TÜBİTAK

Çeşitli Halkalar Üzerinde Klasik Kodların ve Stabilizer Kuantum Kodların Geliştirilmesi

Program Kodu: 3001

Proje No: 116F318

Proje Yürütücüsü:
Doç. Dr. Murat GÜZELTEPE

Araştırmacı(lar):
Dr. Öğr. Üyesi Gökçen ÇETİNEL
Dr. Öğr. Üyesi Nükhet SAZAK
Doç. Dr. Mustafa ERÖZ

Bursiyer(ler):
Ercüment ÇAKIR

NİSAN 2019
SAKARYA

ÖNSÖZ

Bu proje 01.04.2017 tarihinde TÜBİTAK tarafından desteklenerek 116F318 proje numarası ile başlatılmıştır. Proje ekibi proje konusunu Mayıs 2017 tarihine kadar yaptığı çalışmalarla belirlemiş ve Mayıs 2017 tarihinde projeyi çeşitli konularda destek almak ve daha sonra yapılacak daha kapsamlı bir projeye başlangıç yapmak amacı ile TÜBİTAK'a sunmuştur. Sunumdan sonra proje ekibi projenin amacı doğrultusunda projede belirtilen hedeflere düzenli olarak her hafta ve haftada bir gün çalışmaya başlamış ve ilk verilerini projenin kabul tarihinde elde etmiştir.

Bu projenin konusu çeşitli halkalar üzerinde mevcut klasik kodlardan daha verimli kodlar ve çeşitli halkalar üzerindeki kendine ortogonal ve kendine dik kodlar yardımı ile literatürdeki kuantum kodlar göz önüne alınarak optimal kuantum kodlar elde etmektir.

Ayrıca genç bilim insanları yetiştirmek de ayrı bir hedeftir.

İÇİNDEKİLER

ŞEKİLLER

TABLOLAR

ÖZET

Anahtar kelimeler: Kuantum kod, stabilizer kod, nonbinary kuantum kod, lineer kod, devirli kod, toplamsal kod, kod kazancı, minimum enerji.

Bu projede Lipschitz, Hurwitz gibi çeşitli halkalar üzerinde bant genişliği, veri aktarım hızı ve ortalama enerji tüketimi bakımından daha elverişli klasik kodların üretilmesi, bu kodların simülasyonlarının yapılması, bu kodlardan 1-hata düzeltebilen mükemmel olanlarının karakterize edilmesi ve bu kodlardan yararlanılarak kuantum kodların inşa edilmesi amaçlanmıştı. Bu proje kapsamında elde edilen kodlar literatürdeki kodlarla karşılaştırılmıştır. Karşılaştırmalar BPSK (Binary Phase Shift Keying-İkili Faz Kaydırmalı Anahtarlama), QPSK (Quadrature Phase Shift Keying-Dördül Faz Kaydırmalı Anahtarlama) ve QAM (Quadrature Amplitude Modulation-Dördül Genlik Modülasyonu) kullanılarak yapılmıştır. Bu proje kapsamında elde edilecek kodlar ile literatürdeki kodların minimum enerji açısından karşılaştırılması için hata olasılığı-SNR (bir iletim sırasında sinyal gürültü oranı) grafikleri kullanılmıştır. Proje kapsamında elde edilecek kodların, literatürdeki kodlar ile bahsedilen modülasyon türleri açısından kıyaslandığında daha iyi olduğu örülmüştür.

Ayrıca proje kapsamında kuantum kodlar da çalışılmıştır. Bilindiği gibi kendine-dik (self-dual) kodlar ve kendine-ortogonal (self-orthogonal) klasik kodlar kullanılarak kuantum kod elde edilmektedir. Klasik kodlar için klasik devreler ve mantık kapıları olduğu gibi kuantum kodlar için de kuantum devre ve kuantum mantık kapıları vardır. Devreler mantık kapıları kullanılarak elde edilmektedir. Kuantum mantık kapıları Pauli spin matrisleri kullanılarak tanımlanır. Proje kapsamında kullanılacak halkalar için Pauli spin matrisleri ve Hadamard mantık kapısı gibi kuantum mantık kapıları da inşa edilmiştir. Bu mantık kapıları ile kuantum bilgi kodlanmış ve bu bilgi bir kuantum devresi kullanılarak dekodlanmıştır.

Proje kapsamında elde edilen kodlar, sayısal haberleşme sistemlerinde BPSK, QPSK ve QAM gibi iki boyutlu sinyal yıldız kümesinde temsil edilen modülasyon yöntemlerindeki başarımları açısından kıyaslanmıştır. Kıyaslama yapılırken, kod kazancı ve sembol hata olasılığına karşın SNR (Signal to Noise Ratio, İşaret Gürültü Oranı) gibi, haberleşme literatüründe yaygın olarak kullanılan kriterler ele alınmıştır. Daha yüksek kod kazancının sağlanması sunulan kodlama tekniğinin daha uzak mesafeler ile haberleşme açısından daha uygun olduğunu anlamına gelir. Diğer taraftan, aynı SNR değeri için daha düşük sembol hata olasılığına sahip bir kod bulunması daha güvenilir ve dayanıklı bir haberleşme sistemini işaret eder.

THE DEVELOPMENT OF CLASSİCAL CODES AND STABILIZER QUANTUM CODES OVER SOME RING

ABSTRACT

Key Words: Quantum code, stabilizer code, nonbinary quantum code, linear code, cyclic code, additive code, code gain, minimum energy.

The aim of this project is to construct more favorable classical codes over some rings such as Lipschitz and Hurwitz in terms of bandwidth occupancy, data transfer rate and average energy consumption, to present simulations of these codes, to characterize 1-error correcting perfect codes of these codes, and to construct quantum codes by using these codes. Codes obtained within the scope of the project were compared with the ones in the literature. These comparisons were made employing BPSK (Binary Phase Shift Keying), QPSK (Quadrature Phase Shift Keying) and QAM (Quadrature Amplitude Modulation). Error probability - SNR (signal to noise ratio during a transmission) graphics were used to compare obtained codes with the ones in the literature in terms of the minimum energy. It was seen that the codes to be generated within the scope of the project are better than the codes in the literature in terms of above-mentioned modulation types.

Quantum codes were studied within the project. It is well-known that quantum codes can be obtained by self-dual and self-orthogonal classical codes. There are quantum circuits and quantum logical gates for quantum codes as well as the classic circuits and logical gates for classical codes. Quantum logical gates are defined by Pauli spin matrices. Pauli spin matrices and quantum logical gates such as Hadamard gate for these rings were defined in the project. Quantum information were encoded using these logical gates and were decoded using a quantum circuit.

The codes obtained in the project framework were compared in terms of their performances for modulation methods such as, BPSK, QPSK and QAM represented by two-dimensional signal constellations, in digital communications systems. During the comparison, commonly used criteria such as, coding gain and symbol error rate versus SNR (Signal to Noise Ratio) are considered. To provide higher coding gain means that the proposed coding technique is more suitable for communicating over long distances. On the other hand, to attain a code having lower symbol error probability for same SNR values denotes the more reliable and robust communication system.

BÖLÜM 1.

Hurwitz sayıları üzerinde Hurwitz metriğine göre mükemmel kodlar

(1. iş paketi, 1. ve 3. hedef):

Bu çalışmada katkısı olanlar:
Doç. Dr. Murat GÜZELTEPE
Alev ALTINEL

Mükemmel kodların hem uygulama açısından hem de teorik açıdan kodlama teorisinde oldukça önemli bir yeri vardır. Bu güne kadar birçok kodlama teorisi çalışanı yeni mükemmel kodlar bulmak için çalışmıştır. 1950 yılında Hamming ilk mükemmel kodları elde etmiştir. Bu kodlar ikili kodlar üzerine idi. Vasil'ev, Lindström, Schönheim, Lee gibi birçok tanınmış kodlama teorici yeni mükemmel kodlar elde etmiştir.

Proje kapsamında yapılan "Perfect 1-error correcting Hurwitz weight codes" çalışmamız bu alanda yapılmış önemli bir çalışmadır. Bu çalışma

$e_1^2 = e_2^2 = e_3^2 = -1$ ve $e_1e_2 = -e_2e_1 = e_3, e_2e_3 = -e_3e_2 = e_1, e_3e_1 = -e_1e_3 = e_2$

ve

$$H(\mathbb{Z}) = \{a_0 + a_1e_1 + a_2e_2 + a_3e_3 \,|a_0, a_1, a_2, a_3 \in \mathbb{Z}\}$$

olmak üzere

$$\mathcal{H} = H(\mathbb{Z}) \cup H(\mathbb{Z} + \frac{1}{2})$$

olarak tanımlanan Hurwitz sayıları üzerinde yapılmıştır. $\pi = a_0 + a_1e_1 + a_2e_2 + a_3e_3 \in \mathcal{H}$ bir asal Hurwitz sayısı yani p bir asal tamsayı olmak üzere

$$\begin{aligned} p = \pi\pi^\star &= (a_0 + a_1e_1 + a_2e_2 + a_3e_3)(a_0 - a_1e_1 - a_2e_2 - a_3e_3) \\ &= a_0^2 + a_1^2 + a_2^2 + a_3^2 \end{aligned}$$

olsun. π'nin normu $N(\pi) = a_0^2 + a_1^2 + a_2^2 + a_3^2$ olarak tanımlanır. π'nin $\mathcal{H}$ halkasında oluşturdu sağ ideal $\mathcal{H}$ halkasının bir normal alt grubudur ve bu alt grup

$$\langle\pi\rangle = \{\pi\delta \,|\, \delta \in \mathcal{H}\}$$

olarak tanımlanır. Bu alt gruba göre elde edilen sınıfların kümesi

$$\mathcal{H}_\pi = \mathcal{H}/\langle\pi\rangle$$

ile gösterilir.

$\mathcal{E} = \{\pm 1, \pm e_1, \pm e_2, \pm e_3, \frac{1}{2}(\pm 1 \pm e_1 \pm e_2 \pm e_3)\}$

ve $\mathcal{E}_\pi$ ile de $\mathcal{E}$ kümesini içeren sınıfları gösterilsin. Bu takdirde

$u = (u_1, u_2, \ldots, u_n), v = (v_1, v_2, \ldots, v_n) \in \mathcal{H}_\pi^n$ olmak üzere u ile v arasındaki mesafe $d(u,v)$ ile gösterilir ve $j \in \{1,2,\ldots,n\}$ olmak üzere eğer her $i \neq j$ için $u_j = v_j + \epsilon$ olacak şekilde bir $\epsilon \in \mathcal{E}_\pi$ elemanı varsa $d(u,v) = 1$ olur. $C \subset \mathcal{H}_\pi^n$ alt kümesi için eğer $\mathcal{H}_\pi^n - C$ kümesindeki her eleman C'nin bir ve yalnız bir elemanına 1 uzaklığında ise $C \subset \mathcal{H}_\pi^n$ kümesine "bir Hurwitz ağırlıklı hataları düzeltebilen mükemmel kod" denir.
Bu çalışmada aşağıda açıklanan metotla bir Hurwitz ağırlıklı hataları düzeltebilen mükemmel kodlar karakterize edilmiştir.

1.1 Bazı Notasyonlar ve Önermeler

$\lfloor \bullet \rceil$ Sembolü en yakın tam sayıya yuvarlamayı ve $\lfloor\lfloor \bullet \rceil\rceil$ sembolü de en yakın yarı tam sayıya yuvarlamayı göstersin. Bir Hurwitz sayısının yuvarlaması ise sırası ile

$$\lfloor a_0 + a_1e_1 + a_2e_2 + a_3e_3 \rceil = \lfloor a_0 \rceil + \lfloor a_1 \rceil e_1 + \lfloor a_2 \rceil e_2 + \lfloor a_3 \rceil e_3,$$
$$\lfloor\lfloor a_0 + a_1e_1 + a_2e_2 + a_3e_3 \rceil\rceil = \lfloor\lfloor a_0 \rceil\rceil + \lfloor\lfloor a_1 \rceil\rceil e_1 + \lfloor\lfloor a_2 \rceil\rceil e_2 + \lfloor\lfloor a_3 \rceil\rceil e_3$$

olarak tanımlanır.

Önerme 1.1.1. $\pi \in H(\mathbb{Z})$ bir asal ve $q \in \mathcal{H}$ olsun. Bu durumda

$q = \pi\gamma + \delta_1, \quad N(\delta_1) < N(\pi)$

olacak şekilde $\gamma \in H(\mathbb{Z})$ ve $\delta_1 \in \mathcal{H}$ elemanları vardır.

Önerme 1.1.2. $\pi \in H(\mathbb{Z})$ bir asal ve $q \in \mathcal{H}$ olsun. Bu durumda

$q = \pi\gamma + \delta_2, \quad N(\delta_2) < N(\pi)$

olacak şekilde $\gamma \in H\left(\mathbb{Z} + \frac{1}{2}\right)$ ve $\delta_1 \in \mathcal{H}$ elemanları vardır.

Bu mükemmel kodların inşası için bazı kümeler tanımlanacaktır.

$A_i = \{q \in H(\mathbb{Z}) : N(q) = i\}$ ve $w = \frac{1}{2}(1 + e_1 + e_2 + e_3)$ olmak üzere Önerme 1 ve Önerme 2 göz önüne alınarak

$$A_{i_1} = \{q \in A_i : N(\delta_1) \neq N(\delta_2),\ (\delta_1), N(\delta_2) \geq i\}$$

ve

$$A_{i_2} = \{q \in A_i : N(\delta_1) = N(\delta_2) = i\}$$

kümeleri tanımlansın. $A_i = A_{i_1} \cup A_{i_2}$ ve $A_{i_1} \cap A_{i_2} = \varnothing$ olduğu açıktır.

Önerme 1.1.3. Her i için $k \in \mathbb{Z}$ olmak üzere $|A_i| = 24k$ tir.

1.2 Bölüntülerin Oluşturulması

Yukarıdaki açıklamalar altında $\mathcal{H}_\pi$ kümesinin bölüntüsü aşağıdaki gibi tanımlanabilir.

Tanım 1.2.1. $p > 3$ bir asal sayı olsun. Yukarıdaki açıklamalar altında

$$P_{i_1} = A_{i_1}$$

ve

$$P_{i_2} \subset_{\neq} A_{i_2} = \{q \in A_{i_2} : q = \delta_1, N(\delta_1) = N(\delta_2) = i\} - \delta_2\mathcal{E}$$

olarak tanımlansın. Bu taktirde $\mathcal{H}_\pi$ kümesinin parçalanışı

$$P_i = P_{i_1} \cup P_{i_2}$$

olur.

Teorem 1.2.2. $\pi \in H(\mathbb{Z})$; $N(\pi) > 3$ olacak şekilde bir asal Hurwitz sayısı ve $\mathcal{H}_\pi$'nin bölüntüsü $P_{i_1}, P_{i_2}, \ldots, P_{i_n}$ olsun. Bu durumda $g_1 \in P_{i_1} = \mathcal{E}, g_2 \in P_{i_2} = (1+e_1)\mathcal{E}, \ldots, g_n \in P_{i_n}$ olmak üzere

$$H = (g_1,\ g_2,\ g_3,\ g_4,\ \cdots,\ g_n)$$

kontrol matrisine sahip $\mathcal{H}_\pi$ üzerinde tanımlı n uzunluklu bir lineer C kodu bir 1-Hurwitz ağırlıklı hataları düzeltebilen mükemmel koddur.

Yukarıdaki çalışma SCI-E kapsamındaki Mathematical Communications adlı dergide yayınlanmıştır. Bu çalışmada literatüre katılmış kodlama teorisi açısından öneme sahip birçok yeni mükemmel kodlar elde edilmiştir. Ayrıca bu çalışma, akademik topluluklara tanıtmak ve bilgilendirmek amacı ile uluslararası bir sempozyumda sunulmuştur.

BÖLÜM 2.

$A_p[w]$ Kümesi üzerinde mükemmel kodlar

(1. iş paketi, 1. ve 3. hedef):
Bu çalışmada katkısı olanlar:
Doç. Dr. Murat GÜZELTEPE

2.1. Giriş

Mükemmel kod çalışmalarımız sadece Hurwitz sayıları üzerinde değil aynı zamanda başka halkalarda da yapılmıştır. Aşağıdaki çalışmada $A_p[w]$ halkasında bir hata düzeltebilen klasik kodlar tanımlanmıştır. Ayrıca bu makalede uygun bir metrik de tanımlanmıştır.

$w=\frac{1+i\sqrt{3}}{2}, i^2=-1$ olsun. $\mathbb{Z}[w]=\{a+bw : a,b\in\mathbb{Z}\}$ ve $\pi=a+bw,$ $N(\pi)=a^2+ab+b^2=p\equiv 1(\bmod 6)$ bir asal tamsayı olmak üzere $A_p[w]$ ile $\mathbb{Z}[w]/\langle\pi\rangle$ asal kalan sınıfları gösterilsin. $A_p[w]$ kümesinin elemanları aşağıdaki metotla elde edilir.

a) $0\le r\le p-1$ olmak üzere $a+br\equiv 0(\bmod p)$ denkleminin tek çözümü r olsun.

b) $l\in\mathbb{Z}_p$ olsun. Eğer $x+sy\equiv l(\bmod p)$ denkleminin çözümlerinde $N(\alpha)=N(x+yw)$ en küçük ise $x+yw\in A_p[w]$ olur.

Bu yöntemle $\mathbb{Z}_p$ ve $A_p[w]$ bire bir ve örten bir homomorfizma kurulur.

Tanım 2.1.1. $\pi\overline{\pi}=p=a^2+ab+b^2\equiv 1(\bmod 6)$ olmak üzere $\pi=a+bw$ olsun. $\mu:\mathbb{Z}_p\to A_p[w]$

$$\mu(l)=\begin{cases} x+yw, |x|+|y|\le|x'|+|y'| \\ x'+y'\overline{w}, |x'|+|y'|<|x|+|y| \end{cases}$$

olarak tanımlanan fonksiyon $A_p[w]$ ile $\mathbb{Z}_p$ arasında birebir ve örten bir homomorfizna tanımlar.

Tanım 2.1.2. $\gamma=x+yw$ veya $x+y\overline{w}$ in $A_p[w]$ olsun. γ elemanının Mannheim ağırlığı

$W_m(\gamma) = |x| + |y|$

olarak tanımlanır. Ayrıca $\delta \equiv \alpha - \beta \ (mod\ \pi)$, $\delta \in A_p[w]$ olmak üzere α ile β arasındaki Mannheim mesafesi ise

$d_m(\alpha, \beta) = W_m(\delta)$

olarak tanımlanır.

2.2 Tekli Hataları Düzeltebilen Mükemmel Kodlar

$p = 6n+1$ bir asal sayı ve β elemanı $A_p[w]$ cisminin mertebesi $6n$ olan bir elemanı olsun. Bu durumda $A_p[w] = \langle \beta \rangle \cup \{0\}$ olur. $C \subset \left(A_p[w]\right)^n$ kodunun kontrol matrisi

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \beta^{14} & \cdots & \beta^{7(n-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \beta^{6t+1} & (\beta^{6t+1})^2 & \cdots & (\beta^{6t+1})^{(n-1)} \end{pmatrix}$$

ise bu kod tekli hataları düzeltebilen bir mükemmel kod olur.

Yukarıdaki çalışma Journal of Applied Mathematics and Computation adlı dergide “On Perfect Codes Over $A_p[w]$ ” başlığı ile yayımlanmıştır.

BÖLÜM 3.

Hurwitz sayıları üzerinde mükemmel kodlar üzerine

(1-5. iş paketleri, 1-3. hedefler):

Bu çalışmada katkısı olanlar:

Doç. Dr. Murat GÜZELTEPE

3.1 Giriş

Proje kapsamında yapılan “On some perfect code over Hurwitz integers” başlıklı çalışmamız mükemmel kodlar alanında yapılmış önemli bir çalışmadır. Bu çalışmada Hurwitz sayıları yeni bir metrikle donatılar bu metriğe göre bir hata düzeltebilen mükemmel kodlar karakterize edilmiştir. Bu çalışma aşağıdaki gibi hazırlanmıştır.

$\hat{e}_1^2 = \hat{e}_2^2 = \hat{e}_3^2 = -1$ ve $\hat{e}_1\hat{e}_2 = -\hat{e}_2\hat{e}_1 = \hat{e}_3, \hat{e}_2\hat{e}_3 = -\hat{e}_3\hat{e}_2 = \hat{e}_1, \hat{e}_3\hat{e}_1 = -\hat{e}_1\hat{e}_3 = \hat{e}_2$

ve

$$H(\mathbb{Z}) = \{a_0 + a_1\hat{e}_1 + a_2\hat{e}_2 + a_3\hat{e}_3 \,|a_0, a_1, a_2, a_3 \in \mathbb{Z}\}$$

olmak üzere

$$\mathcal{H} = H(\mathbb{Z}) \cup H(\mathbb{Z} + \frac{1}{2})$$

olarak tanımlanan Hurwitz sayıları üzerinde yapılmıştır. $\pi = a_0 + a_1\hat{e}_1 + a_2\hat{e}_2 + a_3\hat{e}_3 \in \mathcal{H}$ bir asal Hurwitz sayısı yani p bir asal tamsayı olmak üzere

$$\begin{aligned} p = \pi\pi^\star &= (a_0 + a_1\hat{e}_1 + a_2\hat{e}_2 + a_3\hat{e}_3)(a_0 - a_1\hat{e}_1 - a_2\hat{e}_2 - a_3\hat{e}_3) \\ &= a_0^2 + a_1^2 + a_2^2 + a_3^2 \end{aligned}$$

ve π’nin normu $N(\pi) = a_0^2 + a_1^2 + a_2^2 + a_3^2$ olarak tanımlanır. π’nin $\mathcal{H}$ halkasında oluşturduğu sağ ideal $\mathcal{H}$ halkasının bir normal alt grubudur ve bu alt grup

$$\langle\pi\rangle = \{\pi\delta \,|\, \delta \in \mathcal{H}\}$$

olarak tanımlanır. Bu alt gruba göre elde edilen sınıfların kümesi

$$\mathcal{H}_\pi = \mathcal{H}/\langle\pi\rangle$$

ile gösterilir.

Tanım 3.1.1. $a_0, a_1, a_2, a_3, a_0', a_1', a_2', a_3' \in \mathbb{Z}$, $a_4, a_4' \in \{\mp 1, \mp\hat{e}_1, \mp\hat{e}_2, \mp\hat{e}_3\}$ ve $w = \frac{1}{2}(1 + \hat{e}_1 + \hat{e}_2 + \hat{e}_3)$ olmak üzere $a_0 + a_1\hat{e}_1 + a_2\hat{e}_2 + a_3\hat{e}_3 + a_4 w = a_0' + a_1'\hat{e}_1 + a_2'\hat{e}_2 + a_3'\hat{e}_3 + a_4' w$ olsun. Ayrıca π bir tek asal Lipschitz sayısı, $\gamma = a_0 + a_1\hat{e}_1 + a_2\hat{e}_2 + a_3\hat{e}_3 + a_4 w \in \mathcal{H}_\pi$ ve

$$A = |a_0| + |a_1| + |a_2| + |a_3| + a_4 a_4^*,$$
$$B = |a_0'| + |a_1'| + |a_2'| + |a_3'| + a_4' a_4'^*$$

olsun. Bu durumda γ nın Hurwitz ağırlığı

$$W_{hur}(\gamma) = \begin{cases} A, & A \le B \\ B, & B < A \end{cases}$$

olarak tanımlanır. Burada $|.|$ sembolü mutlak değeri ve "*" sembolü ise verilen Hurwitz sayısının eşleniğini göstermektedir. $\alpha, \beta \in \mathcal{H}_\pi$ olsun. α ile β arasındaki Hurwitz mesafesi, $\alpha - \beta \equiv \gamma \pmod{\pi}$ olmak üzere,

$$d_{hur}(\alpha, \beta) = W_{hur}(\gamma)$$

olarak tanımlanır.
Bu mesafenin bir metrik olduğunu göstermek kolaydır.

3.2 $\mathcal{H}_\pi$ Üzerinde Bir Hata Düzeltebilen Mükemmel kodlar

$N(\pi) = p$ olmak üzere $\mathcal{H}_\pi$ nin eleman sayısı p^2 dir. n uzunluklu bir sözün (vektörün) l inci girdisinde Hurwitz ağırlığı 1 olan 24 eleman olabilir. Bu elemanlar

$$E = \{\mp 1, \mp\hat{e}_1, \mp\hat{e}_2, \mp\hat{e}_3, \mp w, \mp w^*, \mp\hat{e}_1 w, \mp\hat{e}_2 w, \mp\hat{e}_3 w, \mp\hat{e}_1 w^*, \mp\hat{e}_2 w^*, \mp\hat{e}_3 w^*\}$$

dır. Buna göre n uzunluklu, Hurwitz ağırlığı 1 olan $24n$ tane vektör vardır. Hurwitz ağırlığı sıfır olan yalnız bir vektör olduğundan, Hurwitz ağırlığı 0 veya 1 olan toplam $24n+1$ vektör vardır.

π elemanı $N(\pi) = p \ge 5$ şartını sağlayan bir Hurwitz asalı olsun. Bu durumda $\mathcal{H}_\pi$ nin

$$\mathcal{H}_\pi = \{0\} \cup G_1 \cup \cdots \cup G_{(p^2-1)/24}$$

olacak şekilde bir bölüntüsü vardır. Burada her $t \in E$ ve $i_1 \ne i_2, 1 \le i_1, i_2 \le (p^2-1)/2$ için $tG_{i_1} \ne G_{i_2}$ dir. Ayrıca

$$|G_1| = \cdots = \left|G_{(p^2-1)/24}\right| = 24$$

olur.

Örnek 3.2.1. $\pi = 2 + \hat{e}_1 + \hat{e}_2 + \hat{e}_3$ olsun. Bu durumda

$$G_1 = E = \{\mp 1, \mp\hat{e}_1, \mp\hat{e}_2, \mp\hat{e}_3, \mp w, \mp w^*, \mp\hat{e}_1 w, \mp\hat{e}_2 w, \mp\hat{e}_3 w, \mp\hat{e}_1 w^*, \mp\hat{e}_2 w^*, \mp\hat{e}_3 w^*\},$$
$$G_2 = \{\mp(1 \mp \hat{e}_1), \mp(1 \mp \hat{e}_2), \mp(1 \mp \hat{e}_3), \mp(\hat{e}_1 \mp \hat{e}_2), \mp(\hat{e}_1 \mp \hat{e}_3), \mp(\hat{e}_2 \mp \hat{e}_3)\}$$

olur.

Teorem 3.2.2. π elemanı $N(\pi) = p \geq 5$ şartını sağlayan bir Hurwitz asalı ve $\mathcal{H}_\pi$ nin bir bölüntüsü $\mathcal{H}_\pi = \{0\} \cup G_1 \cup \cdots \cup G_{(p^2-1)/24}$

şeklinde olsun. Bu durumda

$$H_{(n-k)\times n} = \left(H_0^* \middle| H_0^* \middle| H_0^* \middle| H_0^* \middle| H_0^* \middle| H_0^*\right)$$

kontrol matrisine sahip bir C, kodu $p = 5$ ve $n - k = 1$ durumu hariç diğer durumlarda $\mathcal{H}_\pi$ üzerinde $n = \dfrac{(p^2)^{n-k} - 1}{24}$ uzunluklu $1-$Hurwitz hatalarını düzeltebilen bir mükemmel kod olur. Burada

$g_i^1, \ldots, g_i^{24} \in G_i, 1 \leq i \leq 24$, $\mathcal{H}_\pi = \{0\} \cup G_1 \cup \cdots \cup G_{(p^2-1)/24}$ ve $1 \leq j_1, j_2 \leq (p^2-1)/24$ olmak üzere her $j_1 \neq j_2$ için $G_{j_1} \cap G_{j_2} = \varnothing$ dir. Ayrıca burada

$$H_0^* = \begin{pmatrix} g_i^1 & 0 & \cdots & 0 \\ 0 & g_i^1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_i^1 \end{pmatrix}, H_1^* = \begin{pmatrix} g_i^1 & 0 & 0 & 0 & 0 & \cdots & 0 \\ G_j & g_i^1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & G_j & g_i^1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & G_j & g_i^1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & G_j & g_i^1 & \cdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & & g_i^1 \\ 0 & 0 & 0 & 0 & & 0 & G_j \end{pmatrix},$$

$$H_2^* = \begin{pmatrix} g_i^1 & 0 & 0 & 0 & 0 & \cdots & 0 & & g_i^1 \\ 0 & g_i^1 & 0 & 0 & 0 & \cdots & 0 & & 0 \\ G_j & 0 & g_i^1 & 0 & 0 & \cdots & 0 & & 0 \\ 0 & G_j & 0 & \ddots & 0 & \cdots & 0 & & 0 \\ 0 & 0 & 0 & G_j & & & \vdots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & & g_i^1 & & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & G_j & & G_j \end{pmatrix},$$

$$H_3^* = \begin{pmatrix} g_i^1 & g_i^1 & g_i^1 & g_i^1 & g_i^1 & \cdots & g_i^1 & & g_i^1 \\ G_{j_1} & G_{j_1} & G_{j_1} & G_{j_1} & G_{j_1} & \cdots & G_{j_1} & & G_{j_1} \\ G_{j_2} & 0 & 0 & 0 & 0 & \cdots & 0 & & G_{j_2} \\ 0 & G_{j_2} & 0 & \ddots & 0 & \cdots & 0 & \cdots & G_{j_3} \\ 0 & 0 & 0 & 0 & & & \vdots & & \vdots \\ \vdots & \vdots & \vdots & \vdots & & & 0 & & G_{j_{n-k-1}} \\ 0 & 0 & 0 & 0 & \cdots & 0 & G_{j_2} & & 0 \end{pmatrix},$$

$$H_4^* = \begin{pmatrix} g_i^1 & g_i^1 & & g_i^1 & & g_i^1 \\ 0 & G_{j_1} & & G_{j_1} & & G_{j_1} \\ G_{j_1} & 0 & & G_{j_2} & & G_{j_2} \\ G_{j_2} & G_{j_2} & \cdots & \vdots & \cdots & \vdots \\ G_{j_3} & G_{j_3} & & G_{j_{n-k-2}} & & \\ \vdots & \vdots & & 0 & & G_{j_{n-k-1}} \\ G_{j_{n-k-1}} & G_{j_{n-k-1}} & & G_{j_{n-k-1}} & & 0 \end{pmatrix} \text{ve } H_5^* = \begin{pmatrix} g_i^1 \\ G_{j_1} \\ \vdots \\ G_{j_{n-k}} \end{pmatrix}$$

dır.

İspat: Küre-paketleme göz önüne alınırsa $N(\pi) = p \geq 5$ için

$$\left(p^2\right)^k (24n+1) = p^{2k}\left(24\frac{\left(p^2\right)^{n-k}-1}{24}+1\right) = \left(p^2\right)^n$$

olur. $1 \le j_1, j_2 \le \left(p^2-1\right)/24$ olmak üzere her $j_1 \neq j_2$ için $G_{j_1} \cap G_{j_2} = \varnothing$ olduğundan H kontrol matrisi ile tüm bir ağırlığına sahip hata vektörleri çarpılırsa farklı sendromlar oluşur. Son olarak $p=5$ ve $n-k=1$ olursa C kodunun boyutu sıfır olur. Bu ise uygun değildir.

Dekodlama prosedürü şu şekilde çalışır: Kabul edelim ki bir Hurwitz ağırlığına sahip bir hata gelen kodsözün l inci bileşeninde oluşsun. Kodsöz c, hata e ve kanaldan alınan söz r ile gösterilirse $r=c+e$ olup r nin sendromu

$$S(r)=\left(rH^T\right)^T$$

olarak hesaplanır. Eğer kanaldan alınan sözde bir hata var ise alınan sözün sendromu H kontrol matrisinin l inci sütununun bir $\theta \in E$ ile çarpımına eşittir. Bu hatanın l inci bileşende oluştuğunu ve hatanın değerinin de θ olduğunu gösterir.

Örnek 3.2.3. $\pi = 2+\hat{e}_1$ ve $n-k=2$ olsun. Bu durumda $p=5$ ve $\mathcal{H}_\pi = \{0\} \cup G_1 = \{0\} \cup E$ olur. Buna göre kontrol matrisi

$$H_{2\times 26} = \begin{pmatrix} g_1^1 & 0 & g_1^1 & g_1^1 & \cdots & g_1^1 \\ 0 & g_1^1 & g_1^2 & g_1^3 & \cdots & g_1^{24} \end{pmatrix}$$

olup

$$g_1^1 = 1, g_1^2 = -1, g_1^3 = \hat{e}_1, g_1^4 = -\hat{e}_1, g_1^5 = \hat{e}_2, g_1^6 = -\hat{e}_2, g_1^7 = \hat{e}_3, g_1^8 = -\hat{e}_3, g_1^9 = w, g_1^{10} = -w,$$
$$g_1^{11} = w^*, g_1^{12} = -w^*, g_1^{13} = w\hat{e}_1, g_1^{14} = -w\hat{e}_1, g_1^{15} = w\hat{e}_2, g_1^{16} = -w\hat{e}_2, g_1^{17} = w\hat{e}_3, g_1^{18} = -w\hat{e}_3,$$
$$g_1^{19} = w^*\hat{e}_1, g_1^{20} = -w^*\hat{e}_1, g_1^{21} = w^*\hat{e}_2, g_1^{22} = -w^*\hat{e}_2, g_1^{23} = w^*\hat{e}_3, g_1^{24} = -w^*\hat{e}_3$$

şeklinde seçilebilir. Böylece kontrol matrisi

$$H_{2\times 26} = \begin{pmatrix} 1 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 1 & -1 & \hat{e}_1 & \cdots & -w^*\hat{e}_3 \end{pmatrix}$$

olur. Kabul edelim ki kanal gönderilen kodsöz

$$c = (1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad \cdots \quad 0),$$

ve kanalda eklenen hata

$$e = (0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad w^*\hat{e}_3 \quad 0 \quad 0 \quad 0 \quad 0 \quad \cdots \quad 0)$$

olsun. Bu halde $r=c+e$ kanaldan çıkan sözün sendromu

$$S(r) = \left(rH^T\right)^T = \begin{pmatrix} 4-w^*\hat{e}_1 \\ \hat{e}_1 - w \end{pmatrix} \equiv \begin{pmatrix} w^*\hat{e}_3 \\ \hat{e}_3 \end{pmatrix} \left(\text{mod } 2+\hat{e}_1\right)$$

olarak hesaplanır. Bu sendrom kontrol matrisinin 11 inci sütunu ile $w^*\hat{e}_3$ sayısının çarpımına eşittir. Gerçekten

$$\begin{pmatrix} w^* \hat{e}_3 \\ \hat{e}_3 \end{pmatrix} = w^* \hat{e}_3 \begin{pmatrix} 1 \\ w \end{pmatrix}$$

dir. Buradan hatanın 11 inci bileşende meydana geldiği ve hatanın ağırlığının da $w^* \hat{e}_3$ olduğu anlaşılır.

