulanırsa

$$\begin{aligned}\sigma^{\otimes 3}\big(\delta(r_0, \dots, r_{n-1})\big)\\ = (s_0^{n-1}, s_0^0, \dots, s_0^{n-2}, s_0^{n-1} + s_1^{n-1}, \dots, s_0^{n-2} + s_1^{n-2}, s_0^{n-1}\\ + s_2^{n-1}, \dots, s_0^{n-2} + s_2^{n-2}, s_0^{n-1} + s_3^{n-1}, \dots, s_0^{n-2} + s_3^{n-2},\end{aligned}$$

$$\begin{aligned}s_0^{n-1} + s_4^{n-1}, \dots, s_0^{n-2} + s_4^{n-2}, s_0^{n-1} + s_5^{n-1}, \dots, s_0^{n-2} + s_5^{n-2}, s_0^{n-1} + s_1^{n-1} + s_2^{n-1}\\ + s_6^{n-1}, \dots, s_0^{n-2} + s_1^{n-2} + s_2^{n-2} + s_6^{n-2})\end{aligned}$$

elde edilir. O halde $\delta\sigma = \sigma^{\otimes 7}\delta$ dir.

Teorem 3.2.16. C kodunun S_q üzerinde tanımlı n uzunluğunda devirli bir kod olması için gerek ve yeter koşul $\delta(\mathrm{C})$ kodunun F_q üzerinde tanımlı $7n$ uzunluğunda indeksi 7 olan bir quasi-devirli kod olmasıdır.

İspat: C devirli bir kod olsun. Bu durumda $\sigma(C) = C$ dir. δ dönüşümü uygulanırsa $\delta(\sigma(C)) = \delta(C)$ elde edilir. Önerme 3.2.15 den $\delta(\sigma(C)) = \sigma^{\otimes 7}(\delta(C)) = \delta(C)$ dir. O halde $\delta(\mathrm{C})$ indeksi 7 olan bir quasi-devirli koddur.

Tersine $\delta(\mathrm{C})$ indeksi 7 olan bir quasi-devirli kod olsun. O zaman $\sigma^{\otimes 7}(\delta(C)) = \delta(C)$ dir. Önerme 3.2.15 den $\sigma^{\otimes 7}(\delta(C)) = \delta(\sigma(C)) = \delta(C)$ elde edilir. δ bire bir olduğundan $\sigma(C) = C$ dir. O halde C devirli bir koddur.

3.3. S_4 Halkası Üzerinde Tanımlı DNA Kodlar

DNA (Deoksiribo Nükleik Asit) tüm organizmaların canlılık işlevleri ve biyolojik gelişmeleri için gerekli olan genetik talimatları taşıyan bir nükleik asittir. DNA bilgiyi uzun süre saklar. Çift sarmallı DNA da Adenin (A), Sitozin (C), Guanin (G), Timin (T) olmak üzere dört baz bulunur. İki DNA zinciri Watson Crick Complement (WCC) kuralı ile birbirine eşlenir. Bu kural ile Adenin, Timin ile Guanin, Sitozin ile eşleşir. Yani $\bar{A} = T, \bar{G} = C, \bar{T} = A, \bar{C} = G$ dir.

DNA molekülünün bu yapısı, sonlu cisimler ve halkalar üzerinde kodlama teorisine önemli katkılarda bulunmuştur. Bu araştırmalar başlangıçta GF(4) olarak bilinen 4 elemanlı sonlu bir cisim üzerinde gerçekleştirilmiştir (Abualrub vd., 2006). Bu çalışmalar sonrasında 4 elemanlı sonlu halkalar üzerinde farklı lineer kod türleri kullanılarak genişletilmiştir. Bu bölümde $q = 4$ için öncelikle devirli kodlardan daha sonra skew devirli kodlardan DNA kodları inceleyeceğiz.

$S_{D_4} = \{A, T, G, C\}$ DNA alfabesi, $c_i \in S_{D_4}$ olmak üzere $c = (c_0, c_1, \dots, c_{n-1})$ kod sözcükleri kümesi n uzunluğunda bir DNA kod olarak tanımlanır. $F_4 = \{0,1, \beta, \beta^2 = \beta + 1\}$ cismi ile S_{D_4} kümesi arasında

$$A \to 0,\ T \to 1,\ C \to \beta,\ G \to \beta^2$$

olacak şekilde bir dönüşüm tanımlanmıştır (Abualrub vd., 2006). Bu dönüşüm, Gray dönüşümü ve $\xi: S_4 \longrightarrow S_{D_4}^7 = \{\mathrm{A}, \mathrm{T}, \mathrm{G}, \mathrm{C}\}^7$ yardımıyla $S_{D_4}^7$ nin elemanları ile S_4 halkasının elemanları ile eşleşen DNA 7-mersler Tablo 3.3.1 deki gibi verilmiştir.

Tablo 3.3.1 S_4 Halkasının Elemanlarına Karşılık Gelen DNA 7-mersler

$s \in S_4$ Halkanın Elemanları	$\delta(s)$ Gray Görüntü	$\xi(s)$ DNA 7-mersler
0	(0,0,0,0,0,0,0)	$AAAAAAA$
1	(1,1,1,1,1,1,1)	TTTTTTT
β	$(\beta,\beta,\beta,\beta,\beta,\beta,\beta)$	CCCCCCC
β^2	$(\beta^2,\beta^2,\beta^2,\beta^2,\beta^2,\beta^2,\beta^2)$	$GGGGGGG$
w_1	(0,1,0,0,0,0,1)	ATAAAAT
w_2	(0,0,1,0,0,0,1)	AATAAAT
w_3	(0,0,0,1,0,0,0)	AAATAAA
w_4	(0,0,0,0,1,0,0)	AAAATAA
w_5	(0,0,0,0,0,1,0)	AAAAATA
w_1w_2	(0,0,0,0,0,0,1)	AAAAAAT
βw_1	$(0,\beta,0,0,0,0,\beta)$	$ACAAAAC$
$\beta^2 w_1$	$(0,\beta^2,0,0,0,0,\beta^2)$	$AGAAAAG$
$1+w_1$	(1,0,1,1,1,1,0)	$TATTTTA$
$1+\beta w_1$	$(1,\beta^2,1,1,1,1,\beta^2)$	$TGTTTTG$
$1+\beta^2 w_1$	$(1,\beta,1,1,1,1,\beta)$	$TCTTTTC$
$\beta+w_1$	$(\beta,\beta^2,\beta,\beta,\beta,\beta,\beta^2)$	CGCCCCG
$\beta+\beta w_1$	$(\beta,0,\beta,\beta,\beta,\beta,0)$	$CACCCCA$
$\beta+\beta^2 w_1$	$(\beta,1,\beta,\beta,\beta,\beta,1)$	$CTCCCCT$
β^2+w_1	$(\beta^2,\beta,\beta^2,\beta^2,\beta^2,\beta^2,\beta)$	GCGGGGC
$\beta^2+\beta w_1$	$(\beta^2,1,\beta^2,\beta^2,\beta^2,\beta^2,1)$	$GTGGGGT$
$\beta^2+\beta^2 w_1$	$(\beta^2,0,\beta^2,\beta^2,\beta^2,\beta^2,0)$	$GAGGGGA$
⋮	⋮	⋮

Lemma 3.3.1. $f_1(x), f_2(x) \in S_4[x]$ olsun. $derf_1(x) \geq derf_2(x)$, $der\, f_1(x) - derf_2(x) = t$ olmak üzere

i) $[f_1(x)f_2(x)]^* = {f_1}^*(x){f_2}^*(x)$,

ii) $[f_1(x) + f_2(x)]^* = {f_1}^*(x) + x^t {f_2}^*(x)$

dir.

Lemma 3.3.2. i. Herhangi bir $\varrho \in S_4$ için

$$\varrho + \bar{\varrho} = 1,$$

ii. Herhangi bir $\varrho_1, \varrho_2 \in S_4$ için

$$\overline{\varrho_1 + \varrho_2} = \overline{\varrho_1} + \overline{\varrho_2} + 1$$

dir.

İspat: i. $\varrho = s_0 + \sum_{k=1}^{5} w_k s_k + w_1 w_2 s_6 \in S_4$ için

$$\delta(\varrho) = (s_0, s_0 + s_1, s_0 + s_2, s_0 + s_3, s_0 + s_4, s_0 + s_5, s_0 + s_1 + s_2 + s_6)$$

olduğundan $\delta(\varrho)$ e karşılık gelen DNA 7-mers $A_1A_2A_3A_4A_5A_6A_7$ olmak üzere $\varrho + 1 \in S_4$ için

$$\delta(\varrho + 1) = (1 + s_0, 1 + s_0 + s_1, 1 + s_0 + s_2, 1 + s_0 + s_3, 1 + s_0 + s_4, 1 + s_0 + s_5, 1 + s_0 + s_1 + s_2 + s_6)$$

e karşılık gelen DNA 7-mers $\overline{A_1}\,\overline{A_2}\,\overline{A_3}\,\overline{A_4}\,\overline{A_5}\,\overline{A_6}\,\overline{A_7}$ olur. Bu durumda $\varrho + \bar{\varrho} = 1$ elde edilir.

ii. $\overline{\varrho_1 + \varrho_2} = 1 - (\varrho_1 + \varrho_2)$

$= (1 - \varrho_1) + (1 - \varrho_2) + 1$

$= \overline{\varrho_1} + \overline{\varrho_2} + 1.$

Teorem 3.3.3. $C = \bigoplus_{1 \le k \le 7} \alpha_k C_k$ lineer bir kod olsun. C kodunun S_4 üzerinde reversible bir kod olması için gerek ve yeter koşul $1 \le k \le 7$ için C_k kodlarının F_4 üzerinde reversible olmasıdır.

İspat: C kodu S_4 üzerinde tanımlı reversible bir kod, $1 \le k \le 7$ için $z^k = \left(z_0^k, z_1^k, \dots, z_{n-1}^k\right) \in C_k$ olsun. $0 \le i \le n-1$ için $c_i = \sum_{k=1}^{7} \alpha_k z_i^k$ olmak üzere $c = (c_0, c_1, \dots, c_{n-1}) \in C$ dir. C kodu reversible bir kod olduğundan $c^R = (c_{n-1}, \dots, c_1, c_0) \in C$ olur. Bu durumda $1 \le k \le 7$ için $(z^k)^R = \left(z_{n-1}^k, \dots, z_1^k, z_0^k\right) \in C_k$ elde edilir. O halde $1 \le k \le 7$ için C_k kodları reversible kod olur.

Tersine, $1 \leq k \leq 7$ için C_k kodları reversible olsun. Bu durumda $c = (c_0, c_1, \dots, c_{n-1}) \in C$, $0 \leq i \leq n-1$ için $c_i = \sum_{k=1}^{7} \alpha_k z_i^k$ olacak şekilde $1 \leq k \leq 7$ için $z^k = \left(z_0^k, z_1^k, \dots, z_{n-1}^k\right) \in C_k$ vardır. C_k kodları reverible kod olduklarından $(z^k)^R \in C_k$ olur. O halde $c^R = (\, c_{n-1}, \dots, c_1, c_0) \in C$ elde edilir. Bu durumda C kodu reversible bir kod olur.

Teorem 3.3.4. $C = \langle f(x) \rangle, F_q$ üzerinde tanımlı bir kodun reversible olması için gerek ve yeter koşul $f(x)$ polinomunun self-reciprocal olmasıdır (Massey, 1964).

Teorem 3.3.5. $C = \langle r(x) \rangle = \langle \sum_{k=1}^{7} \alpha_k r_k(x) \rangle, S_4$ üzerinde tanımlı devirli bir kod olsun. C kodunun reversible kod olması için gerek ve yeter koşul $1 \leq k \leq 7$ için $r_k(x) \in F_4[x]$ polinomlarının self-reciprocal olmasıdır.

İspat: C kodu reversible bir kod olsun. Bu durumda $1 \leq k \leq 7$ için C_k kodları reversible olduğundan $r_k(x)$ polinomları self-reciprocaldir.

Tersine, $1 \leq k \leq 7$ için $r_k(x)$ polinomları self-reciprocal ve $r(x) \in C$ olsun. Lemma 3.3.1 ve $r_k^*(x) = r_k(x)$ olduğundan $r^*(x) \in C$ dir. Bu durumda C reversible bir kod olur.

Teorem 3.3.6. $C = \bigoplus_{1 \leq k \leq 7} \alpha_k C_k$, S_4 üzerinde tanımlı bir devirli kod olsun. C kodunun reversible complement olması için gerek ve yeter koşul $1 \leq k \leq 7$ için C_k kodlarının F_4 üzerinde reversible bir kod ve $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C$ olmasıdır.

İspat: C reversible complement kod olsun. Dolayısıyla C_k kodları Teorem 3.3.3 den reversible olur. $\forall c = (c_0, c_1, \dots, c_{n-1}) \in C$ için C reversible complement olduğundan $c^{RC} = (\bar{c}_{n-1}, \bar{c}_{n-2} \dots, \bar{c}_0) \in C$ dir. C lineer bir kod olduğu için $(0,0, \dots,0) \in C$ dir. O halde $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C$ olur.

Tersine, C_k kodları reversible ve $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C$ olsun. Bu durumda C reversible kod olur. Yani $\forall c = (c_0, c_1, \dots, c_{n-1}) \in C$ için $c^R = (c_{n-1}, c_{n-2}, \dots, c_0) \in C$ dir. $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C$ olduğundan

$$c^{RC} = (\overline{c_{n-1}}, \overline{c_{n-2}}, \dots, \bar{c}_0)$$

$$= (c_{n-1}, c_{n-2}, \dots, c_0) + (\bar{0}, \bar{0}, \dots, \bar{0}) \in C$$

Dolayısıyla C reversible complement bir kod olur.

$$(0,0,\dots,0)^C = (\bar{0},\bar{0},\dots,\bar{0}) = (1,1,\dots,1) \in C$$

ya da

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1} \in C$$

olması kullanılarak aşağıdaki sonuç elde edilir.

Sonuç 3.3.7. $C = \langle r(x) \rangle = \langle \sum_{k=1}^{7} \alpha_k r_k(x) \rangle, S_4$ üzerinde devirli bir kod olsun. C kodunun reversible complement kod olması için gerek ve yeter koşul $1 \leq k \leq 7$ için $r_k(x)$ polinomlarının self-reciprocal ve $\frac{x^n-1}{x-1} \in C$ olmasıdır.

Sonuç 3.3.8. C, S_4 üzerinde n uzunluğunda d minimum uzaklığa sahip devirli DNA kod olsun. Bu durumda $\xi(\delta(C))$, $7n$ uzunluğunda S_{D_4} üzerinde en az d minimum uzaklığa sahip bir DNA koddur.

Örnek 3.3.9. $n = 5, 1 \leq k \leq 7$ için

$$x^5 - 1 = (x+1)(x^2 + \beta x + 1)(x^2 + \beta^2 x + 1) \in F_4[x]$$

olmak üzere $r_k(x) = (x^2 + \beta x + 1)(x^2 + \beta^2 x + 1)$ olsun. Bu durumda $C_k = \langle r_k(x) \rangle$, F_4 üzerinde 5 uzunluğunda devirli bir kod olur. O halde C kodu da S_4 üzerinde 5 uzunluğunda devirli bir koddur. $r_k(x)$ polinomları self-reciprocal polinomlar olduğundan C_k kodları F_4 üzerinde reversible kod olur. Bu durumda C kodu da S_4 üzerinde reversible kod olur. $(\bar{0},\bar{0},\dots,\bar{0}) \in C$ olduğundan C kodu S_4 üzerinde reversible complement bir kod olur. Böylece C kodu devirli DNA koddur. C kodunun δ altındaki görüntüsü 35 uzunluğunda, 4^7 elemanlı ve Hamming uzaklığı 5 olan bir DNA koddur. C kodunun elemanları;

$AAAAAAAAAAAAA \cdots AAAAAAA$
$AGAAAAGAGAAAAG \cdots AGAAAAG$
$TCTTTTCTCTTTTC \cdots TCTTTTC$
$GGGGGGGGGGGGG \cdots GGGGGGG$
TTTTTTTTTTTTT⋯TTTTTTT
CCCCCCCCCCCCC ⋯ CCCCCCC
$GAGGGGAGAGGGGA \cdots GAGGGGA$
$AAAATAAAAAATAA \cdots AAAATAA$
$TGTTTTGTGTTTTG \cdots TGTTTTG$

$$CTCCCCTCTCCCCT \cdots CTCCCCT$$
$$TTATTTTTTATTTT \cdots TTATTTT$$
$$GAAAAGAGAAAAGA \cdots GAAAAGA$$
$$\vdots \qquad\qquad \vdots$$
$$GAAAAGAGAAAAGA \cdots GAAAAGA$$

şeklindedir.