3.3 $\mathcal{H}_\pi, \mathbb{Z}[\rho]$ ve $\mathbb{Z}[i]$ Üzerindeki Kodların Karşılaştırılması

Aşağıdaki tabloda görüldüğü gibi aynı uzunluklu ve aynı sayıda kodsöz içeren kodlardan $\mathcal{H}_\pi$ üzerindeki kodun minimum enerjisi $A_p[\rho]$ üzerindeki bir koddan daha iyidir.

Tablo 3.1: Ortalama enerji açısından kodların karşılaştırılması

Takım yıldızının eleman ayısı	Temel Halka	Ortalama enerji
49	$\mathcal{H}_\pi$	1,47
49	$A_p[\rho]$	7,22

Diğer yandan aynı boyutlu ve aynı uzunluklu $\mathcal{H}_\pi$ üzerindeki kodun ortalama enerjisi $\mathbb{Z}[i]$ üzerindeki kodun ortalama enerjisinden daha iyidir.

Tablo 3.2: Ortalama enerji açısından kodların karşılaştırılması

Takım yıldızının eleman ayısı	Temel Halka	Ortalama enerji
25	$\mathcal{H}_\pi$	0,96
25	$\mathbb{Z}[i]$	4,16

Şimdi de bant genişliği açısından kodlar karşılaştırılacaktır. Analog ve dijital iletişim sistemlerinin en önemli parametrelerinden biri de bant genişliğidir. Şimdiye kadar bant genişliğinin verimliliğini artırmak için birçok modülasyon çeşitleri ve kodlama teknikleri geliştirildi. İletişim ve kodlama teorisinden bilindiği gibi aynı boyutlu iki koddan kodsöz sayısı fazla olan bant genişliği daha büyük olan kanallar oluşturur. Bant genişliği ve kod hızı açısından $\mathcal{H}_\pi, A_p[\rho]$ ve $\mathbb{Z}[i]$ üzerindeki kodlar şu şekilde karşılaştırılabilir: $\mathbb{Z}[i]_\alpha$ üzerindeki kodların uzunluğu $n = \frac{p^2 - 1}{4}$, $A_p[\rho]$ üzerindeki kodların uzunluğu ise

$n=\frac{p^2-1}{6}$ ve $\mathcal{H}_\pi$ üzerindeki kodların uzunluğu ise $n=\frac{p^2-1}{24}$ tür. Eğer $p\equiv 1(\mathrm{mod}\,12)$ seçilirse, $p\equiv 1(\mathrm{mod}\,6)$ ve $p\equiv 1(\mathrm{mod}\,4)$ olur. Bu durumda $\mathcal{H}_\pi, A_p[\rho]$ ve $\mathbb{Z}[i]_\alpha$ üzerindeki sırasıyla tanımlı C_1, C_2 ve C_3 kodlarının uzunlukları sırasıyla $n_1=\frac{p^2-1}{24}$, $n_2=\frac{p^2-1}{6}$ ve $n_3=\frac{p^2-1}{6}$ olur. C_1, C_2 ve C_3 kodlarının boyutları k_1, k_2 ve k_3 değerleri k 'ya eşitse C_1 kodunun hızı olan R_1 hem C_2 kodunun hızı olan R_2 den hemde C_3 kodunun hızı olan R_3 den küçüktür. Çünkü $R_1=\frac{k_1}{n_1}=\frac{24k}{p^2-1}$, $R_2=\frac{k_2}{n_2}=\frac{6k}{p^2-1}$ ve $R_3=\frac{k_3}{n_3}=\frac{4k}{p^2-1}$ dir. örneğin $p=13$ ve $k=1$ olsun. Bu durumda $R_1=\frac{1}{7}, R_2=\frac{1}{28}$ ve $R_3=\frac{1}{42}$ olur. Bu da C_1 kodunun hızının C_2 ve C_3 kodundan daha hızlı olduğunu gösterir.

Bu çalışma Mathematical Advances in Pure and Applied Sciences adlı dergimizde “On Some Perfect Codes over Hurwitz Integers” başlığı ile yayımlanmıştır.

BÖLÜM 4.

Döngüsel çizge yardımı ile Hurwitz sayıları üzerinde mükemmel kodlar

(1,2,3,4. iş paketleri, 1,2 ve 3. hedefler):
Bu çalışmada katkısı olanlar:
Doç. Dr. Murat GÜZELTEPE
Gökhan GÜNER (Yüksek Lisans öğrencimiz projeye dışardan destek olmuştur).

4.1 Giriş

Son yıllarda birçok araştırmacı Gauss, Lipschitz ve Hurwitz sayıları üzerinde yeni kodlar inşa etmişlerdir. Bu kümeler üzerinde kod inşaa etmeye çalışılmasının temel nedeni, bu kodların dördül genlik modülasyonuna (Quadrature Amplitude Modulation, kısaca QAM) göre Hamming metriğine ve Lee metriğine göre yazılmış kodlardan daha iyi performans sağlamasıdır. 1996 yılında Huber Gauss tamsayılar kümesi üzerinde Mannheim metriğini tanımlayarak bu küme üzerinde bir hata düzeltebilen mükemmel kodlar elde etti [1]. Bu çalışmadan esinlenerek, Huberin bu çalışması Lipschitz sayıları üzerine aktarıldı [1, 8, 9, 10, 11]. Lipschitz sayılarına aktarılan bu kodların QAM için ortalama enerji, bant genişliği ve kod hızı açısından Huber' in kodlarından daha iyi olduğu gösterildi. Daha sonra Lipschitz sayıları üzerinde mükemmel kod bulmak için [12]' da Cayley Çizge kullanıldı ve $t=1$ için mükemmel kodlar tanımlandı.

2013 yılında [5]' de, Hurwitz sayıları üzerinde ilk lineer kodlar tanımlandı ve bu kodların ortalama enerji, bant genişliği ve kod hızı açısından literatürdeki kodlardan daha iyi olduğu gösterildi. Daha sonra Lipschitz ve Hurwitz üzerinde bir çok mükemmel kod bulma yöntemi [12, 13, 14, 15]' de verilmiştir.

Bu çalışmada [8]' de verilmiş olan çizge kuramı kullanılarak Hurwitz sayıları üzerinde $t-$hata düzeltebilen mükemmel kodlar elde edilmiştir. [13, 15]' de Hurwitz sayıları üzerinde bir hata düzeltebilen mükemmel kodlar karakterize edilmiştir.

Ayrıca [5, 13, 15]' de, α asal Hurwitz sayısı olarak alınmasına karşın bu çalışmada α asal değildir. Üstelik bu çalışmada sadece bir hata düzeltebilen mükemmel kodlar değil, aynı zamanda $t-$hata düzeltebilen mükemmel kodlar karakterize edilmiştir.

4.2. $\mathcal{H}_{\alpha}$ Kümesi ve Özellikleri

Tanım 4.2.1. $\mathbb{H}=\{a_0+a_1i+a_2j+a_3k : a_0,a_1,a_2,a_3 \in \mathbb{R}\}$ ile gösterilen Hamilton Kuaterniyonlar kümesi; $\mathbb{R}$ reel sayılar kümesi üzerinde bir serbest modüldür. Bu modülün bazları $1, i, j, k$ dır ve bu bazlar aşağıdaki gibi tanımlanır.

1, $\mathbb{R}$ nin birim elemanı olmak üzere;

1) $i^2=j^2=k^2=-1$,

2) $ij=-ji=k;\ jk=-kj=i;\ ki=-ik=j$

dir.

Ayrıca $q=a_0+a_1i+a_2j+a_3k \in H$ Kuaterniyonunun eşleniği q^* ile gösterilir ve $q^*=a_0-a_1i-a_2j-a_3k$ olarak tanımlanır.

$\mathbb{H}$ üzerinde $q=a_0+a_1i+a_2j+a_3k \in H$ sayısının normu

$N(q)=qq^*=a_0^2+a_1^2+a_2^2+a_3^2$

dir.

Bu norm çarpımsal normdur. Yani

$N(q_1q_2)=N(q_1)N(q_2)$

dir [12].

Tanım 4.2.2. Lipschitz tamsayıları

$\mathbb{H}[\mathbb{Z}]=\{a_0+a_1i+a_2j+a_3k : a_0,a_1,a_2,a_3 \in \mathbb{Z}\}$

olarak tanımlanır [12].

Tanım 4.2.3. Hurwitz sayıları $\mathcal{H}$ ile gösterilir ve

$$\mathcal{H} = \mathbb{H}[\mathbb{Z}] \cup \mathbb{H}\left[\mathbb{Z} + \frac{1}{2}\right]$$
$$= \left\{ \frac{a_0 + a_1 i + a_2 j + a_3 k}{2} : a_0 \equiv a_1 \equiv a_2 \equiv a_3 \pmod 2, a_0, a_1, a_2, a_3 \in \mathbb{Z} \right\}$$

şeklinde tanımlanır [16].

Hamilton Quaternionları üzerinde yukarıda tanımlanan $N(q)$ norm fonksiyonu ve özellikleri Hurwitz sayıları için de geçerlidir.

Tanım 4.2.4. Eğer bir Hurwitz sayısının normu tek tamsayı ise bu sayıya tek Hurwitz sayısı, eğer normu çift tamsayı ise çift Hurwitz sayısı denir.

Bu bölümde yalnızca tek Hurwitz sayıları kullanılacaktır.

Örnek 4.2.1.

$2 + i = 2 + i + 0j + 0k \in \mathcal{H}$ dır.

$\frac{3}{2} + \frac{k}{2} = \frac{3}{2} + 0.\frac{i}{2} + 0.\frac{j}{2} + \frac{k}{2} \notin \mathcal{H}$ dır.

$\frac{11}{2} + i + \frac{3j}{2} + \frac{k}{2} \notin \mathcal{H}$ dır.

$\frac{1}{2} - \frac{3i}{2} + \frac{7j}{2} - \frac{k}{2} \in \mathcal{H}$ dır.

Tanım 4.2.5. $q_1, q_2 \in \mathcal{H}$ olsun. $q_1 - q_2 = \alpha\delta$ olacak şekilde $\exists\, \delta \in \mathcal{H}$ var ise α modülüne göre q_1, q_2 ye soldan denktir denir ve $q_1 \equiv_\ell q_2 \pmod \alpha$ şeklinde gösterilir.

Not 4.2.1. Bu çalışmada sol denklik kullanılacaktır. Benzer sonuçlar sağ denklik kullanılarak da elde edilebilir.

Tanım 4.2.6. $0 \neq \alpha \in \mathcal{H}$ bir tek Hurwitz sayısı olsun. α nın ürettiği sağ ideal $\langle \alpha \rangle = \{\alpha.\lambda : \lambda \in \mathcal{H}\}$ olarak tanımlanır. Bu ideale göre kalan sınıflarının oluşturduğu küme $\mathcal{H}_\alpha$ ile gösterilir.

Teorem 4.2.1. $\mathcal{H}_\alpha$ bir değişmeli gruptur ve $\mathcal{H}_\alpha$, $\mathcal{H}$ üzerinde bir sağ modüldür [12].

Teorem 4.2.2. $0 \neq \alpha \in \mathcal{H}$ ise $\mathcal{H}_\alpha$, $N(\alpha)^2$ elemana sahiptir [12].

Örnek 4.2.2. $\alpha = 1+2j$ için $N(\alpha)^2 = \left(1^2+2^2\right)^2 = 5^2 = 25$ dir. Bu yüzden $\mathcal{H}_\alpha$ 25 elemanlıdır ve

$$\begin{aligned}\mathcal{H}_{1+2j} = \{&0,1,-1,i,-i,j,-j,k,-k,\frac{1}{2}+\frac{i}{2}+\frac{j}{2}+\frac{k}{2},-\frac{1}{2}+\frac{i}{2}+\frac{j}{2}+\frac{k}{2},\frac{1}{2}-\frac{i}{2}+\frac{j}{2}+\frac{k}{2},\\ &\frac{1}{2}+\frac{i}{2}-\frac{j}{2}+\frac{k}{2},\frac{1}{2}+\frac{i}{2}+\frac{j}{2}-\frac{k}{2},-\frac{1}{2}-\frac{i}{2}+\frac{j}{2}+\frac{k}{2},-\frac{1}{2}+\frac{i}{2}-\frac{j}{2}+\frac{k}{2},-\frac{1}{2}+\frac{i}{2}+\frac{j}{2}-\frac{k}{2},\\ &\frac{1}{2}-\frac{i}{2}-\frac{j}{2}+\frac{k}{2},\frac{1}{2}-\frac{i}{2}+\frac{j}{2}-\frac{k}{2},\frac{1}{2}+\frac{i}{2}-\frac{j}{2}-\frac{k}{2},-\frac{1}{2}-\frac{i}{2}-\frac{j}{2}+\frac{k}{2},-\frac{1}{2}-\frac{i}{2}+\frac{j}{2}-\frac{k}{2},\\ &-\frac{1}{2}+\frac{i}{2}-\frac{j}{2}-\frac{k}{2},\frac{1}{2}-\frac{i}{2}-\frac{j}{2}-\frac{k}{2},-\frac{1}{2}-\frac{i}{2}-\frac{j}{2}-\frac{k}{2}\}\end{aligned}$$

olur.

Not 4.2.2. $a \in \mathcal{H}_\alpha$ olsun. a nın sınıfındaki bazı elemanların normu ile a nın normu eşit çıkabilir. Bu sebeple a nın sınıfındaki normu en küçük olan elemanlardan herhangi biri tam temsilci olarak seçilebilir. Örneğin $\alpha = 1+3i+2j+k$ alınırsa $a = \frac{3}{2}+\frac{1}{2}i+\frac{3}{2}j+\frac{1}{2}k$ elemanının sınıfında $-2+k$ elemanı da bulunmaktadır. Yani $\overline{\frac{3}{2}+\frac{1}{2}i+\frac{3}{2}j+\frac{1}{2}k} = \overline{-2+k}$ dır. Bu sınıfta normu 5 olan yalnız bu iki eleman vardır. Bu sınıftaki diğer elemanların normu 5 ten büyüktür. Dolayısı ile tam temsilci olarak $\frac{3}{2}+\frac{1}{2}i+\frac{3}{2}j+\frac{1}{2}k$ veya $-2+k$ elemanlarından herhangi biri seçilebilir. Denk olan bu elemanlar matematiksel olarak $\phi \in \mathcal{H}$ olmak üzere $a+\alpha.\phi \equiv -2+k \pmod{\alpha}$ şeklinde kontrol edilebilir. Bu kontrol Mathematica programı kullanılarak aşağıdaki gibi yapılır.

```
<< Quaternions`
Mod[Quaternion[3/2, 1/2, 3/2, 1/2], Quaternion[1, 3, 2, 1]]
Mod[Quaternion[3/2, 1/2, 3/2, 1/2] + Quaternion[1, 3, 2, 1] ** Quaternion[1/2, 1/2, 1/2, 1/2], Quaternion[1, 3, 2, 1]]
Mod[Quaternion[3/2, 1/2, 3/2, 1/2] + Quaternion[1, 3, 2, 1] ** Quaternion[-1/2, 1/2, 1/2, 1/2], Quaternion[1, 3, 2, 1]]
Mod[Quaternion[3/2, 1/2, 3/2, 1/2] + Quaternion[1, 3, 2, 1] ** Quaternion[1, 0, 0, 0], Quaternion[1, 3, 2, 1]]
Mod[Quaternion[3/2, 1/2, 3/2, 1/2] + Quaternion[1, 3, 2, 1] ** Quaternion[-1, 1, 0, 0], Quaternion[1, 3, 2, 1]]

Quaternion[3/2, 1/2, 3/2, 1/2]
Quaternion[-2, 0, 0, 1]
Quaternion[-2, 0, 0, 1]
Quaternion[3/2, 1/2, 3/2, 1/2]
Quaternion[3/2, 1/2, 3/2, 1/2]
```

Teorem 4.2.3. $0 \neq \alpha \in \mathcal{H}$, $\beta \in \mathcal{H}_\alpha$ ve β , α nın sol böleni olsun.

Buna göre $\langle \beta \rangle$ ile gösterilen β elemanının ürettiği alt grubun eleman sayısı

$$\left|\langle \beta \rangle\right| = \frac{N(\alpha)^2}{N(\beta)^2}$$

dir.

İspat: $\mathcal{H}_\alpha$ nın eleman sayısı $N(\alpha)^2$ ve $\mathcal{H}_\beta$ nın eleman sayısı $N(\beta)^2$ dir. $\beta \mid \alpha$ seçildiğinden Lagrange teoremine göre β nın $\mathcal{H}_\alpha$ içinde ürettiği alt grubun eleman sayısı

$$\left|\langle \beta \rangle\right| = \frac{\left|\mathcal{H}_\alpha\right|}{\left|\mathcal{H}_\beta\right|} = \frac{N(\alpha)^2}{N(\beta)^2}$$

dir.

Örnek 4.2.3. $\alpha = (2+i)(1+i+j) = 1+3i+2j+k$ olsun. $\beta = 2+i$, α nın sol böleni olup

$$\langle \beta \rangle = \{0, 2+i, -2-i, -1+2i, 1-2i, 2j+k, -2j-k, -j+2k, j-2k\}$$

dır.

$$\left|\langle \beta \rangle\right| = 9 = \frac{N(\alpha)^2}{N(\alpha)^2} = \frac{\left(1^2+3^2+2^2+1^2\right)^2}{\left(2^2+1^2\right)^2} = \frac{15^2}{5^2} = 3^2$$

dir.

Tanım 4.2.7. $\beta,\gamma\in\mathcal{H}_\alpha$ olsun. μ elemanı $\beta-\gamma$ nın denklik sınıfındaki normu en küçük eleman olsun. β ile γ arasındaki mesafe $d_\alpha(\beta,\gamma)=N(\mu)$ olarak tanımlanır.

Örnek 4.2.4. $\alpha=1+3i+2j-k$, $\beta=2+i+j$ ve $\gamma=\frac{1}{2}+\frac{i}{2}+\frac{j}{2}-\frac{k}{2}$ için

$\beta-\gamma=\mu=\frac{3}{2}+\frac{i}{2}+\frac{j}{2}+\frac{k}{2}=\frac{3}{2}+\frac{i}{2}+\frac{j}{2}+\frac{k}{2}\pmod{\alpha}$ olduğundan

$d_\alpha(\beta,\gamma)=\left(\frac{3}{2}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2=3$ dür.

Örnek 4.2.5. $\alpha=1+3i+2j-k$, $\beta=1+i+j$, $\gamma=2+j$ için

$\beta-\gamma=-1+i\equiv-1+i\pmod{\alpha}$ olup $d_\alpha(1+i+j,2+j)=(-1)^2+(1)^2=2$ dir.

Örnek 4.2.6. $\alpha=1+3i+2j-k$, $\beta=2-i$, $\gamma=-2i-k$ için

$\beta-\gamma=2+i+k\equiv-2+i\pmod{\alpha}$ olduğundan $d_\alpha(2-i,-2i-k)=(-2)^2+(1)^2=5$

olarak bulunur.

Örnek 4.2.7. $\sigma,\tau\in\mathcal{H}_{1+2i}$, $\sigma=-\frac{1}{2}+\frac{i}{2}-\frac{j}{2}+\frac{k}{2}$, $\tau=-i$ için

$\sigma-\tau=-\frac{1}{2}+\frac{3i}{2}-\frac{j}{2}+\frac{k}{2}\equiv-\frac{1}{2}-\frac{i}{2}-\frac{j}{2}-\frac{k}{2}\pmod{(1+2j)}$ dir. Buna göre

$d_{1+2j}(\sigma,\tau)=\left(-\frac{1}{2}\right)^2+\left(-\frac{1}{2}\right)^2+\left(-\frac{1}{2}\right)^2+\left(-\frac{1}{2}\right)^2=\frac{4}{4}=1$ dir.

Tanım 4.2.8. $\beta\in\mathcal{H}_\alpha$ nın ağırlığı $w_\alpha(\beta)$ ile gösterilir ve $w_\alpha(\beta)=d_\alpha(\beta,0)$ olarak tanımlanır.

Bu tanıma göre $a\equiv b\equiv c\equiv d\pmod{2}$ olmak üzere $\lambda=\frac{a}{2}+\frac{b}{2}i+\frac{c}{2}j+\frac{d}{2}k\in\mathcal{H}_\alpha$ elemanının ağırlığının 1 ve 2 olması durumunda λ değerleri aşağıdaki gibi bulunur.

$w_\alpha(\lambda)=d_\alpha(\lambda,0)=1$ ise $N(\lambda)=\frac{a^2}{4}+\frac{b^2}{4}+\frac{c^2}{4}+\frac{d^2}{4}=1$ dir. Buna göre $a^2+b^2+c^2+d^2=4$ olup iki farklı durum söz konusudur. Ya a,b,c ve d sayılarından herhangi biri ∓ 2 ve diğerleri 0 ya da a,b,c ve d sayılarının herbiri ∓ 1 olur.

Bu durumda ağırlığı 1 olan 24 elemanın 8 tanesi $\mp 1, \mp i, \mp j, \mp k$ ve 16 tanesi $\mp\frac{1}{2}\mp\frac{i}{2}\mp\frac{j}{2}\mp\frac{k}{2}$ dir.

$w_\alpha(\lambda)=d_\alpha(\lambda,0)=2$ ise $N(\lambda)=\frac{a^2}{4}+\frac{b^2}{4}+\frac{c^2}{4}+\frac{d^2}{4}=2$ dir. Buradan $a^2+b^2+c^2+d^2=8$ olur. Buna göre a,b,c ve d sayılarından herhangi ikisi ∓ 2 ve diğerleri 0 olmalıdır.

Örneğin $a=b=\mp 2$ için λ, $1+i, 1-i, -1+i,$ veya $-1-i$ den biri olur. Buna göre ağırlığı 2 olan 24 eleman $\mp 1\mp i, \mp 1\mp j, \mp 1\mp k, \mp i\mp j, \mp i\mp k, \mp j\mp k$ dır.

Not 4.2.3. d_α bazı durumlarda üçgen eşitsizliğini sağlamaz. Fakat bu durumda α ya göre sol denklik sınıfından yararlanılabilir.

Örneğin $\alpha=7+12i$, $\beta=2-6i$, $\gamma=3+2i$ ve $\lambda=2-5i$ için $d_\alpha(\beta,\gamma)\le d_\alpha(\beta,\lambda)+d_\alpha(\lambda,\gamma)$ eşitsizliğinde $\beta-\lambda=-i$, $\lambda-\gamma=-1-7i$ ve $\beta-\gamma=-1-8i\equiv_\ell 6+4i \pmod{\alpha}$ dır. $6^2+4^2\le(-1)^2+\left((-1)^2+(-7)^2\right)$ olduğundan $52\le 51$ çelişkisi oluşur. Ancak sağ denklik sınıfındaki $6+4i$ sayısına sol denklik sınıfında $-\frac{7}{2}+\frac{3i}{2}-\frac{5j}{2}+\frac{9k}{2}$ sayısı karşılık gelir ve bu sayının normu da $\frac{49+9+25+81}{4}=\frac{164}{4}=41$ olup $41<51$ elde edilir.

Bu durum her $\alpha\in\mathcal{H}$ için meydana gelmemektedir. Bu problemden kaçınmak için uygun elemanlar seçilmelidir.

4.3. Hurwitz Sayıları Üzerinde Mükemmel Kümeler ve Mükemmel Kodlar

Tanım 4.3.1. $0\neq\alpha\in\mathcal{H}$ tek Hurwitz sayısı olsun.

1) $V=\mathcal{H}_\alpha$ köşelerin kümesi ve

2) $E=\{(\lambda,\gamma)\in V\times V : d_\alpha(\lambda,\gamma)=1\}$ kümesi kenarların kümesi olarak alınırsa $G_\alpha(V,E)$ bir çizge tanımlar.

$\gamma\in\mathcal{H}_\alpha$ olmak üzere γ ya 1 birim uzaklıkta olan elemanlar, ağırlığı 1 olan 24 elemanın teker teker γ ya eklenmesi ile bulunur.

Düzenli çizge $C_{N(\alpha)^2}(j_1,j_2,\ldots,j_{12})$ çizgesidir. Bu durumda $N(\alpha)=a_0^2+a_1^2+a_2^2+a_3^2=2m+1,\ m\in\mathbb{Z}$ olarak alınacaktır.

Teorem 4.3.1. $e_1\in\{i,j,k\}$ ve $\alpha=a_0+a_1i+a_2j+a_3k=(a_0+a_1i)+(a_2+a_3i)e_1\in\mathcal{H}$ olmak üzere α bir tek Hurwitz sayısı olsun. Bu durumda $C_{N(\alpha)^2}(j_1,j_2,\ldots,j_{12})$ ile G_α izomorf çizgelerdir ve çizge izomorfizması; $x_1,y_1,x_2,y_2\in\mathbb{Z}_{N(\alpha)}$ ve $q_1=a_0x_1+a_1y_1 \pmod{N(\alpha)}$, $q_2=a_2x_2+a_3y_2 \pmod{N(\alpha)}$ olmak üzere

$$\begin{aligned}\psi:\mathbb{Z}_{N(\alpha)}\times\mathbb{Z}_{N(\alpha)}&\to\mathcal{H}_\alpha\\ (q_1,q_2)&\mapsto(x_1+y_1i)+(x_2+y_2i)e_1 \pmod{\alpha}\end{aligned}$$

olarak tanımlanır.

İspat: G_α çizgesinin köşeleri $\mathcal{H}_\alpha$ kümesinden ve $C_{N(\alpha)^2}(j_1,j_2,\ldots,j_{12})$ köşeleri ise $\mathbb{Z}_{N(\alpha)}\times\mathbb{Z}_{N(\alpha)}$ kümesinden seçileceğinden ispat için $\mathcal{H}_\alpha$'nın $\mathbb{Z}_{N(\alpha)}\times\mathbb{Z}_{N(\alpha)}$'ya izomorf olduğunu göstermek yeterlidir. $\mathcal{H}_\alpha$ ve $\mathbb{Z}_{N(\alpha)}\times\mathbb{Z}_{N(\alpha)}$ toplamsal değişmeli grup olup bu grupların bazları sırası ile $e_1,e_2\in\{1,i,j,k\}$ ve $(1,0),(0,1)$ olarak seçilebilir.

$$\begin{aligned}\psi:\mathbb{Z}_{N(\alpha)}\times\mathbb{Z}_{N(\alpha)}&\to\mathcal{H}_\alpha\\ (1,0)&\mapsto e_1\\ (0,1)&\mapsto e_2\end{aligned}$$

fonksiyonunu göz önüne alalım. Bu fonksiyonun birebir ve örten bir grup izomorfizması olduğu açıktır. Şöyle ki; $(a_1,b_1),(a_2,b_2)\in\mathbb{Z}_{N(\alpha)}\times\mathbb{Z}_{N(\alpha)}$ olmak üzere;

$$\begin{aligned}\psi((a_1,b_1)+(a_2,b_2))&=\psi((a_1+a_2,b_1+b_2))\\ &=(a_1+a_2)e_1+(b_1+b_2)e_2\\ &=\psi((a_1,b_1))+\psi((a_2,b_2))\end{aligned}$$

ve

$$\psi\left(\left(a_1,b_1\right)\right)=\psi\left(\left(a_2,b_2\right)\right)$$
$$\Rightarrow a_1e_1+b_1e_2=a_2e_1+b_2e_2$$
$$\Rightarrow \left(a_1,b_1\right)\equiv\left(a_2,b_2\right)\left(\mathrm{mod}\ N\left(\alpha\right)\right)$$

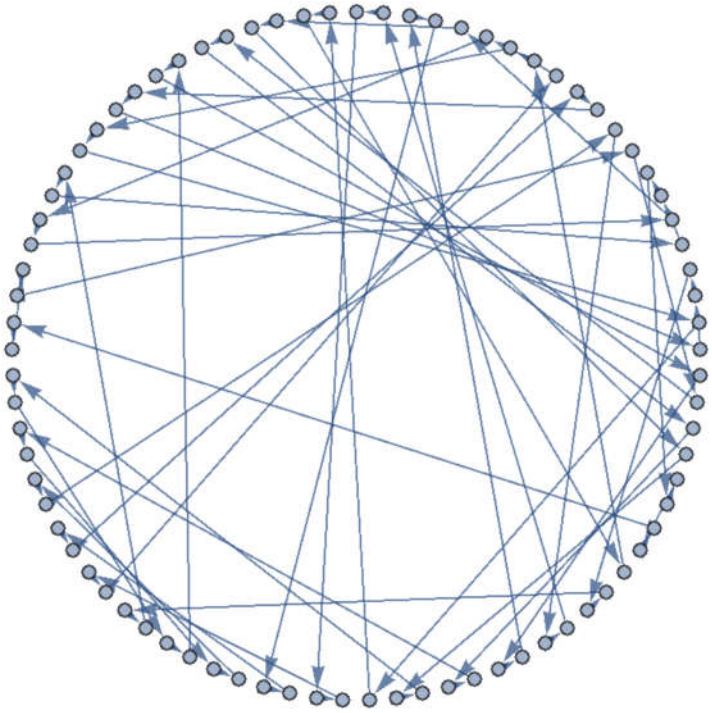
dir.

O halde $\mathcal{H}_\alpha$ ve $\mathbb{Z}_{N(\alpha)}\times\mathbb{Z}_{N(\alpha)}$ izomorf gruplardır.

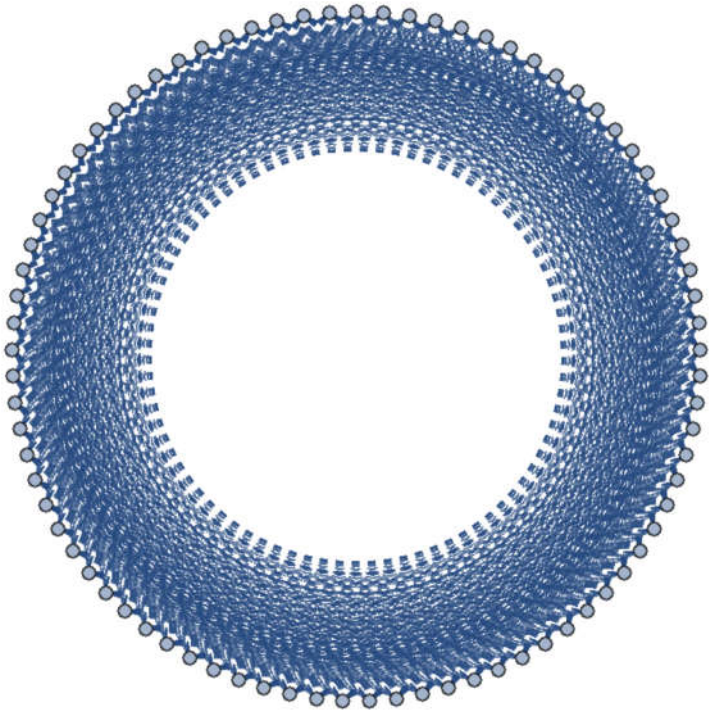
Bu fonksiyonun iyi tanımlı olduğu [15]' de gösterilmiştir.

Örnek 4.3.1. Aşağıda Wolfram Mathematica programı kullanılarak sırası ile $G_{-1+2i+2j}$ ve $C_{81}\left(13,14,\ldots,24\right)$ çizgeleri oluşturulmuştur.

```
<< Quaternions`
α = Quaternion [-1, 2, 2, 0]; k = Norm [α]; A = Table [1, {k}]; Do [ A [[n]] = n, {n, 1, k}]
B = Quaternion [0, 0, 1, 0] * A; GG = Table [1, {k ^ 2}];
Do [Do [GG [[n + k * (m - 1)]] = A [[n]] + B [[m]], {n, 1, k}], {m, 1, k}];
Hα = Table [1, {k ^ 2}]; (*Hα denotes the Hα*)
Do [Hα [[tt]] = Mod [GG [[tt]], α], {tt, 1, k ^ 2}];
MatrixForm [Hα];
BB = Table [1, {k ^ 2}, {4}];
Do [BB [[t, 1]] = Hα [[t, 1]]; BB [[t, 2]] = Hα [[t, 2]]; BB [[t, 3]] = Hα [[t, 3]]; BB [[t, 4]] = Hα [[t, 4]];
  , {t, 1, k ^ 2}];
KK = Table [1, {k ^ 2 - 1}];
Do [KK [[t]] = BB [[t]] → BB [[t + 1]], {t, 1, k ^ 2 - 1}];
KKK = Union [KK, {{0, 0, 0, 0} → {1, 0, 1, 0}}];
G = Graph [KKK, VertexLabelStyle → Directive [Red, Italic, 11], VertexSize → 0.5]
(*The graph G shows G-1+2i+2j.*)
G = CirculantGraph [81, {13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24}, VertexSize → 0.5, EdgeStyle → Dashed ]
EdgeCount [G]
GraphDiameter [G]
```



Şekil 4.1. $G_{-1+2i+2j}$ çizgesi



Şekil 4.2. $G_{1+3i+2j+k}$ Çizgesi.

$\varepsilon = \left\{ \mp 1, \mp i, \mp j, \mp k, \mp\frac{1}{2} \mp \frac{i}{2} \mp \frac{j}{2} \mp \frac{k}{2} \right\}$ kümesi çarpma işlemine göre bir değişmeli olmayan gruptur.

Önerme 4.3.1. α bir tek Hurwitz sayısı, $\rho_1, \rho_2 \in \varepsilon$ ve $\beta_1, \beta_2 \in \mathcal{H}$ olsun. Eğer

$$\beta_1 \equiv \beta_2 \pmod{\alpha}$$

ise

$$\rho_1\beta_1\rho_2 \equiv \rho_1\beta_2\rho_2 \pmod{\rho_1\alpha\rho_2}$$

olur.

İspat: Eğer $\beta_1 \equiv \beta_2 \pmod{\alpha}$ ise $\beta_2 = \beta_1 + \alpha\delta$ olacak şekilde $\delta \in \mathcal{H}$ vardır. Bu eşitliğin her iki yanı soldan ρ_1 ve sağdan ρ_2 ile çarpılırsa

$$\begin{aligned}
\rho_1\beta_2\rho_2 &= \rho_1(\beta + \alpha\delta)\rho_2 \\
&= \rho_1(\beta)\rho_2 + \rho_1(\alpha\delta)\rho_2 \\
&= \rho_1(\beta)\rho_2 + \rho_1\left(\alpha\left(\rho_2\rho_2^{-1}\right)\delta\right)\rho_2 \\
&= \rho_1(\beta)\rho_2 + (\rho_1\alpha\rho_2)\left(\rho_2^{-1}\delta\rho_2\right) \\
&= \rho_1(\beta)\rho_2 + (\rho_1\alpha\rho_2)\delta_1, \delta_1 = \rho_2^{-1}\delta\rho_2 \in \varepsilon \\
&= \rho_1(\beta)\rho_2 + (\rho_1\alpha)\rho_2\delta_1 \\
&= \rho_1(\beta)\rho_2 + (\rho_1\alpha)\rho_3, \rho_3 = \rho_2\delta_1 \in \varepsilon \\
&= \rho_1(\beta)\rho_2 + (\rho_1\alpha\rho_3)
\end{aligned}$$

elde edilir. Bu da

$$\rho_1\beta_1\rho_2 \equiv \rho_1\beta_2\rho_2 \pmod{\rho_1\alpha\rho_2}$$

olduğunu gösterir.

Önerme 4.3.2. α bir tek Hurwitz sayısı olsun. Eğer $\{\varepsilon = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r\}$ kümesi $\mathcal{H}_\alpha$ nın bir bölüntüsü ise $\{\rho_1\varepsilon\rho_2, \rho_1\varepsilon_2\rho_2, \ldots, \rho_1\varepsilon_r\rho_2\}$ kümesi de $\mathcal{H}_{\rho_1\alpha\rho_2}$ kümesinin bir bölüntüsü olur.

İspat: $\rho_1, \rho_2 \in \varepsilon$ olmak üzere, kabul edelim ki $\rho_1\varepsilon\rho_2 \cap \rho_1\varepsilon_2\rho_2 \neq \varnothing$ olsun. Bu durumda $a \in \rho_1\varepsilon\rho_2$ ve $a \in \rho_1\varepsilon_2\rho_2$ olacak şekilde en az bir $a \in \mathcal{H}_\alpha$ vardır. $a \in \rho_1\varepsilon\rho_2$ ve $a \in \rho_1\varepsilon_2\rho_2$ ise sırası ile $a = \rho_1 b\rho_2$ ve $a = \rho_1 c\rho_2$ olacak şekilde $b \in \varepsilon, c \in \varepsilon_2$ ve $\rho_1, \rho_2 \in \varepsilon$ vardır. ε bir çarpımsal grup olduğundan

$a = \rho_1 c \rho_2 \Rightarrow c = \rho_1^{-1} a \rho_2^{-1} \in \varepsilon$

bulunur. Buradan $c \in \varepsilon$ ve $c \in \varepsilon_2$ olup $\varepsilon \cap \varepsilon_2 \neq \varnothing$ çelişkisi olur.

Aşağıdaki önermenin ispatı Önerme 3.2.1. ve Önerme 3.2.2.' den açıktır.

Önerme 4.3.3. $\alpha_1, \alpha_2 \in \mathcal{H}$ olsun. $G_{\alpha_1} \cong G_{\alpha_2}$ olması için gerek ve yeter şart $\alpha_1 = \rho_1 \alpha_2 \rho_2$ olacak şekilde $\rho_1, \rho_2 \in \varepsilon$ sayılarının var olmasıdır.

Örnek 4.3.2. $\alpha_1 = 1 + 3i + 2j + k$ olsun. $j\alpha_1 = j(1 + 3i + 2j + k) = -2 + i + j - 3k = \alpha_2$ olarak seçilirse $G_{\alpha_1} \cong G_{\alpha_2}$ olur.

Tanım 4.3.2. $\alpha \in \mathcal{H}$ olsun. $t \in \mathbb{N}$ için G_α içinde γ merkezli ve t yarıçaplı bir yuvar

$B_t(\gamma) = \{\lambda \in \mathcal{H}_\alpha : d_\alpha(\lambda, \gamma) \leq t\}$

olarak tanımlanır.

Eğer $\lambda \in B_t(\gamma)$ ise γ köşesi λ köşesine $t-$ baskındır denir.

Örnek 4.3.3. $\alpha = 1 + 3i + 2j + k$ olmak üzere $G_{1+3i+2j+k}$ içinde $\gamma = -2j - k$ merkezli ve $t = 1$ yarıçaplı $B_1(-2j - k)$ yuvarı aşağıdaki şekilde bulunur.

Yukarıdaki tanıma göre $B_1(-2j - k) = \{\lambda \in \mathcal{H}_{1+3i+2j+k} : d_{1+3i+2j+k}(\lambda, -2j - k) \leq 1\}$ dir.

Burada birbiri ile karışmaması için λ değerleri indislenmiştir.

$t = 0 \Rightarrow d_\alpha(\lambda, -2j - k) = 0$ olduğundan $\gamma = \lambda_1 = -2j - k$ olup $-2j - k \in B_1(-2j - k)$ dır.

$t = 1 \Rightarrow d_\alpha(\lambda, -2j - k) = 1$ olduğundan $-2j - k$ elemanına ağırlığı 1 olan elemanlar eklenerek α modülosuna göre kalan işlemi yapıldığında λ değerleri aşağıdaki gibi bulunur.

$$\lambda_2 = (-2j - k) - 1 = -1 - 2j - k \equiv \frac{1}{2} - \frac{i}{2} + \frac{j}{2} + \frac{3k}{2} \left(\mathrm{mod}\left(1 + 3i + 2j + k\right)\right)$$

$\Rightarrow \frac{1}{2}-\frac{i}{2}+\frac{j}{2}+\frac{3k}{2} \in B_1(-2j-k)$ olur.

$$\lambda_3 = (-2j-k)+1 = 1-2j-k \equiv -\frac{1}{2}+\frac{i}{2}+\frac{3j}{2}-\frac{k}{2} \pmod{(1+3i+2j+k)}$$

$\Rightarrow -\frac{1}{2}+\frac{i}{2}+\frac{3j}{2}-\frac{k}{2} \in B_1(-2j-k)$ olup, benzer şekilde işlemler yapıldığında $-2j-k \in \mathcal{H}_\alpha$ nın 1 baskın olduğu küme

$$B_1(\gamma) = \{-2j-k, -\frac{1}{2}+\frac{i}{2}+\frac{3j}{2}-\frac{k}{2}, \frac{1}{2}-\frac{i}{2}+\frac{j}{2}+\frac{3k}{2}, \frac{3}{2}+\frac{i}{2}+\frac{j}{2}+\frac{3k}{2}, 1+2i, -j-k,$$
$$-\frac{3}{2}+\frac{i}{2}+\frac{j}{2}-\frac{k}{2}, -2j, \frac{3}{2}-\frac{i}{2}+\frac{j}{2}+\frac{k}{2}, \frac{1}{2}+\frac{i}{2}-\frac{3j}{2}-\frac{k}{2}, -\frac{1}{2}+\frac{i}{2}-\frac{3j}{2}-\frac{k}{2}, \frac{1}{2}-\frac{i}{2}-\frac{3j}{2}-\frac{k}{2},$$
$$-1+i+j, \frac{1}{2}+\frac{i}{2}-\frac{3j}{2}-\frac{3k}{2}, -\frac{1}{2}-\frac{i}{2}-\frac{3j}{2}-\frac{k}{2}, \frac{1}{2}-\frac{3i}{2}+\frac{j}{2}-\frac{3k}{2}, 1+j+k, -1+j,$$
$$\frac{1}{2}-\frac{i}{2}-\frac{3j}{2}-\frac{3k}{2}, -1+i+j-k, -2+j, 1-i+j+k, 1+k, -1+j-k, 1-i+k\}$$

olarak bulunur.

Burada $-2j-k$ köşesi $B_1(-2j-k)$ kümesindeki elemanlara $1-$ baskındır.

Tanım 4.3.3. $S \subset G_\alpha$ ve $t \in \mathbb{Z}^+$ olsun. Eğer G_α nın her köşesi S deki yalnız bir köşe ile $t-$ baskılanırsa S ye bir mükemmel $t-$ baskın küme denir.

Tanım 4.3.4. Bir ağırlıklı hataları düzeltebilen n uzunluklu bir mükemmel grup kod olan C, $\mathcal{H}_\alpha$ grubunun n defa direkt çarpımı olan $\mathcal{H}_\alpha^{\,n}$ kümesinin bir alt grubudur. Burada $\mathcal{H}_\alpha^{\,n} \setminus C$ kümesindeki her elemanın C kümesinde bir ve yalnız bir elemana olan uzaklığı 1 dir [13].

Lemma 4.3.1. $\sigma \neq \tau$ ve $\sigma, \tau \in \langle \beta \rangle$ ise $d_\alpha(\sigma,\tau) = d_\alpha(\beta\gamma, 0)$ olacak şekilde sıfırdan farklı bir $\gamma \in \mathcal{H}_\alpha$ vardır.

İspat: $\sigma, \tau \in \langle \beta \rangle$ ise $\sigma = \beta\delta_1$ ve $\tau = \beta\delta_2$ olacak şekilde $\delta_1, \delta_2 \in \mathcal{H}_\alpha$ vardır. Burada $\sigma \neq \tau$ olduğundan $\delta_1 - \delta_2 \neq 0 \pmod{\alpha}$ dır. Bu durumda $\gamma = \delta_1 - \delta_2 \pmod{\alpha}$ alınırsa $\gamma \in \mathcal{H}_\alpha$ olup,

$$d_\alpha(\sigma,\tau) = d_\alpha(\sigma-\tau, 0) = d_\alpha(\beta\delta_1 - \beta\delta_2, 0) = d_\alpha(\beta(\delta_1-\delta_2), 0) = d_\alpha(\beta\gamma, 0)$$

eşitliği elde edilir.

Teorem 4.3.2.

1) $0 \neq \beta \in \mathcal{H}_\alpha$, $N(\beta) = 5$ ve $\beta \mid \alpha$ ise $\mathcal{H}_\alpha$ üzerindeki $\langle \beta \rangle = S$ sağ modülü, G_α kümesinde mükemmel $1-$baskın kümedir.

2) $0 \neq \beta \in \mathcal{H}_\alpha$, $N(\beta) = 7$ ve $\beta \mid \alpha$ ise $\mathcal{H}_\alpha$ üzerindeki $\langle \beta \rangle = S$ sağ modülü, G_α kümesinde mükemmel $2-$baskın kümedir.

İspat 1: $0 \neq \beta \in \mathcal{H}_\alpha$, $N(\beta) = 5$ ve $\beta \mid \alpha$ olsun.

$S = \langle \beta \rangle$ kümesinin $1-$baskın küme olması için S nin birbirinden farklı herhangi iki elemanı σ ve τ için $d_\alpha(\sigma, \tau) \geq 3$ olmalıdır. En az bir $0 \neq \gamma \in \mathcal{H}_\alpha$ için $d_\alpha(\sigma, \tau) = d_\alpha(\beta\gamma, 0)$ olduğundan ispat için $d_\alpha(\beta\gamma, 0) \geq 3$ olduğunu göstermek yeterlidir. Kabul edelim ki $0 \neq \gamma \in \mathcal{H}$, $\beta\gamma \not\equiv 0 (\bmod \alpha)$ ve $d_\alpha(\beta\gamma, 0) < 3$ olsun.

Buna göre en az bir $a = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{H}_\alpha$ için $\beta\gamma \equiv_\ell a = a_0 + a_1 i + a_2 j + a_3 k (\bmod \alpha)$ ve

$$d_\alpha(\beta\gamma, 0) = N(a) = {a_0}^2 + {a_1}^2 + {a_2}^2 + {a_3}^2 < 3$$

olur. $\beta\gamma \equiv_\ell a (\bmod \alpha)$ olduğundan $\beta\gamma = a + \alpha\gamma_1$ ve β, α nın sol böleni olduğundan $\alpha = \beta\gamma_2$ olacak şekilde $\exists\, \gamma_1, \gamma_2 \in \mathcal{H}$ elemanları vardır.

Buradan

$$\beta\gamma = a + \alpha\gamma_1 = a + (\beta\gamma_2)\gamma_1 = a + \beta(\gamma_2\gamma_1)$$
$$\Rightarrow a = \beta\gamma - \beta(\gamma_2\gamma_1) = \beta(\gamma - \gamma_2\gamma_1)$$
$$\Rightarrow a = \beta(\gamma - \gamma_2\gamma_1)$$

olur. N nin çarpımsal bir norm olduğu göz önüne alınarak son eşitlikte her iki tarafın normu alınır ise

$$N(\beta(\gamma - \gamma_2\gamma_1)) = N(\beta)N(\gamma - \gamma_2\gamma_1) = N(a)$$
$$\Rightarrow N(\gamma - \gamma_2\gamma_1) = \frac{N(a)}{N(\beta)}$$

bulunur.

$\sigma \neq \tau$ seçildiğinden $N(a) \neq 0$ dır. Dolayısı ile

$N(\beta) = 5$ ve $N(a) < 3$

olduğundan

$$\frac{N(a)}{5} = N(\gamma - \gamma_2\gamma_1) \notin \mathbb{Z}$$

çelişkisi oluşur.

Buna göre $d_\alpha(\beta\gamma, 0) \geq 3$ olur.

Yani S sağ modülü, G_α kümesinde mükemmel $1-$baskın kümedir.

İspat 2: $0 \neq \beta \in \mathcal{H}_\alpha$, $N(\beta) = 7$ ve $\beta \mid \alpha$ olsun.

Bu durumda $S = \langle \beta \rangle$ kümesinin farklı iki elemanının oluşturacağı yuvarların yarıçapı 2 olacağından, her $\gamma \in \mathcal{H}$ için $d_\alpha(\beta\gamma, 0) \geq 5$ olduğunun gösterilmesi gerekir.

Yukarıdaki ispata benzer şekilde en az bir $\gamma \in \mathcal{H}$ için $\beta\gamma \not\equiv 0 \pmod{\alpha}$ ve $d_\alpha(\beta\gamma, 0) < 5$ olduğu kabul edildiğinde, $N(\beta) = 7$ ve $N(a) < 5$ olacağından $\frac{N(a)}{7} = N(\gamma - \gamma_2\gamma_1) \notin \mathbb{Z}$ çelişkisi oluşur. Buna göre $d_\alpha(\beta\gamma, 0) \geq 5$ olur. Yani S sağ modülü, G_α kümesinde mükemmel $2-$baskın kümedir.

Not 4.3.1. Teorem 4.3.2 uygun şartlar sağlandığında farklı t değerleri için de benzer şekilde ispatlanabilir. Örneğin $t = 3$ için ağırlığı 3 ve 3 den küçük olan elemanların sayısı bir asal sayının karesine eşit değildir ve Teorem 4.3.2.' nin şartlarını sağlayacak uygun β ve α değerleri bulunamaz. Fakat $t = 4$ olduğunda ağırlığı 4 ve 4 den küçük olan elemanların sayısı $169 = 13^2$ olup Teorem 4.3.2 nin şartlarını sağlayan uygun β ve α sayıları seçilerek mükemmel $4-$baskın kümeler oluşturulabilir.

Sonuç 4.3.1. Ağırlığı t ve t den küçük Hurwitz sayılarının sayısı $N(\beta)^2$ olacak şekilde bir β Hurwitz sayısı var olsun. Bu durumda üzerinde bir mükemmel $t-$baskın küme oluşturulabilecek $\mathcal{H}_\alpha$ kümesinin olması için gerek ve yeter şart $N(\beta)=p$ olacak şekilde bir p asal tamsayısının var olmasıdır.

Teorem 4.3.2.' ye göre $0\neq\beta\in\mathcal{H}_\alpha, N(\beta)=5$ ve $\beta\,|\,\alpha$ ise $\langle\beta\rangle=S$ sağ modülü G_α kümesinde mükemmel $1-$baskın kümedir. Bu küme $\mathcal{H}_\alpha$ nın bir alt grubudur. Bundan yararlanılarak kod sözleri S nin elemanları olan $\mathcal{H}_\alpha$ üzerinde bir $C=S$ kodu tanımlanabilir. S sağ modülü minimum mesafesi 3 ve uzunluğu 1 olan bir mükemmel grup kod tanımlar.

Benzer şekilde $N(\beta)=7$ olduğunda G_α nın bir $2-$baskın S kümesi vardır. Bu küme $\mathcal{H}_\alpha$ nın bir alt grubu olup $\mathcal{H}_\alpha$ üzerinde bir $C=S$ kodu tanımlanabilir. S minimum mesafesi 5 ve uzunluğu 1 olan bir mükemmel grup kod tanımlar.

Örnek 4.3.4. $\beta=2+i$ ve $\alpha=(2+i)(1+i+j)=1+3i+j+k$ olsun.

$\langle\beta\rangle=\{0,2+i,-2-i,-1+2i,1-2i,2j+k,-2j-k,-j+2k,j-2k\}$ olup bu kümedeki 9 elemanın herbiri $\mathcal{H}_\alpha$ kümesinde 25 elemanı $1-$baskılar. Yani toplamda 9 yuvar vardır ve bu dokuz yuvarın her birinde 25 eleman bulunur. Dolayısı ile $\langle\beta\rangle$ kümesi $\mathcal{H}_\alpha$ üzerinde $1-$baskın küme oluşturur.

$\mathcal{H}_\alpha$ üzerinde $C=S=\langle\beta\rangle$ seçilirse C kodu $1-$hata düzeltebilen bir mükemmel kod olur.

Bu örnek aşağıda verilen Wolfram Mathematica programı ile elde edilebilir.

Programdaki "K" tablosunun 1. sütunu $\mathcal{H}_\alpha$ kümesinin elemanlarını ve 2. sütunu da $B\beta2=\langle\beta\rangle$ kümesinin elemanlarının baskıladığı 25 elemanı sırasıyla vermektedir.

Programdaki "SW1" kümesi ağırlığı bir olan Hurwitz sayılarını, "B1γ" kümesi ise $\gamma\in\langle\beta\rangle$ elemanına bir uzaklıktaki elemanların kümesini göstermektedir.

"KKKK" tablosunun 2. sütunu $2+i\in\langle\beta\rangle$ elemanın baskıladığı 25 elemanı göstermektedir. Bu tablo "K" tablosunun ilk 25 elemanını göstermektedir.

"G" ise Şekil 4.3 de gösterilen, köşeleri $\mathcal{H}_\alpha$ kümesinden olan döngüsel çizgeyi ve bu çizgede ki işaretli $1,2,\ldots,9$ noktaları ise $\langle\beta\rangle$ kümesinin elemanlarının yerini göstermektedir.

Şekil 4.4 ise $G_{1+3i+2j+k}$ çizgesine izomorf olan $C_{225}(13,14,\ldots,24)$ döngüsel çizgesini göstermektedir. Bu çizgenin çapı 5 tir. Diğer yandan $G_{1+3i+2j+k}$ kümesindeki elemanlar ile sıfır arasındaki maksimum karesel Öklidyen mesafesi de 5 tir.

```
In[227]:= << Quaternions`
α = Quaternion[1, 3, 2, 1]; k = Norm[α]; A = Table[1, {k}]; Do[ A[[n]] = n, {n, 1, k}]
B = Quaternion[0, 0, 1, 0] * A; GG = Table[1, {k^2}];
Do[Do[GG[[n + k * (m - 1)]] = A[[n]] + B[[m]], {n, 1, k}], {m, 1, k}];
Hα = Table[1, {k^2}];(*Hα denotes the Hα*)
Do[Hα[[tt]] = Mod[GG[[tt]], α], {tt, 1, k^2}];
β = Quaternion[2, 1, 0, 0]; Dimensions[Hα];
B = Table[1, {k^2}]; Do[B[[t]] = Mod[β ** Hα[[t]], α],
 {t, 1, k^2}]; Bβ = Union[B]; Dimensions[Bβ];
Bβ1 = Table[0, {Dimensions[Bβ][[1]]}];
Do[Bβ1[[t]] = If[Bβ[[t]] == Mod[Bβ[[t]] + (α ** Quaternion[1/2, 1/2, 1/2, 1/2]), α], Bβ[[t]]],
  {t, 1, Dimensions[Bβ][[1]]}];
MatrixForm[Bβ1];

Bβ2 = {Quaternion[2, 1, 0, 0], Quaternion[0, 0, -2, -1], Quaternion[0, 0, -1, 2],
 Quaternion[-1, 2, 0, 0], Quaternion[0, 0, 0, 0], Quaternion[0, 0, 2, 1],
 Quaternion[1, -2, 0, 0], Quaternion[0, 0, 1, -2], Quaternion[-2, -1, 0, 0]}
; (*Bβ2 shows the set generated by β. To obtain the set Bβ2,

firstly Bβ is obtained. secondly Bβ1 is checked. Using the commend
 MemberQ, the equivalent elements  are elected. *)
(*The set SW1 denotes the elements of weight 1. *)
```

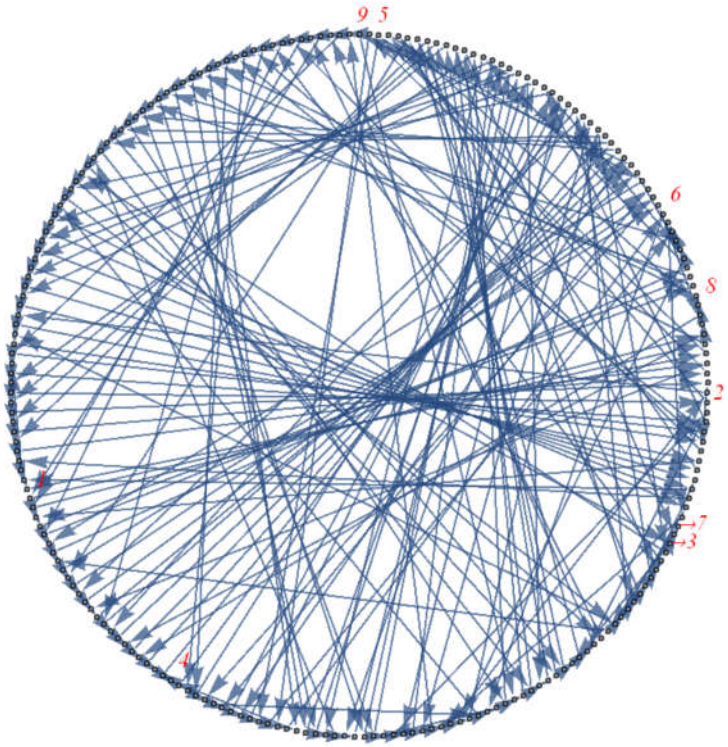
```
SW1 = Table[1, {25}];
Do[Do[SW1[[m + 5 * (n - 1)]] = Mod[Quaternion[m, 1, 0, 0] +
      Quaternion[1, 0, n, 0], Quaternion[2, 1, 0, 0]],
   {m, 1, 5}], {n, 1, 5}];
B1γ = Table[1, {k^2}];
Do[Do[B1γ[[m + 25 * (n - 1)]] = SW1[[m]] + Bβ2[[n]],
   {m, 1, 25}], {n, 1, Dimensions[Bβ2][[1]]}];
MatrixForm[Hα]; Dimensions[B1γ];
K = Table[1, {225}, {2}];
Do[K[[t, 1]] = Hα[[t]]; K[[t, 2]] = Mod[B1γ[[t]], α],
 {t, 1, 225}]; Dimensions[Union[Hα]]; MatrixForm[K];
(*The first column of the matrix K denotes the elemnts of Hα  and the first 25
 rows of the second column of the matrix K are at distance one from the first elemnt
 of Bβ2. The next elements occurs in the same way.  *)
BB = Table[1, {k^2}, {4}];
Do[BB[[t, 1]] = Hα[[t, 1]]; BB[[t, 2]] = Hα[[t, 2]]; BB[[t, 3]] = Hα[[t, 3]]; BB[[t, 4]] = Hα[[t, 4]];
  , {t, 1, k^2}];
KK = Table[1, {k^2 - 1}];
Do[KK[[t]] = BB[[t]] → BB[[t + 1]], {t, 1, k^2 - 1}];
KKK = Union[KK, {{0, 0, 0, 0} → {1, 0, 1, 0}}];
KKKK = Table[1, {25}];
Do[KKKK[[t]] = K[[t]], {t, 1, 25}];
MatrixForm[KKKK]
G = Graph[KKK, VertexLabels → {{0, 0, 0, 0} → "1", {0, 0, -2, -1} → "2", {0, 0, -1, 2} →
      "→3", {-1, 2, 0, 0} → "4", {2, 1, 0, 0} →  5 ", {0, 0, 2, 1} → "6", {1, -2, 0, 0} →
      "→7", {0, 0, 1, -2} → "8", {-2, -1, 0, 0} → "9"},
  VertexLabelStyle → Directive[Red, Italic, 11], VertexSize → 0.5]
(*The graph G shows G1+3i+2j+k. The elemnts of the set <β> occurs {1,2,..9} in that graph.*)

G = CirculantGraph[225, {13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24}, VertexSize → 0.5, EdgeStyle → Dashed]
EdgeCount[G]
GraphDiameter[G]
```

Yukarıdaki programın çıktıları şunlardır:

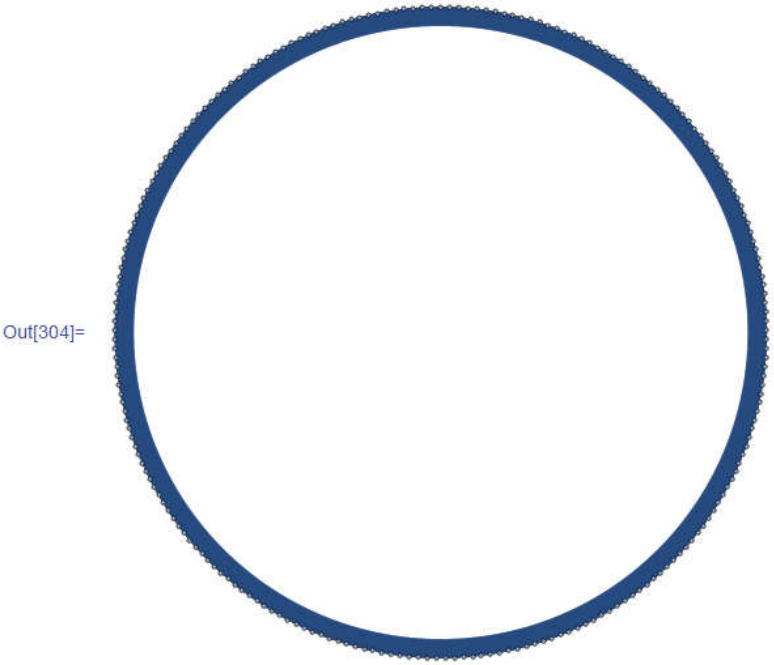
Tablo 4.1. $\mathcal{H}_{1+3i+2j+k}$ kümesi ve $\langle\beta\rangle$ kümesinin baskıladığı elemanlar

Out[252]//MatrixForm=

Quaternion[1, 0, 1, 0]	Quaternion[$-\frac{3}{2}, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}$]
Quaternion[$-\frac{3}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}$]	Quaternion[-1, -1, 1, 0]
Quaternion[$-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}$]	Quaternion[0, -1, 1, 0]
Quaternion[$\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}$]	Quaternion[$\frac{3}{2}, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}$]
Quaternion[$\frac{3}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}$]	Quaternion[$-\frac{1}{2}, \frac{3}{2}, \frac{1}{2}, -\frac{3}{2}$]
Quaternion[$-\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{3}{2}$]	Quaternion[0, 0, 1, 2]
Quaternion[$\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{3}{2}$]	Quaternion[$\frac{3}{2}, \frac{3}{2}, \frac{1}{2}, \frac{1}{2}$]
Quaternion[$\frac{3}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{3}{2}$]	Quaternion[-1, 1, -1, 1]
Quaternion[-1, 0, -1, -1]	Quaternion[$\frac{3}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}$]
Quaternion[0, 0, -1, -1]	Quaternion[-1, 0, -1, 1]
Quaternion[1, 0, -1, -1]	Quaternion[$-\frac{1}{2}, -\frac{3}{2}, \frac{3}{2}, \frac{1}{2}$]
Quaternion[0, -1, 0, 2]	Quaternion[-1, -1, 1, -1]
Quaternion[-2, 0, 1, 0]	Quaternion[0, -1, 1, -1]
Quaternion[-1, 0, 1, 0]	Quaternion[$\frac{3}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}$]
Quaternion[0, 0, 1, 0]	Quaternion[-1, 0, -2, 0]
Quaternion[1, 0, 2, 0]	Quaternion[$-\frac{1}{2}, -\frac{3}{2}, \frac{1}{2}, -\frac{1}{2}$]
Quaternion[$-\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}$]	Quaternion[$\frac{3}{2}, \frac{3}{2}, \frac{1}{2}, -\frac{1}{2}$]
Quaternion[$-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}$]	Quaternion[-1, 1, -1, 0]
Quaternion[$\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}$]	Quaternion[$\frac{3}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}$]
Quaternion[$\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2}$]	Quaternion[-1, 0, -1, 0]
Quaternion[-1, -1, -1, 1]	Quaternion[2, 1, 0, 0]
Quaternion[0, -1, -1, 1]	Quaternion[$-\frac{1}{2}, \frac{1}{2}, -\frac{3}{2}, \frac{1}{2}$]
Quaternion[1, -1, -1, 1]	Quaternion[2, 0, 0, 0]
Quaternion[-1, 0, 0, -1]	Quaternion[$-\frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{1}{2}$]
Quaternion[0, 0, 0, -1]	Quaternion[1, 1, 0, 0]



Şekil 4.3: $\alpha = 1 + 3i + 2j + k$ elemanı ile Hurwitz sayıları üzerinde üretilmiş bir çizge.



Out[305]= 2700

Out[306]= 5

Şekil 4.4: $C_{225}(13,14,\ldots,24)$ çizgesi

Not 4.3.2. Tablo 4.1.' de $\mathcal{H}_{1+3i+2j+k}$ kümesi ve $\langle\beta\rangle$ kümesinin baskıladığı elemanların bir bölümü verilmiştir. Program çalıştırılarak bu iki kümedeki 225 elemanın tamamı görüntülendiğinde sol ve sağ sütundaki bazı elemanlar birbirinden farklı gibi gözükebilir.

Örnek 4.3.5. $\alpha = 3+4i+3j+k$ için $\beta = 2+i+j+k$ elemanı $\mathcal{H}_\alpha$ üzerinde $2-$baskın küme oluşturur. Bu kümeyi oluşturan Mathematica programı aşağıda verilmiştir.

```
In[73]:= << Quaternions`
α = Quaternion[3, 4, 3, 1]; k = Norm[α]; A = Table[1, {k}];
Do[A[[n]] = n, {n, 1, k}]; B = Quaternion[0, 0, 1, 0] * A;
GG = Table[1, {k^2}, {2}]; t = 0; Do[
 Do[GG[[n + t, 1]] = n + t; GG[[n + t, 2]] = A[[m]] + B[[n]],
  {n, 1, k}]; t = t + k, {m, 1, k}];
Hα = Table[1, {k^2}];
Do[Hα[[tt]] = Mod[GG[[tt, 2]], α], {tt, 1, k^2}];
β = Quaternion[2, 1, 1, 1]; B1 = Table[1, {k^2}];
Do[B1[[t]] = β ** Hα[[t]], {t, 1, k^2}];
Bβ2 = Union[Mod[B1, α]]; SW2 = Table[1, {49}];
Do[Do[SW2[[m + 7 * (n - 1)]] = Mod[Quaternion[m, 1, 0, 0] + Quaternion[1, 0, n, 0],
     Quaternion[2, 1, 1, 1]], {m, 1, 7}], {n, 1, 7}];
Dimensions[Union[SW2]]; B2γ = Table[1, {k^2}];
Do[Do[B2γ[[m + 49 * (n - 1)]] = SW2[[m]] + Bβ2[[n]], {m, 1, 49}], {n, 1, 25}];
K = Table[1, {k^2}, {2}];
Do[K[[t, 1]] = Hα[[t]]; K[[t, 2]] = Mod[B2γ[[t]], α],
  {t, 1, k^2}];
```

Aşağıdaki tabloda bazı $t-$baskın küme örnekleri verilmiştir.

Tablo 4.2. Bazı $t-$baskın küme örnekleri

β **değeri**	α değeri	Kaç baskın küme olduğu
$i-2k$	$1+2i-3j+k$	1
$\frac{3}{2}+\frac{i}{2}+\frac{3j}{2}+\frac{k}{2}$	$-\frac{5}{2}+\frac{5i}{2}+\frac{3j}{2}+\frac{k}{2}$	1
$\frac{1}{2}+\frac{i}{2}+\frac{j}{2}+\frac{5k}{2}$	$-\frac{3}{2}+\frac{i}{2}-\frac{5j}{2}+\frac{7k}{2}$	2
$\frac{3}{2}+\frac{3i}{2}+\frac{3j}{2}+\frac{k}{2}$	$\frac{3}{2}+\frac{5i}{2}+\frac{9j}{2}+\frac{5k}{2}$	2
$2+i+j+k$	$3+4i+3j+k$	2
$1+2i+2j+2k$	$-4+5i+5j+5k$	4

BÖLÜM 5.