Örnek 3.3.10. $n = 7, 1 \leq k \leq 7$ için

$$x^7 - 1 = (x-1)(x^3 - x - 1)(x^3 - x^2 - 1) \in F_4[x]$$

olmak üzere $r_k(x) = (x^3 - x - 1)(x^3 - x^2 - 1)$ olsun. Bu durumda $C_k = \langle r_k(x) \rangle$, F_4 üzerinde 7 uzunluğunda devirli bir kod olur. O halde C kodu da S_4 üzerinde 7 uzunluğunda devirli bir koddur. $r_k(x)$ polinomları self-reciprocal polinomlar olduğundan C_k kodları F_4 üzerinde reversible kod olur. Bu durumda C kodu da S_4 üzerinde reversible kod olur. $(\bar{0}, \bar{0}, \ldots, \bar{0}) \in C$ olduğundan C kodu S_4 üzerinde reversible complement bir kod olur. Böylece C kodu devirli DNA koddur. C kodunun δ altındaki görüntüsü 49 uzunluğunda, 4^7 elemanlı ve Hamming uzaklığı 7 olan bir DNA koddur. C kodunun elemanları;

$$\mathrm{TTTTTTTTTTTTT} \cdots \mathrm{TTTTTTT}$$
$$\mathrm{CCCCCCCCCCCCC} \cdots \mathrm{CCCCCCC}$$
$$AAAAAAAAAAAAA \cdots AAAAAAA$$
$$GGGGGGGGGGGGG \cdots GGGGGGG$$
$$\mathrm{CGCCCCGCGCCCCG} \cdots \mathrm{CGCCCCG}$$
$$CGGGGCGCGGGGCG \cdots CGGGGCG$$
$$AAATAAAAAATAAA \cdots AAATAAA$$
$$TTTATTTTTTATTT \cdots TTTATTT$$
$$CACCCCACACCCCA \cdots CACCCCA$$
$$TGGGGTG\ TGGGGTG \cdots TGGGGTG$$
$$GTGGGGTGTGGGGT \cdots GTGGGGT$$
$$ACCCCACACCCCAC \cdots ACCCCAC$$
$$\vdots \qquad\qquad \vdots$$
$$AAAAAATAAAAAAT \cdots AAAAAAT$$

şeklindedir.

3.3.1. S_4 Halkası Üzerinde Tanımlı Skew Devirli Kodlardan DNA Kodlar

Tanım 3.3.1.1. C, S_4 üzerinde n uzunluğunda lineer bir kod olsun.

i) C, skew devirli bir koddur

ii) Herhangi bir $x \in C$ için $x^{RC} \in C$ dir

koşulları sağlanıyorsa C koduna skew devirli DNA kod denir.

Tanım 3.3.1.2. Her $s = s_0 + \sum_{k=1}^{5} w_k s_k + w_1 w_2 s_6 \in S_q$ için

$$m = s_0 + s_1 + s_2 + s_6 + w_1(s_1 + s_2 + s_5 + s_6) + w_2(s_1 + s_2 + s_4 + s_6) + w_3(s_1 + s_2 + s_3 + s_6) + w_4(s_1 + s_6) + w_5(s_2 + s_6) + w_1 w_2 (s_1 + s_2 + s_4 + s_5 + s_6)$$

olmak üzere

$$\Psi: S_q \longrightarrow S_q$$

$$s \longmapsto \Psi(s) = m$$

şeklinde tanımlı Ψ dönüşümü S_q üzerinde tanımlı aşikar olmayan bir otomorfizma olmak üzere

$$S_q[x,\Psi] = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} : a_i \in S_q, n \in \mathbb{N}\}$$

kümesine değişmeli olmayan skew polinom halkası denir.

$S_q[x,\Psi]$ halkasındaki toplama işlemi polinomlardaki toplama işlemidir. Çarpma ise $(tx^i)(bx^j) = t\Psi^i(b)x^{i+j}$ şeklinde tanımlıdır. $s \in S_q$ için $\Psi^2(s) = s$ olduğundan Ψ mertebesi 2 olan bir halka otomorfizmasıdır. Taban elemanlarına bağlı bu otomorfizma aşağıdaki şekilde de ifade edilebilir.

$$1 \leftrightarrow 1$$

$$w_1 \leftrightarrow 1 + w_1 + w_2 + w_3 + w_4 + w_1 w_2$$

$$w_2 \leftrightarrow 1 + w_1 + w_2 + w_3 + w_5 + w_1 w_2$$

$$w_3 \leftrightarrow w_3$$

$$w_4 \leftrightarrow w_2 + w_1 w_2$$

$$w_5 \leftrightarrow w_1 + w_1 w_2$$

$$w_1 w_2 \leftrightarrow 1 + w_1 + w_2 + w_3 + w_4 + w_5 + w_1 w_2$$

Tanım 3.3.1.3. $\emptyset \neq C \subseteq S_q^n$ olmak üzere

i) C, S_q^n nin bir alt modülü

ii) Her $\zeta = (\zeta_0, \zeta_1, \dots, \zeta_{n-1}) \in C$ için

$$\sigma_\Psi(\zeta) = \big(\Psi(\zeta_{n-1}), \Psi(\zeta_0), \dots, \Psi(\zeta_{n-2})\big) \in C$$

koşullarını sağlayan C kümesine S_q üzerinde n uzunluğunda skew devirli kod denir.

Teorem 3.3.1.4. Her $r(x) + \langle x^n - 1\rangle \in S_q[x,\Psi]/\langle x^n - 1\rangle$, $f(x) \in S_q[x,\Psi]$ için

$$. : S_q[x,\Psi] \times S_q[x,\Psi]/\langle x^n - 1\rangle \longrightarrow S_q[x,\Psi]/\langle x^n - 1\rangle$$

$$f(x)(r(x) + \langle x^n - 1\rangle) = f(x)r(x) + \langle x^n - 1\rangle$$

şeklinde tanımlı soldan çarpma işlemi ve polinomlardaki toplama işlemine göre $S_q[x,\Psi]/\langle x^n - 1\rangle$ bir sol $S_q[x,\Psi]$-modüldür.

Teorem 3.3.1.5. Bir C kodunun skew devirli kod olması için gerek ve yeter koşul $S_q[x,\Psi]/\langle x^n - 1\rangle$ in bir sol $S_q[x,\Psi]$-alt modül olmasıdır.

Teorem 3.3.1.6. C bir skew devirli kod ve $r(x)$ minimal dereceli polinom olsun. $r(x)$ monik polinom ise $C = \langle r(x)\rangle$ ve $r(x), x^n - 1$ in bir sağ bölenidir.

Önerme 3.3.1.7. $a, b, c \in F_q^n$ için $\lambda(a, b, c) = (c, b, a)$ olmak üzere $\delta\Psi = \lambda\sigma^{\otimes 7}\delta$ dir.

İspat: Önerme 3.2.15 e benzer şekilde yapılır.

Teorem 3.3.1.8. S_q üzerinde tanımlı n uzunluğunda bir skew devirli kodun Gray dönüşümü altındaki görüntüsü F_q üzerinde tanımlı $7n$ uzunluğunda indeksi 7 olan bir quasi-devirli koda denktir.

İspat: C, S_q üzerinde tanımlı n uzunluğunda bir skew devirli kod olsun. Bu durumda $\Psi(C) = C$ dir. δ dönüşümü uygulanırsa $\delta\big(\Psi(C)\big) = \delta(C)$ elde edilir.

Önerme 3.3.1.7 dan $\delta(\Psi(C)) = \lambda\left(\sigma^{\otimes 7}(\delta(C))\right) = \delta(C)$ dir. O halde δ(C), F_q üzerinde tanımlı $7n$ uzunluğunda indeksi 7 olan bir quasi-devirli koda denktir.

Lemma 3.3.1.9. $f_1(x), f_2(x) \in S_4[x,\Psi]$, $der f_1(x) \geq der f_2(x)$, $der f_1(x) - der f_2(x) = t$ olmak üzere

i) $[f_1(x)f_2(x)]^* = {f_1}^*(x){f_2}^*(x)$,

ii) $[f_1(x) + f_2(x)]^* = {f_1}^*(x) + x^t {f_2}^*(x)$

dir.

Lemma 3.3.1.10. Herhangi bir $\varsigma \in S_4$ için

$$\Psi(\varsigma) + \Psi(\bar{\varsigma}) = 1$$

dir.

Teorem 3.3.1.11. n çift sayı, $r(x)$, $x^n - 1$ polinomunun minimal dereceli monik bir sağ böleni olmak üzere $C = \langle r(x) \rangle$, S_4 üzerinde tanımlı n uzunluğunda bir skew devirli kod olsun. C kodu reversible complement bir kod ise $r(x)$ polinomu self reciprocal ve $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C$dir.

İspat: C reversible complement kod olsun. C lineer bir kod olduğu için $(0,0,\dots,0) \in C$ dir. O halde $(\bar{0}, \bar{0}, \dots, \bar{0}) \in C$ olur.

C de $r(x) = r_0 + r_1 x + r_2 x^2 + \cdots + x^m$ minimal dereceli monik polinomunu ele alalım. Bu polinomun vektör karşılığı $(r_0, r_1, r_2, \dots, 0, \dots, 0)$ dır. C reversible complement kod olduğundan $(r_0, r_1, r_2, \dots, 0, \dots, 0)^{RC} \in C$ olur. Yani

$$r(x)^{RC} = 1 + x + \cdots + x^{n-m-2} + r_{m-1}x^{n-m} + \cdots + r_1 x^{n-2} + r_0 x^{n-1}$$

dir. C lineer bir kod olduğundan $r(x)^{RC} + \frac{x^n - 1}{x - 1} \in C$ dir. Buradan

$$x^{n-m-1} + (\overline{r_{m-1}} + 1)x^{n-m} + \cdots + (\overline{r_1} + 1)x^{n-2} + (\overline{r_0} + 1)x^{n-1} \in C$$

elde edilir. Bu ifadeyi sağdan x^{m-n+1} ile çarparsak

$$(1 + (\overline{r_{m-1}} + 1)\Psi(1)x + \cdots + (\overline{r_1} + 1)\Psi^{m-1}(1)x^{m-1} + (\overline{r_0} + 1)\Psi^m(1)x^m) \in C$$

elde edilir. Böylece $1+(\overline{r_{m-1}}+1)x+\cdots+(\overline{r_1}+1)x^{m-1}+(\overline{r_0}+1)x^m \in C$ olur. Bu durumda $r^*(x)=1+r_{m-1}x+\cdots+r_0x^{n-1} \in C$ dir. $C=\langle r(x)\rangle$ olduğundan $r^*(x)=g(x)r(x)$ olacak şekilde $g(x) \in S_4[x,\Psi]$ vardır. Bu durum $g(x)$ polinomunun 1 olmasını gerektirir. O halde $r^*(x)=r(x)$ ve $r(x)$ self-reciprocal polinomdur.

Teorem 3.3.1.12. n çift sayı, $r(x)$, x^n-1 in minimal dereceli monik bir sağ böleni olmak üzere $C=\langle r(x)\rangle$, S_4 üzerinde tanımlı n uzunluğunda bir skew devirli kod olsun. $r(x)$ polinomu self-reciprocal ve $(\bar{0},\bar{0},\ldots,\bar{0}) \in C$ ise C kodu reversible complement bir kod olur.

İspat: $C=\langle r(x)\rangle$, S_4 üzerinde tanımlı n uzunluğunda bir skew devirli kod olsun. Eğer $g(x)= g_0+g_1x+g_2x^2+\cdots+g_kx^k \in C$ ise o zaman $g(x)=q(x)r(x)$ olacak şekilde $q(x) \in S_4[x,\Psi]$ vardır. Lemma 3.3.1.9 dan $g^*(x)=q^*(x)r^*(x)$ elde edilir. Bu durumda $r(x)$ polinomu self-reciprocal olduğundan herhangi bir $g(x) \in C$ için $g^*(x)=q^*(x)r(x) \in C$ olur. C skew devirli bir kod olduğundan,

$$g(x)x^{n-k-1}=g_0x^{n-k-1}+g_1x^{n-k}+g_2x^{n-k+1}+\cdots+g_kx^{n-1} \in C$$

dir. $1+x+x^2+\cdots+x^{n-1}=\frac{x^n-1}{x-1} \in C$ ve C kodu lineer olduğundan

$$g(x)x^{n-k-1}+\frac{x^n-1}{x-1}=1+x+\cdots+x^{n-k-2}+(1+g_0)x^{n-k-1}+\cdots+(1+g_k)x^{n-1} \in C$$

dir. Buradan

$$1+x+\cdots+x^{n-k-2}+\overline{g_0}x^{n-k-1}+\cdots+\overline{g_k}x^{n-1}=\left(g^*(x)\right)^{RC} \in C$$

elde edilir. Böylece C kodu reversible complement bir kod olur.

$s=s_0+\sum_{k=1}^{5}w_ks_k+w_1w_2s_6 \in S_4$ ve $\Psi(s)$ elemanları birbirlerinin tersi (reverse) olacak şekilde eşleşir. Örneğin

$$\xi(w_1)=ATAAAAT$$

iken

$$\xi\left(\Psi(w_1)\right)=\xi(1+w_1+w_2+w_3+w_4+w_1w_2)$$

$$= TAAAATA$$

Bu ifadeyi $n = 2$ için yaparsak

$$\xi(s, s') = \xi(w_1, 1 + w_2) = (ATAAAAT, TTATTTA)$$

$$\xi\big(\Psi(s', s)\big) = \xi(w_1 + w_2 + w_3 + w_5 + w_1w_2, 1 + w_1 + w_2 + w_3 + w_4 + w_1w_2)$$

$$= (ATTTATT, TAAAATA)$$

Bu dönüşümü genellersek $l = (l_0, l_1, \dots, l_{n-1}) \in S_4^n$ için

$$\big(\xi(l_0), \xi(l_1), \dots, \xi(l_{n-1})\big)^{\mathrm{R}} = \Big(\xi\big(\Psi(l_{n-1})\big), \xi\big(\Psi(l_{n-2})\big), \dots, \xi\big(\Psi(l_1)\big), \xi\big(\Psi(l_0)\big)\Big)$$

olarak elde edilir.

Tanım 3.3.1.13. C, S_4 üzerinde tanımlı n uzunluğunda bir kod olsun. Herhangi bir $c \in C$ için $\xi(c)^R \in \xi(C)$ ise C koduna (ona denk olan $\xi(C)$) reversible DNA kod denir.

Tanım 3.3.1.14. $p(x) = t_0 + t_1x + \cdots + t_mx^m \in S_4[x]$, m. dereceden bir polinom olsun. $0 \le i \le m$ için $t_i = t_{m-i}$ oluyarsa $p(x)$ polinomuna palindromik polinom, $t_i = \Psi(t_{m-i})$ oluyorsa $p(x)$ polimomuna Ψ-palindromik polinom denir.

Otomorfizmanın mertebesi 2 olduğundan skew devirli kodlar n tek olduğunda devirli koda denk olur. Dolayısıyla bu kısımda n nin çift olduğu durumlar göz önüne alınacaktır.

Teorem 3.3.1.15. $C = \langle r(x) \rangle$, S_4 üzerinde n uzunluğunda skew devirli kod, $r(x), x^n - 1$ in bir sağ böleni ve $der(r(x))$ tek sayı olsun. $r(x)$, Ψ-palindromik polinom ise $\xi(C)$, reversible DNA kod olur.