Lipschitz sayıları üzerinde $\theta-$ devirli kodlar

(1,3,4,5. iş paketleri, 1,2 ve 5. hedefler):

Bu çalışmada katkısı olanlar:

Doç. Dr. Murat GÜZELTEPE

Dr. Öğr. Üyesi Gökçen ÇETİNEL

Dr. Öğr. Üyesi Nükhet SAZAK

5.1 Giriş

Proje kapsamında yapılan "Constacyclic codes over Lipschitz integers" çalışmamız bu alanda yapılmış önemli bir çalışmadır. Bu çalışma

$i^2=j^2=k^2=-1$ ve $ij=-ji=k, jk=-kj=i, ki=-ik=j$

olmak üzere

$$H(\mathbb{Z})=\{a_0+a_1i+a_2j+a_3k \,|a_0,a_1,a_2,a_3\in\mathbb{Z}\}$$

olarak tanımlanan Lipschitz sayıları üzerinde yapılmıştır. $\pi=a_0+a_1i+a_2j+a_3k\in H(\mathbb{Z})$ bir asal Lipschitz sayısı ve p bir asal tamsayı olmak üzere

$$\begin{aligned} p=\pi\pi^{\star} &=(a_0+a_1i+a_2j+a_3k)(a_0-a_1i-a_2j-a_3k)\\ &=a_0^2+a_1^2+a_2^2+a_3^2 \end{aligned}$$

olsun. π'nin normu $N(\pi)=a_0^2+a_1^2+a_2^2+a_3^2$ olarak tanımlanır. $H(\mathbb{Z})$ halkasının birimsel elemanları $\pm1,\pm i,\pm j,\pm k$ dir.

Tanım 5.1.1. $\pi\neq0$ bir Lipschitz tamsayısı olsun. $\alpha,\beta\in H(\mathbb{Z})_{\pi}$ olmak üzere, α ile β arasındaki $d_L(\alpha,\beta)=|a_0|+|a_1|+|a_2|+|a_3|$ ve γ nın Lipschitz ağırlığı ise $w_L(\gamma)=|a_0|+|a_1|+|a_2|+|a_3|$

olarak tanımlanır. Burada $\alpha-\beta\equiv\gamma=a_0+a_1i+a_2j+a_3k \pmod{\pi}$ ve γ elemanı $\overline{\alpha-\beta}$ kalan sınıfındaki $|a_0|+|a_1|+|a_2|+|a_3|$ toplamı en küçük olan elemandır.

5.2 Bir Lipschitz Ağırlığını Düzelten Kodlar (OLEC)

α elemanı $\alpha^{p^2-1}=1$ şartını sağlayan $H(\mathbb{Z})_\pi$ nin bir elemanı, p bir asal tek tam sayı, $\pi = a_0 + a_1 i + a_2 j + a_3 k$ ve $p = \pi\pi^*$ olsun. α elemanı kullanılarak

$$H = \begin{pmatrix} \alpha^0 & \alpha^1 & \cdots & \alpha^{\left(\left(p^2-1\right)/2\right)-1} \end{pmatrix}$$

yazılan kontrol matrisine sahip $n = \dfrac{p^2-1}{2}$ kodu bir Lipschitz ağırlığını düzeltebilen bir koddur.

Teorem 5.2.1. p bir tek asal sayı, $p = \pi\pi^*$ ve β $H(\mathbb{Z})_\pi$ nin mertebesi $2n$ olan bir elemanı olsun. Bu durumda

$$H = \begin{bmatrix} \beta^0 & \beta^1 & \beta^2 & \cdots & \beta^{n-1} \\ \beta^0 & \beta^3 & \beta^6 & \cdots & \beta^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta^0 & \beta^{2t+1} & \beta^{2(2t+1)} & \cdots & \beta^{(n-1)(2t+1)} \end{bmatrix}$$

(1)

kontrol matrisine sahip bir C kodu $0 \le w_L(e_s), w_L(e_t) \le 1$ olmak üzere $e(x) = e_s x^s + e_t x^t$ şeklindeki hataları düzeltebilir.

İspat: Kabul edelim ki kanaldan gelen r vektörünün l_1 ve l_2 bileşenlerinde $0 \le w_L(e_1), w_L(e_2) \le 1$ olmak üzere e_1 ve e_2 hataları oluşsun. r nin sendromu

$$S(r) = \left(rH^T\right)^T = \begin{pmatrix} s_1 \\ s_3 \end{pmatrix}$$

dir. β nın kuvvetleri değişmeli olduğundan s_1 ve s_3 sendromları $s_1' = \theta_1 s_1$ ve $s_3' = \theta_1 s_3$, $\theta_1 \in \{\pm 1, \pm i, \pm j, \pm k\}$ olacak şekilde değiştirilebilir. Hataların yerlerini ve değerlerini hesaplamamızı sağlayan $\sigma(z)$ polinomu

$\sigma(z) = (z - \beta^{l_1})(z - \beta^{l_2}) = z^2 - (\beta^{l_1} + \beta^{l_2})z + \beta^{l_1}\beta^{l_2} = z^2 - s_1' z + \varepsilon$ olarak tanımlanır. Burada ε sendromlardan hesaplanır. $s_1' = \beta^{l_1} + \beta^{l_2}$, $s_3' = \beta^{3l_1} + \beta^{3l_2}$, $\varepsilon = \beta^{l_1 + l_2}$ olduğu göz önüne alınırsa

$$\left(s_1'\right)^3 - s_3' = 3\varepsilon\beta^{l_1} + 3\varepsilon\beta^{l_2} + \beta^{3l_2} + \beta^{3l_1} - \left(\beta^{3l_2} + \beta^{3l_1}\right) = 3\varepsilon\left(\beta^{l_1} + \beta^{l_2}\right) \qquad (2)$$

ve buradan da

$$\frac{\left(s_1'\right)^3 - s_3'}{3s_1'} = \frac{3\varepsilon\left(\beta^{l_1} + \beta^{l_2}\right)}{3\left(\beta^{l_1} + \beta^{l_2}\right)} = \varepsilon \pmod{\pi}$$

elde edilir. $\sigma(z)$ polinomunun kökleri n modülosuna göre β^{l_1} ve β^{l_2} olsun l_1 ve l_2 hataların yerlerini gösterir. Hataların değerleri ise sırasıyla $\theta_1\beta^{l_1} / \beta^{l_1 (\mathrm{mod}\, n)}, \theta_1\beta^{l_2} / \beta^{l_2 (\mathrm{mod}\, n)}$ olarak hesaplanır. Bu durumda üç hal ortaya çıkar.

i. $s_1' = s_3' = 0$ ise hata yoktur.

ii. $\left(s_1'\right)^3 = s_3' \neq 0$ ise bir hata oluşmuştur.

iii. $\left(s_1'\right)^3 \neq s_3'$ ve $s_1' \neq 0$ ise iki hata oluşmuştur.

Teorem 5.2.2. Eğer $N(\pi) \geq 13$ olan π sayısı $H(\mathbb{Z})$ de bir asal ise (1) deki kontrol matrisine sahip bir kodun minimum mesafesi 4'e eşit ya da 4'ten büyüktür.

İspat: Kod çözücünün tekli ve ikili hataları tespit edilebildiğini göstermek ispat için yeterlidir. Kabul edelim ki ağırlığı 1 olan bir hata meydana gelmiş olsun. Bu durumda $\left(s_1'\right)^3 = s_3' \neq 0$ olur. (2) denkleminden

$$z_{1,2} = \frac{s_1' \pm \sqrt{\frac{s_3'}{s_1'}}}{2} = \frac{s_1' \pm s_1'}{2}$$

elde edilir. Önceki teoremden kod çözücünün bu hataları ayırt edebildiği anlaşılır.

5.3 Bir Lipschitz Ağırlıklı Hataları Düzeltebilen $\theta-$Devirli Kodlar (OLECC)

Tanım 5.3.1. C kodu $H(\mathbb{Z})$ üzerinde bir lineer kod olsun. $\theta \in \{\pm i, \pm j, \pm k\}$ olmak üzere eğer her $(c_0,\ c_1,\ \cdots,\ c_{n-1}) \in C$ için $(\theta c_{n-1},\ c_0,\ \cdots,\ c_{n-2}) \in C$ oluyorsa C koduna $\theta-$ devirli kod denir.

p bir asal tamsayı, $\pi = a_0 + a_1 i + a_2 j + a_3 k$ bir Lipschitz asal sayısı, $p = \pi\pi^*$ ve $\alpha^{\left(p^2-1/8\right)} = \pm i, \pm j, \pm k$ olacak şekilde $\alpha \in H(\mathbb{Z})$ olsun. Bu takdirde

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{\left(p^2-1\right)/8-1} \end{pmatrix}$$

kontrol matrisine sahip bir C kodu bir Lipschitz ağırlığını düzeltebilen bir $\theta-$devirli kod olur.(Kısaca OLECC) Bir OLECC kodunu uzunluğu $n=\frac{p^2-1}{8}$ dir. OLECC kodları mükemmel kod olduğundan oldukça önemlidir.

Teorem 5.3.2. $p=4n+1\geq 17$ bir asal tamsayı, π bir Lipschitz asal sayısı, $p=\pi\pi^*$ ve γ $H(\mathbb{Z})_\pi$ nin $4n$ inci mertebeden bir elemanı olsun. $t<n$ için

$$H=\begin{pmatrix} \gamma^0 & \gamma^1 & \gamma^2 & \cdots & \gamma^{n-1} \\ \gamma^0 & \gamma^5 & \gamma^{10} & \cdots & \gamma^{5(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma^0 & \gamma^{4t+1} & \gamma^{2(4t+1)} & \cdots & \gamma^{(n-1)(4t+1)} \end{pmatrix}$$

kontrol matrisine sahip bir C kodu $0\leq w_L(e_s), w_L(e_t)\leq 1$ olmak üzere $e(x)=e_s x^s+e_t x^t$ şeklindeki hataları düzeltebilir.

İspat: Kabul edelim ki kanaldan gelen r vektörünün l_1 ve l_2 bileşenlerinde $0\leq w_L(e_1), w_L(e_2)\leq 1$ olmak üzere e_1 ve e_2 hataları oluşsun. r nin sendromu

$S(r)=rH^{tr}=(s_1,s_5)$

dir. γ nın kuvvetleri değişmeli olduğundan s_1 ve s_5 sendromları $s_1'=\theta_1 s_1$ ve $s_5'=\theta_1 s_5$, $\theta_1\in\{\pm 1,\pm i,\pm j,\pm k\}$ olacak şekilde değiştirilebilir. Hataların yerlerini ve değerlerini hesaplamamızı sağlayan $\sigma(z)$ polinomu

$\sigma(z)=(z-\gamma^{l_1})(z-\gamma^{l_2})=z^2-(s_1')z+\varepsilon$ olarak tanımlanır. Burada ε sendromlardan hesaplanır. $s_1'=\gamma^{l_1}+\gamma^{l_2}$, $s_5'=\gamma^{5l_1}+\gamma^{5l_2}$ ve $\varepsilon=\gamma^{l_1+l_2}$ olduğu göz önüne alınırsa

$$\varepsilon^2-(s_1')^2\varepsilon+\frac{(s_1')^5-s_5'}{5s_1'}=0$$

elde edilir. $\sigma(z)$ polinomunun kökleri n modülosuna göre γ^{l_1} ve γ^{l_2} olsun. l_1 ve l_2 hataların yerlerini gösterir. Ayrıca hataların değerleri ise sırasıyla $\theta_1\gamma^{l_1}/\gamma^{l_1(\mathrm{mod}\,n)}, \theta_1\gamma^{l_2}/\gamma^{l_2(\mathrm{mod}\,n)}$ olarak hesaplanır. Bu durumda üç hal ortaya çıkar.

i. $s_1'=s_5'\ (\mathrm{mod}\ \pi)$ ise hata yoktur.

ii. $\left(s_1'\right)^5 = s_5' \neq 0$ ise bir hata oluşmuştur.

iii. $\left(s_1'\right)^5 \neq s_5'$ ve $s_1' \neq 0$ ise iki hata oluşmuştur.

Örnek 5.3.3. $\pi = 4 + k$, $\gamma = 1 + k$ ve C

$$H = \begin{pmatrix} \gamma^0 & \gamma^1 & \gamma^2 & \gamma^3 \\ \gamma^0 & \gamma^5 & \gamma^{10} & \gamma^{15} \end{pmatrix}$$

matrisi ile tanımlanan bir kod olsun.

γ nın kuvvetleri Tablo I de gösterildiği gibidir. Alınan r sözü $(-2,\ -2k,\ 1-i,\ i)$ olsun. Şimdi dekodlama aşamalarını uygulayalım.

i. Sendrom hesaplama:

$$S(r) = rH^{tr} = (-2i, -i + j) = (s_1,\ \ s_2)(mod\ \pi)$$

$\theta_1 = i$ alınırsa $\left(s_1'\right)^5 = s_5'$ elde edilir ve bu iki hata oluştuğunu gösterir.

ii. $$\varepsilon^2 - \left(s_1'\right)^2 \varepsilon + \frac{\left(s_1'\right)^5 - s_5'}{5s_1'} = 0 \Rightarrow (1+2k)\varepsilon^2 + k(1+2k)\varepsilon + 1 = 0 (\mathrm{mod}\,\pi)$$

formülü kullanılarak $\varepsilon = 1 - k(mod\,\pi)$ ve $\sigma(z)$ polinomunun köklerinin γ^3 ve γ^{10} olduğu elde edilir. Bu durumda hataların yerleri $l_1 = 3 \equiv 3\ (mod\ 4)$ ve $l_2 = 10 \equiv 2(mod\ 4)$, hataların değerleri ise sırasıyla $\theta_1\gamma^3\ /\gamma^3 = i$ ve $\theta_1\gamma^{10}\ /\gamma^2 = -i$ olur. O halde c düzeltilmiş kodsözü

$$c = r - e = (-2,\ -2k,\ 1,\ 0)$$

olarak elde edilir.

Teorem 5.3.4. $p = 6n + 1 \geq 31$ bir asal tam sayı ve γ, $H(\mathbb{Z})_\pi$ de mertebesi $6n$ olan bir eleman ve $N(\pi) = p$ olsun. Bu durumda kontrol matrisi

$$H = \begin{pmatrix} 1 & \gamma & \gamma^2 & \cdots & \gamma^{n-1} \\ 1 & \gamma^7 & \gamma^{14} & \cdots & \gamma^{7(n-1)} \\ 1 & \gamma^{13} & \gamma^{26} & \cdots & \gamma^{13(n-1)} \\ 1 & \gamma^{19} & \gamma^{38} & \cdots & \gamma^{19(n-1)} \end{pmatrix}$$

olan bir C kodu, Lipschitz ağırlığı $0 \leq w_L(e_s), w_L(e_t) \leq d_{\max}$ olan her hata çiftini düzeltebilir. Burada

$$d_{\max} = \max\left\{ w_L(q) \,\middle|\, q \in H(\mathbb{Z})_\pi \right\}$$

olarak tanımlanır.

İspat: Kabul edelim ki $r=c+e$ gelen vektör vektörünün l_1 ve l_2 bileşenlerinde hata meydana gelsin. Bu durumda r'nin sendromu

$$S(r)=\left(rH^T\right)^T=\begin{pmatrix} S_1=\gamma^{L_1}+\gamma^{L_2} \\ S_7=\gamma^{7L_1}+\gamma^{7L_2} \\ S_{13}=\gamma^{13L_1}+\gamma^{13L_2} \\ S_{19}=\gamma^{19L_1}+\gamma^{19L_2} \end{pmatrix}$$

olarak hesaplanır. Burada $L_1\equiv l_1 \pmod n$ ve $L_2\equiv l_2 \pmod n$ dir. $0\le t\le 8$ olmak üzere $\theta_t\in\{\pm 1,\pm i,\pm j,\pm k\}$ olsun. Bir bileşendeki hata örneğin i iken diğer bileşendeki hata k olabilir. γ'nın kuvvetleri değişmeli olduğundan elde edilen sendromların γ'nın kuvvetleri cinsinden yazılabilmesi için bu sendromlar γ'nın kuvvetleri olarak yazılamıyorsa ilgilileri yazılabileceğinden uygun olarak bu sendromlar

$$S'(r)=\begin{pmatrix} S_1'=\theta_1 S_1\theta_2 \\ S_7'=\theta_3 S_7\theta_4 \\ S_{13}'=\theta_5 S_{13}\theta_6 \\ S_{19}'=\theta_7 S_{19}\theta_8 \end{pmatrix}$$

şeklinde yeniden düzenlenebilir. Bu yeni sendromlar γ'nın kuvvetleri olacak şeklide $\theta_t\in\{\pm 1,\pm i,\pm j,\pm k\}$ ler seçilebilir. $\varepsilon=\gamma^{L_1+L_2}$ olmak üzere sendromlar kullanılarak

$$S_1'S_{13}'-\left(S_7'\right)^2=\varepsilon Z^2-4\varepsilon^7,$$
$$S_1'S_{19}'-S_7'S_{13}'=\varepsilon Z^3-4\varepsilon^7 Z,$$
$$S_7'S_{19}'-\left(S_{13}'\right)^2=\varepsilon^6\left(Z^2-4\varepsilon^7\right),$$

elde edilir. Burada $Z=\gamma^{6L_1}+\gamma^{6L_2}$ dir. Bu eşitlikler yardımı ile

$$Z=\frac{S_1'S_{19}'-S_7'S_{13}'}{S_1'S_{13}'-\left(S_7'\right)^2} \quad \text{ve} \quad \varepsilon^6=\frac{S_7'S_{19}'-\left(S_{13}'\right)^2}{S_1'S_{13}'-\left(S_7'\right)^2}$$

hesaplanır. Bunlar yardımı ile

$$x^2-Zx+\varepsilon^6=0$$

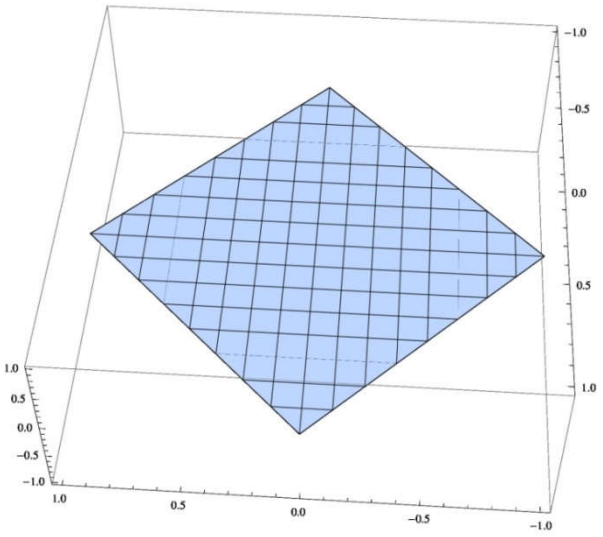
denklemi çözülür. Bu denklemin kökleri hataların yerlerini ve ağırlıklarını bulmamızı sağlar.

Tablo V. x^4-k nın bir kökü olan $\gamma=1+k$ nın kuvvetleri.

$\gamma^0=1$	$\gamma^1=1+k$	$\gamma^2=2k$	$\gamma^3=-1-2k$	$\gamma^4=k$

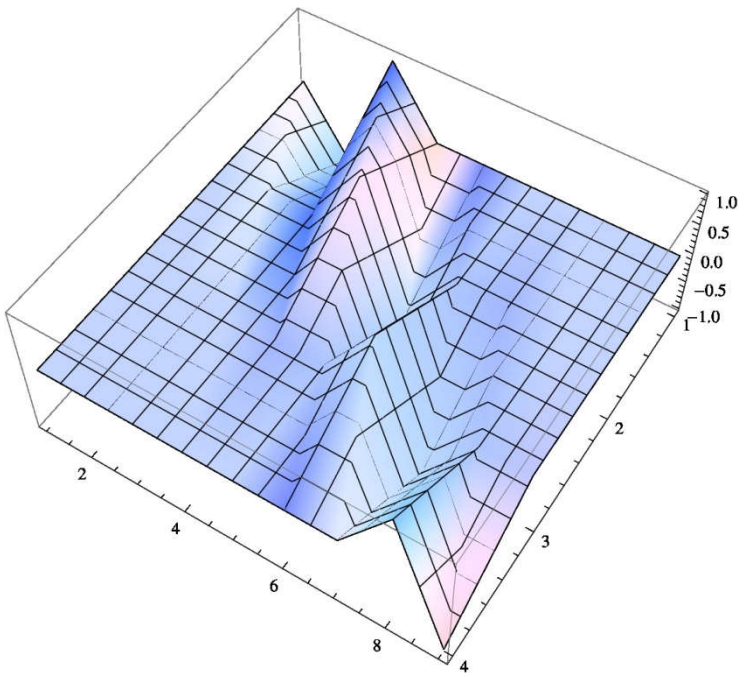
5.4 θ – Devirli Kodlar ile Gauss Tamsayıları Üzerindeki Kodların Karşılaştırılması

$\mathbb{Z}[i]_{\pi}$ takım yıldızı bir kare latis formundadır. Örneğin Şekil 1.1 de $\mathbb{Z}[i]_{2+i} = \{0, \pm 1, \pm i\}$ takım yıldızının bir kare latis oluşturduğu görülmektedir.



Şekil 1.1: $\mathbb{Z}[i]_{2+i}$ takım yıldızı.

$H(\mathbb{Z})_{\pi}$ takım yıldızı da bir latis formundadır. Örneğin $H(\mathbb{Z})_{1+i+j} = \{0, \pm 1, \pm i, \pm j, \pm k\}$. takım yıldızı Şekil 1.2 de gösterildiği gibi bir latis formundadır.



Şekil 1.2: $H(\mathbb{Z})_{1+i+j}$ takım yıldızı.

Tablo VI da takım yıldızındaki elemanların sayısı eşit olmak üzere bu iki takım yıldızı üzerinde yazılmış kodlar ortalama enerji, kod hızı ve mükemmmel kod olup olmama açısından karşılaştırılmıştır. $\mathbb{Z}[i]_\pi$ üzerindeki kodlar kısaca OMEC, $H(\mathbb{Z})_\pi$ üzerindeki kodlar kısaca OLEC ve $H(\mathbb{Z})_\pi$ üzerindeki $\theta-$ devirli kodlar da kısaca OLECC şeklinde gösterilir.

Önerilen kodlama şemasının performansını değerlendirmek için sayısal haberleşme sistemleri için tanımlanan yaygın olarak kullanılan önemli ölçütler cinsinden şemayı incelemeliyiz. Bu önemli ölçütlerden ikisi kod kazancı ve sembol hata olasılığıdır. Asimptotik kod kazancı veya kısaca kod kazancı, bir kodun performansı için bir ölçüdür. Kod kazancı, genellikle desibel cinsinden verilir, kodlamalı ve kodlamasız istenilen bit hata oranını (BER) elde etmek için gereken E_b/N_0 oranındaki azalma olarak tanımlanmaktadır. Başka bir deyişle, kod kazancı bir kodlama şemasının iyileşmesini temsil etmektedir. Kod kazancı, minimum mesafe ve kod hızının bir fonksiyonudur. Verilen bir kod için en iyi kod, en yüksek minimum mesafeyi sağlayan koddur.

Lipschitz tamsayılarından elde edilen devirli kodların, BPSK/QPSK modülasyon senaryoları altında sağladığı kod kazançları farklı p değerleri için Tablo VII'de verilmektedir. Kod kazancı ve karşılık gelen iyileşmeyi hesaplamak için Tablo VI oluşturulmuştur. Tabloda önerilen kodun E_s, E_b ve $10\log 4E_b$ değerleri verilmektedir. Bu tabloda bit enerjisi (E_b) ve sembol enerjisi (E_s) arasındaki ilişki $E_b = \dfrac{E_s}{\log_2 p^2}$ olarak verilebilir.

BPSK/QPSK modülasyon şemaları için referans değer $10\log 4E_b$'dir. Bu değer, iyileşme miktarını belirlemek için kod kazancından çıkarılmalıdır. Kod kazançları ve referans değerleri arasındaki farklar Tablo VII'yi en soldaki sütununda verilmektedir. Aşağıdaki örnekte Tablo VII'yi oluşturmak için kullanılan kod kazancının hesaplamasını açıklanmaktadır.

Örnek 5.4.2. $GF(7)$ [18] üzerinde $[20,7,11]_7$ Hamming mesafeli Reed-Solomon kodunu ve $\pi = 2+i+j+k$ üzerinde OLECC kodu ele alalım. Kod kazancı aşağıdaki eşitlik ile hesaplanır:

$$G = 10\log\left(\frac{7}{20}.\frac{5}{6}.3.11\right) = 9,834\,dB.$$

İyileşme miktarını göstermek için elde edilen kod kazancından $10\log 4E_b = 3,2056\ dB$ referans değerinin çıkarılması gerektiğine dikkat edilmelidir. Elde edilen değere göre,

önerilen kodlamanın $p=7$ için kod kazancında yaklaşık 6.628 dB iyileşme sağladığı söylenebilir (Tablo VII, ilk satıra bakınız). Bir genelleme yapıldığında, önerilen kodlama yönteminin sağladığı iyileşmenin [6dB-10dB] arasında olduğu görülmüştür.

Kod kazancına ek olarak, sayısal haberleşme sistemlerinin performansını değerlendirmek için kullanılan başka bir ölçüt bit veya sembol hata olasılığıdır. Sabit bir bit veya sembol hata oranı için, iki kodlama şeması arasındaki SNR farkı, şemanın daha düşük hata oranı sağlama başarısını göstermektedir [17]. Şekil 1.3'den görüldüğü gibi, önerilen kodlama şeması referans [1]'de incelenen kodlama ile karşılaştırıldığında daha düşük SNR değerleri vermektedir.

Tablo VI. Önerilen kodlar için sayısal değerler.

p	π	E_s	E_b	$10\log 4E_b$
7	$2+i+j+k$	2,939	0,523	3,206dB
13	$2+2i+2j+k$	4,431	0,582	3,670dB
17	$4+i$	5,648	0,691	4,414dB
29	$5+2i$	9,656	0,994	5,993 dB
37	$6+i$	12,324	1,183	6,750 dB
41	$5+4i$	13,658	1,275	7,075 dB
53	$7+2i$	17,660	1,542	7,900 dB
61	$6+5i$	20,328	1,714	8,360 dB
73	$8+5i$	24,328	1,956	8,955 dB

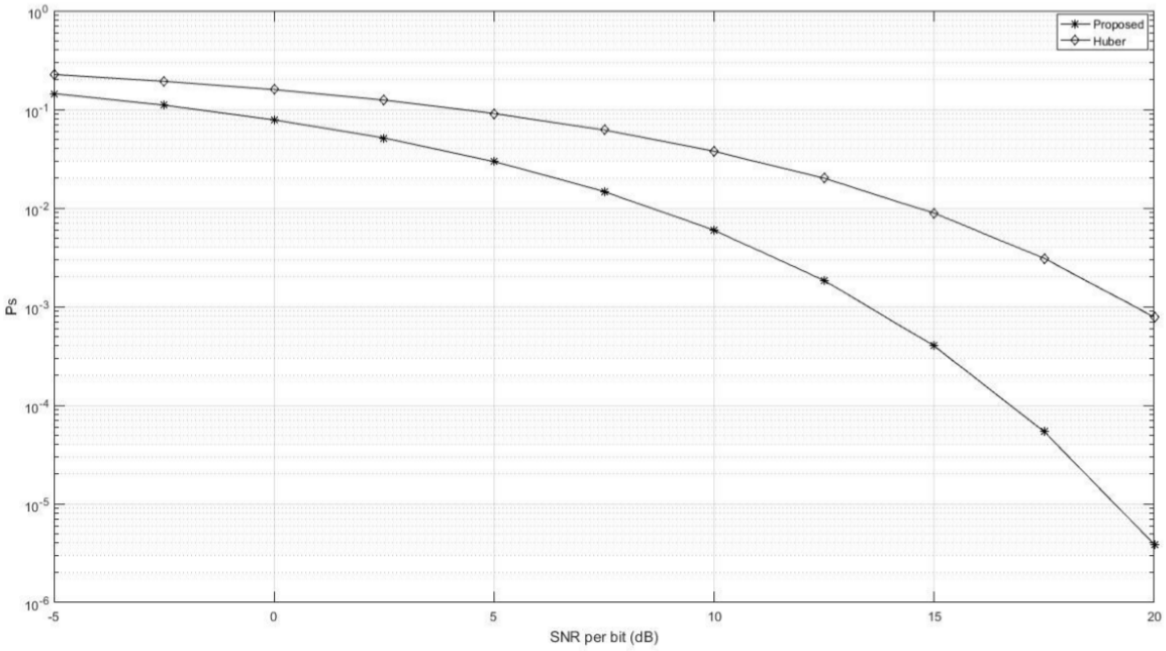
Tablo VII. Kod kazancı ve iyileşme.

p	Kod kazancı	İyileşme
7	9,834 dB	6,628 dB
13	11,005 dB	7,335 dB
41	14,504 dB	7,429 dB

Bu SNR eğrisinin grafiği MATLAB da aşağıdaki program yardımı ile çizilmiştir.

```
clc;clear all;
x=[-5:2.5:20];
y=db2mag(x);
```

```
Es=20.328;
Es1=10.164;
for i=1:size(y,2);
No(i)=Es/y(i);
EbNodb(i)=20*log10(Es/No(i));
EbNo(i)=(Es/No(i));
No1(i)=Es1/y(i);
EbNodb1(i)=20*log10(Es1/No1(i));
EbNo1(i)=(Es1/No1(i));
end
for i=1:size(y,2)
Ps(i)=qfunc(sqrt(2*Es/No(i)));
Ps1(i)=qfunc(sqrt(2*Es1/No(i)));
end
semilogy(EbNodb,Ps);
hold on; grid on
semilogy(EbNodb1,Ps1);
```



Şekil 1.3: $p = 61$ için AWGN kanalı üzerinden iletim için SNR karşılık sembol hata oranlarının referans [1] ile karşılaştırılması.

5.5 Sonuç

Bu çalışmada, Lipschitz tamsayıları üzerinde devirli kodlar önerilmektedir. Bu kodlar için Lipschitz metriğine dayalı bir kod çözme süreci de ortaya konulmaktadır. Sayısal haberleşme sistemleri için önerilen kodların kullanılabilirliğini ispatlamak için, AWGN kanal durumunda kodların performans değerlendirmesi incelenmektedir. Elde edilen sonuçlar, sunulan kodlama şemasının AWGN kanal durumunda kod kazancı ve sembol hata oranları bakımından sayısal haberleşme sistemlerinde performans artışı sağladığını göstermektedir. Kod kazancı tablosuna göre, kodlarımızın 6 dB'in üzerinde bir kod kazancı artışı sağladığını söyleyebiliriz. Ayrıca, haberleşme sisteminin güvenilirliğinin bir göstergesi olan sembol hata olasılıkları farklı SNR değerleri için hesaplanarak şekil üzerinde gösterilmiştir. Önerilen kodlama şeması ve [1]'de verilen şema arasındaki SNR farkı, önerilen Lipschitz metriğine dayalı kodlama şemasının başarısını açıkça göstermektedir.

BÖLÜM 6.

F_p Üzerinde Kuantum Kodlar

(1,2,3,6,7,8. iş paketleri, 4,6. ve 7. hedefler):

Bu çalışmada katkısı olanlar:

Doç. Dr. Murat GÜZELTEPE

Ercüment ÇAKIR

Bu çalışma bursiyerin tezi olmuştur.

6.1 Giriş

Bugüne kadar birçok yazar farklı halkalar veya farklı cisimler üzerinde hata düzeltebilen klasik kodlar ve kuantum kodlar üzerine çalışmıştır. Aşağıda yapılmış çalışmalar bunlara birer örnektir. 1950 de Hamming hata tespit edebilen ve hata düzeltilebilen kodları Hamming metriğine göre $\mathbb{Z}_2$ sonlu cismi üzerinde elde etmiştir [3]. 1958 de Lee $\mathbb{Z}_m$ sonlu halkası üzerinde Lee metriğine göre hata düzeltebilen kodlar elde etmiştir [4]. 1994 te Huber Gauss tamsayıları üzerinde Mannheim metriğine göre hata düzeltebilen kodlar tanımlamıştır [1]. Ayrıca Huber bu çalışmasında bu kodların iki boyutlu uzayda Mannheim metriğinin QAM (Quadrature Amplitude Modulation) için Lee ve Hamming metrikten daha uygun olduğunu göstermiştir. 2001 de Neto ve diğerleri kuadratik cisimler üzerinde yeni bir mannheim metriğine göre lineer kodlar inşa etmiştir [2]. 2009 da Martinez ve diğerleri ve bundan bağımsız olarak Özen ve Güzeltepe Lipschitz sayıları üzerinde Lipschitz metriğini tanımlayarak yeni lineer kodlar oluşturmuşlardır. 2013 te Güzeltepe Hurwitz sayıları üzerinde Hurwitz metriğini tanımlayarak kod hızı, minimum enerji ve bant genişliği açısından o güne kadar elde edilmiş kodlardan daha iyi kodlar oluşturmuştur [5].

Ayrıca günümüze kadar $\mathbb{F}_2+u\mathbb{F}_2$, $\mathbb{F}_2+v\mathbb{F}_2$, $\mathbb{F}_q+v\mathbb{F}_q$, $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ gibi birçok halka üzerinde hem klasik hem de kuantum kod çalışması yapılmıştır.

Bu bölümde F_π sonlu cismi tanımlanıp, bu cismin cebirsel özelikleri incelenecektir. Daha sonra bu cisim üzerindeki klasik devirli kodlar yardımıyla kuantum kodlar inşa edilecektir. Bu klasik kodların minimum mesafeleri bir Mathematica programı ile hesaplanacaktır. Hazırlanan bu program kuantum kodlar için bir veri tabanı formundadır.

6.2. F_p Kümesi ve Cebirsel Özellikleri

F_p kümesini tanımlamak için $N(\pi_1)=N(\pi_2)=p$ olan $\pi_1,\pi_2\in\mathbb{Z}[w]$ asal elemanları alınıp, $\mathbb{Z}[w]_{\pi_1}$ ve $\mathbb{Z}[w]_{\pi_2}$ kümeleri oluşturulacaktır. Bu kümelerde sırası ile $\bmod\pi_1$ ve $\bmod\pi_2$ kalan sınıfları vardır. Bu kalan sınıfları tam temsilciler kullanılarak yazılmaktadır. Yani $\pi_1=a+bw$ ve $u=x+yw\in\mathbb{Z}[w]_{\pi_1}$ ise $|x|+|y|\le|a|+|b|$ ve $v=x'+y'w\in\overline{x+yw}$ için $|x'|+|y'|\le|x|+|y|$ dir. Bu kümeler oluşturulduktan sonra $\mathbb{Z}[w]_{\pi_1}$ ile $\mathbb{Z}[w]_{\pi_2}$ kümelerinin izomorf olduğu gösterilerek, bu kümelerin elemanları ile F_p kümesi inşa edilecektir.

6.2.1. Teorem $\pi_1=a+bw$, $\pi_2=b+aw$ sayıları $\mathbb{Z}[w]$ kümesinde ilgili olmayan iki asal ve $\mathbb{Z}[w]_{\pi_1}$ ile $\mathbb{Z}[w]_{\pi_2}$ sırasıyla $\bmod\pi_1$ ve $\bmod\pi_2$ kalan sınıflar olsun. Bu durumda $\mathbb{Z}[w]_{\pi_1}$ ile $\mathbb{Z}[w]_{\pi_2}$ birbirine izomorftur.

İspat:

$f:\mathbb{Z}[w]_{\pi_1}\to\mathbb{Z}[w]_{\pi_2}$,

$f(x+yw)=x+yw^*$ fonksiyonunu göz önüne alalım. Bu fonksiyon iyi tanımlıdır. Çünkü

$x_1+y_1w=x_2+y_2w\ (\bmod\ \pi_1)$ iken $f(x_1+y_1w)=f(x_2+y_2w)$

olur. Gerçekte $x_1+y_1w=x_2+y_2w\Rightarrow x_1=x_2, y_1=y_2$ olduğunda

$$f(x_1+y_1w)=x_1+y_1w^*=x_2+y_2w^*=f(x_2+y_2w)$$

olur. f birebirdir. Çünkü

$$f(x_1+y_1w)=f(x_2+y_2w)\ \left(0\le N(x_1+y_1w),N(x_1+y_1w)\le N(\pi_1)\right)$$

$$\Rightarrow x_1+y_1w^*=x_2+y_2w\ ,\left(0\le N(x_1+y_1w^*),N(x_1+y_1w^*)\le N(\pi_2)=N(\pi_1)\right)$$

$$\Rightarrow x_1=x_2,\ y_1=y_2$$

$$\Rightarrow x_1+y_1w=x_2+y_2w$$

olur. f fonksiyonu birebir, $\mathbb{Z}[w]_{\pi_1}$ ile $\mathbb{Z}[w]_{\pi_2}$ kümelerinin eleman sayıları eşit ve sonlu olduğundan f fonksiyonu örtendir.

$\forall a=a_1+a_2w,\ b=b_1+b_2w\in\mathbb{Z}[w]_{\pi_1}$ için

$$
\begin{aligned}
f(a+b) &= f\left(\left(a_1+a_2w\right)+\left(b_1+b_2w\right)\right)\\
&= f\left(\left(a_1+b_1\right)+\left(a_2+b_2\right)w\right)\\
&= \left(a_1+b_1\right)+\left(a_2+b_2\right)w^*\\
&= \left(a_1+a_2w^*\right)+\left(b_1+b_2w^*\right)\\
&= f\left(a_1+a_2w\right)+f\left(b_1+b_2w\right)\\
&= f(a)+f(b)
\end{aligned}
$$

ve

$$
\begin{aligned}
f(ab) &= f\left(\left(a_1+a_2w\right)\left(b_1+b_2w\right)\right)\\
&= f\left(a_1b_1-a_2b_2+\left(a_1b_2+a_2b_1+a_2b_2\right)w\right)\\
&= a_1b_1-a_2b_2+\left(a_1b_2+a_2b_1+a_2b_2\right)w^*\\
&= \left(a_1+a_2w^*\right)\left(b_1+b_2w^*\right)\\
&= f\left(a_1+a_2w\right)f\left(\left(b_1+b_2w\right)\right)\\
&= f(a)f(b)
\end{aligned}
$$

olduğundan f fonksiyonu homomorfizmadır. f, fonksiyonu, birebir, örten ve homomorfizma olduğundan bir izomorfizmadır. Dolayısıyla $\mathbb{Z}[w]_{\pi_1} \cong \mathbb{Z}[w]_{\pi_2}$ olur.

6.2.2. Tanım $\mathbb{Z}[w]_{\pi_1}$ ve $\mathbb{Z}[w]_{\pi_2}$ yukarıdaki gibi tanımlansın. $a+bw \in \mathbb{Z}[w]_{\pi_1}$ ve $f(a+bw) = a'+b'w \in \mathbb{Z}[w]_{\pi_2}$ olmak üzere

$$F_p = \left\{a+bw : |a|+|b| \le |a'|+|b'|\right\} \cup \left\{a'+b'w^* : |a'|+|b'| < |a|+|b|\right\}$$

olarak tanımlanır.

6.2.3. Teorem Yukarıda tanımlanan F_p kümesi eleman sayısı $N(\pi) = p$ olan sonlu bir cisimdir.

İspat: F_p kümesinin adi toplama işlemine göre bir değişmeli grup, ayrıca çarpma işlemine göre kapalı olduğu kolayca görülebilir. Yani F_p bir tamlık bölgesidir. Diğer yandan her $0 \neq a \in F_p$ elemanı bir asal kalan sınıf olduğundan tersi vardır. Dolayısıyla F_p bir sonlu cisimdir.

6.2.4. Örnek $p = 7$, $\pi_1 = 2+w$ ve $\pi_2 = 1+2w$ olsun. Bu durumda

$\mathbb{Z}[w]_{\pi_1} = \{0, 1, -w, 1-w, -1+w, w, -1\}$ ve

$$\mathbb{Z}[w]_{\pi_2} = \{0, 1, -1+w, w, -w, 1-w, -1\}$$

olur. $f : \mathbb{Z}[w]_{\pi_1} \to \mathbb{Z}[w]_{\pi_2}$ fonksiyonu $f(x+yw) = x + yw^*$ olarak tanımlanırsa

$$f(0) = 0$$
$$f(1) = 1$$
$$f(-w) = -w^* = -1 + w$$
$$f(1-w) = 1 - w^* = w$$
$$f(-1+w) = -1 + w^* = -w$$
$$f(w) = w^* = 1 - w$$
$$f(-1) = -1$$

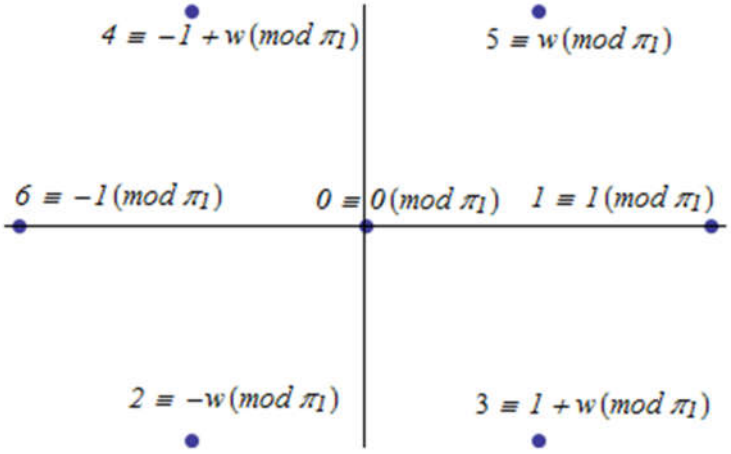
elde edilir. Bu durumda F_7 kümesi

$$F_7 = \left\{\bar{0}, \bar{1}, \overline{-w}, \overline{w^*}, \overline{-w^*}, \bar{w}, \overline{-1}\right\}$$

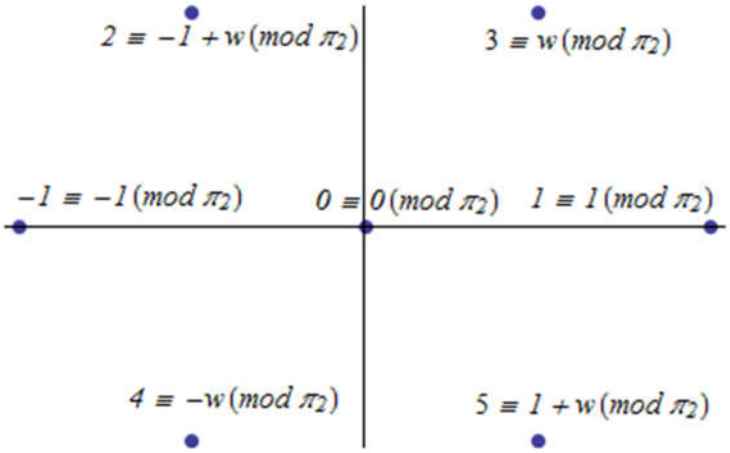
şeklinde elde edilir. $\mathbb{Z}[w]_{\pi_1}$ ile $\mathbb{Z}[w]_{\pi_2}$ kümelerinin yardımıyla $\mathbb{Z}_7$ kümesinin elemanları ile F_7 kümesinin elemanlarının eşleştirilmesi Tablo 1 deki gibidir. Şekil 1, Şekil 2 ve Şekil 3 de ise sırasıyla $\mathbb{Z}[w]_{\pi_1}$, $\mathbb{Z}[w]_{\pi_2}$ ve F_7 kümesinin elemanlarının kompleks düzlemdeki konumları gösterilmiştir.

Tablo 1: $\mathbb{Z}_7$ kümesinin elemanları ile F_7 kümesinin elemanlarının eşleştirilmesi

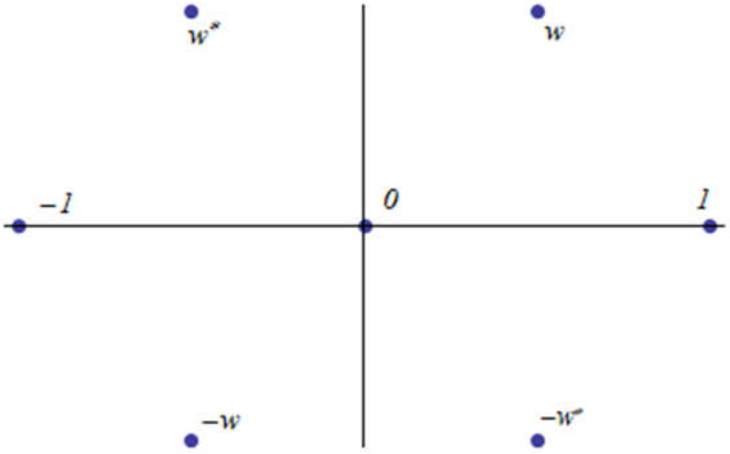
$\mathbb{Z}_7$	$\mathbb{Z}[w]_{\pi_1}$	$\mathbb{Z}[w]_{\pi_2}$	F_7
0	0	0	0
1	1	1	1
2	$-w$	$-1+w$	$-w$
3	$1-w$	w	w^*
4	$-1+w$	$-w$	$-w^*$
5	w	$1-w$	w
6	-1	-1	-1



Şekil 1. $\mathbb{Z}[w]_{\pi_1}$ kümesinin elemanları



Şekil 2. $\mathbb{Z}[w]_{\pi_2}$ kümesinin elemanları



Şekil 3. F_7 Kümesi elemanlarının kompleks düzlemde yeri

6.3. F_p Üzerinde Kuantum Kodlar

$w=\frac{1}{2}+\frac{i\sqrt{3}}{2}=\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}$ elemanı birimin $6.$ mertebeden köküdür. $w\in F_p$ olduğundan, F_7 de mertebesi $6n$ olan bir eleman her zaman vardır. Bu eleman β olsun. Yani $\beta^{6n}=1$ dir. $\beta^{6n}=1$ ise $\beta^n=\pm w$ olur. Bu durumda x^n-w ve x^n+w polinomları $t=0,1,\ldots n-1$ olmak üzere β elemanının yardımı ile

$$x^n-w=(x-\beta)\left(x-\beta^7\right)\ldots\left(x-\beta^{6t+1}\right)$$

$$x^n+w=(x+\beta)\left(x+\beta^7\right)\ldots\left(x+\beta^{6t+1}\right)$$

şeklinde çarpanlarına ayrılır.

x^n-w polinomu ile x^n+w polinomlarının çarpımı ise aşağıdaki gibi çarpanlarına ayrılır.

$$x^{2n}+w^*=(x-\beta)\left(x-\beta^7\right)\ldots\left(x-\beta^{6t+1}\right)(x+\beta)\left(x+\beta^7\right)\ldots\left(x+\beta^{6t+1}\right) \qquad (*)$$

Not: $p=13$ için $\beta^2=w$ şartını sağlayan $\beta=2$ dir. Ancak $\beta^2=-w$ olduğundan F_{13} de

$$x^2+w=\left(x-\beta^4\right)\left(x+\beta^4\right)$$

olarak çarpanlarına ayrılır.

6.3.1. Tanım $\theta\in\{w,w^*\}$ olmak üzere $z=a+b\theta\in F_p$ elemanının ağırlığı

$$w_M(z)=|a|+|b|$$

ve

$z_1=a_1+b_1\theta$, $z_2=a_2+b_2\theta\in F_p$ için z_1 ile z_2 arasındaki mesafe $z_1-z_2\equiv z=a+b\theta\in F_p$ olmak üzere

$$d_M(z_1,z_2)=w_M(z)=|a|+|b|$$

olarak tanımlanır.

6.3.2. Teorem $\theta\in\{w,w^*\}$ olsun. Eğer $x+y\theta\in F_p$ ise $\forall m+n\theta\in\overline{x+y\theta}$ için $|x|+|y|\le|m|+|n|$ dir.

İspat: $\theta = w$ olsun. Bu durumda $m + nw \in \mathbb{Z}[w]_{\pi_1}$ olur. $\mathbb{Z}[w]_{\pi_1}$ in tanımından $|x| + |y| \leq |m| + |n|$ olur. $\theta = w^*$ olsun. Bu durumda $f(m + nw^*) = m + nw \in \mathbb{Z}[w]_{\pi_2}$ olur. $\mathbb{Z}[w]_{\pi_2}$ nin tanımından $|x| + |y| \leq |m| + |n|$ olur.

6.3.2. Teorem Yukarıda tanımlanan d_M mesafesi F_p üzerinde bir metriktir.

İspat: $i.$ $\forall z = a + b\theta \in F_\pi$ için $d_M(z,z) = w_M(a + b\theta - (a + b\theta)) = w(0) = 0$

dır.

$d_M(z_1, z_2) = 0 \Rightarrow \quad w(z_1 - z_2) = 0 \Rightarrow \quad z_1 \equiv z_2 \pmod{\pi_1} \Rightarrow z_1 \in \mathbb{Z}[w]_{\pi_1}$ ve $z_2 \in \mathbb{Z}[w]_{\pi_1}$

olduğundan $\overline{z_1} = \overline{z_2}$ dir.

$ii.$ $z_1, z_2 \in F_p$ olmak üzere $d(z_1, z_2) = d(z_2, z_1)$ dir. Gerçekten de

$$\begin{aligned} d_M(z_1, z_2) &= w_M(z_1 - z_2) \\ &= |a_1 - a_2| + |b_1 - b_2| \\ &= |a_2 - a_1| + |b_2 - b_1| \\ &= w(z_2 - z_1) = d(z_2, z_1) \end{aligned}$$

olur.

$iii.$ $d_M(z_1, z_2) = w_M(z_1 - z_2) = w_M(\delta_1) = |a_1| + |b_1|$ burada $\delta_1 \equiv \overline{z_1 - z_2} = a_1 + b_1\theta \in F_p$ ve $|a_1| + |b_1|$ minimumdur.

$d_M(z_1, z_3) = w_M(z_1 - z_3) = w_M(\delta_2) = |a_2| + |b_2|$ ve $\delta_2 \equiv \overline{z_1 - z_3} = a_2 + b_2\theta \in F_p$ dir.

$d_M(z_3, z_2) = w_M(z_3 - z_2) = w_M(\delta_3) = |a_3| + |b_3|$ ve $\delta_3 \equiv \overline{z_3 - z_2} = a_3 + b_3\theta \in F_p$ dir. Ancak

$w_M(\delta_2 + \delta_3) \geq w_M(\delta_1)$

dir. Çünkü $\delta_2 + \delta_3 \in \overline{z_1 - z_2}$ ve biliyoruz ki $\forall x + y\theta \in \overline{z_1 - z_2}$ için $|a_1| + |b_1| \leq |x| + |y|$ dir.

6.3.3. Teorem $\mathbb{F}_p$ de $[n, k_1, d_1]$ parametrelerine sahip C_1 kodunun üreteç polinomu $g_1(x)$ ve $[n, k_2, d_2]$ parametrelerine sahip C_2 kodunun üreteç polinomu $g_2(x)$ olsun. Eğer $g_1(x) | g_2(x)$ ise $C_2 \subseteq C_1$ dir [13].

6.3.4. Teorem C_1 ve C_2 yukarıdaki şartları sağlayan devirli kodlar olsun. Bu durumda $\mathbb{F}_p$ üzerinde $\left[\left[n, k_1 - k_2, \min\left\{d_1, d_2^{\perp}\right\}\right]\right]_p$ parametreli bir kuantum kod vardır [6].

(*) eşitliği ve 6.3.3. Teorem göz önüne alındığında $g_1(x) | g_2(x)$ olacak şekilde $g_1(x)$ ve $g_2(x)$ üreteç polinomları, $f_1, f_2, \ldots f_n, f_{n+1}, \ldots, f_{2n}$ polinomları kullanılarak farklı ihtimaller dahilinde seçilebilir.

6.3.6. Örnek $p = 13$ olsun. Bu durumda F_{13} kümesi

$$F_{13} = \left\{0, 1, 2, -w^*, w, -2w, -2w^*, 2w^*, 2w, -w, w^*, -2, -1\right\}$$

olarak hesaplanır. $\beta = 2 \in F_{13}$ alınırsa, F_{13} üzerinde $x^2 - w$ ile $x^2 + w$

$$x^2 - w = (x - \beta)\left(x - \beta^7\right),$$

$$x^2 + w = \left(x - \beta^4\right)\left(x + \beta^4\right)$$

şeklinde çarpanlarına ayrılır. Buradan da

$$x^4 + w^* = (x - \beta)\left(x - \beta^7\right)\left(x - \beta^4\right)\left(x + \beta^4\right) = f_1 f_2 f_3 f_4$$

elde edilir.

$g_1(x)$ ile $g_2(x)$ üreteç polinomları $g_1(x) | g_2(x)$ olacak şekilde seçilirse, oluşabilecek kuantum kod parametreleri Tablo 2 de verilmiştir. Tablo 3 te $p = 19$ ve $\beta = 2$ alınmıştır.

6.3.7. Örnek $p = 19$ olsun. Bu durumda F_{19} kümesi

$$F_{19} = \left\{0, 1, 2, -2w, 1 - 2w, 2w^*, -1 - w^*, -w^*, w, 1 + w, -1 - w, -w, w^*, 1 + w^*, -2w^*, -1 + 2w, 2w, -2, -1\right\}$$

olarak hesaplanır. $\beta = 3 \in F_{19}$ alınırsa, F_{19} üzerinde $x^3 - w$ ile $x^3 + w$

$$x^3 - w = (x - \beta)\left(x - \beta^7\right)\left(x - \beta^{13}\right),$$

$$x^3 + w = (x + \beta)\left(x + \beta^7\right)\left(x + \beta^{13}\right)$$

olarak çarpanlarına ayrılır. Buradan da

$$x^6 + w^* = (x - \beta)\left(x - \beta^7\right)\left(x - \beta^{13}\right)(x + \beta)\left(x + \beta^7\right)\left(x + \beta^{13}\right) = f_1 f_2 f_3 f_4 f_5 f_6$$

elde edilir.

$g_1(x)$ ile $g_2(x)$ üreteç polinomları $g_1(x)|g_2(x)$ olacak şekilde seçilirse, oluşabilecek kuantum kod parametreleri Tablo 3 de verilmiştir.

Yukarıdakiler dikkate alınarak elde edilebilecek mümkün tüm kuantum kodlar aşağıdaki Mathematica programı kullanılarak hesaplanabilir. Şekil 4 de program ve Şekil 5 de programın çıktılarının bir kısmı verilmektedir. Bu program kodlama teorisinde bir databank olarak kullanılabilir.

```
Do[
 If[Element[p = 6 * n + 1, Primes],
  {nn = (p - 1) / 6;
   Do[
     Do[
      If[t^2 + t * k + k^2 == p, {a = t, b = k}]
      , {t, 1, p}]
     , {k, 1, p}]
    tt = a + b - 1;
   AR = Table[1, {p}, {2}];
   Do[If[Mod[a + b * s, p] == 0, r = s], {s, 0, p - 1}]
    f[g_] := (Reap[Do[Do[If[Mod[x + y * r, p] == g && Abs[x] + Abs[y] < Abs[tt] + Abs[tt], Sow[x]],
          {x, -tt, tt}], {y, -tt, tt}]][[2, 1]]);
   h[u_] := Reap[Do[Do[If[Mod[x + y * r, p] == u && Abs[x] + Abs[y] < Abs[tt] + Abs[tt], Sow[y]],
        {x, -tt, tt}], {y, -tt, tt}]][[2, 1]];
   Do[While[f[kk] && h[kk], {x, y}]; ttt = Ordering[Abs[f[kk]] + Abs[h[kk]], 1][[1]];
    AR[[kk + 1, 1]] = f[kk][[ttt]]; AR[[kk + 1, 2]] = h[kk][[ttt]], {kk, 0, p - 1}];
   Do[
     Do[
      If[t^2 + t * k + k^2 == p, {a = t, b = k}]
      , {t, 1, p}]
     , {k, 1, p}]
    tt = a + b - 1;
   BR = Table[1, {p}, {2}];
   Do[If[Mod[b + a * s, p] == 0, r = s], {s, 0, p - 1}]
    f[n_] := (Reap[Do[Do[If[Mod[x + y * r, p] == n && Abs[x] + Abs[y] < Abs[tt] + Abs[tt], Sow[x]],
          {x, -tt, tt}], {y, -tt, tt}]][[2, 1]]);
   h[m_] := Reap[Do[Do[If[Mod[x + y * r, p] == m && Abs[x] + Abs[y] < Abs[tt] + Abs[tt], Sow[y]],
        {x, -tt, tt}], {y, -tt, tt}]][[2, 1]];
   Do[While[f[kk] && h[kk], {x, y}]; ttt = Ordering[Abs[f[kk]] + Abs[h[kk]], 1][[1]];
    BR[[kk + 1, 1]] = f[kk][[ttt]]; BR[[kk + 1, 2]] = h[kk][[ttt]], {kk, 0, p - 1}];
```

```
A = Table[1, {p}, {2}];
Do[If[Abs[AR[[i + 1, 1]]] + Abs[AR[[i + 1, 2]]] < Abs[BR[[i + 1, 1]]] + Abs[BR[[i + 1, 2]]],
    {A[[i + 1, 1]] = AR[[i + 1, 1]], A[[i + 1, 2]] = AR[[i + 1, 2]]} ,  {A[[i + 1, 1]] = BR[[i + 1, 1]] ,
     A[[i + 1, 2]] = BR[[i + 1, 2]]}], {i, 0, p - 1}]
  T[k_, l_, m_, n_] := Function[Mod[ (k + m) + (l + n) * r, p]][k, l, m, n];
A[[T[1, 0, 1, 0] + 1]];
Ç[k_, l_, m_, n_] := Function[Mod[ (k * m - l * n) + (k * n + l * n + l * m) * r, p]][k, l, m, n];
A[[Ç[2, 0, 2, 0] + 1]];
K[k_, l_] := Function[Mod[ (k + r * l), p]][k, l];
(*A[[KK=K[2,0]^nn+1]];*)
Do[aa = Mod[tt^nn, p]; If[aa == r || aa == p - r, A[[tt + 1]]], {tt, 1, p - 1}];
B = Table[1, {nn}];
Do[B[[gg]] = FactorList[x^nn + r, Modulus → p][[gg + 1, 1]], {gg, 1, nn}];
BB = Table[1, {nn}];
Do[BB[[gg]] = FactorList[x^nn - r, Modulus → p][[gg + 1, 1]], {gg, 1, nn}];

CC = Subsets[B];
CCC = Table[1, {2^nn - 1}];
Do[CCC[[kk - 1]] = Expand[∏_{j=1}^{Dimensions[CC[[kk]]][[1]]} CC[[kk]][[j]], Modulus → p], {kk, 2, 2^nn}];
DDD = Table[1, {2^nn - 1}];
Do[DDD[[kk - 1]] = Expand[∏_{j=1}^{Dimensions[DD[[kk]]][[1]]} DD[[kk]][[j]], Modulus → p], {kk, 2, 2^nn}];

v = ∑_{i=1}^{nn} Binomial[nn, i];
KK = Table[1, {v^2}];
t = 0;
Do[
 Do[t = t + 1;
  KK[[t]] = Expand[CCC[[k]] * DDD[[kk]], Modulus → p]
  , {k, 1, v}]
 , {kk, 1, v}];
fs = Union[KK, CCC, DDD];
zzmaks = (∑_{i=1}^{2*nn} (2 * nn) ! / (i ! * (2 * nn - i) !));
GD1 = Table[1, {2 * nn}];
sayı = 0;
```

```
Do[
 Do[
  If[PolynomialRemainder[fs[[zz2]], fs[[zz1]], x, Modulus → p] == 0,
   {sayı = sayı + 1,  G1 = Table[1, {2 * nn}];
    Do[G1[[i + 1]] = Coefficient[fs[[zz1]], x, i], {i, 0, 2 * nn - 1}]
     G = Table[1, {2 * nn - Exponent[fs[[zz1]], x]}];
    Do[G[[j + 1]] = RotateRight[G1, j], {j, 0, 2 * nn - 1 - Exponent[fs[[zz1]], x]}];
    G // MatrixForm
      PP = Tuples[Range[0, p - 1], 2 * nn - Exponent[fs[[zz1]], x]];
    LK = Table[1, {p^(2 * nn - Exponent[fs[[zz1]], x])}];
    Do[
     LK[[i]] = Mod[∑_{j=1}^{2*nn-Exponent[fs[[zz1]],x]} PP[[i, j]] * G[[j]], p]
     , {i, 1, p^(2 * nn - Exponent[fs[[zz1]], x])}];
    d = nn * tt;
    Do[If[∑_{i=1}^{2*nn} (Abs[A[[LK[[k, i]] + 1]][[1]]] + Abs[A[[LK[[k, i]] + 1]][[2]]]) < d,
      d = ∑_{i=1}^{2*nn} (Abs[A[[LK[[k, i]] + 1]][[1]]] + Abs[A[[LK[[k, i]] + 1]][[2]]])],
     {k, 2, Dimensions[LK][[1]]}];
```

```
G2 = Table[1, {2 * nn}];
Do[G2[[i + 1]] = Coefficient[fs[[zz2]], x, i], {i, 0, 2 * nn - 1}]
 GG = Table[1, {2 * nn - Exponent[fs[[zz2]], x]}];
Do[GG[[j + 1]] = RotateRight[G2, j], {j, 0, 2 * nn - 1 - Exponent[fs[[zz2]], x]}];
GG // MatrixForm
  PP2 = Tuples[Range[0, p - 1], 2 * nn - Exponent[fs[[zz2]], x]];
LK2 = Table[1, {p^(2 * nn - Exponent[fs[[zz2]], x])}];
Do[
 LK2[[i]] = Mod[ Sum[PP2[[i, j]] * GG[[j]], {j, 1, 2*nn-Exponent[fs[[zz2]],x]}], p]
 , {i, 1, p^(2 * nn - Exponent[fs[[zz2]], x])}];

fs2 = PolynomialQuotient[fs[[Dimensions[fs]]][[1]], fs[[zz2]], x, Modulus → p];
Do[GD1[[i + 1]] = Coefficient[fs2, x, i]
 , {i, 0, 2 * nn - 1}];
GD = Table[1, {2 * nn - Exponent[fs2, x]}];
Do[
 GD[[j + 1]] = RotateRight[GD1, j]
 , {j, 0, 2 * nn - 1 - Exponent[fs2, x]}];
PPD = Tuples[Range[0, p - 1], 2 * nn - Exponent[fs2, x]];
LKD = Table[1, {p^(2 * nn - Exponent[fs2, x])}];
Do[
 LKD[[rr]] = Mod[ Sum[PPD[[rr, j]] * GD[[j]], {j, 1, 2*nn-Exponent[fs2,x]}], p]
 , {rr, 1, p^(2 * nn - Exponent[fs2, x])}];
      dd = nn * tt;
      Do[If[ Sum[(Abs[A[[LKD[[k, i]] + 1]][[1]]] + Abs[A[[LKD[[k, i]] + 1]][[2]]]), {i, 1, 2*nn}] < dd,
        dd = Sum[(Abs[A[[LKD[[k, i]] + 1]][[1]]] + Abs[A[[LKD[[k, i]] + 1]][[2]]]), {i, 1, 2*nn}]],
       {k, 2, Dimensions[LKD][[1]]}],
      minmsf = Min[d, dd];
      Print[{"p=", p, "sayı=", sayı, "g1(x)=", fs[[zz1]],   "g2(x)=", fs[[zz2]],
        "d1=", d, "d2=", dd, "kuantum kod=",
        {2 * nn, Exponent[fs[[zz2]], x] - Exponent[fs[[zz1]], x], minmsf}]]
    , {zz2, 1, zzmaks - 1}]
   , {zz1, 1, zzmaks - 1}]]
 , {n, 1, 2}]
```

Şekil 4: Mathematica Programı.

{p=, 7, sayı=, 1, g1(x)=, 2 + x, g2(x)=, 2 + x, d1=, 2, d2=, 2, kuantum kod=, {2, 0, 2}}

{p=, 7, sayı=, 2, g1(x)=, 5 + x, g2(x)=, 5 + x, d1=, 2, d2=, 2, kuantum kod=, {2, 0, 2}}

{p=, 13, sayı=, 1, g1(x)=, 4 + x, g2(x)=, 4 + x, d1=, 2, d2=, 4, kuantum kod=, {4, 0, 2}}

{p=, 13, sayı=, 2, g1(x)=, 4 + x, g2(x)=, $10 + x^2$, d1=, 2, d2=, 2, kuantum kod=, {4, 1, 2}}

{p=, 13, sayı=, 3, g1(x)=, 4 + x, g2(x)=, $11 + 10\,x + x^2$, d1=, 2, d2=, 4, kuantum kod=, {4, 1, 2}}

{p=, 13, sayı=, 4, g1(x)=, 4 + x, g2(x)=, $2 + 11\,x + x^2$, d1=, 2, d2=, 4, kuantum kod=, {4, 1, 2}}

{p=, 13, sayı=, 5, g1(x)=, 4 + x, g2(x)=, $12 + 3\,x + 4\,x^2 + x^3$, d1=, 2, d2=, 2, kuantum kod=, {4, 2, 2}}

{p=, 13, sayı=, 6, g1(x)=, 4 + x, g2(x)=, $8 + 10\,x + 6\,x^2 + x^3$, d1=, 2, d2=, 2, kuantum kod=, {4, 2, 2}}

{p=, 13, sayı=, 7, g1(x)=, 4 + x, g2(x)=, $5 + 10\,x + 7\,x^2 + x^3$, d1=, 2, d2=, 2, kuantum kod=, {4, 2, 2}}

{p=, 13, sayı=, 8, g1(x)=, 6 + x, g2(x)=, 6 + x, d1=, 2, d2=, 6, kuantum kod=, {4, 0, 2}}

{p=, 13, sayı=, 9, g1(x)=, 6 + x, g2(x)=, $3 + x^2$, d1=, 2, d2=, 2, kuantum kod=, {4, 1, 2}}

{p=, 13, sayı=, 10, g1(x)=, 6 + x, g2(x)=, $2 + 2\,x + x^2$, d1=, 2, d2=, 4, kuantum kod=, {4, 1, 2}}

{p=, 13, sayı=, 11, g1(x)=, 6 + x, g2(x)=, $11 + 10\,x + x^2$, d1=, 2, d2=, 4, kuantum kod=, {4, 1, 2}}

{p=, 13, sayı=, 12, g1(x)=, 6 + x, g2(x)=, $12 + 3\,x + 4\,x^2 + x^3$, d1=, 2, d2=, 2, kuantum kod=, {4, 2, 2}}

{p=, 13, sayı=, 13, g1(x)=, 6 + x, g2(x)=, $8 + 10\,x + 6\,x^2 + x^3$, d1=, 2, d2=, 2, kuantum kod=, {4, 2, 2}}

{p=, 13, sayı=, 14, g1(x)=, 6 + x, g2(x)=, $1 + 3\,x + 9\,x^2 + x^3$, d1=, 2, d2=, 2, kuantum kod=, {4, 2, 2}}

{p=, 13, sayı=, 15, g1(x)=, 7 + x, g2(x)=, 7 + x, d1=, 2, d2=, 6, kuantum kod=, {4, 0, 2}}

{p=, 13, sayı=, 16, g1(x)=, 7 + x, g2(x)=, $3 + x^2$, d1=, 2, d2=, 2, kuantum kod=, {4, 1, 2}}

{p=, 13, sayı=, 17, g1(x)=, 7 + x, g2(x)=, $11 + 3\,x + x^2$, d1=, 2, d2=, 4, kuantum kod=, {4, 1, 2}}

{p=, 13, sayı=, 18, g1(x)=, 7 + x, g2(x)=, $2 + 11\,x + x^2$, d1=, 2, d2=, 4, kuantum kod=, {4, 1, 2}}

{p=, 13, sayı=, 19, g1(x)=, 7 + x, g2(x)=, $12 + 3\,x + 4\,x^2 + x^3$, d1=, 2, d2=, 2, kuantum kod=, {4, 2, 2}}

{p=, 13, sayı=, 20, g1(x)=, 7 + x, g2(x)=, $5 + 10\,x + 7\,x^2 + x^3$, d1=, 2, d2=, 2, kuantum kod=, {4, 2, 2}}

Şekil 5: Mathematica Programının Çıktıları.