İspat: $r(x) = t_0 + t_1x + \cdots + t_{2m-1}x^{2m-1}$, Ψ-palindromik polinom olsun. O halde $0 \le i \le 2m - 1$ için $t_{\mathrm{i}} = \Psi(t_{2m-1-i})$ olur. $q(x) = d_0 + d_1x + \cdots + d_{2v-1}x^{2v-1}$, $h = 1,2, \dots, n - 1$ için $q(x)r(x)$ de b_h, x^h ın katsayısı olsun. Bu durumda $u < \frac{n}{2}$ için $q(x)r(x)$ de x^u nun katsayısı

$$b_u = \sum_{k=0}^{u} d_k \Psi^k(t_{u-k})$$

ve x^{n-u} nun katsayısı $b_{n-u} = \sum_{k=0}^{u} d_{2v-1-k}\Psi^{2v-1-k}(\ t_{2m-1-(u-k)})$ dir. O halde $q(x)r(x) = \sum_{f=0}^{2v-1}\ d_f x^f r(x)$ polinomu $b = (b_0, b_1, \ldots, b_{n-1})$ vektörüne karşılık gelir.

z vektörüne karşılık gelen polinom $\sum_{f=0}^{2k-1}\Psi(d_f)x^{2k-1-f}r(x)$ olmak üzere

$$\xi(b)^{\mathrm{R}} = \left(\xi(b_0), \xi(b_1), \ldots, \xi(b_{n-1})\right)$$

vektörü $\xi(z)$ vektörüne eşit olur. $z = (z_0, z_1, \ldots, z_{n-1}) \in C$ olduğundan $\xi(C)$ bir reversible DNA kod olur.

Teorem 3.3.1.16. $r(x), x^n - 1$ in bir sağ böleni ve $der(r(x))$ çift sayı olmak üzere $C = \langle r(x)\rangle, S_4$ üzerinde n uzunluğunda skew devirli kod olsun. $r(x)$, palindromik polinam ise $\xi(C)$, reversible DNA kod olur.

İspat: $r(x) = t_0 + t_1 x + \cdots + t_{2m}x^{2m}$, palindromik polinom olsun. O halde $0 \le i \le 2m$ için $t_{\mathrm{i}} = t_{2m-i}$ olur.

$q(x) = d_0 + d_1 x + \cdots + d_{2v}x^{2v}$, $h = 1,2, \ldots, n-1$ için $q(x)r(x)$ de b_h, x^h ın katsayısı olsun. Bu durumda $u < \frac{n}{2}$ için $q(x)r(x)$ de x^u nun katsayısı

$$b_u = \sum_{k=0}^{u} d_k \Psi^k(t_{u-k})$$

ve x^{n-u} nun katsayısı $b_{n-u} = \sum_{k=0}^{u} d_{2v-k}\Psi^{2v-k}(\ t_{2m-(u-k)})$ dir. O halde $q(x)r(x) = \sum_{f=0}^{2v}\ d_f x^f r(x)$ polinomu $b = (b_0, b_1, \ldots, b_{n-1})$ vektörüne karşılık gelir.

z vektörüne karşılık gelen polinom $\sum_{f=0}^{2k}\Psi(d_f)x^{2k-f}r(x)$ olmak üzere

$$\xi(b)^{\mathrm{R}} = \left(\xi(b_0), \xi(b_1), \ldots, \xi(b_{n-1})\right)$$

vektörü $\xi(z)$ vektörüne eşit olur. $z = (z_0, z_1, \ldots, z_{n-1}) \in C$ olduğundan $\xi(C)$ bir reversible DNA kod olur.

Teorem 3.3.1.17. $x^n - 1 = g(x)r(x) \in S_4[x,\Psi]$, $der(r(x))$ tek sayı olsun. Bu durumda $r(x)$ bir Ψ -palindromik polinom ise $g(x)$ palindromik bir polinom olur.

İspat: $r(x) = t_0 + t_1x + \cdots + t_{2m-1}x^{2m-1}$ olsun. n çift olduğundan $g(x) = d_0 + d_1x + \cdots + d_{2v-1}x^{2v-1}$ olur. $r(x)$, Ψ-palindromik polinom olduğundan $0 \leq i \leq 2m-1$ için $t_i = \Psi(t_{2m-1-i})$ dir. $h = 1,2,\ldots,n-1$ için $g(x)r(x)$ de b_h, x^h ın katsayısı olsun. Bu durumda $u < \frac{n}{2}$ için $g(x)r(x)$ de x^u nun katsayısı

$$b_u = \sum_{k=0}^{u} d_k \Psi^k(t_{u-k})$$

ve x^{n-u} nun katsayısı $b_{n-u} = \sum_{k=0}^{u} d_{2v-1-k}\Psi^{2v-1-k}(\, t_{2m-1-(u-k)})$ dir. $b_0 = b_n = 0$ ve $1 \leq i \leq n-1$ için $b_i = 0$ olması kullanılarak $0 \leq i \leq v-1$ için $d_i = d_{2v-1-i}$ olduğu tümevarımla kolaylıkla görülür. O halde $g(x)$ palindromik bir polinom olur.

Teorem 3.3.1.18. $x^n - 1 = g(x)r(x) \in S_4[x,\Psi]$, $der(r(x))$ çift sayı olsun. Bu durumda $g(x)$ bir palindromik polinom ise $r(x)$ polinomuda palindromik bir polinom olur.

İspat: Teorem 3.3.1.17 ye benzer şekilde yapılır.

3.4. S_q Halkası Üzerinde Tanımlı Devirli Kodlardan Kuantum Kodlar

Teorem 3.4.1. $C = \bigoplus_{1 \leq k \leq 7} \alpha_k C_k, S_q$ üzerinde tanımlı n uzunluğunda devirli bir kod, $C_k = \langle r_k(x) \rangle$ olsun. $C^{\perp} \subseteq C$ olması için gerek ve yeter koşul $1 \leq k \leq 7$ için

$$x^n - 1 \equiv 0\big(mod\ r_k(x)r_k^*(x)\big)$$

olmasıdır.

İspat: $1 \leq k \leq 7$ için $x^n - 1 \equiv 0\big(mod\ r_k(x)r_k^*(x)\big)$ olsun. Teorem 2.79 dan

$$C_k^{\perp} \subseteq C_k, \qquad 1 \leq k \leq 7$$

dir. Buradan

$$\alpha_k C_k^{\perp} \subseteq \alpha_k C_k, \qquad 1 \leq k \leq 7$$

olup

$$\bigoplus_{1 \leq k \leq 7} \alpha_k C_k^{\perp} \subseteq \bigoplus_{1 \leq k \leq 7} \alpha_k C_k$$

ifadesi elde edilir. Böylece

$$\langle \sum_{k=7}^{7} \alpha_k h_k^*(x) \rangle \subseteq \langle \sum_{k=7}^{7} \alpha_k r_k(x) \rangle$$

dir. O halde $C^{\perp} \subseteq C$ dir.

Diğer taraftan $C^{\perp} \subseteq C$ olsun. Bu durumda

$$\bigoplus_{1 \le k \le 7} \alpha_k C_k^{\perp} \subseteq \bigoplus_{1 \le k \le 7} \alpha_k C_k$$

dir. $1 \le k \le 7$ için sırasıyla modülo α_i ye göre düşünüldüğünde $C_k^{\perp} \subseteq C_k$ ifadesi elde edilir. Böylece her $1 \le k \le 7$ için

$$x^n - 1 \equiv 0 \big(mod\ r_k(x) r_k^*(x)\big)$$

dir.

Sonuç 3.4.2. $C = \bigoplus_{1 \le k \le 7} \alpha_k C_k, S_q$ üzerinde tanımlı n uzunluğunda bir devirli kod olsun. $C^{\perp} \subseteq C$ olması için gerek ve yeter koşul $1 \le k \le 7$ için $C_k^{\perp} \subseteq C_k$ olmasıdır.

Örnek 3.4.3. $n = 21$ için

$$x^n - 1 = (x+1)(x^2+x+1)(x^3+x^2+1)(x^3+x+1)(x^6+x^4+x^2+x+1)(x^6+x^5+x^4+x^2+1)$$

$$= r_1(x) r_2(x) r_3(x) r_4(x) r_5(x) r_6(x) \in F_2[x]$$

olsun. Böylece

$$r_1^*(x) = x + 1 = r_1(x),$$

$$r_2^*(x) = x^2 + x + 1 = r_2(x),$$

$$r_3^*(x) = x^3 + x + 1 = r_4(x),$$

$$r_4^*(x) = x^3 + x^2 + 1 = r_3(x),$$

$$r_5^*(x) = x^6 + x^5 + x^4 + x^2 + 1 = r_6(x)$$

$$r_6^*(x) = x^6 + x^4 + x^2 + x + 1 = r_5(x)$$

dir. $C = \langle \alpha_1 r_3(x), \alpha_2 r_3(x), \alpha_3 r_3(x), \alpha_4 r_4(x), \dots, \alpha_7 r_7(x) \rangle$ olsun. $3 \le k \le 7$ için $r_k(x) r_k^*(x)$ polinomu $x^n - 1$ polinomunu böldüğünden $C^{\perp} \subseteq C$ dir.

Teorem 3.4.4. $C = \bigoplus_{1\le j\le 7} \alpha_j C_j, S_q$ üzerinde tanımlı n uzunluğunda devirli bir kod ve $C^{\perp} \subseteq C$ olsun. d_L, C kodunun minimum Lee uzaklığı ve k, $\delta(\mathcal{C})$ kodunun boyutu olmak üzere $\left[[7n, 2k-7n, d_L]\right]$ parametrelerine sahip hata düzeltici bir kuantum kodu vardır.

İspat: Herhangi bir $c \in \delta(C^{\perp}) = \left(\delta(C)\right)^{\perp}$ olsun. δ birebir ve örten olduğundan $c = \delta(c')$ olacak şekilde $c' \in C^{\perp}$ vardır. $C^{\perp} \subseteq C$ olduğundan $c' \in C$ dir. Buradan $c = \delta(c') \in \delta(C)$ olup $\left(\delta(C)\right)^{\perp} \subseteq \delta(C)$ bulunur. $\delta(C)$ kodu F_q üzerinde $[7n, k, d_H]$ parametrelerine sahip lineer kod olup Teorem 2.79 dan $\left[[7n, 2k-7n, d_L]\right]$ parametrelerine sahip hata düzeltici bir kuantum kodu vardır.

Örnek 3.4.5. $q = 9$ ve $n = 20$ olsun.

$$x^{20}-1 = (x+1)(x+2)(x^2+1)(x^4+x^3+2x+1)(x^4+x^3+x^2+x+1)(x^4 + 2x^3+x+1)(x^4+2x^3+x^2+2x+1) \in F_9[x]$$

dir. $r_1(x) = \cdots = r_7(x) = x^4+x^3+2x+1$ olsun. Bu durumda $i = 1, 2, \ldots, 7$ için $C_i = \langle r_i(x)\rangle$ kodları F_9 üzerinde parametreleri $[20, 16, 4]$ olan devirli kodlardır. Teorem 3.2.10 dan C kodu S_9 üzerinde 20 uzunluğunda devirli bir koddur. $1 \le i \le 7$ için bütün $r_i(x)r_i^*(x)$ ler $x^{20}-1$ in böleni olduğundan Teorem 3.4.1 e göre $C^{\perp} \subseteq C$ dir. Ayrıca $\delta(C)$ kodu F_9 üzerinde parametreleri $[140, 112, 4]$ olan lineer bir koddur. Bu durumda Teorem 3.3.4 e göre S_9 üzerinde $\left[[140, 84, 4]\right]$ parametrelerine sahip kuantum kod vardır.

Örnek 3.4.6. $q = 5$ ve $n = 31$ olsun.

$$x^{31}-1 = (x+4)(x^3+x+4)(x^3+2x+4)(x^3+x^2+x+4)(x^3+x^2+3x + 4)(x^3+2x^2+x+4)(x^3+2x^2+4x+4)(x^3+3x^2+4)(x^3 + 4x^2+4)(x^3+4x^2+3x+4)(x^3+4x^2+4x+4) \in F_5[x]$$

dir. $r_1(x) = \cdots = r_7(x) = x^3+x+4$ olsun. Bu durumda $i = 1, 2, \ldots, 7$ için $C_i = \langle r_i(x)\rangle$ kodları F_5 üzerinde parametreleri $[31, 28, 3]$ olan devirli kodlardır. Teorem 3.2.10 dan C kodu S_5 üzerinde üzerinde 31 uzunluğunda devirli bir koddur. $1 \le i \le 7$ için bütün $r_i(x)r_i^*(x)$ ler $x^{31}-1$ in böleni olduğundan Teorem 3.4.1 e göre $C^{\perp} \subseteq C$ dir. Ayrıca $\delta(C)$ kodu F_5 üzerinde parametreleri $[217, 196, 3]$ olan lineer

koddur. Bu durumda Teorem 3.3.4 e göre S_5 üzerinde $[[217, 175, 3]]$ parametrelerine sahip kuantum kod vardır.

Örnek 3.4.7. $q = 17$ ve $n = 34$ olsun.

$$x^{34} - 1 = (x + 1)^{17}(x - 1)^{17} \in F_{17}[x]$$

dir. $r_1(x) = \cdots = r_7(x) = x^4 - 2x^3 + 2x - 1$ olsun. Bu durumda $i = 1,2, \ldots,7$ için $C_i = \langle r_i(x) \rangle$ kodları F_{17} üzerinde parametreleri $[34, 30, 4]$ olan devirli kodlardır. Teorem 3.2.10 dan C kodu S_{17} üzerinde 34 uzunluğunda devirli bir koddur. $1 \leq i \leq 7$ için bütün $r_i(x)r_i^*(x)$ ler $x^{34} - 1$ in böleni olduğundan Teorem 3.4.1 e göre $C^{\perp} \subseteq C$ dir. Ayrıca $\delta(C)$ kodu F_{17} üzerinde parametreleri $[238,210, 4]$ olan lineer bir koddur. Bu durumda Teorem 3.3.4 e göre S_{17} üzerinde $[[238, 182, 4]]$ parametrelerine sahip kuantum kod vardır.

Bazı n ve q değerleri için kuantum kodlarının parametreleri aşağıdaki gibidir.

n	q	$r_1(x) = \cdots = r_5(x)$	$r_6(x) = r_7(x)$	$\delta(C)$	$[[n, k, d]]$
6	9	$x - 2$	$x - 2$	[42,35,2]	[[42,28,2]]
10	5	$x^4 + 3x^2 + 1$	$x^4 + 3x^2 + 1$	[70,42,3]	[[70,14,3]]
10	5	$x^2 + 3x - 1$	$x^2 - 3x + 1$	[70,56,2]	[[70,42,2]]
12	7	$x^4 + 5x^3 + x^2 + 3x + 5$	$x^4 + 5x^3 + x^2 + 3x + 5$	[84,56,3]	[[84,28,3]]
22	5	$x^{10} + 3x^9 + 2x^7 + 4x^6 + 2x^5 + x^4 + 2x^3 + 3x + 4$	$x^{10} + 3x^9 + 2x^7 + 4x^6 + 2x^5 + x^4 + 2x^3 + 3x + 4$	[154,84,7]	[[154,14,7]]
31	5	$x^3 + x^2 + x - 1$	$x^3 + x - 1$	[217,196,3]	[[217,175,3
39	13	$x^3 + 7x^2 + 8x + 10$	$x^3 + 7x^2 + 8x + 10$	[273,252,3]	[[273,231,3

4. R_q HALKASI ÜZERİNDEKİ DNA VE KUANTUM KODLAR

Bu bölümde, R_q halkası üzerinde R_q-devirli ve R_q-skew devirli kodlar tanımlanarak R_q-devirli kodlardan DNA kodlar, R_q-skew devirli kodlardan kuantum kodlar incelendi.