Tablo 2: Mannheim ve Hamming mesafesine göre F_{13} için kuantum kod parametreleri

$g_1(x)$	$g_2(x)$	Mannheim metriğine göre QEEC	Hamming metriğine göre QEEC
f_1	f_1	$[[4,0,2]]_{13}$	$[[4,0,2]]_{13}$
f_1	f_1f_2	$[[4,1,2]]_{13}$	$[[4,1,2]]_{13}$
f_1	$f_1f_2f_3$	$[[4,2,2]]_{13}$	$[[4,2,2]]_{13}$
f_1f_2	f_1f_2	$[[4,0,2]]_{13}$	$[[4,0,2]]_{13}$
f_1f_2	$f_1f_2f_3$	$[[4,1,2]]_{13}$	$[[4,1,2]]_{13}$
f_1f_4	f_1f_4	$[[4,0,4]]_{13}$	$[[4,0,3]]_{13}$
$f_1f_2f_3$	$f_1f_2f_3$	$[[4,0,2]]_{13}$	$[[4,0,2]]_{13}$

Tablo 3: Mannheim ve Hamming mesafesine göre F_{13} için kuantum kod parametreleri

$g_1(x)$	$g_2(x)$	Mannheim metriğine göre QEEC	Hamming metriğine göre QEEC
f_1	f_1	$[[6,0,2]]_{19}$	$[[6,0,2]]_{19}$
f_1	f_1f_2	$[[6,1,2]]_{19}$	$[[6,1,2]]_{19}$
f_1	$f_1f_2f_3$	$[[6,2,2]]_{19}$	$[[6,2,2]]_{19}$
f_1	$f_1f_2f_3f_4$	$[[6,3,2]]_{19}$	$[[6,3,2]]_{19}$
f_1	$f_1f_2f_3f_4f_5$	$[[6,4,2]]_{19}$	$[[6,4,2]]_{19}$
f_1f_2	f_1f_2	$[[6,0,2]]_{19}$	$[[6,0,2]]_{19}$
f_1f_2	$f_1f_2f_3$	$[[6,1,2]]_{19}$	$[[6,1,2]]_{19}$
f_1f_2	$f_1f_2f_3f_4$	$[[6,2,2]]_{19}$	$[[6,2,2]]_{19}$
f_1f_2	$f_1f_2f_3f_4f_5$	$[[6,3,2]]_{19}$	$[[6,3,2]]_{19}$
f_1f_4	f_1f_4	$[[6,0,3]]_{19}$	$[[6,0,2]]_{19}$
f_1f_4	$f_1f_4f_5$	$[[6,1,3]]_{19}$	$[[6,1,2]]_{19}$
f_1f_4	$f_1f_3f_4f_5$	$[[6,2,3]]_{19}$	$[[6,2,2]]_{19}$
f_1f_6	f_1f_6	$[[6,0,4]]_{19}$	$[[6,0,3]]_{19}$
f_1f_6	$f_1f_3f_6$	$[[6,1,4]]_{19}$	$[[6,1,3]]_{19}$
f_1f_6	$f_1f_2f_5f_6$	$[[6,2,4]]_{19}$	$[[6,2,3]]_{19}$
$f_1f_2f_6$	$f_1f_2f_6$	$[[6,0,5]]_{19}$	$[[6,0,4]]_{19}$
$f_1f_2f_6$	$f_1f_2f_5f_6$	$[[6,1,4]]_{19}$	$[[6,1,3]]_{19}$
$f_1f_2f_6$	$f_1f_2f_3f_5f_6$	$[[6,2,2]]_{19}$	$[[6,2,2]]_{19}$
$f_1f_2f_4$	$f_1f_2f_4$	$[[6,0,5]]_{19}$	$[[6,0,3]]_{19}$
$f_1f_2f_4$	$f_1f_2f_4f_6$	$[[6,1,4]]_{19}$	$[[6,1,3]]_{19}$
$f_1f_2f_4$	$f_1f_2f_4f_5$	$[[6,1,3]]_{19}$	$[[6,1,3]]_{19}$
$f_1f_2f_4f_5$	$f_1f_2f_4f_5$	$[[6,0,3]]_{19}$	$[[6,0,2]]_{19}$
$f_1f_2f_4f_5$	$f_1f_2f_4f_5f_6$	$[[6,1,2]]_{19}$	$[[6,1,2]]_{19}$
$f_1f_3f_5f_6$	$f_1f_3f_5f_6$	$[[6,0,4]]_{19}$	$[[6,0,3]]_{19}$
$f_1f_2f_3f_4f_5$	$f_1f_2f_3f_4f_5$	$[[6,0,2]]_{19}$	$[[6,0,2]]_{19}$

BÖLÜM 7.

R_π Üzerinde Yeni Sinyal Yıldız Kümesi

(1,2,3,6,7,8. iş paketleri, 4,6. ve 7. hedefler):

Bu çalışmada katkısı olanlar:

Doç. Dr. Murat GÜZELTEPE

Ercüment ÇAKIR

Bu çalışmada bursiyerin tezinin bir bölümünü oluşturmaktadır.

7.1 Giriş

Bu bölümde R_π sonlu halkası tanımlanıp, bu halkanın cebirsel özelikleri incelenecektir. $N(\pi)=m$ elemanlı bir takım yıldızının (Constellation) kod kazancı için önce bu takım yıldızının ortalama enerji hesabı olan E_π hesaplanacaktır. M takım yıldızının boyutu ve d_M de bu takım yıldızında kullanılan metrik olsun. Bu durumda m elemanlı bir takım yıldızı üzerinde inşa edilen kodun takım yıldızının değer katsayısı olan CFM (Constellation Figure of Merit) değeri

$$CFM=\frac{Md_M^2}{2E_\pi}$$

ile hesaplanır. CFM arttıkça kod kazancının arttığı bilinmektedir. Dolayısıyla daha iyi bir kodlama elde edilir. CFM değeri hesaplarken M ve 2 sabit olduğundan amaç ortalama enerjiyi küçültürken minimum mesafeyi büyültmektir. Bu çalışmada p elemanlı bir takım yıldızı $p|m$ olmak üzere m elemanlı bir takım yıldızına gömülecektir ve CFM değerleri karşılaştırılacaktır. Bu takım yıldızı Eisenstein-Jacobi tamsayıları kullanılarak oluşturulacaktır.

7.2. R_π Kümesi ve Cebirsel Özellikleri

p_1 ve p_2, $p_1\equiv p_2\equiv 1\pmod 6$ şartını sağlayan farklı iki tek asal tamsayı, $N(\pi)=N(\pi')=p_1p_2=m$ olmak üzere $\mathbb{Z}[w]_\pi$ ve $\mathbb{Z}[w]_{\pi'}$ sırasıyla $\bmod \pi$ ve $\bmod \pi'$ de

kalan sınıflar olsun. Bu durumda $\mathbb{Z}[w]_{\pi}$ ve $\mathbb{Z}[w]_{\pi'}$ kümeleri halkadır ve bu halkalar birbirine izomorftur.

7.2.1. Tanım: $\mathbb{Z}[w]_{\pi}$ ve $\mathbb{Z}[w]_{\pi'}$ yukarıdaki gibi tanımlansın. $x+yw \in \mathbb{Z}[w]_{\pi}$ ve $f(x+yw) = x'+y'w \in \mathbb{Z}[w]_{\pi'}$

olmak üzere

$$R_{\pi} = \{x+yw : |x|+|y| \le |x'|+|y'|\} \cup \{x'+y'w^* : |x'|+|y'| < |x|+|y|\}$$

olarak tanımlanır.

7.2.2. Örnek: $p_1 = 7$ ve $p_2 = 13$ olsun. Bu durumda $\pi_1 = 1+2w$, $\pi_2 = 3+w$ olmak üzere $\pi = (1+2w)(3+w) = 1+9w$ ve $\pi' = 9+w$ olur. Bu durumda $m = 7.13 = 91$ olup R_{π} halkasının elemanları Tablo 4 deki gibi olur.

Tablo 4: $\mathbb{Z}_{91}$ kümesi ile R_{π} kümesinin elemanlarının eşleştirilmesi

$\mathbb{Z}_{91}$	$\mathbb{Z}[w]_{\pi}$	$\mathbb{Z}[w]_{\pi'}$	R_{π}	$\mathbb{Z}_{91}$	$\mathbb{Z}[w]_{\pi}$	$\mathbb{Z}[w]_{\pi'}$	R_{π}
0	0	0	0	46	$-5-4w$	$5w$	$5w^*$
1	1	1	1	47	$-4-4w$	$1+5w$	$1+5w^*$
2	2	2	2	48	$-3-4w$	$2+5w$	$-3-4w$
3	3	3	3	49	$-2-4w$	$3+5w$	$-2-4w$
4	4	4	4	50	$-1-4w$	$-5+4w$	$-1-4w$
5	5	$-4-w$	5	51	$-4w$	$-4+4w$	$-4w$
6	$-4+w$	$-3-w$	$-3-w^*$	52	$1-4w$	$-3+4w$	$1-4w$
7	$-3+w$	$-2-w$	$-2-w^*$	53	$2-4w$	$-2+4w$	$2-4w$
8	$-2+w$	$-1-w$	$-1-w^*$	54	$3-4w$	$-1+4w$	$-1+4w^*$
9	$-1+w$	$-w$	$-w^*$	55	$4-4w$	$+4w$	$+4w^*$
10	$+w$	$1-w$	$+w$	56	$-5-3w$	$1+4w$	$1+4w^*$
11	$1+w$	$2-w$	$1+w$	57	$-4-3w$	$2+4w$	$2+4w^*$
12	$2+w$	$3-w$	$2+w$	58	$-3-3w$	$3+4w$	$-3-3w$
13	$3+w$	$4-w$	$3+w$	59	$-2-3w$	$-5+3w$	$-2-3w$
14	$4+w$	$-4-2w$	$4+w$	60	$-1-3w$	$-4+3w$	$-1-3w$
15	$5+w$	$-3-2w$	$-3-2w^*$	61	$-3w$	$-3+3w$	$-3w$
16	$-4+2w$	$-2-2w$	$-2-2w^*$	62	$1-3w$	$-2+3w$	$1-3w$
17	$-3+2w$	$-1-2w$	$-1-2w^*$	63	$2-3w$	$-1+3w$	$-1+3w^*$

18	$-2+2w$	$-2w$	$-2w^*$	64	$3-3w$	$+3w$	$+3w^*$
19	$-1+2w$	$1-2w$	$-1+2w$	65	$4-3w$	$1+3w$	$1+3w^*$
20	$+2w$	$2-2w$	$+2w$	66	$-5-2w$	$2+3w$	$2+3w^*$
21	$1+2w$	$3-2w$	$1+2w$	67	$-4-2w$	$3+3w$	$-4-2w$
22	$2+2w$	$4-2w$	$2+2w$	68	$-3-2w$	$-5+2w$	$-3-2w$
23	$3+2w$	$-4-3w$	$3+2w$	69	$-2-2w$	$-4+2w$	$-2-2w$
24	$4+2w$	$-3-3w$	$4+2w$	70	$-1-2w$	$-3+2w$	$-1-2w$
25	$5+2w$	$-2-3w$	$-2-3w^*$	71	$-2w$	$-2+2w$	$-2w$
26	$-4+3w$	$-1-3w$	$-1-3w^*$	72	$1-2w$	$-1+2w$	$1-2w$
27	$-3+3w$	$-3w$	$-3w^*$	73	$2-2w$	$+2w$	$+2w^*$
28	$-2+3w$	$1-3w$	$1-3w^*$	74	$3-2w$	$1+2w$	$1+2w^*$
29	$-1+3w$	$2-3w$	$-1+3w$	75	$4-2w$	$2+2w$	$2+2w^*$
30	$+3w$	$3-3w$	$+3w$	76	$-5-w$	$3+2w$	$3+2w^*$
31	$1+3w$	$4-3w$	$1+3w$	77	$-4-w$	$-5+w$	$-4-w$
32	$2+3w$	$-4-4w$	$2+3w$	78	$-3-w$	$-4+w$	$-3-w$
33	$3+3w$	$-3-4w$	$3+3w$	79	$-2-w$	$-3+w$	$-2-w$
34	$4+3w$	$-2-4w$	$-2-4w^*$	80	$-1-w$	$-2+w$	$-1-w$
35	$5+3w$	$-1-4w$	$-1-4w^*$	81	$-w$	$-1+w$	$-w$
36	$-4+4w$	$-4w$	$-4w^*$	82	$1-w$	$+w$	$+w^*$
37	$-3+4w$	$1-4w$	$1-4w^*$	83	$2-w$	$1+w$	$1+w^*$
38	$-2+4w$	$2-4w$	$-2+4w$	84	$3-w$	$2+w$	$2+w^*$
39	$-1+4w$	$3-4w$	$-1+4w$	85	$4-w$	$3+w$	$3+w^*$
40	$+4w$	$4-4w$	$+4w$	86	-5	-5	-5
41	$1+4w$	$-4-5w$	$-5w$	87	-4	-4	-4
42	$1-5w$	$-3-5w$	$1-5w$	88	-3	-3	-3
43	$2-5w$	$-2-5w$	$2-5w$	89	-2	-2	-2
44	$3-5w$	$-1-5w$	$-1-5w^*$	90	-1	-1	-1
45	$4-5w$	$-5w$	$-5w^*$	91	0	0	0

7.2.3. Tanım: $\pi \in \mathbb{Z}[w]$ ve $N(\pi) = m$ olmak üzere R_π kümesinin ortalama enerjisi, tüm elemanları eşit olasılıkla kullanıldığındaki umulan enerjidir. Bu enerji E_π ile gösterilir ve

$$E_\pi = \frac{1}{N(\pi)} \sum_{z \in R_\pi} w_M(z)$$

ile hesaplanır.

7.2.4. Tanım CFM (Constellation Figure of Merit), ortalama enerji ve minimum mesafesi d_M olan iki boyutlu sinyal enerjisinin normalize edilmiş halidir. $M-$ boyutlu yıldız kümesi için CFM aşağıdaki eşitlik yardımı ile hesaplanmaktadır.

$$CFM(R_\pi) = \frac{M.d_M}{2.E_\pi}$$

R_π kümesinin boyutu $M = 2$ olduğundan, R_π kümesi için $CFM(R_\pi) = \frac{d_M}{E_\pi} = \frac{N(\pi).d_M}{\sum_{z \in R_\pi} w_M(z)}$

olarak hesaplanır.

Yüksek değere sahip CFM bir $AWGN$ kanalı üzerinde en iyi iletim performansına sahip olmaktadır.

7.2.5. Tanım: Bit başına enerji (E_b) ile ortalama enerji (E_π) arasındaki bağıntı

$$E_b = \frac{E_\pi}{Log_2^p}$$

olarak tanımlanır.

7.3. R_π Kümesinin Bölüntüsü

Bu bölümde R_π halkasının küme parçalanışından ve bu küme parçalanışlarının CFM değerleri hesaplamalarından bahsedeceğiz.

7.3.1. Teorem: $\mathbb{Z}_m$ ile R_π izomorftur.

İspat: $0 \le r \le m-1$, $a + br \equiv 0 \pmod m$, $x + yr \equiv l \pmod m$ ve $x + yw = x' + y'w^*$ olsun.

$g : \mathbb{Z}_m \to R_\pi$

$$g = (l) = \begin{cases} x + yw, & |x| + |y| \le |x'| + |y'| \\ x' + y'w^*, & |x'| + |y'| < |x| + |y| \end{cases}$$

fonksiyonunu göz önüne alalım [7]. g nin birebir ve örten bir halka homomorfizması olduğu aşikardır. Dolayısıyla $\mathbb{Z}_m \cong R_\pi$ dir.

$\pi_1, \pi_2 \in \mathbb{Z}[w]$ iki asal, $\pi = \pi_1\pi_2 = a+bw$, $\pi' = b+aw$ ve $N(\pi) = m$ ise $R_\pi \cong \mathbb{Z}_m$ dir. N çarpımsal norm olduğundan $N(\pi_1) = p_1$ ve $N(\pi_2) = p_2$ alınırsa $m = p_1p_2$ olur. Bu durumda R_π kümesi, $R_\pi^{(0)} = \{g(0), g(p_1), g(2*p_1),\ldots, g((p_2-1)*p_1)\}$ ve $R_\pi^{(i)} = \{g(i+0), g(i+p_1), g(i+2*p_1),\ldots, g(i+(p_2-1)*p_1)\}$ $(1 \le i \le p_1)$ olmak üzere $R_\pi = R_\pi^{(1)} \cup R_\pi^{(2)} \cup \cdots \cup R_\pi^{(p_1)}$ olacak şekilde $R_\pi^{(1)}, R_\pi^{(2)},\ldots, R_\pi^{(p_1)} \subset R_\pi$ alt kümelerine bölünür. $\mathbb{Z}_\pi^{(p_1)} = \{0, p_1, 2*p_1,\ldots,(p_2-1)*p_1\}$ ve $1 \le i \le p_1$ için $\mathbb{Z}_\pi^{(i)} = \{z : z-i \in \mathbb{Z}_\pi^{(p_1)}\}$ olmak üzere $R_\pi^{(1)}, R_\pi^{(2)},\ldots, R_\pi^{(p_1)} \subset R_\pi$ kümeleri sırasıyla $\mathbb{Z}_\pi^{(1)}, \mathbb{Z}_\pi^{(2)},\ldots,\mathbb{Z}_\pi^{(p_1)}$ kümelerine izomorf olur.

7.3.2. Teorem: R_π nin p_1 tane alt kümeye bölüntüsü $R_\pi^{(1)}, R_\pi^{(2)},\ldots, R_\pi^{(p_1)} \subset R_\pi$ olsun. Bu durumda $\forall 0 \ne z \in R_\pi^{(p_1)}$ için

$$w_M(z) \ge w_M(\pi_1)$$

dir.

İspat: $z \in R_\pi^{(p_1)}$ ise $\mathbb{Z}_m^{(p_1)}$ da z ile eşleşen eleman z' olsun. Bu durumda $z' = p_1t$ olacak şekilde $\exists t \in \mathbb{Z}$ vardır. Dolayısıyla

$$z = \pi_1(u+vw)$$

olur. O halde $z \in \overline{\pi_1}$ dir. 6.3.2. Teorem'den

$$w_M(z) \ge w_M(\pi_1)$$

olur.

7.3.3. Örnek: $\pi_1 = 1+2w,\ \pi_2 = 3+w \in \mathbb{Z}[w]$ olsun. Bu durumda $\pi = \pi_1\pi_2 = (1+2w)(3+w) = 1+9w$ ve $\pi' = 9+w$ olur. $\mathbb{Z}[w]_\pi$ ve $\mathbb{Z}[w]_{\pi'}$ den R_π halkası 7.2.2. Örnek deki gibi elde edilir. Bu durumda

$$R_\pi^{(13)} = \left\{\begin{matrix} 0,-2-w^*,4+w,1+2w,1-3w^*,-1-4w^*,1-5w,-2-4w,1+4w^*,-1+3w^*, \\ -1-2w,-4-w,2+w^* \end{matrix}\right\}$$

R_π halkasının 13 elemanlı bir küme parçalanışı olur ve $R_\pi^{(13)} \cong \mathbb{Z}_{13}$ olduğundan $R_\pi^{(13)}$ sonlu bir cisimdir. $R_\pi^{(13)}$ için ortalama enerji

$$E_{R_\pi^{(13)}} = \frac{1}{13}\sum_{z\in R_\pi^{(13)}} w_M(z) = \frac{52}{13} = 4,$$

$R_\pi^{(13)}$ için CFM değeri ise

$$CFM\left(R_\pi^{(13)}\right) = \frac{d_M}{E_{R_\pi^{(13)}}} = \frac{3.13}{52} = 0,75$$

olarak hesaplanır.

$F_{13} = \{0,1,2,-w^*,w,-2w,-2w^*,2w^*,2w,-w,w^*,-2,-1\}$ cismi için ortalama enerji ve CFM değeri

$$E_{F_{13}} = \frac{1}{13}\sum_{z\in F_{13}} w_M(z) = \frac{18}{13} = 1,3846,$$

$$CFM(F_{13}) = \frac{d_M}{E_{F_{13}}} = \frac{1.13}{18} = 0,7\overline{2}$$

olarak hesaplanır.

F_{13} ile $R_\pi^{(13)}$ için CFM değerleri karşılaştırıldığında R_π halkasına gömülü 13 elemanlı $R_\pi^{(13)}$ cismi için daha yüksek CFM değeri elde edilmiştir.

Aşağıdaki tabloda aynı eleman sayısına sahip takım yıldızlarının CFM değerleri verilmiştir

Tablo 5: F_p ile $R_\pi^{(n)}$ takım yıldızlarının CFM değerlerinin karşılaştırılması

Takım Yıldızı Eleman Sayısı (p)	π_1	π_2	$\pi = \pi_1\pi_2$	$CFM(F_p)$	$CFM\left(R_\pi^{(p)}\right)$
13	$3+w$	$1+2w$	$1+9w$	0,72222	0,75
13	$3+w$	$2+w$	$5+6w$		0,8125
13	$3+w$	$3+4w$	$5+19w$		0,784483
19	$3+2w$	$2+w$	$4+9w$	0,59375	0,662791
19	$3+2w$	$4+3w$	$6+23w$		0,671717
31	$5+w$	$1+3w$	$2+19w$	0,442857	0,48062
31	$5+w$	$2+w$	$9+8w$		0,553571
37	$3+4w$	$2+w$	$2+15w$	0,4111	0,454918
37	$4+3w$	$3+2w$	$6+23w$		0,484293

43	$6+w$	$2+w$	$11+9w$	0,377193	0,444828
43	$6+w$	$3+2w$	$16+17w$		0,473568

7.4. R_π Üzerinde Kod Kazancı

Bu kısımda, R_π kümesinin küme parçalanışları üzerinde tanımlı kodlar ile F_p kümesi üzerinde tanımlı kodların eleman sayıları eşit olması durumundaki kod kazancı (KK) hesaplanacaktır.

$\pi \in \mathbb{Z}[w]$ bir asal sayı, $N(\pi)=p$ ve $[n_1,k_1,d_H]_p$ kodu $\mathbb{F}_p$ üzerinde tanımlı bir lineer kod olmak üzere eleman sayısı p ve bit başına enerjisi E_b olan bir küme üzerindeki $[n_2,k_2,d_2]_p$ parametreli bir lineer kod için kod kazancı

$$KK = 10\log\left(\frac{k_1}{n_1}\frac{k_2}{n_2}d_H d_2\right) - 10\log 4E_b$$

olarak hesaplanır.

7.4.1. Örnek: $p=13$ olsun, F_{13} ile $R_\pi^{(13)}$ kümeleri 7.3.3. Örnek deki gibi olmak üzere $\mathbb{F}_{13}$ üzerinde $[170,5,150]_{13}$ lineer kodunu göz önüne alalım. Bu durumda $F_{13}=\{0,1,2,-w^*,w,-2w,-2w^*,2w^*,2w,-w,w^*,-2,-1\}$ olur ve F_{13} üzerinde $[1,1,1]_{13}$ lineer kodu vardır. Benzer şekilde

$$R_\pi^{(13)} = \begin{Bmatrix} 0,-2-w^*,4+w,1+2w,1-3w^*,-1-4w^*,1-5w,-2-4w,1+4w^*,-1+3w^*, \\ -1-2w,-4-w,2+w^* \end{Bmatrix}$$

olur ve $R_\pi^{(13)}$ üzerinde $[1,1,3]_{13}$ lineer kodu vardır.

F_{13} üzerinde kod kazancı

$$KK(F_{13}) = 10\log\left(\frac{5}{170}.\frac{1}{1}.150.1\right) - 10\log 4E_b = 6.45 - 1.75 = 4.7\ dB$$

olarak hesaplanır. $R_\pi^{(13)}$ üzerinde kod kazancı ise

$$KK\left(R_\pi^{13}\right)=10\log\left(\frac{5}{170}.\frac{1}{1}.150.3\right)-10\log 4E_b=11.22-6.36=4.86\ dB$$

olarak hesaplanır. Sonuç olarak $R_\pi^{(13)}$ üzerindeki kod kazancının F_{13} üzerindeki kod kazancından daha yüksek olduğu gözlemlenmiştir. $\pi\in\mathbb{Z}[w]$ nun seçimine göre $R_\pi^{(13)}$ ile F_{13} arasındaki kod kazancı farkları Tablo 6 daki gibi hesaplanmıştır.

Tablo 6: $R_\pi^{(13)}$ ile F_{13} arasındaki kod kazancı değerleri

Takım Yıldızı	Kod Parametresi	Ortalama Enerji (E_π)	Bit Başına Enerji (E_b)	$10\log(4E_b)$	Kod Kazancı (KK)	Yeni Kod Kazancı
F_{13}	$[1,1,1]_{13}$	1.38462	0.37418	1.75136	4.69487	0
$R_{1+9w}^{(13)}$	$[1,1,3]_{13}$	4	1.08095	6.35866	4.85868	0.16381
$R_{5+6w}^{(13)}$	$[1,1,3]_{13}$	3.69231	0.9978	6.01103	5.20631	0.51144
$R_{3+14w}^{(13)}$	$[1,1,5]_{13}$	6.46154	1.74615	8.44144	5.04438	0.34951
$R_{7+11w}^{(13)}$	$[1,1,5]_{13}$	6.15385	1.663	8.22952	5.2563	0.56143
$R_{2+19w}^{(13)}$	$[1,1,6]_{13}$	8.15385	2.20348	9.45169	4.77595	0.08108
$R_{14+9w}^{(13)}$	$[1,1,6]_{13}$	7.38462	1.9956	9.02133	5.20631	0.51144
$R_{5+19w}^{(13)}$	$[1,1,7]_{13}$	8.92308	2.41136	9.84322	5.05388	0.35901
$R_{9+16w}^{(13)}$	$[1,1,7]_{13}$	8.61538	2.32821	9.68522	5.21188	0.51701
$R_{3+22w}^{(13)}$	$[1,1,7]_{13}$	9.53846	2.57766	10.13286	4.76424	0.06937
$R_{17+10w}^{(13)}$	$[1,1,7]_{13}$	11.0769	2.99341	10.78226	4.11484	-0.58003
$R_{7+24w}^{(13)}$	$[1,1,9]_{13}$	11.3846	3.07656	10.90125	5.0873	0.39243

BÖLÜM 8.

$\mathbb{F}_q + \alpha\mathbb{F}_q$ Üzerindeki klasik kodlar yardımı ile kuantum kod elde etme

(6, 7 ve 8. iş paketleri, 4. ve 5. hedefler):

Bu çalışmada katkısı olanlar:

Doç. Dr. Murat GÜZELTEPE

Arş. Gör. Mustafa Sarı (Yıldız Teknik Üniversitesi)

8.1. Giriş

$i^2 = -1$ olmak üzere $\alpha = a + bi$ bir asal Gauss tamsayısı ve alfanın normu

$N(\alpha) = \alpha\alpha^* = (a+bi)(a-bi) = a^2 + b^2 = p \equiv 1 \pmod 4$

olsun. Bu çalışmada $R_q = \mathbb{F}_q + \alpha\mathbb{F}_q$ halkasından $\mathbb{F}_q^{2n}$ vektör uzayına bir φ Gray fonksiyonu tanımlanmıştır. R_q halkası üzerinde devirli kodlar ve bu kodların dikleri karakterize edilmiştir. Bu kodlardan diklerini kapsayan yani kendine ortogonal ve kendine dik olanlar için gerek ve yeter koşullar belirtilmiştir. φ Gray fonksiyonu yardımı ile $\mathbb{F}_q$ üzerindeki kuantum kodlar karakterize edilmiştir.

q bir asalın kuvveti olmak üzere $\mathbb{F}_q$, q elemanlı bir cisim olsun. $\mathbb{F}_q$ üzerinde n uzunluklu bir kod $\mathbb{F}_q^n$'nin boştan farklı bir alt kümesi olarak tanımlanır. $\mathbb{F}_q^n$ bir vektör uzaydır. Eğer $\mathbb{F}_q^n$'nin boştan farklı bir alt kümesi aynı zamanda $\mathbb{F}_q$ üzerinde bir vektör uzayı ise bu alt kümeye lineer kod denir. $x = (x_0 \quad x_1 \quad \cdots \quad x_{n-1})$ vektörünün sıfırdan farklı bileşenlerinin sayısına bu vektörün Hamming ağırlığı denir ve $w_H(x)$ ile gösterilir. $x = (x_0 \quad x_1 \quad \cdots \quad x_{n-1})$ vektörü ile $y = (y_0 \quad y_1 \quad \cdots \quad y_{n-1})$ vektörleri arasındaki Hamming mesafesi ise bu vektörlerin farkının Hamming ağırlığına eşittir. Yani $d_H(x,y) = w_H(x-y)$ olarak tanımlanır. $u = (\beta_1 \quad \beta_2 \quad \cdots \quad \beta_n), v = (\gamma_1 \quad \gamma_2 \quad \cdots \quad \gamma_n) \in R_q^n$ vektörleri arasındaki Mannheim mesafesi

$$d_M(u,v) = \sum_{t=1}^{n} \left(|x_t| + |y_t| \right)$$

olarak tanımlanır. Burada her t için $\beta_t - \gamma_t \equiv x_t + y_t i \pmod p$ olup $|x_t| + |y_t|$ minimumdur.

$x=(x_0 \quad x_1 \quad \cdots \quad x_{n-1})$ ile $y=(y_0 \quad y_1 \quad \cdots \quad y_{n-1})$ arasındaki Öklid iç çarpımı

$$\langle x,y\rangle=\sum_{t=1}^{n}x_t y_t$$

ve bu vektörler arasındaki Hermit iç çarpım ise

$$\langle x,y\rangle_h=\sum_{t=1}^{n}x_t y_t^*$$

olarak tanımlanır.

Bir kodun elemanlarına kodsöz denir. Bir C kodunun minimum Hamming mesafesi bu koddaki farklı iki kodsöz arasındaki mesafelerin minimumu olarak tanımlanır ve $d_H(C)$ sembolü ile gösterilir. Benzer tanımlama Mannheim metriği için de yapılabilir. n uzunluklu, k boyutlu ve d_H minimum Hamming mesafeli $\mathbb{F}_q$ üzerinde tanımlı bir lineer kod $[n,q,d_H]_q$ parametreleri ile gösterilir. Benzer yollar R_q üzerinde tanımlı Mannheim mesafeli bir lineer kod $[n,q,d_M]_q$ parametreleri ile gösterilir.

Öklid ve Hermit iç çarpımlarına göre bir C kodunun diki sırası ile

$$C^{\perp}=\{y\in\mathbb{F}_q^n:\forall x\in C,\langle x,y\rangle=0\},$$
$$C^{\perp_h}=\{v\in R_q^n:\forall u\in C,\langle u,v\rangle_h=0\}$$

olarak tanımlanır.

$\mathbb{C}$ kompleks sayılar kümesi olmak üzere $\mathbb{C}^{q^n}=\mathbb{C}^q\times\mathbb{C}^q\times\cdots\times\mathbb{C}^q$, $q-$boyutlu vektör uzayını göz önüne alalım. $\mathbb{C}^{q^n}$ vektör uzayının M üreteç kümesine sahip bir alt vektör uzayına $((n,M,d))_q$ parametreli bir kuantum kod denir. Eğer $M=q^k$ ise bu kuantum kod $[[n,k,d]]_q$ şeklinde gösterilir. Kuantum kodlarla klasik kodlar arasındaki ilişki aşağıdaki teorem yardımı ile açıklanabilir.

Teorem 8.1.1. C ve C_1 sırası ile $[n,k,d]_q$ ve $[n,k_1,d_1]_q$ parametrelerine sahip iki klasik lineer kod olsun. Eğer $C_1\subseteq C$ ise $[[n,k-k_1,d']]_q$ parametrelerine sahip bir kuantum kod vardır. Burada

$$d'=\min\{w_H(x):x\in(C-C_1)\cup(C_1^{\perp}-C^{\perp})\}$$

olarak tanımlanır.

8.2 R_q^n den $\mathbb{F}_q^{2n}$'e Gray Fonksiyonu

$\alpha = a + bi$ ve $N(\alpha) = p \equiv 1 \pmod 4$ olsun. $\varphi : R_q^n \to \mathbb{F}_q^{2n}$ fonksiyonu her $i \in \{0,1,\ldots,n-1\}$ için $r_i = x_i + y_i\alpha$ olmak üzere

$$\varphi(r_0, r_1, \ldots, r_{n-1}) = (-y_0 b, \ldots, -y_{n-1} b, x_0 + y_0 a, \ldots, x_{n-1} + y_{n-1} a)$$

olarak tanımlanır. Bu Gray fonksiyonu yardımı ile bir $r \in R_q$ elemanının Lee ağırlığı $w_L(r)$ ile gösterilir ve $w_L(r) = w_H(\varphi(r))$ olarak tanımlanır.

$u \in R_q^n$ vektörünün Lee ağırlığı

$$w_L(u) = \sum_{i=1}^{n} w_H(\varphi(\beta_i))$$

olarak tanımlanır.

Teorem 8.2.1. $\varphi : (R_q^n, d_L) \to (\mathbb{F}_q^{2n}, d_H)$ fonksiyonu lineerdir ve mesafeyi korur.

Teorem 8.2.2. C, R_q üzerinde n uzunluklu bir lineer kod olsun. Eğer $C^{\perp_h} \subseteq C$ ise $(\varphi(C))^{\perp} \subseteq \varphi(C)$ olur.

Sonuç 8.2.3. Eğer $C^{\perp_h} \subseteq C$ lineer kodunun minimum Lee mesafesi d_L ve üreteç matrisi $G_{(k_1+k_2+k)\times n}$ tipinde ise $\left[\left[2n, 2(2k_1 + k_2 + k_3 - n), d \geq d_L\right]\right]_q$ parametreli bir kuantum kod vardır.

Burada I_k lar birim matrisler ve A_i ile B_i matrisleri $\mathbb{F}_q$ üzerinde tanımlı matrisler olmak üzere

$$G = \begin{pmatrix} I_{k_1} & \alpha^* B_1 & \alpha A_1 & \alpha A_1 + \alpha^* B_2 & \alpha A_3 + \alpha^* B_3 \\ 0 & \alpha I_{k_2} & 0 & \alpha A_4 & 0 \\ 0 & 0 & \alpha^* I_{k_3} & 0 & \alpha^* B_4 \end{pmatrix}$$

olarak tanımlanır.

Sonuç 8.2.4. Eğer $C^{\perp_h} \subseteq C$ lineer kodunun minimum Hamming mesafesi d_H ve üreteç matrisi $G_{(k_1+k_2+k)\times n}$ tipinde ise $\left[\left[n, 2k_1 + k_2 + k_3 - n, d \geq d_H\right]\right]_q$ parametreli bir kuantum kod vardır.

8.3 R_q Üzerindeki devirli kodlar yardımı ile kuantum kodlar

R_q üzerinde n uzunluklu bir devirli kod $\frac{R_q[x]}{(x^n-1)}$ halkasının bir ideali olarak tanımlanır. Bu sebeple $\frac{R_q[x]}{(x^n-1)}$ halkasının ideal yapısını incelemek gereklidir. Her $x \in R_q^n$ vektörü $x_1, x_2 \in \mathbb{F}_q^n$ olmak üzere $x = \alpha x_1 + \alpha^* x_2$ olacak şekilde tek türlü yazılır. Bu özellik R_q üzerinde n uzunluklu lineer ve devirli kodların karakterize edilmesini sağlar.