4.1. R_q Halkası

$R_q = F_q S_q = \{(r_1, r_2): r_1 \in F_q, r_2 \in S_q\}$ halkası birimli, değişmeli bir halkadır. $n = \gamma + \mu$ olmak üzere $\emptyset \neq C \subseteq F_q^\gamma S_q^\mu$ koduna R_q üzerinde bir kod denir. R_q halkası bilinen toplama işlemine göre kapalıdır fakat çarpma işlemine göre kapalı değildir. Dolayısıyla bir S_q-modül yapısı oluşturmaz. Modül yapısı olması için aşağıdaki gibi yeni bir işlem tanımlayacağız.

$s = s_0 + w_1 s_1 + w_2 s_2 + w_3 s_3 + w_4 s_4 + w_5 s_5 + w_1 w_2 s_6 \in S_q$ olmak üzere

$$\rho: S_q \longrightarrow F_q$$

$$s \longmapsto s_0$$

şeklinde tanımlansın. Herhangi bir $v_1, v_2 \in S_q$ için $\rho(v_1 + v_2) = \rho(v_1) + \rho(v_2)$ ve $\rho(v_1 v_2) = \rho(v_1)\rho(v_2)$ olduğundan ρ dönüşümü bir halka homomorfizmasıdır. Bu homomorfizma yardımıyla herhangi bir $l \in S_q, (r_1, r_2) \in R_q$ için çarpım

$$l \cdot (r_1, r_2) = (\rho(l) r_1, l r_2)$$

şeklinde tanımlanır. Bu çarpım $y = (a_0, a_1, \dots, a_{\gamma-1}, b_0, b_1, \dots, b_{\mu-1}) \in F_q^\gamma S_q^\mu$, $\gamma, \mu \in \mathbb{N}$ ve $l \in S_q$ için

$$l \cdot y = (\rho(l)a_0, \rho(l)a_1, \dots, \rho(l)a_{\gamma-1}, lb_0, lb_1, \dots, lb_{\mu-1})$$

şeklinde $F_q^\gamma S_q^\mu$ halkasına genelleştirilebilir.

Önerme 4.1.1. $F_q^\gamma S_q^\mu$ halkası yukarıda tanımlanan çarpma işlemine göre bir S_q-modüldür.

İspat: $\forall\, y_1, y_2 \in F_q^\gamma S_q^\mu$ ve $\forall\, l_1, l_2 \in S_q$ için modül tanımından $F_q^\gamma S_q^\mu$ halkası bir S_q-modül olur.

4.2. R_q Halkası Üzerinde Tanımlı Devirli Kodlar

Tanım 4.2.1. $\emptyset \neq C \subseteq F_q^\gamma S_q^\mu$ kümesi $F_q^\gamma S_q^\mu$ halkasının bir S_q-alt modülü ise C ye R_q-lineer kod denir.

C kodu $\mu = 0$ olduğunda F_q üzerinde, $\gamma = 0$ olduğunda S_q üzerinde lineer bir kod olur. F_q üzerindeki kodu C_γ, S_q üzerindeki kodu C_μ olarak alırsak C kodu $C = C_\gamma \otimes C_\mu$ şeklinde ayrılabilir.

Tanım 4.2.2. C, $n = \gamma + \mu$ uzunluğunda bir R_q-lineer kod olsun. $y = (a_0, a_1, \dots, a_{\gamma-1}, b_0, b_1, \dots, b_{\mu-1}) \in F_q^\gamma S_q^\mu$ olmak üzere

$$T : F_q^\gamma S_q^\mu \longrightarrow F_q^\gamma S_q^\mu$$

$$T(a_0, a_1, \dots, a_{\gamma-1}, b_0, b_1, \dots, b_{\mu-1}) = (a_{\gamma-1}, a_0, \dots, a_{\gamma-2}, b_{\mu-1}, b_0, \dots, b_{\mu-2})$$

şeklinde bir T devirli öteleme dönüşümü tanımlansın. $T(C) = C$ oluyorsa C koduna R_q-devirli kod denir.

$R_{\gamma,\mu} = \frac{F_q[x]}{\langle x^\gamma - 1\rangle} \times \frac{S_q[x]}{\langle x^\mu - 1\rangle}$, $a(x) = a_0 + a_1 x + \cdots + a_{\gamma-1}x^{\gamma-1} \in F_q[x]/\langle x^\gamma - 1\rangle$ ve $b(x) = b_0 + b_1 x + \cdots + b_{\mu-1}x^{\mu-1} \in S_q[x]/\langle x^\mu - 1\rangle$ olmak üzere $y = (a_0, \dots, a_{\gamma-1}, b_0, \dots, b_{\mu-1}) \in F_q^\gamma S_q^\mu$ elemanına karşılık gelen polinom temsili $f(x) = (a(x), b(x))$ ile tanımlanabilir. Bu durumda $F_q^\gamma S_q^\mu$ halkasının elemanları ile $R_{\gamma,\mu}$ halkasının elemanları arasında birebir bir eşleme vardır.

$e(x) = e_0 + e_1 x + \cdots + e_t x^t \in S_q[x]$ ve $(a(x), b(x)) \in R_{\gamma,\mu}$ için $\rho(e(x)) = \rho(e_0) + \rho(e_1)x + \cdots + \rho(e_t)x^t \in F_q[x]$ ve $\rho(e(x))a(x)$, $F_q[x]/\langle x^\gamma - 1\rangle$ deki klasik polinom çarpımı, $e(x)b(x)$, $S_q[x]/\langle x^\mu - 1\rangle$ deki polinom çarpımı olmak üzere $e(x) \cdot (a(x), b(x)) = (\rho(e(x))a(x), e(x)b(x))$ olsun. Bu durumda $R_{\gamma,\mu}$ bir $S_q[x]$-modül olur.

Teorem 4.2.3. $n = \gamma + \mu$ uzunluğundaki bir C kodunun R_q-devirli kod olması için gerek ve yeter koşul C kodunun $R_{\gamma,\mu}$ nün bir $S_q[x]$-alt modül olmasıdır.

İspat: C kodu R_q-devirli kod olsun. Bu durumda $y \in C$ elemanına karşılık gelen polinom $y(x) = (a(x), b(x))$ olmak üzere $xy(x) \in C$ olur. C lineer

olduğundan herhangi bir $e(x) \in S_q[x]$ için $e(x)y(x) \in C$ elde edilir. Böylece C kodu $R_{\gamma,\mu}$ nün bir $S_q[x]$-alt modülü olur.

Tersine, C kodu $R_{\gamma,\mu}$ nün bir $S_q[x]$-alt modülü olsun. Bu durumda herhangi bir $y(x) \in C$ ve $k \in \mathbb{N}$ için $x^k y(x) \in C$ olur. O halde C kodu R_q-devirli kod olur.

Herhangi bir $y(x) = (a(x), b(x)) \in R_{\gamma,\mu}$ için

$$\tau_\gamma : R_{\gamma,\mu} \longrightarrow F_q[x]/\langle x^\gamma - 1\rangle$$

$$y(x) \longmapsto a(x)$$

ve

$$\tau_\mu : R_{\gamma,\mu} \longrightarrow S_q[x]/\langle x^\mu - 1\rangle$$

$$y(x) \longrightarrow b(x)$$

dönüşümleri tanımlansın.

Önerme 4.2.4. C kodu $n = \gamma + \mu$ uzunluğunda bir R_q-devirli kod olsun. Bu durumda $\tau_\gamma(C) = C_\gamma$ kodu γ uzunluğunda F_q üzerinde devirli bir kod ve $\tau_\mu(C) = C_\mu$ kodu μ uzunluğunda S_q üzerinde devirli bir kod olur.

İspat: Tanım 4.2.2 ve kodun polinom temsili kullanılarak istenilen elde edilir.

Teorem 4.2.5. C kodu $n = \gamma + \mu$ uzunluğunda bir R_q-devirli kod olsun. $f(x)$, C_γ kodunun üreteç polinomu, $h(x)$, C_μ kodunun üreteç polinomu ve $f(x)|x^\gamma - 1, h(x)|x^\mu - 1$ olmak üzere C kodunun üreteç polinomu

$$C = \langle (f(x),0), (g(x), h(x))\rangle$$

şeklindedir.

İspat: C, R_q-devirli kod olduğundan C_γ kodu F_q üzerinde devirli bir kod olur. O halde, C_γ, $F_q[x]/\langle x^\gamma - 1\rangle$ in bir idealidir. A kümesi

$$A = \{(a(x), b(x)) \in C : b(x) = 0\}$$

şeklinde tanımlansın. Bu durumda $\tau_\gamma(A) = A$ ve $\tau_\gamma(A)$, $F_q[x]/\langle x^\gamma - 1\rangle$ in bir esas ideali olur. $\tau_\gamma(A) = \langle f(x)\rangle$ olsun. Bu durumda $f(x) \mid x^\gamma - 1$ olmak üzere A, $(f(x),0)$ ile üretilir. Ayrıca $h(x) \mid x^\mu - 1$ olmak üzere $C_\mu = \langle h(x)\rangle$ dir.

Herhangi bir $s(x) \in C$ alalım. Böylece $a(x) \in F_q[x]/\langle x^\gamma - 1\rangle$ ve $b(x) \in S_q[x]/\langle x^\mu - 1\rangle$ için

$$\begin{aligned} s(x) &= \big(s_1(x), s_2(x)\big) \\ &= (s_1(x), 0) + \big(0, s_2(x)\big) \\ &= (a(x)f(x), 0) + \big(0, b(x)h(x)\big) \end{aligned}$$

şeklinde yazabiliriz. $g(x) \in F_q[x]/\langle x^\gamma - 1\rangle$ olmak üzere $(g(x), b(x)h(x)) \in C$ olsun. Bu durumda

$$\begin{aligned} s(x) &= (a(x)f(x), 0) + \big(\rho\big(b(x)\big)g(x), 0\big) + \Big(\rho\big(b(x)\big)g(x), b(x)h(x)\Big) \\ &= \big(a(x)f(x) + \rho\big(b(x)\big)g(x), 0\big) + b(x).\big(g(x), h(x)\big) \\ &= l(x)(f(x), 0) + b(x).\big(g(x), h(x)\big) \end{aligned}$$

dir. Burada son adım $\big(a(x)f(x) + \rho\big(b(x)\big)g(x), 0\big)$ ın A kümesinin elemanı olmasından elde edilir. Böylece $C \subseteq \langle (f(x),0), (g(x), h(x))\rangle$ dir. Tersine, $\langle (f(x),0), (g(x), h(x))\rangle \subseteq$ C olduğu açıktır. O halde C kodunun üreteç polinomu $C = \langle (f(x),0), (g(x), h(x))\rangle$ dir.

Daha önce tanımladığımız S_q dan F_q^7 ye δ Gray dönüşümünü kullanarak $F_q^\gamma S_q^\mu$ üzerinde bir Gray dönüşümünü tanımlayalım.

Tanım 4.2.6. Her $(a, s) = (a, \sum_{i=1}^{7} \alpha_i s_i) \in R_q$ için

$$\psi: R_q \longrightarrow F_q^8$$

$$\psi(a, s) = \big(a, \delta(s)\big)$$

şeklinde tanımlı ψ lineer dönüşümüne R_q üzerinde tanımlı Gray dönüşümü denir.

Bu Gray dönüşümü $F_q^\gamma S_q^\mu$ den $F_q^{\gamma+7\mu}$ ye genelleştirilebilir.

Herhangi bir $\boldsymbol{d} = (\boldsymbol{a}, \boldsymbol{b}) \in F_q^\gamma S_q^\mu$ için, $\boldsymbol{a}$ elemanının Hamming ağırlığı $w_H(\boldsymbol{a})$, $\boldsymbol{b}$ elemanının Lee ağırlığı $w_L(\boldsymbol{b})$ olmak üzere $\boldsymbol{d}$ elemanının Gray ağırlığı $w_G(\boldsymbol{a}, \boldsymbol{b}) = w_H(\boldsymbol{a}) + w_L(\boldsymbol{b})$ şeklinde tanımlanır.

Teorem 4.2.7. ψ Gray dönüşümü $F_q^{\gamma} S_q^{\mu}$ den $F_q^{\gamma+7\mu}$ ye uzaklık koruyan F_q-lineer bir dönüşümdür.

İspat: $\varepsilon \in F_q$ ve $0 \leq i \leq \mu - 1, j = 1,2$ için

$$b^1 = \left(b_0^1, b_1^1, \dots, b_{\gamma-1}^1\right), b^2 = \left(b_0^2, b_1^2, \dots, b_{\gamma-1}^2\right) \in F_q^{\gamma},$$

$$v^1 = \left(v_0^1, v_1^1, \dots, v_{\mu-1}^1\right), v^2 = \left(v_0^2, v_1^2, \dots, v_{\mu-1}^2\right) \in S_q^{\mu},$$

$v_i^j = s_0^i + \sum_{k=1}^{5} w_k s_k^i + w_1 w_2 s_6^i \in S_q$ olmak üzere $a^1 = (b^1, v^1)$, $a^2 = (b^2, v^2) \in F_q^{\gamma} S_q^{\mu}$ olsun. Bu durumda

$$\begin{aligned} \psi(a^1 + a^2) &= \left(b^1 + b^2, \delta(v^1 + v^2)\right) \\ &= \left(b^1 + b^2, \delta(v^1) + \delta(v^2)\right) \\ &= \left(b^1, \delta(v^1)\right) + \left(b^2, \delta(v^2)\right) \\ &= \psi(a^1) + \psi(a^2) \end{aligned}$$

ve

$$\begin{aligned} \psi(\varepsilon a^1) &= \left(\varepsilon b^1, \delta(\varepsilon v^1)\right) \\ &= \left(\varepsilon b^1, \varepsilon\delta(v^1)\right) = \varepsilon\psi(a^1) \end{aligned}$$

elde edilir. O halde ψ bir F_q-lineer dönüşüm olur.

Ayrıca ψ bir F_q-lineer dönüşüm olduğundan

$$d_G(a^1, a^2) = w_G(a^1 - a^2) = w_H\left(\psi(a^1 - a^2)\right) = d_H\left(\psi(a^1), \psi(a^2)\right)$$

dir. Böylece ψ, uzaklık koruyan bir dönüşüm olur.

Teorem 4.2.8. C kodu $n = \gamma + \mu$ uzunluğunda, d_G minimum uzaklıklı, M elemanlı bir R_q-lineer bir kod olmak üzere $\psi(C), F_q$ üzerinde tanımlı bir $(\gamma + 7\mu, M, d_H)$-koddur. Ayrıca $d_G = d_H$.

İspat: Teorem 3.2.3 ve ψ dönüşümünün tanımından $\psi(C), \gamma + 7\mu$ uzunluğunda ve $d_H = d_G$ dir. ψ, 1-1 ve örten olduğundan $|C| = |\psi(C)|$ dir. Dolayısıyla $\psi(C)$ bir $(\gamma + 7\mu, M, d_H)$-koddur.

$\sigma^{\otimes 7}$, Tanım 3.2.14 deki dönüşüm olmak üzere

$$\sigma^{\otimes 8} = \sigma_g^{\otimes 7}\colon\ F_q^n \times F_q^{7n} \ \rightarrow\ F_q^n \times F_q^{7n}$$

dönüşümü $\sigma^{\otimes 7}$ dönüşümünün genelleştirilmesi olsun. Önerme 3.2.15 ve Teorem 3.2.16 ya benzer şekilde aşağıdaki önerme ve teoremi verebiliriz.

Önerme 4.2.9. ψ, R_q üzerinde tanımlı Gray dönüşümü olmak üzere

$$\psi\sigma = \sigma^{\otimes 8}\psi$$

dir.

Teorem 4.2.10. C, $n = \gamma + \mu$ uzunluğunda bir R_q-lineer kod olsun. $n = \gamma + \mu$ uzunluğunda bir R_q-devirli kodun ψ Gray dönüşümü altındaki görüntüsü F_q üzerinde tanımlı indeksi 8 olan bir genelleştirilmiş quasi-devirli koddur.

C, $n = \gamma + \mu$ uzunluğunda bir R_q-lineer bir kod olmak üzere $1 \leq i \leq 7$ için

$$C_0 = \{a\colon (a, s) \in C, \exists\ s_k \in F_q^{\mu}\},$$

$$C_{\mathrm{i}} = \{s_i\colon (a, s) \in C, \exists\ a \in F_q^{\gamma}, s_1, \dots, s_{i-1}, s_{i+1}, \dots, s_7 \in F_q^{\mu}\}$$

şeklinde tanımlansın.

Lemma 4.2.11. C, $n = \gamma + \mu$ uzunluğunda bir R_q-lineer bir kod olmak üzere $\psi(C) = C_0 \otimes \cdots \otimes C_7$ ve $|\psi(C)| = \prod_{i=0}^{7} |C_i|$ dir.

Tanım 4.2.12. C, $n = \gamma + \mu$ uzunluğunda bir R_q-devirli kod ve C_γ (aynı şekilde C_μ) C kodunun ilk γ (son μ) bileşenleri üzerindeki kanonik iz düşümü olsun. Eğer C kodu C_γ ve C_μ nın direkt çarpımı olarak ifade edilebiliyorsa, yani $C = C_\gamma \otimes C_\mu$ ise, bu durumda C koduna ayrılabilir kod denir.

Teorem 4.2.13. $C = C_\gamma \otimes C_\mu$, $n = \gamma + \mu$ uzunluğunda bir R_q-lineer kod olsun. C kodunun ayrılabilir bir R_q-devirli kod olması için gerek ve yeter koşul C_γ ve C_μ kodlarının sırasıyla F_q ve S_q üzerinde γ ve μ uzunluğunda devirli kodlar olmasıdır.

İspat: C, R_q-devirli kod, $(a_0, a_1, \dots, a_{\gamma-1}) \in C_\gamma, (b_0, b_1, \dots, b_{\mu-1}) \in C_\mu$ olmak üzere $y = (a_0, a_1, \dots, a_{\gamma-1}, b_0, b_1, \dots, b_{\mu-1}) \in C$ olsun. C, R_q-devirli kod olduğundan

$(a_{\gamma-1}, a_0, \dots, a_{\gamma-2}, b_{\mu-1}, b_0, \dots, b_{\mu-2}) \in C$ olur. Böylece $(a_{\gamma-1}, a_0, \dots, a_{\gamma-2}) \in C_\gamma$ ve $(b_{\mu-1}, b_0, \dots, b_{\mu-2}) \in C_\mu$ elde edilir. O halde C_γ ve C_μ kodları sırasıyla F_q ve S_q üzerinde γ ve μ uzunluğunda devirli kodlardır.

Tersine C_γ ve C_μ kodları sırasıyla F_q ve S_q üzerinde γ ve μ uzunluğunda devirli kodlar olsun. Bu durumda $(a_0, a_1, \dots, a_{\gamma-1}) \in C_\gamma, (b_0, b_1, \dots, b_{\mu-1}) \in C_\mu$ olmak üzere $(a_{\gamma-1}, a_0, \dots, a_{\gamma-2}) \in C_\gamma$ ve $(b_{\mu-1}, b_0, \dots, b_{\mu-2}) \in C_\mu$ elde edilir. Böylece $(a_{\gamma-1}, a_0, \dots, a_{\gamma-2}, b_{\mu-1}, b_0, \dots, b_{\mu-2}) \in C_\gamma \otimes C_\mu = C$ dir. O halde C, $n = \gamma + \mu$ uzunluğunda bir R_q-devirli koddur.

Sonuç 4.2.14. $C = C_\gamma \otimes C_\mu$, $n = \gamma + \mu$ uzunluğunda bir R_q-lineer kod olsun. C kodunun bir R_q-devirli kod olması için gerek ve yeter koşul $1 \leq i \leq 7$ için C_0 ve C_i kodlarının F_q üzerinde sırasıyla γ ve μ uzunluğunda devirli kodlar olmasıdır.

Ayrıca, C ayrılabilir olduğundan $x^\gamma - 1$ in bir böleni $f(x)$, $x^\mu - 1$ in bir böleni $h(x)$ ve $C_\gamma = \langle f(x) \rangle$, $C_\mu = \langle h(x) \rangle$ olmak üzere $C = \langle (f(x),0), (0, h(x)) \rangle$ dir.

Sonuç 4.2.15. $C = \langle (f(x),0), (g(x), h(x)) \rangle$ bir R_q-devirli kod olsun. Bu durumda aşağıdaki ifadeler denktir.

i) C ayrılabilir bir koddur,

ii) $f(x) \mid g(x)$,

iii) $C_\gamma = \langle f(x) \rangle, C_\mu = \langle h(x) \rangle$,

iv) $C = \langle (f(x),0), (0, h(x)) \rangle$.

Sonuç 4.2.16. $C = C_\gamma \otimes C_\mu$, $n = \gamma + \mu$ uzunluğunda ayrılabilir bir R_q-devirli kod olsun. $C_\gamma = \langle f(x) \rangle$, $C_\mu = \langle h(x) \rangle$ olmak üzere $C = \langle f(x) \rangle \otimes \langle h(x) \rangle$ dir.

4.3. R_4-Devirli DNA Kodlar

Bu bölümde $q = 4$ için DNA kodunu inceleyeceğiz.

Tanım 4.3.1. C bir R_4-lineer kod olsun.

i) C, R_4-devirli koddur,

ii) Herhangi bir $\vartheta = (\vartheta_1, \vartheta_2) \in C$ için $\vartheta^{RC} = (\vartheta_1^{RC}, \vartheta_2^{RC}) \in C$ dir.

koşulları sağlanıyorsa C koduna R_4-devirli DNA kod denir.

Teorem 4.3.2. $C = C_\gamma \otimes C_\mu = \langle (f(x),0), (0, h(x)) \rangle$ bir R_4-devirli kod olsun. C kodunun reversible olması için gerek ve yeter koşul C_γ ve C_μ kodlarının sırasıyla F_4 ve S_4 üzerinde reversible kodlar olmasıdır.

İspat: C bir R_4-devirli kod ve $\vartheta = (\vartheta_1, \vartheta_2) \in C$ olsun. C_γ ve C_μ kodları sırasıyla F_4 ve S_4 üzerinde reversible kodlar ise $\vartheta_1^R \in C_\gamma$ ve $\vartheta_2^R \in C_\mu$ olur. Bu durumda $\vartheta^R = (\vartheta_1^R, \vartheta_2^R) \in C = C_\gamma \otimes C_\mu$ dir ve C kodu reversible olur.

Tersine, C kodu reversible olsun. O halde $\vartheta = (\vartheta_1, \vartheta_2) \in C$ için $\vartheta^R = (\vartheta_1^R, \vartheta_2^R) \in C = C_\gamma \otimes C_\mu$ dir. Böylece $\vartheta_1^R \in C_\gamma$ ve $\vartheta_2^R \in C_\mu$ olur. Bu durumda C_γ ve C_μ kodları sırasıyla F_4 ve S_4 üzerinde reversible kodlar olur.

Teorem 4.3.3. $C = C_\gamma \otimes C_\mu = \langle (f(x),0), (0, h(x)) \rangle$ bir R_4-devirli kod olsun. C kodunun reversible complement olması için gerek ve yeter koşul C_γ ve C_μ kodlarının sırasıyla F_4 ve S_4 üzerinde reversible complement kodlar olmasıdır.

İspat: C bir R_4-devirli kod ve $\vartheta = (\vartheta_1, \vartheta_2) \in C$ olsun. C_γ ve C_μ kodları sırasıyla F_4 ve S_4 üzerinde reversible complement kodlar ise $\vartheta_1^{RC} \in C_\gamma$ ve $\vartheta_2^{RC} \in C_\mu$ olur. Bu durumda $\vartheta^{RC} = (\vartheta_1^{RC}, \vartheta_2^{RC}) \in C = C_\gamma \otimes C_\mu$ dir ve C kodu reversible complement olur.

Tersine, C kodu reversible complement olsun. O halde $\vartheta = (\vartheta_1, \vartheta_2) \in C$ için $\vartheta^{RC} = (\vartheta_1^{RC}, \vartheta_2^{RC}) \in C = C_\gamma \otimes C_\mu$ dir. Böylece $\vartheta_1^{RC} \in C_\gamma$ ve $\vartheta_2^{RC} \in C_\mu$ olur. Bu durumda C_γ ve C_μ kodları sırasıyla F_4 ve S_4 üzerinde reversible complement kodlar olur.

Örnek 4.3.4. $C = C_\gamma \otimes C_\mu$ bir ayrılabilir R_4-devirli kod ve $n = 3 + 5$ olsun.

$$x^3 - 1 = (x+1)(x+\beta^2)(x+\beta) \in F_4[x],$$

$$x^5 - 1 = (x+1)(x^2+\beta x+1)(x^2+\beta^2 x+1) \in F_4[x],$$

$f(x) = (x+\beta)(x+\beta^2), h(x) = x^2+\beta^2 x+1$ olsun. Bu durumda $C_\gamma = \langle f(x) \rangle$, F_4 üzerinde 3 uzunluğunda devirli bir kod ve $C_\mu = \langle h(x) \rangle$, S_4 üzerinde 5 uzunluğunda devirli bir kod olur. $f(x)$, self-reciprocal ve $x-1$ ile bölünmez olduğundan C_γ, F_4

üzerinde reversible complement kod olur. Benzer şekilde C_μ, S_4 üzerinde reversible complement koddur. Böylece C reversible complement kod olup devirli DNA kod olur. C kodunun ψ altındaki görüntüsü 38 uzunluğunda, 4^{22} elemanlı ve Hamming uzaklığı 3 olan bir DNA koddur.

Örnek 4.3.5. $C = C_\gamma \otimes C_\mu$ bir ayrılabilir R_4-devirli kod ve $n = 13 + 5$ olsun.

$$x^5 - 1 = (x+1)(x^2 + \beta x + 1)(x^2 + \beta^2 x + 1) \in F_4[x],$$

$$x^{13} - 1 = (x-1)(x^6 + \beta x^5 + \beta^2 x^3 + \beta x - 1)(x^6 + \beta^2 x^5 + \beta x^3 + \beta^2 x - 1) \in F_4[x]$$

$f(x) = (x^6 + \beta x^5 + \beta^2 x^3 + \beta x - 1)(x^6 + \beta^2 x^5 + \beta x^3 + \beta^2 x - 1), h(x) = x^2 + \beta x + 1$ olsun. Bu durumda $C_\gamma = \langle f(x) \rangle$, F_4 üzerinde 13 uzunluğunda devirli bir kod ve $C_\mu = \langle h(x) \rangle$, S_4 üzerinde 5 uzunluğunda devirli bir kod olur. $f(x)$, self-reciprocal ve $x - 1$ ile bölünmez olduğundan C_γ, F_4 üzerinde reversible complement kod olur. Benzer şekilde C_μ, S_4 üzerinde reversible complement koddur. Böylece C reversible complement kod olup devirli DNA kod olur. C kodunun ψ altındaki görüntüsü 48 uzunluğunda, 4^{22} elemanlı ve Hamming uzaklığı 5 olan bir DNA koddur.

4.4. R_q-Kuantum Kodlar

4.4.1. R_q-Skew Devirli Kodlar

Tanım 4.4.1.1. $q = p^m$ ve θ_t, $\theta_t(a) = a^{p^t}$ olacak şekilde F_q üzerinde tanımlı bir Frobenius otomorfizması olsun. Her $s = s_0 + \sum_{k=1}^{5} w_k s_k + w_1 w_2 s_6 \in S_q$ için

$$\Gamma_t : S_q \longrightarrow S_q$$

$$s \longmapsto \Gamma_t(s) = {s_0}^{p^t} + \sum_{k=1}^{5} w_k s_k^{p^t} + w_1 w_2 {s_6}^{p^t}$$

şeklinde tanımlı Γ_t dönüşümü S_q üzerinde tanımlı aşikar olmayan bir otomorfizma olmak üzere

$$S_q[x, \Gamma_t] = \{b_0 + b_1 x + \cdots + b_n x^n : b_i \in S_q, n \in \mathbb{N}\}$$

kümesine değişmeli olmayan skew polinom halkası denir.

$S_q[x,\Gamma_t]$ halkasındaki toplama işlemi polinomlardaki toplama işlemidir. Çarpma ise $\left(ax^i\right)\left(bx^j\right) = a{\Gamma_t}^i(b)x^{i+j}$ şeklinde tanımlıdır. $s \in S_q$ için ${\Gamma_t}^2(s) = s$ olduğundan Γ_t mertebesi 2 olan bir halka otomorfizmasıdır. Bu otomorfizmanın mertebesi $|\langle\Gamma_t\rangle| = \frac{m}{\gcd(m,t)}$ şeklindedir. Ayrıca $t \mid m$ olduğunda $|\langle\Gamma_t\rangle| = \frac{m}{t}$ dir.

Tanım 4.4.1.2. $\emptyset \neq C \subseteq S_q^n$ olmak üzere

i) C, S_q^n nin bir alt modülü,

ii) Her $\zeta = (\zeta_0, \zeta_1, \dots, \zeta_{n-1}) \in C$ için

$$\sigma_{\Gamma_t}(\zeta) = \left(\Gamma_t(\zeta_{n-1}), \Gamma_t(\zeta_0), \dots, \Gamma_t(\zeta_{n-2})\right) \in C$$

koşullarını sağlayan C kümesine S_q üzerinde n uzunluğunda skew devirli kod denir.

Teorem 4.4.1.3. Her $r(x) + \langle x^n - 1\rangle \in S_q[x,\Gamma_t]/\langle x^n - 1\rangle$, $f(x) \in S_q[x,\Gamma_t]$ için

$$. : S_q[x,\Gamma_t] \times S_q[x,\Gamma_t]/\langle x^n - 1\rangle \longrightarrow S_q[x,\Gamma_t]/\langle x^n - 1\rangle$$

$$f(x)\left(r(x) + \left\langle x^n - 1\right\rangle\right) = f(x)r(x) + \langle x^n - 1\rangle$$

şeklinde tanımlı soldan çarpma işlemi ve polinomlardaki toplama işlemine göre $S_q[x,\Gamma_t]/\langle x^n - 1\rangle$ bir sol $S_q[x,\Gamma_t]$-modüldür.

Teorem 4.4.1.4. Bir C kodunun S_q üzerinde skew devirli kod olması için gerek ve yeter koşul $S_q[x,\Gamma_t]/\langle x^n - 1\rangle$ in bir sol $S_q[x,\Gamma_t]$-alt modül olmasıdır.

İspat: C, S_q üzerinde skew devirli kod ve $\zeta = (\zeta_0, \zeta_1, \dots, \zeta_{n-1}) \in C$ olsun. ζ kod sözcüğüne karşılık gelen polinom $\zeta(x) = \zeta_0 + \zeta_1 x + \cdots + \zeta_{n-1}x^{n-1}$ olmak üzere

$$\begin{aligned} x \cdot \zeta(x) &= x(\zeta_0 + \zeta_1 x + \cdots + \zeta_{n-1}x^{n-1}) \\ &= \Gamma_t(\zeta_0)x + \Gamma_t(\zeta_1)x^2 + \cdots + \Gamma_t(\zeta_{n-1})x^n \end{aligned}$$

dir. $x^n = 1$ olduğundan

$$\begin{aligned} x \cdot \zeta(x) &= \Gamma_t(\zeta_{n-1}) + \Gamma_t(\zeta_0)x + \cdots + \Gamma_t(\zeta_{n-2})x^{n-1} \\ &= \sigma_{\Gamma_t}(\zeta) \in C \end{aligned}$$

elde edilir. Benzer şekilde $i \geq 2$ için $x^i\zeta(x) \in C$ olur. C bir lineer kod olduğundan $r(x) \in S_q[x, \Gamma_t]$ için $r(x)\zeta(x) \in C$ dir. Bu durumda C, $S_q[x, \Gamma_t]/\langle x^n - 1\rangle$ nın bir sol $S_q[x, \Gamma_t]$-alt modülü olur.