Teorem 8.3.1. R_q üzerinde n uzunluklu her C lineer kod olsun. Bu durumda $C = \alpha C_1 \oplus \alpha^* C_2$ olacak şekil $\mathbb{F}_q$ üzerinde n uzunluklu C_1 ve C_2 kodları iki lineer kodları vardır. Üstelik R_q üzerinde C devirli ise C_1 ve C_2 de $\mathbb{F}_q$ üzerinde devirlidir.

Teorem 8.3.2. Eğer $C = \alpha C_1 \oplus \alpha^* C_2$ kodu R_q üzerinde n uzunluklu bir devirli kod ise $h_1(x)$ ve $h_2(x)$ polinomları sırası ile C_1 ve C_2 kodlarının kontrol polinomları olmak üzere

$$C^{\perp_h} = \langle \alpha h_2^R(x) + \alpha^* h_1^R(x) \rangle$$

olarak tanımlanır. Burada $h^R(x) = x^{\deg(h(x))} h(x^{-1})$ olarak tanımlanır.

Teorem 8.3.3. Kabul edelim ki $(n,q)=1$, C_i klasik kodlarının $\mathbb{F}_q$ üzerinde üreteç polinomları $g_i(x)$ ve ξ birimin n inci kökü olmak üzere C_i için

$$Z_i = \{ i : g(\xi^i) = 0, i \in [0, n-1] \} \text{ ve } Z_i^{-1} = \{ -i \pmod n : i \cup Z_i \}$$

olsun. Bu durumda $C = \alpha C_1 \oplus \alpha^* C_2$ için aşağıdakiler denktir.

i) $C^{\perp_h} \subseteq C$,
ii) $C_2^{\perp} \subseteq C_1$,
iii) $C_1^{\perp} \subseteq C_2$,
iv) $x^n - 1 \equiv 0 \pmod{g_1(x) g_2^R(x)}$,
v) $x^n - 1 \equiv 0 \pmod{g_1^R(x) g_2(x)}$,
vi) $Z_1 \cap Z_2^{-1} = \varnothing$,
vii) $Z_1^{-1} \cap Z_2 = \varnothing$.

Sonuç 8.3.4. $(n,q)=1$ olmak üzere $C=\alpha C_1 \oplus \alpha^* C_2 = \langle \alpha g_1(x) + \alpha^* g_2(x) \rangle$ kodu R_q üzerinde n uzunluklu bir devirli kod olsun. Bu durumda

$$\left[\left[2n, 2\left(n-\sum_{i=1}^{2} derg_i(x)\right), d \geq d_L\right]\right]_q \text{ ve } \left[\left[n, n-\sum_{i=1}^{2} derg_i(x), d \geq d_H\right]\right]_q$$

kuantum kodları vardır.

Örnek 8.3.5. $\mathbb{F}_5$ üzerinde $x^9-1=(x+4)(1+x^3+x^6)(1+x+x^2)=f_1 f_2 f_3$ olup R_5 üzerinde aşikâr olmayan tüm kodlar Tablo 7 de verilmektedir. Burada $\alpha = 2+i$ dir.

Tablo 7: R_5 üzerindeki tüm aşikâr olmayan kuantum kodlar.

$g_1(x)$	$g_2(x)$	Gray görüntü	Kuantum kod Lee ağırlığı	Kuantum kod Hamming ağırlığı
f_2	f_3	$[18,10,4]_5$	$[[18,2,4]]_5$	$[[9,1,\geq 2]]_5$
f_2	f_1	$[18,11,4]_5$	$[[18,4,4]]_5$	$[[9,2,\geq 2]]_5$
f_2	$f_1 f_3$	$[18,9,4]_5$	$[[18,0,4]]_5$	$[[9,0,\geq 2]]_5$
f_3	f_2	$[18,10,4]_5$	$[[18,2,4]]_5$	$[[9,1,\geq 2]]_5$
f_3	f_1	$[18,15,2]_5$	$[[18,12,2]]_5$	$[[9,6,\geq 2]]_5^*$
f_3	$f_1 f_2$	$[18,9,4]_5$	$[[18,0,4]]_5$	$[[9,0,\geq 2]]_5$
$f_2 f_3$	f_1	$[18,9,4]_5$	$[[18,0,4]]_5$	$[[9,0,\geq 2]]_5$
f_1	f_2	$[18,11,4]_5$	$[[18,4,4]]_5$	$[[9,2,\geq 2]]_5$
f_1	f_3	$[18,15,2]_5$	$[[18,12,2]]_5$	$[[9,6,\geq 2]]_5^*$
f_1	$f_2 f_3$	$[18,9,4]_5$	$[[18,0,4]]_5$	$[[9,0,\geq 2]]_5$
$f_1 f_2$	f_3	$[18,9,4]_5$	$[[18,0,4]]_5$	$[[9,0,\geq 2]]_5$
$f_1 f_3$	f_2	$[18,9,4]_5$	$[[18,0,4]]_5$	$[[9,0,\geq 2]]_5$
1	f_1	$[18,17,2]_5$	$[[18,16,2]]_5^*$	$[[9,8,\geq 1]]_5^*$
1	f_2	$[18,12,2]_5$	$[[18,6,2]]_5$	$[[9,3,\geq 1]]_5$

1	f_3	$[18,16,2]_5$	$[[18,14,2]]_5$	$[[9,7,\geq 1]]_5$
1	$f_1 f_2$	$[18,11,2]_5$	$[[18,4,2]]_5$	$[[9,2,\geq 1]]_5$
1	$f_1 f_3$	$[18,15,2]_5$	$[[18,12,2]]_5$	$[[9,6,\geq 1]]_5$
1	$f_2 f_3$	$[18,10,2]_5$	$[[18,2,2]]_5$	$[[9,1,\geq 1]]_5$
f_1	1	$[18,17,2]_5$	$[[18,16,2]]_5^*$	$[[9,8,\geq 1]]_5^*$
f_2	1	$[18,12,2]_5$	$[[18,6,2]]_5$	$[[9,3,\geq 1]]_5$
f_3	1	$[18,16,2]_5$	$[[18,14,2]]_5$	$[[9,7,\geq 1]]_5$
$f_1 f_2$	1	$[18,11,2]_5$	$[[18,4,2]]_5$	$[[9,2,\geq 1]]_5$
$f_1 f_3$	1	$[18,15,2]_5$	$[[18,12,2]]_5$	$[[9,6,\geq 1]]_5$
$f_2 f_3$	1	$[18,10,2]_5$	$[[18,2,2]]_5$	$[[9,1,\geq 1]]_5$

Tablo 7'de (*) ile işaretli kodlar kuantum MDS kodlardır.

Örnek 8.3.6. $\mathbb{F}_{29}$ üzerinde $x^{31}-1=f_1 f_2 f_3 f_4$ olup R_{29} üzerinde bazı aşikâr olmayan kuantum kodlar Tablo 8 de verilmektedir. Burada $\alpha = 5+2i$ dir.

Tablo 8: R_{29} üzerindeki tüm aşikâr olmayan kuantum kodlar.

$g_1(x)$	$g_2(x)$	Kuantum kod (Hamming ağırlığı)	Kuantum kod (Lee ağırlığı)
$f_1 f_2$	f_3	$[[62,20,\geq 8]]_{29}$	$[[31,10,8]]_{5+2i}$
$f_2 f_3$	f_4	$[[62,2,\geq 8]]_{29}$	$[[31,1,8]]_{5+2i}$
$f_2 f_3$	$f_1 f_4$	$[[62,0,\geq 9]]_{29}$	$[[31,0,8]]_{5+2i}$

Tablo 8 de verilen kodlar literatüre kazandırılmıştır.

Aşağıdaki tabloda Mannheim metriğine göre hesaplanmış kuantum kodlar bulunmaktadır. Bu kodlar oluşturulurken ve minimum mesafeleri hesaplanırken aşağıdaki Mathematica programı kullanılmıştır.

Tablo 9: Bazı yeni kuantum kodlar.

Klasik kodun üreteç matrisi	Bu koddan elde edilen kuantum kod
$G=\begin{pmatrix}1 & 0 & 9\alpha & 6\alpha & 9+11\alpha\end{pmatrix}$	$\left[\left[5,3,10\right]\right]_{3+2i}$
$G=\begin{pmatrix}1 & 0 & 9\alpha & 6\alpha & 9+11\alpha \\ 5\alpha & 1 & 5+10\alpha & 11\alpha & 12+9\alpha \\ 12\alpha & 8+3\alpha & 1 & 11\alpha & 5\end{pmatrix}$	$\left[\left[5,1,15\right]\right]_{3+2i}$
$G=\begin{pmatrix}1 & 0 & 3+6\alpha & 3+6\alpha & 5+10\alpha & 4+6\alpha \\ 0 & 1 & 6+12\alpha & 7+\alpha & 2\alpha & 1+3\alpha \\ 9+5\alpha & 9+5\alpha & 1 & 8\alpha & 9\alpha & 12+9\alpha \\ 12+11\alpha & 5+10\alpha & 2+4\alpha & 1 & 7\alpha & 7+11\alpha \\ 9\alpha & 9+5\alpha & 9+5\alpha & 12\alpha & 1 & 3+4\alpha\end{pmatrix}$	$\left[\left[6,4,12\right]\right]_{3+2i}$
$G=\begin{pmatrix}1 & 0 & 9+5\alpha & 12\alpha & 2\alpha & 12+5\alpha \\ 0 & 1 & 10+7\alpha & 3\alpha & 10\alpha & 12+3\alpha \\ 9+5\alpha & 9+5\alpha & 1 & 8\alpha & 9\alpha & 12+9\alpha \\ 12+11\alpha & 5+10\alpha & 2+4\alpha & 1 & 7\alpha & 7+11\alpha\end{pmatrix}$	$\left[\left[6,2,15\right]\right]_{3+2i}$
$G=\begin{pmatrix}1 & 0 & 11\alpha & 12\alpha & 2+4\alpha & 9+11\alpha \\ 0 & 1 & 8+3\alpha & 11\alpha & 8\alpha & 7+5\alpha \\ 4+8\alpha & 0 & 0 & 5+10\alpha & 12\alpha & 9+11\alpha\end{pmatrix}$	$\left[\left[6,0,15\right]\right]_{3+2i}$
$G=\begin{pmatrix}1 & 12+11\alpha & 8\alpha & 2\alpha & 12 & 8+7\alpha & 10+5\alpha & 3+12\alpha \\ 12\alpha & 1 & 5+10\alpha & 11\alpha & 2+6\alpha & 1+9\alpha & 2+8\alpha & 6+7\alpha \\ 5\alpha & 9\alpha & 1 & 8+3\alpha & 11+8\alpha & 2 & 11+\alpha & 12+6\alpha \\ \alpha & 1 & 11+\alpha & 1 & 11+4\alpha & 9+3\alpha & 7+10\alpha & 8+6\alpha\end{pmatrix}$	$\left[\left[8,0,24\right]\right]_{3+2i}$

8.4 R_q Üzerinde kuantum mantık kapıları ve kuantum ışınlama

Yukarıda R_q üzerinde oluşturulan kuantum kodlar için kuantum mantık kapıları R_q üzerinde baz vektörleri aşağıdaki gibi tanımlanır. Literatürde $p-$boyutlu kuantum hal uzayı için baz vektörleri

$$|0\rangle=\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}_{p\times 1},|1\rangle=\begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix}_{p\times 1},\cdots,|p-1\rangle=\begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}_{p\times 1}$$

olup bu bazlar yardımı ile

$q-$boyutlu kuantum hal uzayı için baz vektörleri ve tensör çarpım kullanılarak tanımlanır. $p-$li bir kuantum hal uzayı için Pauli spin matrisler $P_p=\{I,X_a,Z_a,Y_a\}$ olup bu spin matrisleri

$$(X_i)_{s,t}=\delta_{t,(s+i\,(\mathrm{mod}\,p))},(Z_i)_{s,t}=\xi^{i.s(\mathrm{mod}\,p)}\delta_{s,t}$$

olarak tanımlanır. Burada δ, Kronecker delta fonksiyonunu göstermektedir. Ayrıca $p-$li bir kuantum hal uzayı için Hadamard kapısı ise

$$H_p=\frac{1}{\sqrt{p}}\left(a_{s,t}\right)=\xi^{(s-1)(t-1)\,(\mathrm{mod}\,p)}$$

dir. Bu kapılardan yararlanılarak R_p üzerindeki kuantum kodlar için kuantum kapılarını şu şekilde tanımlayabiliriz:

$r=r_1+r_2\alpha\in R_p$ ve X_{r_1},X_{r_2},Z_{r_1} ve Z_{r_2} $\mathbb{F}_p$ üzerinde tanımlı kuantum mantık kapıları olsun. Bu durumda R_p üzerindeki kunatum mantık kapılarını

$$X_r'=X_{r_1}\otimes X_{r_2},\ Z_r'=Z_{r_1}\otimes Z_{r_2},H_r'=H_p\otimes H_p$$

olarak tanımlayabiliriz. Ayrıca kuantum enkodlama ve dekodlama için gerekli olan *CNOT* kapısını da

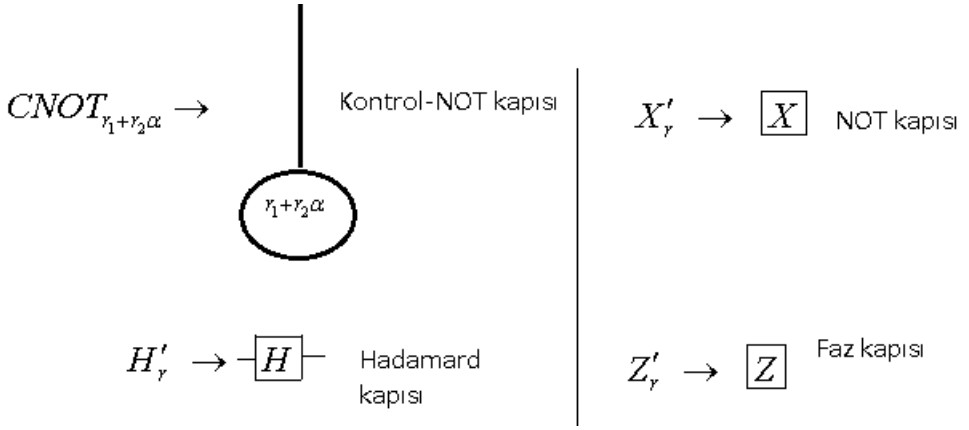
$$CNOT_{r_1+r_2\alpha}\left|r_1+r_2\alpha\quad r_1+r_2\alpha\right\rangle=\left|r_1+r_2\alpha\quad 0\right\rangle,$$
$$CNOT_{r_1+r_2\alpha}\left|r_3+r_4\alpha\quad 0\right\rangle=\left|r_3+r_4\alpha\quad 0\right\rangle,\left(r_1+r_2\alpha\neq r_3+r_4\alpha\right)$$

şeklinde tanımlayabiliriz. $CNOT_{r_1+r_2\alpha}$ matrisi $p^4\times p^4$ tipinde bir kare matristir.

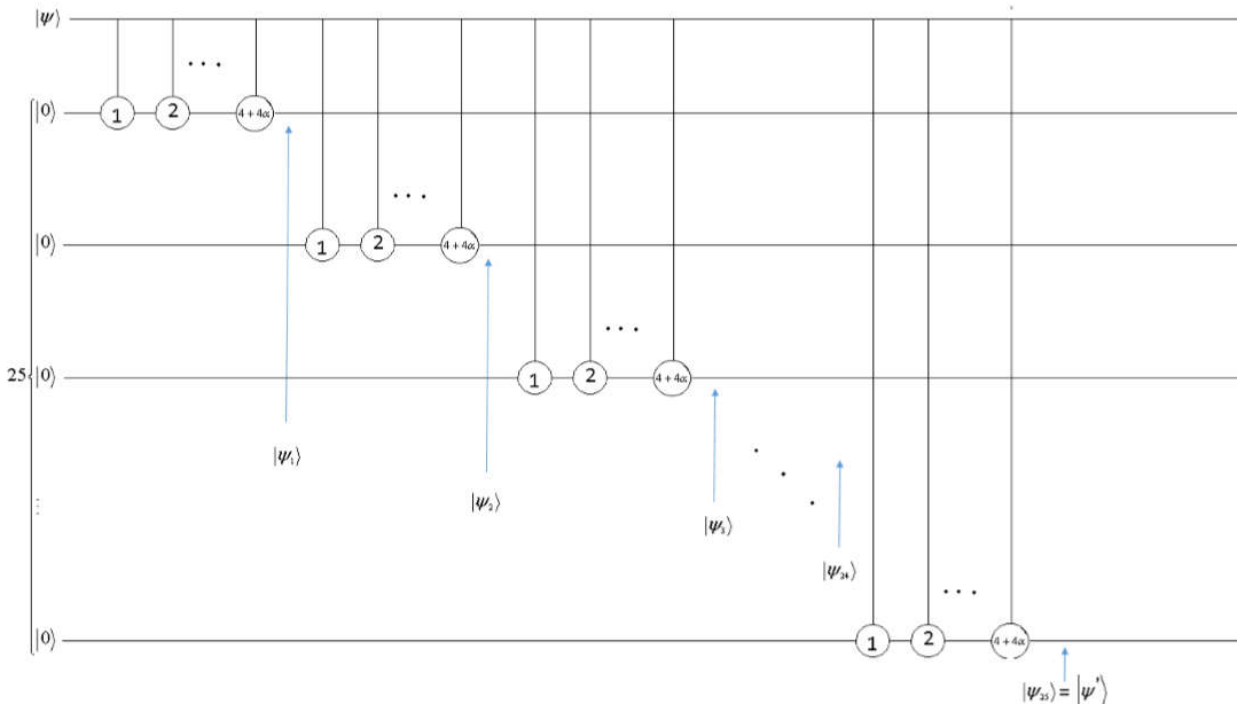
Örnek 8.4.1. $p=5,\alpha=2+i$ olmak üzere

$$|\psi\rangle=a_0|0\rangle+a_0|0\rangle+a_0|0\rangle+a_0|0\rangle+a_1|1\rangle+a_2|2\rangle+a_3|3\rangle+a_4|4\rangle$$
$$+a_5|\alpha\rangle+a_6|2\alpha\rangle+\cdots+a_8|4\alpha\rangle+a_9|1+\alpha\rangle+\cdots+a_{24}|4+4\alpha\rangle$$

kuantum hali, kuantum devrede kuantum kapıları



şeklinde gösterilirse, R_5'de şu şekilde enkodlanabilir:



Şekil 6: Kuantum ışınlama (enkodlama) örneği.

Bu kuantum devrede $|\psi_i\rangle$ halleri aşağıdaki gibidir.

$$|\psi_1\rangle = a_0\left|\underbrace{0\cdots0}_{26}\right\rangle + a_1\left|11\underbrace{0\cdots0}_{24}\right\rangle + a_3\left|22\underbrace{0\cdots0}_{24}\right\rangle + a_3\left|33\underbrace{0\cdots0}_{24}\right\rangle + a_4\left|44\underbrace{0\cdots0}_{24}\right\rangle$$
$$+ a_5\left|\alpha\alpha\underbrace{0\cdots0}_{24}\right\rangle + a_6\left|(1+\alpha)(1+\alpha)\underbrace{0\cdots0}_{24}\right\rangle + \cdots + a_{24}\left|(4+4\alpha)(4+4\alpha)\underbrace{0\cdots0}_{24}\right\rangle,$$

$$|\psi_2\rangle = a_0\left|\underbrace{0\cdots0}_{26}\right\rangle + a_1\left|111\underbrace{0\cdots0}_{23}\right\rangle + a_2\left|222\underbrace{0\cdots0}_{23}\right\rangle + a_3\left|333\underbrace{0\cdots0}_{23}\right\rangle + a_4\left|444\underbrace{0\cdots0}_{23}\right\rangle$$
$$+ a_5\left|\alpha\alpha\alpha\underbrace{0\cdots0}_{23}\right\rangle + \cdots + a_{24}\left|(4+4\alpha)(4+4\alpha)(4+4\alpha)\underbrace{0\cdots0}_{23}\right\rangle,$$

$$|\psi_3\rangle = a_0\left|\underbrace{0\cdots0}_{26}\right\rangle + a_1\left|1111\underbrace{0\cdots0}_{22}\right\rangle + a_2\left|2222\underbrace{0\cdots0}_{22}\right\rangle + a_3\left|3333\underbrace{0\cdots0}_{22}\right\rangle + a_4\left|4444\underbrace{0\cdots0}_{22}\right\rangle$$
$$+ a_5\left|\alpha\alpha\alpha\alpha\underbrace{0\cdots0}_{22}\right\rangle + \cdots + a_{24}\left|(4+4\alpha)(4+4\alpha)(4+4\alpha)(4+4\alpha)\underbrace{0\cdots0}_{22}\right\rangle ,$$

$$|\psi_{24}\rangle = a_0\left|\underbrace{0\cdots0}_{26}\right\rangle + a_1\left|\underbrace{1\cdots1}_{25}0\right\rangle + a_2\left|\underbrace{2\cdots2}_{25}0\right\rangle + a_3\left|\underbrace{3\cdots3}_{25}0\right\rangle + a_4\left|\underbrace{4\cdots4}_{25}0\right\rangle$$
$$+ a_5\left|\underbrace{\alpha\cdots\alpha}_{25}0\right\rangle + \cdots + a_{24}\left|\underbrace{(4+4\alpha)\cdots(4+4\alpha)}_{25}0\right\rangle ,$$

$$|\psi_{25}\rangle = a_0\left|\underbrace{0\cdots0}_{26}\right\rangle + a_1\left|\underbrace{1\cdots1}_{26}\right\rangle + a_2\left|\underbrace{2\cdots2}_{26}\right\rangle + a_3\left|\underbrace{3\cdots3}_{26}\right\rangle + a_4\left|\underbrace{4\cdots4}_{26}\right\rangle$$
$$+ a_5\left|\underbrace{\alpha\cdots\alpha}_{26}\right\rangle + \cdots + a_{24}\left|\underbrace{(4+4\alpha)\cdots(4+4\alpha)}_{26}\right\rangle .$$

Böyle kuantum devreye giren

$$|\psi\rangle = a_0|0\rangle + a_0|0\rangle + a_0|0\rangle + a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle + a_4|4\rangle$$
$$+ a_5|\alpha\rangle + a_6|2\alpha\rangle + \cdots + a_8|4\alpha\rangle + a_9|1+\alpha\rangle + \cdots + a_{24}|4+4\alpha\rangle$$

kuantum hali bu devrede

$$|\psi_{25}\rangle = a_0\left|\underbrace{0\cdots0}_{26}\right\rangle + a_1\left|\underbrace{1\cdots1}_{26}\right\rangle + a_2\left|\underbrace{2\cdots2}_{26}\right\rangle + a_3\left|\underbrace{3\cdots3}_{26}\right\rangle + a_4\left|\underbrace{4\cdots4}_{26}\right\rangle$$
$$+ a_5\left|\underbrace{\alpha\cdots\alpha}_{26}\right\rangle + \cdots + a_{24}\left|\underbrace{(4+4\alpha)\cdots(4+4\alpha)}_{26}\right\rangle$$

şeklinde enkodlanmış olur. Yukarıdaki Tablo 7, Tablo 8 ve Tablo 9 daki kodlar bu kuantum mantık kapıları kullanılarak kuantum dolanıklık ve diğer kuantum hatalarına karşı enkodlanır. Gerekli ölçümler de kolayca tanımlanırsa enkodlanan kuantum hali dekodlanabilir.

BÖLÜM 9.

R_{2^m} Halkası üzerindeki lineer kodlardan kuantum kod üretme

(6, 7 ve 8. iş paketleri, 4. ve 5. hedefler):

Bu çalışmada katkısı olanlar:
Doç. Dr. Murat GÜZELTEPE
Doç. Dr. Mustafa ERÖZ

9.1 Giriş

Bu çalışmada $R_{2^m} = \mathbb{F}_{2^m} + \alpha\mathbb{F}_{2^m} + \beta\mathbb{F}_{2^m} + \gamma\mathbb{F}_{2^m}$ halkası üzerindeki klasik kodlar yardımı ile kuantum kodlar oluşturulmuştur. Burada α, β ve γ sırası ile $1+i, 1+j$ ve $1+k$ kuaterniyon sayılarını göstermektedir. $u^2 = v^2 = 0$ olmak üzere $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$ halkası üzerindeki klasik kodlar yardımı ile de kuantum kodlar elde edilebilmektedir. Bizim bu halka yerine R_{2^m} halkasını kullanmamızın sebebi R_{2^m} halkası üzerinde tanımlanan norm metriği ile klasik kodun dolayısı ile kuantum kodun minimum mesafesinin daha kolay hesaplanabilmesidir.

$\mathbb{F}_{2^m}$; $g(x)$ derecesi m olan $\mathbb{Z}_2[x]$ de bir indirgenemez polinom olmak üzere

$$\mathbb{F}_{2^m} = \mathbb{Z}_2[x]/(p(x))$$

şeklinde $\mathbb{F}_2$ nin bir cisim genişlemesi olsun. $\phi : \mathbb{F}_{2^m} \to \mathbb{F}_2^m$ Gray fonksiyonu

$$\phi\left(a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}\right) = (a_0, a_1, \ldots, a_{m-1})$$

olarak tanımlanır.

$R_{2^m} = \mathbb{F}_{2^m} + \alpha\mathbb{F}_{2^m} + \beta\mathbb{F}_{2^m} + \gamma\mathbb{F}_{2^m}$ halkası bir değişmeli halkadır. Bu halkanın eleman sayısı

$$\left|R_{2^m}\right| = 2^{4m}$$

dir. R_2 halkası bir yerel halkadır. Fakat bir temel ideal bölgesi değildir. Sadece bir maksimal ideali vardır ve bu ideal temel ideal değildir. Bu halkanın idealleri şu şekilde tanımlanabilir:

$$\langle 0\rangle = \{0\} \subset \langle 1+i+j+k\rangle = \{0, 1+i+j+k\} \subset \langle\alpha\rangle$$
$$= \{0, 1+i, j+k, 1+i+j+k\}, \langle\beta\rangle, \langle\gamma\rangle \subset \langle\alpha\rangle \oplus \langle\beta\rangle$$
$$= \langle\alpha\rangle \oplus \langle\gamma\rangle = \langle\beta\rangle \oplus \langle\gamma\rangle \subset \langle 1\rangle = R_2.$$

Maksimal ideali ise

$$\langle\alpha\rangle\oplus\langle\beta\rangle=\{0,1+i,1+j,1+k,i+j,i+k,j+k,1+i+j+k\}$$

idealidir. Bir $q=a+b\alpha+c\beta+d\gamma$ elemanının eşleniği $\overline{q}=a+b\overline{\alpha}+c\overline{\beta}+d\overline{\gamma}$ ve bu elemann normu ise

$$N(q)=q\overline{q}=a^2+2b^2+2c^2+2d^2+2ab+2ac+2ad+2bc+2bd+2cd$$

olarak tanımlanır.

$\psi_{2^m}:\mathbb{F}_{2^m}+\alpha\mathbb{F}_{2^m}+\beta\mathbb{F}_{2^m}+\gamma\mathbb{F}_{2^m}\to\mathbb{F}_{2^m}^4$ fonksiyonunu

$$\psi_{2^m}\left(a+b\alpha+c\beta+d\gamma\right)=\left(b,\quad c,\quad d,\quad a+b+c+d.\right)$$

olarak tanımlayalım. Bu fonksiyon bir Gray fonksiyondur.

Teorem 9.1.1. Eğer $u\in R_{2^m}^n$ vektörü için $N(u)=w(\psi_{2^m}(u))$ ve $wt(N(u))=wt(w(\psi_{2^m}(u)))$ olur.

Teorem 9.1.2. ψ_{2^m} fonksiyonu birebir ve lineer bir fonksiyondur.

9.2 R_{2^m} Halkası Üzerinde Lineer Kodlar

R_{2^m} halkasının idealleri

$$\langle 0\rangle=\{0\}$$
$$\langle\alpha+\beta+\gamma\rangle=(\alpha+\beta+\gamma)R_{2^m},\left|\langle\alpha+\beta+\gamma\rangle\right|=2^m$$
$$\langle\alpha\rangle=(\alpha)R_{2^m},\left|\langle\alpha\rangle\right|=2^{2m}$$
$$\langle\beta\rangle=(\beta)R_{2^m},\left|\langle\beta\rangle\right|=2^{2m}$$
$$\langle\alpha\rangle+\langle\beta\rangle=(\alpha)R_{2^m}+(\beta)R_{2^m},\left|\langle\alpha\rangle+\langle\beta\rangle\right|=2^{3m}$$

olarak tanımlanabilir. Bu halkanın birimsel elemanları ise

$$R_{2^m}^*=R_{2^m}-\left(\langle\alpha\rangle+\langle\beta\rangle\right),\left|R_{2^m}^*\right|=\left(2^{3m}\right)\left(2^m-1\right)$$

kümesidir.

Tanım 9.2.1. R_{2^m} üzerinde n uzunluklu lineer C kodu bir $R_{2^m}^n$'nin bir $R_{2^m}-$alt modülü olarak tanımlanır.

Teorem 9.2.2. Eğer C kodu R_{2^m} üzerinde tanımlı n uzunluklu bir lineer kod ise bu kodun eleman sayısı

$2^k = 2^{4mk_1}2^{3mk_2}2^{2mk_3}2^{2mk_4}2^{2mk_5}2^{mk_6}$

olur.

Teorem 9.2.3. Eğer C kodu R_{2^m} üzerinde tanımlı, n uzunluklu, 2^k elemanlı ve minimum Öklid mesafesi d olan bir lineer kod ise bu durumda $\psi_{2^m}(C)$, $\mathbb{F}_{2^m}$ üzerinde bir $[4n,k,d]$ ve $\phi(\psi(C))$ ise $\mathbb{F}_2$ üzerinde bir $[4mn,k,d]$ lineer kod olurlar.

Teorem: Eğer C kodu R_{2^m} üzerinde n uzunluklu kendine-dik bir kod ise o zaman $\psi_{2^m}(C)$ $\mathbb{F}_{2^m}$ üzerinde $4n$ uzunluklu ve $\phi(\psi(C))$ ise $\mathbb{F}_2$ üzerinde $4mn$ uzunluklu kendine-dik kod olurlar. lineer kod olurlar.

Teorem 9.2.4. $C_1,\ldots,C_6$ kodları her $s \neq t$ için $C_s \cap C_t = \{0\}$ şartını sağlayan $\mathbb{F}_{2^m}$ üzerinde tanımlı lineer kodlar, C de R_{2^m} de tanımlı bir lineer kod ve M de R_{2^m}'nin maksimal ideali olsun. Bu durumda C kodu

$C = \left(R_{2^m} \setminus M\right)C_1 \oplus \left(\langle\alpha\rangle + \langle\beta\rangle\right)C_2 \oplus \left(\langle\alpha\rangle\right)C_3 \oplus \left(\langle\beta\rangle\right)C_4 \oplus \left(\langle\gamma\rangle\right)C_5 \oplus \left(\langle\alpha+\beta+\gamma\rangle\right)C_6$

olarak tanımlanabilir. Bu durumda

$|C| = 2^{4mk_1+3mk_2+2mk_3+2mk_4+2mk_5+mk_6}$

olur. Burada $k_1,\ldots,k_6$ sayıları sırası ile $C_1,\ldots,C_6$ lineer kodlarının boyutlarını göstermektedir.

Teorem 9.2.5. Eğer C kodu R_{2^m} üzerinde kendine-dik $\left[n,\frac{n}{2},d\right]$ parametreli bir kod ise o zaman $\psi_{2^m}(C)$ de $\mathbb{F}_{2^m}$ üzerinde $\left[4n,2n,\geq d\right]$ parametreli kendine-dik bir kod ve $\phi(\psi_{2^m}(C))$ ise $\mathbb{F}_2$ üzerinde $\left[4mn,2mn,\geq d\right]$ parametreli bir kod olur.