Tersine, C, $S_q[x, \Gamma_t]$ nın bir sol $S_q[x, \Gamma_t]$-alt modülü olsun. Böylece $\zeta = (\zeta_0, \zeta_1, \cdots, \zeta_{n-1}) \in C$ için $\sigma_{\Gamma_t}(\zeta) = x\zeta(x) \in C$ elde edilir. Bu durumda C, S_q üzerinde n uzunluğunda skew devirli kod olur.

Teorem 4.4.1.5. C bir skew devirli kod ve $r(x)$ minimal dereceli polinom olsun. $r(x)$ monik polinom ise $C = \langle r(x)\rangle$ ve $r(x), x^n - 1$ polinomunun bir sağ bölenidir.

Teorem 4.4.1.6. $C = \bigoplus_{1\leq k\leq 7} \alpha_k C_k$, S_q üzerinde tanımlı lineer bir kod olmak üzere C kodunun skew devirli bir kod olması için gerek ve yeter koşul $1 \leq k \leq 7$ için C_k kodlarının F_q üzerinde skew devirli kod olmasıdır.

İspat: C, S_q üzerinde tanımlı bir skew devirli kod ve $1 \leq k \leq 7$ için $z^k = \left(z_0^k, z_1^k, \dots, z_{n-1}^k\right) \in C_k$ olsun. $0 \leq i \leq n-1$ için $c_i = \sum_{k=1}^{7} \alpha_k z_i^k$ olmak üzere $(c_0, c_1, \dots, c_{n-1}) \in C$ dir. C skew devirli kod olduğundan

$$(\Gamma_t(c_{n-1}), \Gamma_t(c_0), \dots, \Gamma_t(c_{n-2})) = \sum_{k=1}^{7} \alpha_k \left(\theta_t(z_{n-1}^k), \theta_t(z_0^k), \dots, \theta_t(z_{n-2}^k)\right) \in C$$

olur. Böylece $1 \leq k \leq 7$ için $\left(\theta_t(z_{n-1}^k), \theta_t(z_0^k), \dots, \theta_t(z_{n-2}^k)\right) \in C_k$ elde edilir. O halde $1 \leq k \leq 7$ için C_k kodları F_q üzerinde tanımlı skew devirli kodlardır.

Tersine $1 \leq k \leq 7$ için C_k kodları F_q üzerinde tanımlı skew devirli kodlar ve $0 \leq i \leq n-1$ için $c_i = \sum_{k=1}^{7} \alpha_k z_i^k$ olmak üzere $(c_0, c_1, \dots, c_{n-1}) \in C$ olsun. O zaman $1 \leq k \leq 7$ için $z^k = \left(z_0^k, z_1^k, \dots, z_{n-1}^k\right) \in C_k$ olur. $1 \leq k \leq 7$ için C_k kodları skew devirli kodlar olduğundan

$$(\Gamma_t(c_{n-1}), \Gamma_t(c_0), \dots, \Gamma_t(c_{n-2})) = \sum_{k=1}^{7} \alpha_k \left(\theta_t(z_{n-1}^k), \theta_t(z_0^k), \dots, \theta_t(z_{n-2}^k)\right) \in C$$

olur. O halde C, S_q üzerinde tanımlı skew devirli bir koddur.

Sonuç 4.4.1.7. C, S_q üzerinde tanımlı bir skew devirli kod ise C kodunun duali $C^{\perp}$ de skew devirli kod olur.

Teorem 4.4.1.8. $C = \bigoplus_{1\le k\le 7} \alpha_k C_k, S_q$ üzerinde tanımlı skew devirli kod olsun. $1 \le k \le 7$ için $\mathrm{r}_k(x), C_k$ kodlarının üreteç polinomları olmak üzere

$$C = \langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x) \rangle$$

ve

$$|C| = q^{7n-\left(\sum_{k=1}^{7} \mathrm{der}(r_k(x))\right)}$$

dir.

İspat: $C = \bigoplus_{1\le k\le 7} \alpha_k C_k$ olsun. $1 \le k \le 7$ için $C_k = \langle r_k(x) \rangle$ olduğundan

$$C = \left\{ a(x) : \ a(x) = \sum_{k=1}^{7} \alpha_k g_k(x) r_k(x) \, , g_k(x) \in F_q[x, \theta_t], 1 \le k \le 7 \right\}$$

şeklindedir. O halde $C \subseteq \langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x) \rangle$ dir.

$1 \le k \le 7$ için $h_k(x) \in S_q[x, \Gamma_t]/\langle x^n - 1 \rangle$ olmak üzere herhangi bir eleman

$$\sum_{k=1}^{7} \alpha_k h_k(x) r_k(x) \in \langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x) \rangle$$

olsun. Bu durumda $1 \le k \le 7$ için $\alpha_k h_k(x) = \alpha_k f_k(x)$ olacak şekilde $f_k(x) \in F_q[x, \theta_t]$ elemanları vardır. Böylece

$$\langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x) \rangle \subseteq C$$

olur. O halde

$$C = \langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x) \rangle$$

elde edilir. Ayrıca $C = \prod_{k=1}^{7} |C_k|$ olduğundan

$$|C| = q^{7n-\left(\sum_{k=1}^{7} \mathrm{der}(r_k(x))\right)}$$

dir.

Teorem 4.4.1.9. C, S_q üzerinde tanımlı bir skew devirli kod, $1 \leq k \leq 7$ için $r_k(x), C_k$ kodlarının üreteç polinomları olsun. $C = \langle r(x) \rangle$ olacak sekilde bir tek $r(x) = \sum_{k=1}^{7} \alpha_k r_k(x)$ vardır ve $r(x)$, $x^n - 1$ polinomunun bir sağ bölenidir.

İspat: Teorem 4.4.1.8 den $C = \langle \alpha_1 r_1(x), \alpha_2 r_2(x), \dots, \alpha_7 r_7(x) \rangle$ dir. $r(x) = \sum_{k=1}^{7} \alpha_k r_k(x)$ olarak alınırsa $\langle r(x) \rangle \subseteq C$ olur. Ayrıca $1 \leq k \leq 7$ için $\alpha_k r_k(x) = \alpha_k r(x)$ dir. Bu durumda $C \subseteq \langle r(x) \rangle$ elde edilir. O halde $C = \langle r(x) \rangle$ dir.

$1 \leq k \leq 7$ için $r_k(x)$ polinomları $x^n - 1$ polinomunun sağ bölenleri olduğundan $x^n - 1 = s_k(x) r_k(x)$ olacak şekilde $s_k(x) \in F_q[x, \theta_t]$ vardır. Bu durumda

$$\left(\sum_{k=1}^{7} \alpha_k s_k(x) \right) r(x) = \sum_{k=1}^{7} \alpha_k s_k(x) \sum_{k=1}^{7} \alpha_k r_k(x)$$

$$= \sum_{k=1}^{7} \alpha_k s_k(x)\, r_k(x)$$

$$= \sum_{k=1}^{7} \alpha_k (x^n - 1)$$

$$= x^n - 1$$

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

Sonuç 4.4.1.10. $C = \bigoplus_{1 \leq k \leq 7} \alpha_k C_k, S_q$ üzerinde n uzunlukluğunda bir skew devirli kod olmak üzere

$$C^{\perp} = \bigoplus_{1 \leq k \leq 7} \alpha_k C_k^{\perp}$$

dir. Ayrıca C kodunun S_q üzerinde self-dual olması için gerek ve yeter koşul $1 \leq k \leq 7$ için C_k kodlarının F_q üzerinde self-dual olmasıdır.

Sonuç 4.4.1.11. $C = \bigoplus_{1 \leq k \leq 7} \alpha_k C_k, S_q$ üzerinde tanımlı n uzunluğunda bir skew devirli kod ve $C^{\perp}$, C kodunun duali olsun. $1 \leq k \leq 7$ için $h_k(x) = (x^n - 1)/r_k(x)$ polinomlarının ters sıralı polinomları $h_k^*(x) = x^{der(h_k(x))} h_k(x^{-1})$ olmak üzere

$$C^{\perp} = \langle \sum_{i=1}^{7} \alpha_i h_i^*(x) \rangle$$

ve

$$|C^{\perp}| = q^{\sum_{i=1}^{7} der(r_i(x))}$$

dir.

Teorem 4.4.1.12. n tek sayı ve C, n uzunluğunda S_q üzerinde tanımlı bir skew devirli kod ise C kodu n uzunluğunda S_q üzerinde bir devirli koda denk olur.

Sonuç 4.4.1.13. n tek sayı ve $p_i(x) \in F_q[x, \theta_t]$ olmak üzere $x^n - 1 = \prod_{i=1}^{t} p_i^{k_i}(x)$ olsun. Bu durumda n uzunluğunda S_q üzerinde tanımlı skew devirli kodların sayısı $\prod_{i=1}^{t}(k_i + 1)^7$ dir.

Tanım 4.4.1.14. Herhangi bir

$$d = (x_0, x_1, \dots, x_{\gamma-1}, y_0, y_1, \dots, y_{\mu-1}),$$

$$d' = (x_0', x_1', \dots, x_{\gamma-1}', y_0', y_1', \dots, y_{\mu-1}') \in F_q^{\gamma} S_q^{\mu}$$

için iç çarpım

$$d \cdot d' = \sum_{i=0}^{\gamma-1} x_i x_i' + \sum_{j=0}^{\mu-1} y_j y_j'$$

olmak üzere $n = \gamma + \mu$ uzunluğunda C, R_q-lineer kodununun duali

$$C^{\perp} = \{d' \in F_q^{\gamma} S_q^{\mu} : \forall\, d \in C, d \cdot d' = 0\}$$

Tanım 4.4.1.15. C, $n = \gamma + \mu$ uzunluğunda bir R_q-lineer kod olsun.

$y = (a_0, a_1, \dots, a_{\gamma-1}, b_0, b_1, \dots, b_{\mu-1}) \in F_q^{\gamma} S_q^{\mu}$ olmak üzere

$$\tau : F_q^{\gamma} S_q^{\mu} \longrightarrow F_q^{\gamma} S_q^{\mu}$$

$$\tau(\mathrm{y}) = (\theta_t(a_{\gamma-1}), \theta_t(a_0), \dots, \theta_t(a_{\gamma-2}), \Gamma_t(b_{\mu-1}), \Gamma_t(b_0), \dots, \Gamma_t(b_{\mu-2}))$$

şeklinde bir τ skew devirli öteleme dönüşümü tanımlansın. $\tau(C) = C$ oluyorsa C koduna R_q-skew devirli kod denir.

$$R_{\gamma,\mu} = \frac{F_q[x,\theta_t]}{\langle x^\gamma - 1\rangle} \times \frac{S_q[x,\Gamma_t]}{\langle x^\mu - 1\rangle},$$

$$a(x) = a_0 + a_1 x + \cdots + a_{\gamma-1}x^{\gamma-1} \in \frac{F_q[x,\theta_t]}{\langle x^\gamma - 1\rangle},$$

$$b(x) = b_0 + b_1 x + \cdots + b_{\mu-1}x^{\mu-1} \in \frac{S_q[x,\Gamma_t]}{\langle x^\mu - 1\rangle},$$

olmak üzere $y = (a_0, \dots, a_{\gamma-1}, b_0, \dots, b_{\mu-1}) \in F_q^\gamma S_q^\mu$ elemanına karşılık gelen polinom temsili $f(x) = (a(x), b(x))$ ile tanımlanabilir. Bu durumda $F_q^\gamma S_q^\mu$ halkasının elemanları ile $R_{\gamma,\mu}$ halkasının elemanları arasında birebir bir eşleme vardır.

$e(x) = e_0 + e_1 x + \cdots + e_t x^t \in S_q[x,\Gamma_t]$ ve $(a(x), b(x)) \in R_{\gamma,\mu}$ için $\rho(e(x)) = \rho(e_0) + \rho(e_1)x + \cdots + \rho(e_t)x^t \in F_q[x,\theta_t]$ ve $\rho(e(x))a(x)$, $F_q[x,\theta_t]/\langle x^\gamma - 1\rangle$ deki polinom çarpımı, $e(x)b(x)$, $S_q[x,\Gamma_t]/\langle x^\mu - 1\rangle$ deki polinom çarpımı olmak üzere $e(x)\cdot(a(x), b(x)) = (\rho(e(x))a(x), e(x)b(x))$ olsun. Bu durumda $R_{\gamma,\mu}$ bir sol $S_q[x,\Gamma_t]$-modül olur.

Teorem 4.4.1.16. $n = \gamma + \mu$ uzunluğundaki bir C kodunun R_q-skew devirli kod olması için gerek ve yeter koşul C kodunun $R_{\gamma,\mu}$ nün bir sol $S_q[x,\Gamma_t]$-alt modül olmasıdır.

İspat: C kodu R_q-skew devirli kod olsun. Bu durumda $y \in C$ elemanına karşılık gelen polinom $y(x) = (a(x), b(x))$ olmak üzere $xy(x) \in C$ olur. C lineer olduğundan herhangi bir $e(x) \in S_q[x,\Gamma_t]$ için $e(x)y(x) \in C$ elde edilir. Böylece C kodu $R_{\gamma,\mu}$ nün bir sol $S_q[x,\Gamma_t]$-alt modülü olur.

Tersine, C kodu $R_{\gamma,\mu}$ nün bir sol $S_q[x,\Gamma_t]$-alt modülü olsun. Bu durumda herhangi bir $y(x) \in C$ ve $k \in \mathbb{N}$ için $x^k y(x) \in C$ olur. O halde C kodu bir R_q-skew devirli kod olur.

Herhangi bir $y(x) = (a(x), b(x)) \in R_{\gamma,\mu}$ için

$$\tau'_\gamma : R_{\gamma,\mu} \longrightarrow F_q[x,\theta_t]/\langle x^\gamma - 1\rangle$$

$$y(x) \longmapsto a(x)$$

ve

$$\tau'_{\mu}: R_{\gamma,\mu} \longrightarrow S_q[x, \Gamma_t]/\langle x^{\mu} - 1\rangle$$

$$y(x) \longrightarrow b(x)$$

dönüşümleri tanımlansın.

Önerme 4.4.1.17. C kodu $n = \gamma + \mu$ uzunluğunda bir R_q-skew devirli kod olsun. Bu durumda $\tau'_{\gamma}(C) = C_{\gamma}$ kodu γ uzunluğunda F_q üzerinde skew devirli bir kod ve $\tau'_{\mu}(C) = C_{\mu}$ kodu μ uzunluğunda S_q üzerinde skew devirli bir kod olur.

İspat: Tanım 4.4.1.15 ve kodun polinom temsili kullanılarak istenilen elde edilir.

Teorem 4.4.1.18. C kodu $n = \gamma + \mu$ uzunluğunda bir R_q-skew devirli kod olsun. $f(x)$, C_{γ} kodunun üreteç polinomu, $h(x)$, C_{μ} kodunun üreteç polinomu ve $f(x)$, $x^{\gamma} - 1$ polinomunun sağ böleni, $h(x)$, $x^{\mu} - 1$ polinomunun sağ böleni olmak üzere C kodunun üreteç polinomu

$$C = \langle (f(x),0), (g(x), h(x))\rangle$$

şeklindedir.

İspat: C, R_q-skew devirli kod olduğundan C_{γ} kodu F_q üzerinde skew devirli bir kod olur. O halde, C_{γ}, $F_q[x, \theta_t]/\langle x^{\gamma} - 1\rangle$ in bir sol $F_q[x, \theta_t]$-alt modülüdür. H kümesi

$$H = \{(a(x), b(x)) \in C: b(x) = 0\}$$

şeklinde tanımlansın. Bu durumda $\tau'_{\gamma}(H) = H$ ve $\tau'_{\gamma}(H)$, $F_q[x, \theta_t]/\langle x^{\gamma} - 1\rangle$ in bir sol $F_q[x, \theta_t]$-alt modülü olur. $\tau'_{\gamma}(H) = \langle f(x)\rangle$ olsun. Bu durumda $f(x)$, $x^{\gamma} - 1$ polinomunun sağ böleni olmak üzere H, $(f(x),0)$ ile üretilir. Ayrıca $h(x)$, $x^{\mu} - 1$ polinomunun sağ böleni olmak üzere $C_{\mu} = \langle h(x)\rangle$ dir.

Herhangi bir $s(x) \in C$ alalım. Böylece $a(x) \in F_q[x, \theta_t]/\langle x^{\gamma} - 1\rangle$ ve $b(x) \in S_q[x, \Gamma_t]/\langle x^{\mu} - 1\rangle$ için

$$s(x) = \big(s_1(x), s_2(x)\big)$$

$$= (s_1(x), 0) + \big(0, s_2(x)\big)$$

$$= (a(x)f(x), 0) + \big(0, b(x)h(x)\big)$$

şeklinde yazabiliriz. $g(x) \in F_q[x, \theta_t]/\langle x^\gamma - 1\rangle$ olmak üzere $(g(x), b(x)h(x)) \in C$ olsun. Bu durumda

$$s(x) = (a(x)f(x), 0)\big(\rho\big(b(x)\big)g(x), 0\big) + \Big(\rho\big(b(x)\big)g(x), b(x)h(x)\Big)$$

$$= \big(a(x)f(x) + \rho\big(b(x)\big)g(x), 0\big) + b(x).\big(g(x), h(x)\big)$$

$$= l(x)(f(x), 0) + b(x).\big(g(x), h(x)\big)$$

dir. Burada son adım $\big(a(x)f(x) + \rho\big(b(x)\big)g(x), 0\big)$ ın H kümesinin elemanı olmasından elde edilir. Böylece $C \subseteq \langle (f(x),0), (g(x), h(x))\rangle$ dir. Tersine, $\langle (f(x),0), (g(x), h(x))\rangle \subseteq \mathrm{C}$ olduğu açıktır. O halde C kodunun üreteç polinomu $C = \langle (f(x),0), (g(x), h(x))\rangle$ dir.

$C, n = \gamma + \mu$ uzunluğunda bir R_q-skew devirli kod olmak üzere $1 \le i \le 7$ için

$$C_0 = \{a: (a, s) \in C, \exists\, s_k \in F_q^\mu\},$$

$$C_{\mathrm{i}} = \{s_i: (a, s) \in C, \exists\, a \in F_q^\gamma, s_1, \dots, s_{i-1}, s_{i+1}, \dots, s_7 \in F_q^\mu\}$$

şeklinde tanımlansın.

Lemma 4.4.1.19. $C, n = \gamma + \mu$ uzunluğunda bir R_q-skew devirli bir kod olmak üzere $\psi(C) = C_0 \otimes \cdots \otimes C_7$ ve $|\psi(C)| = \prod_{i=0}^{7} |C_i|$ dir.

Tanım 4.4.1.20. $C, n = \gamma + \mu$ uzunluğunda bir R_q-skew devirli kod ve C_γ (aynı şekilde C_μ) C kodunun ilk γ (son μ) bileşenleri üzerindeki kanonik iz düşümü olsun. Eğer C kodu C_γ ve C_μ nın direkt çarpımı olarak ifade edilebiliyorsa, yani $C = C_\gamma \otimes C_\mu$ ise, bu durumda C koduna ayrılabilir kod denir.

Teorem 4.4.1.21. $C = C_\gamma \otimes C_\mu$, $n = \gamma + \mu$ uzunluğunda bir R_q-lineer kod olsun. C kodunun ayrılabilir bir R_q-skew devirli kod olması için gerek ve yeter koşul C_γ ve C_μ kodlarının sırasıyla F_q ve S_q üzerinde γ ve μ uzunluğunda skew devirli kodlar olmasıdır.

İspat: C, R_q-skew devirli kod, $(a_0, a_1, \dots, a_{\gamma-1}) \in C_\gamma, (b_0, b_1, \dots, b_{\mu-1}) \in C_\mu$ olmak üzere $y = (a_0, a_1, \dots, a_{\gamma-1}, b_0, b_1, \dots, b_{\mu-1}) \in C$ olsun. C, R_q-skew devirli kod olduğundan $(\theta_t(a_{\gamma-1}), \theta_t(a_0), \dots, \theta_t(a_{\gamma-2}), \Gamma_t(b_{\mu-1}), \Gamma_t(b_0), \dots, \Gamma_t(b_{\mu-2})) \in C$ olur. Böylece $(\theta_t(a_{\gamma-1}), \theta_t(a_0), \dots, \theta_t(a_{\gamma-2})) \in C_\gamma$ ve $(\Gamma_t(b_{\mu-1}), \Gamma_t(b_0), \dots, \Gamma_t(b_{\mu-2})) \in C_\mu$ elde edilir. O halde C_γ ve C_μ kodları sırasıyla F_q ve S_q üzerinde γ ve μ uzunluğunda skew devirli kodlardır.

Tersine C_γ ve C_μ kodları sırasıyla F_q ve S_q üzerinde γ ve μ uzunluğunda skew devirli kodlar olsun. Bu durumda $(a_0, a_1, \dots, a_{\gamma-1}) \in C_\gamma, (b_0, b_1, \dots, b_{\mu-1}) \in C_\mu$ olmak üzere $(\theta_t(a_{\gamma-1}), \theta_t(a_0), \dots, \theta_t(a_{\gamma-2})) \in C_\gamma$, $(\Gamma_t(b_{\mu-1}), \Gamma_t(b_0), \dots, \Gamma_t(b_{\mu-2})) \in C_\mu$ elde edilir. Böylece $(\theta_t(a_{\gamma-1}), \theta_t(a_0), \dots, \theta_t(a_{\gamma-2}), \Gamma_t(b_{\mu-1}), \Gamma_t(b_0), \dots, \Gamma_t(b_{\mu-2})) \in C_\gamma \otimes C_\mu = C$ dir. O halde C, $n = \gamma + \mu$ uzunluğunda bir R_q-skew devirli koddur.

Sonuç 4.4.1.22. $C = C_\gamma \otimes C_\mu$, $n = \gamma + \mu$ uzunluğunda bir R_q-lineer kod olsun. C kodunun bir R_q-skew devirli kod olması için gerek ve yeter koşul $1 \leq i \leq 7$ için C_0 ve C_i kodlarının F_q üzerinde sırasıyla γ ve μ uzunluğunda skew devirli kodlar olmasıdır.

Ayrıca, C ayrılabilir olduğundan $x^\gamma - 1$ in bir sağ böleni $f(x)$, $x^\mu - 1$ in bir sağ böleni $h(x)$ ve $C_\gamma = \langle f(x) \rangle$, $C_\mu = \langle h(x) \rangle$ olmak üzere $= \langle (f(x),0), (0, h(x)) \rangle$ dir.

Teorem 4.4.1.23. $C = C_\gamma \otimes C_\mu$, $n = \gamma + \mu$ uzunluğunda bir R_q-skew devirli kod ve $C = \langle (f(x),0), (0, h(x)) \rangle$ olsun. Bu durumda ${C_\gamma}^\perp \subseteq C_\gamma$ ve ${C_\mu}^\perp \subseteq C_\mu$ olması için gerek ve yeter koşul $C^\perp \subseteq C$ olmasıdır.

İspat: ${C_\gamma}^\perp \subseteq C_\gamma$ ve ${C_\mu}^\perp \subseteq C_\mu$ ve $a_1, b_1 \in {C_\gamma}^\perp$ ve $a_2, b_2 \in {C_\mu}^\perp$ olsun. Bu durumda $a = (a_1, a_2), b = (b_1, b_2) \in C^\perp$ ve F_q cisminde ve S_q halkasında sırasıyla $a_1 b_1 = 0$ ve $a_2 b_2 = 0$ olur. Böylece $ab = 0$ elde edilir. O halde $C^\perp \subseteq C$ dir. Benzer şekilde ${C_\gamma}^\perp \subseteq C_\gamma$ ve ${C_\mu}^\perp \subseteq C_\mu$ olduğu kolaylıkla görülür.

Teorem 4.4.1.24. C_γ ve C_μ kodları sırasıyla F_q ve S_q üzerinde self-ortogonal skew devirli kodlar olmak üzere $C = C_\gamma \otimes C_\mu$ olsun. O halde C kodu self-ortogonal R_q-skew devirli kod olur.

İspat: $a=(a_1,a_2),\ a'=(a_1',a_2')\in C$ olsun. Bu durumda $a_1,a_1'\in C_\gamma=\langle f(x)\rangle$ ve $a_2,a_2'\in C_\mu=\langle h(x)\rangle$ dir. C_γ ve C_μ kodları sırasıyla F_q ve S_q üzerinde self-ortogonal skew devirli kodlar olduğundan $C_\gamma\subseteq {C_\gamma}^\perp$ ve $C_\mu\subseteq {C_\mu}^\perp$ dir. Buradan

$$a_1a_1'=0\in F_q,\qquad a_2a_2'=0\in S_q$$

olur. Böylece $aa'=a_1a_1'+a_2a_2'=0$ elde edilir. O halde $C\subseteq C^\perp$ dir ve C kodu self-ortogonal R_q-skew devirli kod olur.

4.4.2. R_q-Skew Devirli Kodlardan Kuantum Kodlar

$\mathbb{C}^q$, q boyutlu Hilbert uzayı olmak üzere, $(\mathbb{C}^q)^{\otimes n}$ nin q^k boyutlu alt uzayına n uzunluğunda, k boyutlu, d minimum uzaklığında kuantum kod denir ve $[[n,k,d]]$ ile gösterilir.

F_q üzerinde, n uzunluğunda bir skew devirli C kodu $\frac{F_q[x,\theta_t]}{\langle x^n-1\rangle}$ in bir sol $F_q[x,\theta_t]$-alt modülüdür. $g(x)$, x^n-1 polinomunun sağ böleni ve $x^n-1=h(x)g(x)$ olmak üzere $C=\langle g(x)\rangle$ olsun. $h(x)=h_0+h_1x+\cdots+h_{n-r}x^{n-r}$ için $h^\dagger(x)=h_{n-r}+\theta_t(h_{n-r-1})x+\cdots+{\theta_t}^{n-r}(h_0)x^{n-r}$ olmak üzere C kodunun duali $C^\perp$, n uzunluğunda bir skew devirli kod olur ve $C^\perp=\langle h^\dagger(x)\rangle$ dir. Eğer θ_t aşikar otomorfizma ise $h^*(x)=h_{n-r}+h_{n-r-1}x+\cdots+h_0x^{n-r}$ olmak üzere $h^\dagger(x)=h^*(x)$ elde edilir.

Lemma 4.4.2.1. ϑ, θ_t otomorfizmasının mertebesi olmak üzere $C=\langle f(x)\rangle$, F_q üzerinde α uzunluğunda skew devirli bir kod ve $(\alpha,\vartheta)=1$ olsun. Bu durumda $C^\perp\subseteq \mathrm{C}$ olması için gerek ve yeter koşul $f^*(x)$, $f(x)$ polinomunun reciprocal polinomu olmak üzere $x^\alpha-1\equiv 0(\mathrm{mod} f(x)f^*(x))$ olmasıdır (Islam ve Prakash, 2019).

Lemma 4.4.2.2. $x^\alpha-1=h(x)g(x)$ olmak üzere $C=\langle f(x)\rangle$, F_q üzerinde α uzunluğunda bir skew devirli kod olsun ve θ_t otomorfizmasının mertebesi α yı bölsün. Bu durumda $C^\perp\subseteq C$ olması için gerek ve yeter koşul $h^\dagger(x)h(x)$ in sağdan $x^\alpha-1$ e bölünebilir olmasıdır (Li vd., 2020).

Lemma 4.4.2.2 den aşağıdaki teorem elde edilebilir.

Teorem 4.4.2.3. $1 \leq i \leq 7$ için $x^{\gamma} - 1 = h(x)f(x)$, $x^{\mu} - 1 = h_i(x)r_i(x)$, $C_{\gamma} = \langle f(x) \rangle$ ve $C_{\mu} = \langle \alpha_1 r_1(x) + \cdots + \alpha_7 r_7(x) \rangle$ sırasıyla F_q ve S_q üzerinde skew devirli kodlar olmak üzere $C = C_{\gamma} \otimes C_{\mu}$, $n = \gamma + \mu$ uzunluğunda bir R_q-skew devirli kod olsun ve θ_t, Γ_t otomorfizmalarının mertebeleri sırasıyla γ ve μ yü bölsün. Bu durumda $C^{\perp} \subseteq C$ olması için gerek ve yeter koşul $h^{\dagger}(x)h(x)$ ve $h_i^{\dagger}(x)h_i(x)$ in sırasıyla sağdan $x^{\gamma} - 1$ ve $x^{\mu} - 1$ e bölünebilir olmasıdır.

Teorem 4.4.2.4. $1 \leq i \leq 7$ için $x^{\gamma} - 1 = h(x)f(x)$, $x^{\mu} - 1 = h_i(x)r_i(x)$ olmak üzere $C = C_{\gamma} \otimes C_{\mu}$, $n = \gamma + \mu$ uzunluğunda bir R_q-skew devirli kod olsun ve θ_t, Γ_t otomorfizmalarının mertebeleri sırasıyla γ ve μ yü bölsün. $h^{\dagger}(x)h(x)$ ve $h_i^{\dagger}(x)h_i(x)$ sırasıyla sağdan $x^{\gamma} - 1$ ve $x^{\mu} - 1$ e bölünebilir ise k, $\psi(C)$ kodunun boyutu ve d_H Hamming uzaklığı olmak üzere $\left[[\gamma + 7\mu, 2k - (\gamma + 7\mu), d_H]\right]$ parametrelerine sahip bir kuantum kod vardır.

Örnek 4.4.2.5. $F_{25} = F_5[\lambda]$ ve herhangi bir $a \in F_{25}$ elemanı için $\theta_1(a) = a^5$ ve

$$x^{10} - 1 = (x+1)^3(x-1)^3(x+\lambda^{16})^2(x+\lambda^{20})^2 \in F_{25}[x, \theta_1]$$

olsun. $1 \leq i \leq 7$ için eğer $r_i(x) = (x + \lambda^8)(x + 1)$ ve $f(x) = (x + \lambda^{16})(x - 1)$ alınırsa $C_{\gamma} = \langle f(x) \rangle$ ve $C_{\mu} = \langle \sum_{i=1}^{7} \varepsilon_i r_i(x) \rangle$ sırasıyla F_9 ve S_9 üzerinde skew devirli kod olur. Bu durumda $\psi(C)$, [80,64,3] parametrelerine sahip skew devirli kod olur. $h^{\dagger}(x)h(x)$ ve $h_i^{\dagger}(x)h_i(x)$ sağdan $x^{10} - 1$ e bölünebilir ve $C^{\perp} \subseteq C$ elde edilir. Burada

$$h(x) = x^8 + \lambda^{23}x^7 + \lambda^9x^6 + \lambda^5x^5 + \lambda^{22}x^4 + \lambda^{17}x^3 + \lambda^5x^2 + \lambda^{11}x + \lambda^8,$$

$$h^{\dagger}(x) = \lambda^8x^8 + \lambda^7x^7 + \lambda^5x^6 + \lambda^{13}x^5 + \lambda^{22}x^4 + \lambda x^3 + \lambda^9x^2 + \lambda^{19}x + 1,$$

$$h_i(x) = x^8 + \lambda^{16}x^7 + \lambda^{19}x^6 + \lambda^{22}x^5 + \lambda^{17}x^4 + \lambda^{10}x^3 + \lambda^3x^2 + \lambda^4x + \lambda^4,$$

$$h_i^{\dagger}(x) = \lambda^4x^8 + \lambda^{20}x^7 + \lambda^3x^6 + \lambda^2x^5 + \lambda^{17}x^4 + \lambda^{14}x^3 + \lambda^{19}x^2 + \lambda^8x + 1$$

şeklindedir. O halde $\left[[80,48,3]\right]$ paramtrelerine sahip kuantum kodu elde edilir.

Örnek 4.4.2.6. $\lambda^2 = \lambda + 1$ için $F_9 = F_3[\lambda]$ ve herhangi bir $a \in F_9$ elemanı için $\theta_1(a) = a^3$ ve

$$x^{12} - 1 = (x+\lambda)^2(x+\lambda^2)^4(x+\lambda^3)(x+\lambda^5)(x+\lambda^6)^2(x+\lambda^7)^2 \in F_9[x, \theta_1]$$

olsun. $1 \leq i \leq 7$ için eğer $r_i(x) = (x + \lambda^6)(x + \lambda^7)(x + \lambda^2)$ ve $f(x) = (x + \lambda)(x + \lambda^6)(x + \lambda^2)$ alınırsa $C_\gamma = \langle f(x) \rangle$ ve $C_\mu = \langle \sum_{i=1}^{7} \varepsilon_i r_i(x) \rangle$ sırasıyla F_9 ve S_9 üzerinde skew devirli kod olur. Bu durumda $\psi(C)$, $[96,72,3]$ parametrelerine sahip skew devirli kod olur. $h^\dagger(x)h(x)$ ve $h_i^\dagger(x)h_i(x)$ sağdan $x^{12} - 1$ e bölünebilir ve $C^\perp \subseteq \mathrm{C}$ elde edilir. Burada

$$h(x) = x^9 + x^8 + \lambda^5 x^7 + \lambda x^6 + \lambda^3 x^5 + \lambda^2 x^4 + \lambda x^3 + \lambda^5 x^2 + \lambda^2 x + \lambda^3,$$

$$h^\dagger(x) = \lambda x^9 + \lambda^2 x^8 + \lambda^7 x^7 + \lambda x^6 + \lambda^6 x^5 + \lambda^3 x^4 + \lambda^3 x^3 + \lambda^5 x^2 + x + 1,$$

$$h_i(x) = x^9 + \lambda^3 x^8 + \lambda^2 x^7 + x^6 + \lambda^7 x^5 + \lambda^6 x^4 + \lambda^6 x^3 + 2x^2 + \lambda^5 x + \lambda^5,$$

$$h_i^\dagger(x) = \lambda^7 x^9 + \lambda^5 x^8 + 2x^7 + \lambda^6 x^6 + \lambda^2 x^5 + \lambda^7 x^4 + x^3 + \lambda^2 x^2 + \lambda x + 1$$

şeklindedir. O halde $[[96,48,3]]$ paramtrelerine sahip kuantum kodu elde edilir.

Örnek 4.4.2.7. $\lambda^2 = \lambda + 1$ için $F_9 = F_3[\lambda]$ ve herhangi bir $a \in F_9$ elemanı için $\theta_1(a) = a^3$ ve

$$x^6 - 1 = (x + \lambda^2)^2(x + \lambda^6)^2(x + 1)(x + 2) \in F_9[x, \theta_1]$$

olsun. $1 \leq i \leq 7$ için eğer $f(x) = r_i(x) = x^2 + \lambda^6 x + 1$ alınırsa $C_\gamma = \langle f(x) \rangle$ ve $C_\mu = \langle \sum_{i=1}^{7} \alpha_i r_i(x) \rangle$ sırasıyla F_9 ve S_9 üzerinde skew devirli kod olur. Bu durumda $h^\dagger(x)h(x)$ ve $h_i^\dagger(x)h_i(x)$ sağdan $x^6 - 1$ e bölünebilir ve $C^\perp \subseteq \mathrm{C}$ elde edilir. O halde $[[48,16,3]]$ paramtrelerine sahip kuantum kodu elde edilir.

Örnek 4.4.2.8. $\lambda^2 = \lambda + 1$ için $F_9 = F_3[\lambda]$ ve herhangi bir $a \in F_9$ elemanı için $\theta_1(a) = a^3$ ve

$$x^8 - 1 = (x^2 - \lambda^6)(x^2 + \lambda^6 x + \lambda^3)(x - \lambda^5)(x^2 - \lambda^3 x + 1)(x + \lambda^6) \in F_9[x, \theta_1]$$

olsun. $1 \leq i \leq 7$ için eğer $f(x) = r_i(x) = f(x) = r_i(x) = x + \lambda^6$ alınırsa $C_\gamma = \langle f(x) \rangle$ ve $C_\mu = \langle \sum_{i=1}^{7} \alpha_i r_i(x) \rangle$ sırasıyla F_9 ve S_9 üzerinde skew devirli kod olur. Bu durumda $h^\dagger(x)h(x)$ ve $h_i^\dagger(x)h_i(x)$ sağdan $x^8 - 1$ e bölünebilir ve $C^\perp \subseteq \mathrm{C}$ elde edilir. O halde $[[64,48,2]]$ paramtrelerine sahip kuantum kodu elde edilir.

5. SONUÇ VE ÖNERİLER

Bu çalışmada zengin cebirsel yapıya sahip lineer kodların önemli bir sınıfı olan devirli kodlar ve minimum uzaklığı yüksek kodlar elde edebilmek için devirli kodlardan daha geniş bir sınıf olan skew devirli kodlar araştırılarak bu kodların DNA ve kuantum uygulamaları çalışılmıştır. İlk olarak tanımladığımız S_q halkası üzerinde devirli kodların cebirsel yapısı incelenmiş ve Gray görüntüsü belirlenmiştir. S_q halkası üzerinde aşikar olmayan bir otomorfizma tanımlanarak skew devirli kodlar karakterize edilmiştir. Bu iki tip koddan elde edilen DNA kodlar ve devirli kodlardan elde edilen kuantum kodlar tanımlanmıştır. S_q halkasını kullanarak oluşturulan ve mix alfabe denilen R_q halkası üzerinde tanımlı lineer kodların cebirsel yapısı açıklanmıştır. R_q-devirli ve R_q-skew devirli kodlar tanımlanarak, R_q-devirli kodlardan DNA kodlar ve R_q-skew devirli kodlardan kuantum kodlar tanımlanmış ve özellikleri belirlenmiştir. Ayrıca bu kod türlerine çeşitli örnekler verilmiştir.

Gelecekteki araştırmalarda, S_q halkası ve mix alfabe üzerinde daha fazla detaylı analizler yapılarak farklı lineer kod türleri çalışılabilir. Ayrıca S_q halkası genelleştirilerek yeni bir halka ailesi ve mix alfabe tanımlanarak benzer çalışmalar yapılabilir. MAGMA programı kullanılarak daha iyi parametrelere sahip optimal kodlar elde edilebilir.

KAYNAKLAR

Abualrub, T., Ghrayeb, A., Zeng, X. N. (2006). "Construction of cyclic codes over GF (4) for DNA computing". *Journal of the Franklin Institute*, 343(4-5), 448-457.

Adleman, L., (1994). "Molecular Computation of Solutions to Combinational Problems". *Science,* 266,1021-1024.

Alahmadi, A., Altassan, A., Alyoubi, A., Gupta, M. K., Shoaib, H. (2021)." Cyclic and Quasi-Cyclic DNA Codes". *arXiv preprint arXiv:2110.09789*.

Ashraf, M., Mohammad, G., (2014). "Quantum codes from cyclic codes over $F_3 + vF_3$", *Int. J. Quantum Inform.*, 12, 1450042.

Bathala, S., Bhaintwal, M. (2017). "The structure of duals of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ and some DNA codes". *International Journal of Information and Coding Theory*, *4*(1), 79-100.

Benbelkacem, N., Ezerman, M. F., Abualrub, T., Aydin, N., Batoul, A. (2022). "Skew cyclic codes over $\mathbb{F}_4 R$". *Journal of Algebra and Its Applications*, *21*(04), 2250065.

Blake, I. F. (1972). "Codes over Certain Rings*".* *Information and Control*, *20*, 396-404.

Boucher, D., Geiselmann, W., Ulmer, F., (2007). "Skew cyclic codes", *Applicable Algebra in Eng. Comm. and Computing*, 18, 379-389.

Boucher, D., Ulmer, F., (2009). "Coding with skew polynomial rings", *Journal of Symbolic Computation*, 44, 1644-1656.

Calderbank, A. R., Rains, E. M., Shor, P. M., Sloane, N. J. (1998). "Quantum error correction via codes over GF(4)". *IEEE Transactions on Information Theory*, 44(4), 1369-1387.

Calderbank, A. R., Shor, P. W. (1996). "Good quantum error-correcting codes exist*"*. *Physical Review A.* 54(2). 1098-1105.

Çallıalp, F. (2013). *Örneklerle soyut cebir.* İstanbul: Birsen Yayınevi.

Çallıalp, F., Kuruoğlu, N. (1996). *Lineer cebir*. Samsun: Ondokuz Mayıs Üniversitesi Yayınları.

Dertli, A. (2016). *Halkalar üzerinde tanımlı kodlar hakkında bazı araştırmalar.* Doktora Tezi. Ondokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı, Samsun.

Dinh, H. Q., Singh, A. K., Pattanayak, S., Sriboonchitta, S. (2018). "Cyclic DNA codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 + v^2\mathbb{F}_2 + uv^2\mathbb{F}_2$". *Designs, Codes and Cryptography*, *86*, 1451-1467.

Dinh, H. Q., Pathak, S., Upadhyay, A. K., Yamaka, W. (2020). "New DNA codes from cyclic codes over mixed alphabets". *Mathematics*, *8*(11), 1977.

Dixita, L., Bansari, R., Manish, K. G. (2016). "The Art of DNA Strings: Sixteen Years of DNA Coding Theory". *arXiv:1607.00266v1*.

Gao, J., Wang, Y. (2018). "u-constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$ and their applications of constructing new non-binary quantum". *Quantum Information Processing,* 17 (1), 1-9.

Grassl, M., Beth, T., 2004. "On optimal quantum codes". *Int. J. Quantum Inform.*, 2, 5564.

Güzeltepe, M. (2014). *Gauss ve kuaterniyon tam sayılarından kuantum kod elde etme.* Ankara: Gece Kitaplığı Yayınları.

Hammons, A. R., Kumar, V., Calderbank, A. R., Sloane, N. J. A., Solé, P., (1994). "The Z_4 linearity of Kerdock, Preparata, Goethals and related codes", *IEEE Trans. Inf. Theory*, 40, 301-319.

Hebbache, Z., Sharma, A. (2022). "$Z_4Z_4[u^3 = 1]$-Cyclic codes and their reversible codes". *Models & Optimisation and Mathematical Analysis Journal*, 10(01), 26-29.

Head, T. (1987). "Formal language theory and DNA: an analysis of the generative capacity of specific recombinant behaviors". *Bulletin of mathematical biology*, *49*(6), 737-759.

Hill, R. (1986). *A first course in coding theory*. Oxford: The Oxford University Press.

Huffman, W. C., Pless, V. (2003). *Fundamentals of error correcting codes.* New York: Cambridge University Press.

Hungerford, T. W. (1973). *Algebra.* New York: Springer.

Islam, H., Prakash, O. (2019). "Quantum codes from the cyclic codes over $F_p[u, v, w]/\langle u^2 - 1, v^2 - 1, w^2 - 1, uv - vu, vw - wv, wu - uw\rangle$". *Journal of Applied Mathematics & Computing*, 60, 625-635.

Jitman, S., Ling, S., Udamkavanich, P. (2010). "Skew constacyclic codes over finite chain rings". *Advences in Mathematics of Communications*, 6(1), 39-63.

Kai, X., Zhu, S. (2011). *"*Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4 + \mathrm{u}\mathbb{F}_4$*". Journal of Quantum Information,* 9(02), 689-700.

Kaye, P., Laflamme, R., Mosca, M. (2006). *An introducion to quantum computing.* Oxford: Oxford University Press.

Li, J., Gao, J., Wang, Y. (2018). "Quantum codes from $(1 - 2v)$-constacyclic codes over the ring $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$". *Discrete Mathematics, Algorithms and Applications*, 10(04), 1850046.

Li, J., Gao, J., Fu, F. W., Ma, F. (2020). $\mathbb{F}_qR$-linear skew constacyclic codes and their application of constructing quantum codes. *Quantum Information Processing*, *19*, 1-23.

Ling, S., Xing, C. (2004). *Coding theory a first course.* New York: Cambridge University Press.

Massey, J. L. (1964). "Reversible codes". *Information and Control*, *7*(3), 369-380.

McDonald, B.R, 1974. *Finite Rings With Identity*, Marcel Dekker Inc., New York.

Prakash, O., Islam, H., Patel, S., Solé, P. (2021). "New quantum codes from skew constacyclic codes over a class of non-chain rings $R_{e,q}$". *International Journal of Theoretical Physics*, *60*, 3334-3352.

Prakash, O., Singh, A., Verma, R. K., Solé, P., Cheng, W. (2023). "DNA Code from Cyclic and Skew Cyclic Codes over $F_4[v]/\langle v^3\rangle$". *Entropy*, *25*(2), 239.

Prange, E. (1957). "Cyclic Error-Correcting Codes in Two Symbols". *Cambridge: Air Force Cambridge Research Center*-TN-57-103.

Qian, J. (2013). *"*Quantum codes from cyclic codes over $\mathbb{F}_2 + \mathrm{u}\mathbb{F}_2$*". Journal of Information and Computational Science,* 10(6), 1715-1722.

Qian, J., Ma, W., Guo, W. (2009). "Quantum codes from cyclic codes over finite ring". *International Journal of Quantum Information*, *7*(06), 1277-1283.

Roman, S. (1992). *Coding and information theory.* Springer: Graduate Text in Mathematics.

Sarma, A., (2012). Quantum Codes Over Finite Frobenius Rings, Master of Science,Texas A&M University.

Shannon, C., (1948). “A Mathematical Theory of Communication”, *The Bell System Technical Journal*, 27, 379-423, 623-656.

Shor, P. W. (1995). “Scheme for reducing decoherence in quantum computer memory”. *Physical review A*, *52*(4), R2493.

Steane, A. M. (1996). “Simple quantum error-correcting codes”. *Physical Review A*, *54*(6), 4741.

Şiap İ., Abualrub T., Aydın N., Seneviratne P., (2011). “Skew cyclic codes of arbitrary length”, *International Journal of Information and Coding Theory*, 2, 10-20.

Taşçı, D. (2007). *Soyut cebir*. Ankara: Alp Yayınevi.

Yin, X., Ma, W. (2011). “Gray map and quantum codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$”. IEEE 10th International Conference an Trust, Security and Privacy in Computing and Communications, 897-899.

ÖZ GEÇMİŞ

Rabia DERTLİ, Nallıhan Şehit Vural Arıcı Anadolu Lisesi'ni bitirdikten sonra Ondokuz Mayıs Üniversitesi Fen-Edebiyat Fakültesi, Matematik bölümünden 2017 tarihinde mezun oldu. 2020 yılında OMÜ LEE Matematik Ana Bilim Dalı Yüksek Lisans programını bitirdi, 2020 yılında Matematik ABD doktora programına başladı. Temel ilgi alanları, cebir, sayılar teorisi ve kodlama teorisidir.

İletişim Bilgileri

ORCID ID : 0000-0002-4149-3062

Yayınlar:

1. Dertli, R., & Eren, Ş. (2023). DNA Codes from Cyclic Codes over F_qS_q. *5.International Cappadocia Scientific Research Congress,* November 5-7, https://en.cappadociacongress.org.

2. Dertli, R., & Eren, Ş. (2023). Quantum codes from Skew Cyclic Codes over F_qS_q. *5.International Black Sea Modern Scientific Research Congress,* November 8-10, https://tr.blackseacountries.org/congres.

3. Dertli, R., & Eren, Ş. (2023). Quantum codes from Cyclic Codes over S_q. *3.Uluslararası İstanbul Güncel Bilimsel Araştırmalar Kongresi,* 8 - 9 Şubat 2023, https://www.izdas.org/istanbul.

4. Dertli, R., & Eren, Ş. (2022). Reversible DNA Codes from Cyclic and Skew Cyclic Codes over S_4. *2.Uluslararası Karadeniz Modern Bilimsel Araştırmalar Kongresi,* 21 - 22 Aralık 2022, https://www.izdas.org/karadeniz.