Örnek 9.2.6. $m=2$, $n=4$ ve $k=2$ olsun. $\mathbb{F}_4=\{0,1,w,w^2\}$ olarak alınabilir. Burada $w^2+w+1=0, w^3=1$ dir. R_{2^2} üzerinde bir C kodunun üreteç matrisi

$$G=\begin{pmatrix} 1 & \alpha+\lambda & 1+\alpha+\beta & w(\alpha+\beta) \\ \alpha+\lambda & 1+\alpha+\beta+\gamma & w(\alpha+\beta) & 1+\alpha+\beta \end{pmatrix}$$
$$=\begin{pmatrix} 1 & i+k & 1+i+j & w(i+j) \\ i+k & i+j+k & w(i+j) & 1+i+j \end{pmatrix}$$

olsun. Bu durumda bu kod R_{2^2} üzerinde bir kendine-dik kod olur. Bu kodun minimum Öklid mesafesi 6 dır. Dolayısı ile R_{2^2} üzerinde bir $[[4,0,6]]$ kuantum kodu vardır. Böylece $[[4,0,6]]$ kuantum kodu literatüre kazandırılmıştır. Bu G matrisinin yardımı ile $\psi_{2^2}(C)$ kodunun üreteç matrisi olan G' matrisi şu şekilde elde edilir:

Önce G matrisinin satırları kuaterniyonların bazları ile çarpılarak

$$A=\begin{pmatrix} 1 & i+k & 1+i+j & w(i+j) \\ i & 1+j & 1+i+k & w(1+k) \\ j & i+k & 1+j+k & w(1+k) \\ k & 1+j & i+j+k & w(i+j) \\ i+k & i+j+k & w(i+j) & 1+i+j \\ 1+j & 1+j+k & w(1+k) & 1+i+k \\ i+k & 1+i+k & w(1+k) & 1+j+k \\ 1+j & 1+i+j & w(i+j) & i+j+k \end{pmatrix}$$

matrisi yazılır. Bu matris yardımı ile

$$G'=\psi_{2^2}(A)=\begin{pmatrix} 0&0&0&1&1&0&1&0&1&1&0&1&w&w&0&0 \\ 1&0&0&0&0&1&0&1&1&0&1&1&0&0&w&w \\ 0&1&0&0&1&0&1&0&0&1&1&1&0&0&w&w \\ 0&0&1&0&0&1&0&1&1&1&1&0&w&w&0&0 \\ 1&0&1&0&1&1&1&0&w&w&0&0&1&1&0&1 \\ 0&1&0&1&0&1&1&1&0&0&w&w&1&0&1&1 \\ 1&0&1&0&1&0&1&1&0&0&w&w&0&1&1&1 \\ 0&1&0&1&1&1&0&1&w&w&0&0&1&1&1&0 \end{pmatrix}$$

matrisi elde edilir. G' üreteç matrisine sahip $\psi_{2^2}(C)$ kodu $\mathbb{F}_4$ üzerinde $[16,8,6]$ parametreli kendine-dik bir koddur. Bu kod yardımı ile $[[16,0,6]]$ optimal kuantum kodu elde edilir. G' üreteç matrisi yardımı ile de $\mathbb{F}_2$ üzerinde $\phi(\psi_{2^m}(C))$ kodunun üreteç matrisi G'' şu şekilde oluşturulur: G' nün standart formu

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w^2 & w & w^2 & w^2 & 1 & 0 & w^2 & w \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & w & w^2 & w^2 & w^2 & 0 & 1 & w & w^2 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & w^2 & w^2 & w^2 & w & w^2 & w & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & w^2 & w^2 & w & w^2 & w & w^2 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & w^2 & w & w & w^2 & w & w \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & w & w^2 & w^2 & w & w & w \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & w^2 & w & 1 & 0 & w & w & w & w^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & w & w^2 & 0 & 1 & w & w & w^2 & w
\end{pmatrix}$$

şeklindedir. Bu standart form matrisi ve ϕ fonksiyonu yardımı ile

$$G'' = \begin{pmatrix}
1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,1,1,1,1,1,1,0,0,0,1,1,0,1 \\
0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1,1,0,1,0,0,1,0,0,1,0,1,1 \\
0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,0,0,1,0,0,1,1,1 \\
0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,1,0,1,0,0,0,0,0,1,1,1,0 \\
0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,0,1,1,1,0,1,1,0,0,0 \\
0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,0,1,0,1,0,1,1,1,0,1,1,0,1,0,0 \\
0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,1,1,1,1,0,1,1,1,0,1,1,1,0,0,1,0 \\
0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,1,0,1,1,1,0,1,1,1,0,0,0,0,1 \\
0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,1,1,0,1,0,1,1,1,0,1,0,1 \\
0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,1,0,1,1,1,1,1,1,0,1,1,1,1 \\
0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,1,0,0,1,1,1,1,1,1,0,1,0,1,0,1,1 \\
0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,1,1,1,1,1,0,1,0,1,1,1,1,1,1,1,1 \\
0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,1,0,1,1,0,0,0,0,1,0,1,0,1,1,1 \\
0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,1,0,1,0,1,1,0,1,0,0,1,1,1,1,1,0 \\
0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1,1,0,0,1,0,0,1,0,1,1,1,0,1 \\
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,1,1,0,1,1
\end{pmatrix}$$

olarak hesaplanır. Bu G'' üreteç matrisine sahip $\phi(\psi_{2^m}(C))$ kodu $\mathbb{F}_2$ üzerinde $[32,16,6]$ parametreli kendine-dik bir koddur. Bu kod yardımı ile $[[32,0,6]]$ kuantum kodu elde edilir.

Örnek 9.2.7. $m=1$, $n=4$ ve $k=2$ olsun. R_2 üzerinde bir C kodunun üreteç matrisi

$$G=\begin{pmatrix} 1 & \alpha+\lambda & 1+\alpha+\beta & \alpha+\beta \\ \alpha+\lambda & 1+\alpha+\beta+\gamma & \alpha+\beta & 1+\alpha+\beta \end{pmatrix}$$

olsun. Bu durumda C kodu R_2 üzerinde minimum mesafesi 4 olan kendine- dik bir kod olur. Bu kodun kendine dik olduğu ve minimum mesafesinin 4 olduğunu aşağıdaki Mathematica programı ile hesaplamak mümkündür. Bu C kodu yardımı ile R_2 üzerinde bir $[[4,0,4]]$ kodu elde edilir.

```
In[1]:= << Quaternions`
        m = 1;
        k = 2;
        α = Quaternion[1, 1, 0, 0];
        β = Quaternion[1, 0, 1, 0];
        γ = Quaternion[1, 0, 0, 1];
        A = {Quaternion[0, 0, 0, 0], Quaternion[1, 0, 0, 0]};
        R = Table[0, {2^(4*m)}];
        R2 = Table[0, {2^(4*m)}];
        art = 0;
        Do[
          Do[
           Do[
            Do[
             art = art + 1; (*Print["art=",art," ",A[[k1]]+α**A[[k2]]+β**A[[k3]]+γ**A[[k4]]];*)
             R[[art]] = A[[k1]] + α ** A[[k2]] + β ** A[[k3]] + γ ** A[[k4]]
             , {k4, 1, 2}]
            , {k3, 1, 2}]
           , {k2, 1, 2}]
          , {k1, 1, 2}];
        Do[
          R2[[t]] = Quaternion[Mod[R[[t, 1]], 2], Mod[R[[t, 2]], 2], Mod[R[[t, 3]], 2], Mod[R[[t, 4]], 2]]
          , {t, 1, 2^(4*m)}];

        RT = {R2[[9]], R2[[10]], R2[[11]], R2[[12]], R2[[13]], R2[[14]], R2[[15]], R2[[16]]};
        RC = {R2[[1]], R2[[2]], R2[[3]], R2[[4]], R2[[5]], R2[[6]], R2[[7]], R2[[8]]};
```

```
TT = Tuples[R2, k];
LK = Table[1, {16^k}];
LKM = Table[1, {Dimensions[LK][[1]]}];
a = 500;

K2 = ( Quaternion[1, 0, 0, 0]  Quaternion[0, 1, 0, 1]  Quaternion[1, 1, 1, 0]  Quaternion[0, 1, 1, 0]
       Quaternion[0, 1, 0, 1]  Quaternion[0, 1, 1, 1]  Quaternion[0, 1, 1, 0]  Quaternion[1, 1, 1, 0] );
Do[
  LK[[i]] = Sum[TT[[i, j]] ** K2[[j]], {j, 1, 2}], {i, 1, 16^k}];
Do[LKM[[t]] = {Quaternion[Mod[LK[[t, 1, 1]], 2], Mod[LK[[t, 1, 2]], 2], Mod[LK[[t, 1, 3]], 2], Mod[LK[[t, 1, 4]], 2]],
    Quaternion[Mod[LK[[t, 2, 1]], 2], Mod[LK[[t, 2, 2]], 2], Mod[LK[[t, 2, 3]], 2], Mod[LK[[t, 2, 4]], 2]],
    Quaternion[Mod[LK[[t, 3, 1]], 2], Mod[LK[[t, 3, 2]], 2], Mod[LK[[t, 3, 3]], 2], Mod[LK[[t, 3, 4]], 2]],
    Quaternion[Mod[LK[[t, 4, 1]], 2], Mod[LK[[t, 4, 2]], 2], Mod[LK[[t, 4, 3]], 2], Mod[LK[[t, 4, 4]], 2]]}
  , {t, 1, Dimensions[LK][[1]]}];
Do[If[Sum[Norm[LKM[[j, i]]], {i, 1, 4}] < a, a = Sum[Norm[LKM[[j, i]]], {i, 1, 4}]], {j, 2, 16^k}];
a
K2 // MatrixForm
```

Out[24]= 4

$$\begin{pmatrix} \text{Quaternion}[1,0,0,0] & \text{Quaternion}[0,1,0,1] & \text{Quaternion}[1,1,1,0] & \text{Quaternion}[0,1,1,0] \\ \text{Quaternion}[0,1,0,1] & \text{Quaternion}[0,1,1,1] & \text{Quaternion}[0,1,1,0] & \text{Quaternion}[1,1,1,0] \end{pmatrix}$$

BÖLÜM 10.

Hurwitz sayıları üzerinde yeni sinyal yıldız kümeleri ve yeni blok kodlar

(1,3,4,5. iş paketleri, 1,2 ve 5. hedef):

Bu çalışmada katkısı olanlar:

Doç. Dr. Murat GÜZELTEPE

Ramazan Duran (Projede çalışan doktora öğrencimiz)

10.1 Giriş

Bu bölümde Hurwitz sayıları üzerinde yeni bir metotla yeni sinyal yıldız kümeleri oluşturulacaktır. Bu sinyal yıldız kümeleri üzerinde tanımlanacak blok kodların kod kazancının daha iyi olduğu gösterilecektir.

Tanım 10.1.1 : Hurwitz tamsayılar kümesi

$$H(\mathbb{Z})=\left\{\alpha=\alpha_1+\alpha_2 i+\alpha_3 j+\alpha_4 k \;:\; \alpha\in H(\mathbb{R}) \text{ ve } \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4\in\mathbb{Z} \text{ veya } \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4\in\mathbb{Z}+\frac{1}{2}\right\} \qquad (12)$$

şeklinde tanımlanmaktadır. $\alpha\in H(\mathbb{R})$ olmak üzere α nın eşleniği

$$\alpha^{*}=\alpha_1-\alpha_2 i-\alpha_3 j-\alpha_4 k \qquad (13)$$

ve normu da

$$N(\alpha)=\alpha\cdot\alpha^{*}=\alpha_1^2+\alpha_2^2+\alpha_3^2+\alpha_4^2 \qquad (14)$$

bağıntılarıyla tanımlanmaktadır. $\alpha\in H(\mathbb{R})$ ve $\alpha\neq 0$ olmak üzere α nın tersi

$$\alpha^{-1}=\frac{\alpha^{*}}{N(\alpha)} \qquad (15)$$

ile tanımlanmaktadır. $H(\mathbb{Z})$, $H(\mathbb{R})$ nin bir altkümesidir. Hurwitz tamsayıları için iki tane nokta notasyonu tanımlanmaktadır. Bunlardan ilki $\lfloor\bullet\rceil$ nokta notasyonu bir reel sayıyı kendisine en yakın tamsayıya yuvarlanması olarak tanımlanmaktadır. İkincisi ise $\lfloor\!\lfloor\bullet\rceil\!\rceil$ nokta notasyonu bir reel sayıyı kendisine en yakın yarım tamsayıya yuvarlanması olarak tanımlanmaktadır. $\alpha\in\mathbb{R}$ için α Hurwitz tamsayısı

$$\lfloor\alpha\rceil=\lfloor\alpha_1\rceil+\lfloor\alpha_2\rceil i+\lfloor\alpha_3\rceil j+\lfloor\alpha_4\rceil k \qquad (16)$$

veya

$$\lfloor\!\lfloor\alpha\rceil\!\rceil=\lfloor\!\lfloor\alpha_1\rceil\!\rceil+\lfloor\!\lfloor\alpha_2\rceil\!\rceil i+\lfloor\!\lfloor\alpha_3\rceil\!\rceil j+\lfloor\!\lfloor\alpha_4\rceil\!\rceil k \qquad (17)$$

şeklinde tanımlanmaktadır.

Örnek 10.1.2: $\alpha = \frac{2}{3} + \frac{7}{5}i + \frac{1}{4}j + \frac{23}{8}k$ kuaterniyonunda (16) eşitliği kullanılarak

$$\begin{aligned} \lfloor \alpha \rceil &= \lfloor \tfrac{2}{3} \rceil + \lfloor \tfrac{7}{5} \rceil i + \lfloor \tfrac{1}{4} \rceil j + \lfloor \tfrac{23}{8} \rceil k \\ &= 1 + 1 \cdot i + 0 \cdot j + 3 \cdot k \\ &= 1 + i + 3 \cdot k \end{aligned}$$

Hurwitz tamsayısı elde edilmektedir.

Örnek 10.1.3: $\alpha = \frac{3}{4} - \frac{7}{5}i + \frac{1}{4}j - \frac{23}{8}k$ kuaterniyonunda (17) eşitliği kullanılarak

$$\begin{aligned} \lfloor\!\lfloor \alpha \rceil\!\rceil &= \lfloor\!\lfloor \tfrac{3}{4} \rceil\!\rceil - \lfloor\!\lfloor \tfrac{7}{5} \rceil\!\rceil i + \lfloor\!\lfloor \tfrac{1}{4} \rceil\!\rceil j - \lfloor\!\lfloor \tfrac{23}{8} \rceil\!\rceil k \\ &= \frac{1}{2} - \frac{3}{2} \cdot i + \frac{1}{2} \cdot j - \frac{5}{2} \cdot k \end{aligned}$$

Hurwitz tamsayısı elde edilmektedir.

Bir Hurwitz tamsayısı asal Hurwitz tamsayısıdır gerekli ve yeterli koşul normu asal sayıdır. Bir kuaterniyonun bileşenlerinin en büyük ortak böleni 1 ise primitiftir. Bir α Hurwitz tamsayısı için iki tane modulo fonksiyonu aşağıdaki gibi tanımlanmaktadır.

$$\mu_1(\alpha) = \alpha \bmod \lambda = \alpha - \lambda \cdot \lfloor \alpha \cdot \lambda^{-1} \rceil \tag{18}$$

$$\mu_2(\alpha) = \alpha \bmod \lambda = \alpha - \lambda \cdot \lfloor\!\lfloor \alpha \cdot \lambda^{-1} \rceil\!\rceil \tag{19}$$

(18) ve (19) daki eşitliklere göre modulo fonksiyonu $H(\mathbb{Z})$ den $H(\mathbb{Z})$ e bir fonkisyondur. (18) ve (19) daki modulo fonksiyonlarıyla Hurwitz tamsayıların kalan sınıf halkası

$$\mu(z) = \left\{ \min\left\{ \mu_1(z), \mu_2(z) \right\} : \ z \in H(\mathbb{Z}) \right\} \tag{20}$$

şeklinde tanımlanabilmektedir. Hurwitz tamsayılarının kalan sınıf halkasının eleman sayısı mükemmel kare tamsayıdır. Olası sinyal yıldızkümesinin sayısını genişletmek için λ primitif bir Hurwitz tamsayısı olmak üzere $H_\lambda = \left\{ \mu(z) \ : z \in \mathbb{Z} \right\}$ altgrubunu ele alacağız. Burada $H(\mathbb{Z})$ nin bir altkümesi olarak $\mathbb{Z}$ ya da $\mathbb{Z} + \frac{1}{2}$ yi alacağız. Bir adi tamsayı imajiner kısmı sıfır olan bir Hurwitz tamsayıdır. H_λ kümesi $N(\lambda) = \lambda \cdot \lambda^{-1}$ kadar elemana sahiptir. Hurwitz tamsayılarıyla kod kümesi oluştururken λ bir asal Hurwitz tamsayısı olmak üzere Hurwitz tamsayıların kalan sınıf halkalarını alacağız. $\mathbb{Z}_n$, n elemana sahip adi tamsayıların kalan sınıf halkası olarak bilinmektedir. Bir primitif Hurwitz tamsayısı için (18) ve (19) daki modulo

fonksiyonları, $\mathbb{Z}_{N(\lambda)}$ ve H_λ arasında toplama işlemine göre bir izomorfizmdir. Çünkü ters görüntüsü vardır ve $\forall z_1, z_2 \in \mathbb{Z}_{N(\lambda)}$ için $\mu_1(z_1+z_2)=\mu_1(z_1)+\mu_1(z_2)$, $\mu_2(z_1+z_2)=\mu_2(z_1)+\mu_2(z_2)$ ve (20) deki eşitlikten $\mu(z_1+z_2)=\mu(z_1)+\mu(z_2)$ modulo eşitlikleri sağlanmaktadır.

Örnek 10.1.4: $\lambda = 6+3i+2j+2k$ primitif bir Hurwitz tamsayısı olsun. $N(\lambda)=6^2+3^2+2^2+2^2=53$ tür. Dolayısıyla H_λ kümesi 53 elemana sahiptir. Aynı zamanda normu asal sayı olduğundan $\lambda = 6+3i+2j+2k$ sayısı Hurwitz asal tamsayısıdır.

Örnek 10.1.5: $\lambda = \frac{1}{2}+\frac{5}{2}i+\frac{7}{2}j+\frac{13}{2}k$ bir Hurwitz tamsayısı olsun. $N(\lambda)=\left(\frac{1}{2}\right)^2+\left(\frac{5}{2}\right)^2+\left(\frac{7}{2}\right)^2+\left(\frac{13}{2}\right)^2=61$ dir. Dolayısıyla H_λ kümesi 61 elemana sahiptir.

Bu bölümde, AWGN kanalı üzerinde iletim performanslarına göre Gauss ve Hurwitz sinyal yıldızkümelerini karşılaştıracağız. İlk önce bazı uzaklık ve performans ölçülerini tanımlayacağız.

λ Hurwitz tamsayısı olmak üzere M-boyutlu bir yıldızkümesinin spektral etkinliği boyut başı bit sayısına göre ölçümü aşağıdaki eşitlikten elde edilmektedir.

$$b_\lambda = \frac{\log_2\left(N(\lambda)\right)}{M}$$

Bir yıldızkümesinin ortalama enerjisi tüm elemanları eşit olasılıkla kullanıldığındaki umulan enerjidir. Bu enerji Hurwitz tamsayısı ve Gauss tamsayısı için aşağıdaki bağıntılar yardımıyla bulunmaktadır.

$$E_\lambda = \frac{1}{N(\lambda)}\sum_{z\in H_\lambda} N(z)$$

$$E_\lambda = \frac{1}{N(\lambda)}\sum_{z\in G_\lambda} N(z)$$

İki Hurwitz tamsayısının ya da Gauss tamsayısının kare öklidyen uzaklığı

$$d_E(y,z)=N(z-y)$$

ve yıldızkümelerinin minimum kare öklidyen uzaklığı

$$\delta_\lambda^2 = \min_{z,y\in H_\lambda, z\neq y} d_E(y,z)$$

$$\delta_\lambda^2 = \min_{z,y\in G_\lambda, z\neq y} d_E(y,z)$$

bağıntılarıyla elde edilmektedir.

CFM (constellation figure of merit) ortalama enerji ve minimum kare öklidyen uzaklığının kombine edilmiş ve iki boyutlu sinyal enerjisinin normalize edilmiş halidir. M-boyutlu yıldızkümesi için CFM aşağıdaki eşitlik yardımıyla bulunmaktadır.

$$CFM(\lambda) = \frac{M\delta_\lambda^2}{2E_\lambda}$$

Yüksek değere sahip CFM bir AWGN kanalı üzerinde en iyi iletim performansına sahip olmaktadır.

10.2 Hurwitz Sayıları Üzerinde Yeni Yıldız Kümeleri ve Yeni Blok Kodlar

Bu bölümde Hurwitz tamsayıları halkasının küme ayrıştırılması incelenmektedir. Aynı özellikleri Gauss tamsayıları için de düşünebiliriz . H_λ Hurwitz tamsayılarının bir kalan sınıf halkası, $N(\lambda)$ bir tamsayı olmak üzere $\mathbb{Z}_{N(\lambda)} = \{0,1,\ldots,N(\lambda)-1\}$ tamsayılarının kalan sınıf halkasından elde edilmektedir. Eğer $N(\lambda)$ asal bir sayı değilse $\mathbb{Z}_{N(\lambda)}$ kümesini eşit boyutlu altkümelere ayrıştırabiliriz. $\mathbb{Z}_{N(\lambda)} = c\cdot d$ olsun. H_λ kümesini herbiri d elemanlı c tane $H_\lambda^{(0)},\ldots,H_\lambda^{(c-1)}$ şeklindeki altkümelere ayrıştırabiliriz. Bu kümeler $\mathbb{Z}_{N(\lambda)}^{(0)} = \{0,c,2c,\ldots,(d-1)c\}$ ve $\mathbb{Z}_{N(\lambda)}^{(1)},\ldots,\mathbb{Z}_{N(\lambda)}^{(c-1)}$, $\mathbb{Z}_{N(\lambda)}^{(0)}$ ın kosetleri olmak üzere $\mathbb{Z}_{N(\lambda)}^{(0)},\ldots,\mathbb{Z}_{N(\lambda)}^{(c-1)}$ tamsayı kümelerine karşılık gelmektedir. $\mathbb{Z}_{N(\lambda)}^{(0)}$, $\mathbb{Z}_{N(\lambda)}$ nin bir toplamsal altgrubu olmasından dolayı $H_{N(\lambda)}^{(0)}$ da $H_{N(\lambda)}$ nın bir toplamsal altgrubu olduğu sonucu ortaya çıkmaktadır. Çünkü $\mu(\bullet)$ modulo fonksiyonu toplamaya göre bir izomorfizmdir. Aşağıda verilecek olan lemmalar ve teorem ile her $H_\lambda^{(l)}$ altkümesinin minimum kare öklidyen uzaklığı δ^2 yi hesaplayacağız.

Lemma 10.2.1: $\mu(\bullet)$, λ primitif Hurwitz tamsayısının modulo fonkisyonu olsun. Her α Lipschitz tamsayısı için

$$N\left(\mu(\alpha)\right) \le N(\alpha)$$

dır.

Lemma 10.2.2: $N(\lambda) = c \cdot d$ ve altkümeleri $H_\lambda^{(0)}, \ldots, H_\lambda^{(c-1)}$ olan H_λ kümesini ele alalım. Herbir altkümenin minimum kare öklidyen uzaklığı δ^2 için

$$\delta^2 \ge \min_{\alpha \in H_\lambda^{(0)} - \{0\}} N(\alpha)$$

elde edilmektedir.

Teorem 10.2.3: $N(\lambda) = c \cdot d$ ve altkümeleri $H_\lambda^{(0)}, \ldots, H_\lambda^{(c-1)}$ olan H_λ kümesini ele alalım. Herbir altkümenin minimum kare öklidyen uzaklığı δ^2 için

$$\delta^2 \ge c$$

elde edilmektedir.

Örnek 10.2.4: 15 elemanlı $H_{3+2i+j+k}$ kümesi 5 elemanlı 3 altkümeye ayrıştırılabilmektedir. (18) eşitliği kullanılarak

$$\begin{aligned} H_{(1)3+2i+j+k} = \{ & 0,\ 1,\ 2,\ -2i-2j-k,\ -1+i-2k, i-2k, \\ & 1+i-2k,\ 2+i-2k,\ -2-i+2k,\ -1-i+2k, \\ & -i+2k,\ 1-i+2k,\ 2i+j+k,\ -2,\ -1\} \end{aligned} \tag{21}$$

elde edilmektedir. (19) eşitliği kullanılarak

$$\begin{aligned} H_{(2)3+2i+j+k} = \Big\{ & -\frac{7}{2}+\frac{1}{2}i+\frac{1}{2}j+\frac{3}{2}k,\ -\frac{5}{2}+\frac{1}{2}i+\frac{1}{2}j+\frac{3}{2}k,\ -\frac{3}{2}+\frac{1}{2}i+\frac{1}{2}j+\frac{3}{2}k,\ -\frac{1}{2}+\frac{1}{2}i+\frac{1}{2}j+\frac{3}{2}k, \\ & \frac{1}{2}+\frac{1}{2}i+\frac{1}{2}j+\frac{3}{2}k,\ -\frac{3}{2}-\frac{3}{2}i-\frac{1}{2}j+\frac{1}{2}k,\ -\frac{1}{2}-\frac{3}{2}i-\frac{1}{2}j+\frac{1}{2}k,\ \frac{1}{2}-\frac{3}{2}i-\frac{1}{2}j+\frac{1}{2}k, \\ & -\frac{1}{2}+\frac{3}{2}i+\frac{1}{2}j-\frac{1}{2}k,\ \frac{1}{2}+\frac{3}{2}i+\frac{1}{2}j-\frac{1}{2}k,\ -\frac{3}{2}-\frac{1}{2}i-\frac{1}{2}j-\frac{3}{2}k,\ -\frac{1}{2}-\frac{1}{2}i-\frac{1}{2}j-\frac{3}{2}k, \\ & \frac{1}{2}-\frac{1}{2}i-\frac{1}{2}j-\frac{3}{2}k,\ \frac{3}{2}-\frac{1}{2}i-\frac{1}{2}j-\frac{3}{2}k,\ \frac{5}{2}-\frac{1}{2}i-\frac{1}{2}j-\frac{3}{2}k\Big\} \end{aligned}$$

(22)

elde edilmektedir. (21) kümesinden

$$\begin{aligned} H_{(1)3+2i+j+k}^{(0)} = \{ & \mu(0)=0,\ \mu(3)=-2i-j-k, \mu(6)=1+i-2k, \\ & \mu(9)=-1-i+2k,\ \mu(12)=2i+j+k\} \end{aligned} \tag{23}$$

ve (22) kümesinden

$$H^{(0)}_{(2)3+2i+j+k} = \Big\{ \mu(0) = -\frac{7}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{3}{2}k,\ \mu(3) = -\frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{3}{2}k,\ \mu(6) = -\frac{1}{2} - \frac{3}{2}i - \frac{1}{2}j + \frac{1}{2}k,$$
$$\mu(9) = \frac{1}{2} + \frac{3}{2}i + \frac{1}{2}j - \frac{1}{2}k,\ \mu(12) = \frac{1}{2} - \frac{1}{2}i - \frac{1}{2}j - \frac{3}{2}k \Big\} \quad (24)$$

elde edilmektedir. (23) ve (24) altkümelerinden $\mathbb{Z}_{15} = \{0,3,6,9,12\}$ altgrubuna karşılık gelen Hurwitz tamsayıları kümesi

$$H^{(0)}_{3+2i+j+k} = \Big\{ \mu(0) = 0,\ \mu(3) = -\frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{3}{2}k,\ \mu(6) = -\frac{1}{2} - \frac{3}{2}i - \frac{1}{2}j + \frac{1}{2}k,$$
$$\mu(9) = \frac{1}{2} + \frac{3}{2}i + \frac{1}{2}j - \frac{1}{2}k,\ \mu(12) = \frac{1}{2} - \frac{1}{2}i - \frac{1}{2}j - \frac{3}{2}k \Big\}$$

oluşturulmaktadır. Teorem 1 göre $\delta^2 \geq 3$ tir. Bu kümenin sıfırdan farklı herbir elemanın normu 3 tür. Bu yüzden Lemma 2 den herbir altkümenin minimum kare öklidyen uzaklığı $\delta^2 \geq 3$ elde eilmektedir.

Örnek 10.2.5: 35 elemanlı $H_{4+3i+3j+k}$ kümesi 7 elemanlı 5 altkümeye ayrıştırılabilmektedir. (18) eşitliği kullanılarak

$$\begin{aligned} H_{(1)4+3i+3j+k} = \{ & 0,\ 1,\ 2,\ 3,\ 4,\ 1-3i-3j-k,\ -4+2j-k,\ -3+2j-k, \\ & -2+2j-k,\ -1+2j-k,\ 2j-k,\ 1+2j-k,\ 2+2j-k, \\ & 3+2j-k,\ -3i-j-2k,\ 1-3i-j-2k,\ 2-3i-j-2k, \\ & 3-3i-j-2k,\ -3+3i+j+2k,\ -2+3i+j+2k, \\ & -1+3i+j+2k,\ 3i+j+2k,\ -3-2j+k\ ,-2-2j+k, \\ & -1-2j+k,\ -2j+k,\ 1-2j+k,\ 2-2j+k,\ 3-2j+k, \\ & 4-2j+k,\ -1+3i+3j+k,\ -4,\ -3,\ -2,\ -1 \} \end{aligned} \quad (25)$$

kümesi elde edilmektedir. (19) eşitliği kullanılarak

$$H_{(2)4+3i+3j+k}=\Big\{-\frac{11}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ -\frac{9}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ -\frac{7}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ -\frac{5}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,$$
$$-\frac{5}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ -\frac{3}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ -\frac{1}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ \frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,$$
$$\frac{1}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ \frac{3}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ \frac{5}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ -\frac{1}{2}-\frac{3}{2}i-\frac{7}{2}j+\frac{1}{2}k,$$
$$\frac{1}{2}-\frac{3}{2}i-\frac{7}{2}j+\frac{1}{2}k,\ \frac{3}{2}-\frac{3}{2}i-\frac{7}{2}j+\frac{1}{2}k,\ -\frac{7}{2}+\frac{3}{2}i+\frac{3}{2}j+\frac{1}{2}k,\ -\frac{5}{2}+\frac{3}{2}i+\frac{3}{2}j+\frac{1}{2}k,$$
$$-\frac{3}{2}+\frac{3}{2}i+\frac{3}{2}j+\frac{1}{2}k,\ -\frac{1}{2}+\frac{3}{2}i+\frac{3}{2}j+\frac{1}{2}k,\ \frac{1}{2}+\frac{3}{2}i+\frac{3}{2}j+\frac{1}{2}k,\ \frac{3}{2}+\frac{3}{2}i+\frac{3}{2}j+\frac{1}{2}k,$$
$$-\frac{3}{2}-\frac{3}{2}i-\frac{3}{2}j-\frac{1}{2}k,\ -\frac{1}{2}-\frac{3}{2}i-\frac{3}{2}j-\frac{1}{2}k,\ \frac{1}{2}-\frac{3}{2}i-\frac{3}{2}j-\frac{1}{2}k,\ \frac{3}{2}-\frac{3}{2}i-\frac{3}{2}j-\frac{1}{2}k,$$
$$\frac{5}{2}-\frac{3}{2}i-\frac{3}{2}j-\frac{1}{2}k,\ \frac{7}{2}-\frac{3}{2}i-\frac{3}{2}j-\frac{1}{2}k,\ -\frac{3}{2}+\frac{3}{2}i+\frac{7}{2}j-\frac{1}{2}k,\ -\frac{1}{2}+\frac{3}{2}i+\frac{7}{2}j-\frac{1}{2}k,$$
$$\frac{1}{2}+\frac{3}{2}i+\frac{7}{2}j-\frac{1}{2}k,\ -\frac{5}{2}-\frac{3}{2}i+\frac{1}{2}j-\frac{3}{2}k,\ -\frac{3}{2}-\frac{3}{2}i+\frac{1}{2}j-\frac{3}{2}k,\ -\frac{1}{2}-\frac{3}{2}i+\frac{1}{2}j-\frac{3}{2}k,$$
$$\frac{1}{2}-\frac{3}{2}i+\frac{1}{2}j-\frac{3}{2}k,\ \frac{3}{2}-\frac{3}{2}i+\frac{1}{2}j-\frac{3}{2}k,\ \frac{5}{2}-\frac{3}{2}i+\frac{1}{2}j-\frac{3}{2}k,\ \frac{7}{2}-\frac{3}{2}i+\frac{1}{2}j-\frac{3}{2}k,$$
$$\frac{9}{2}-\frac{3}{2}i+\frac{1}{2}j-\frac{3}{2}k\Big\} \tag{26}$$

kümesi elde edilmektedir. (25) kümesinden

$$H^{(0)}_{(1)4+3i+3j+k}=\big\{\mu(0)=0,\ \mu(5)=1-3i-3j-k,\ \mu(10)=2j-k,\ \mu(15)=1-3i-j-2k,$$
$$\mu(20)=-1+3i+j+2k,\ \mu(25)=-2j+k,\ \mu(30)=-1+3i+3j+k\big\} \tag{27}$$

elde edilmektedir. (26) kümesinden

$$H^{(0)}_{(2)4+3i+3j+k}=\Big\{\mu(0)=-\frac{11}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ \mu(5)=-\frac{1}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ \mu(10)=\frac{1}{2}-\frac{3}{2}i-\frac{7}{2}j+\frac{1}{2}k,$$
$$\mu(15)=-\frac{1}{2}+\frac{3}{2}i+\frac{3}{2}j+\frac{1}{2}k,\ \mu(20)=\frac{1}{2}-\frac{3}{2}i-\frac{3}{2}j-\frac{1}{2}k,\ \mu(25)=-\frac{1}{2}+\frac{3}{2}i+\frac{7}{2}j-\frac{1}{2}k, \tag{28}$$
$$\mu(30)=\frac{1}{2}-\frac{3}{2}i+\frac{1}{2}j-\frac{3}{2}k\Big\}$$

elde edilmektedir. (27) ve (28) kümelerinden $\mathbb{Z}_{35}=\{0,5,10,15,20,25,30\}$ altgrubuna karşılık gelen Hurwitz tamsayıları kümesi aşağıdaki gibidir.

$$H^{(0)}_{4+3i+3j+k}=\Big\{\mu(0)=0,\ \mu(5)=-\frac{1}{2}+\frac{3}{2}i-\frac{1}{2}j+\frac{3}{2}k,\ \mu(10)=2j-k,\ \mu(15)=-\frac{1}{2}+\frac{3}{2}i+\frac{3}{2}j+\frac{1}{2}k,$$
$$\mu(20)=\frac{1}{2}-\frac{3}{2}i-\frac{3}{2}j-\frac{1}{2}k,\ \mu(25)=-2j+k,\ \mu(30)=\frac{1}{2}-\frac{3}{2}i+\frac{1}{2}j-\frac{3}{2}k\Big\}$$

Teorem 10.2.3'e göre $\delta^2\geq 5$ tir. Görüleceği üzere teorem 1 deki sınırlama kuralı bu örnek için zor olmaktadır.

UYGULAMALAR

Örnek 1: $\lambda = 3+3i+j+k$ önerilmiş Hurwitz tamsayısı olsun. Bu önerilmiş λ Hurwitz sayısının normu $N(\lambda)=20$ dir. Önerilmiş λ Hurwitz tamsayısı herbiri 10 elemanlı 2 farklı kümeye ayrıştırılabilir. Önerilmiş λ Hurwitz tamsayısının küme elemanları
(18) deki modulo 1 fonksiyonu uygulanırsa;

$$\begin{aligned} H_{(1)\lambda} = \{ & \mu_1(0)=0, \mu_1(1)=1, \mu_1(2)=2, \mu_1(3)=3, \mu_1(4)=-2-2k, \mu_1(5)=-1-2k, \\ & \mu_1(6)=-2k, \mu_1(7)=1-2k, \mu_1(8)=2-2k, \mu_1(9)=3-2k, \mu_1(10)=-2-4k, \\ & \mu_1(11)=-3+2k, \mu_1(12)=-2+2k, \mu_1(13)=-1+2k, \mu_1(14)=2k, \mu_1(15)=1+2k, \\ & \mu_1(16)=2+2k, \mu_1(17)=-3, \mu_1(18)=-2, \mu_1(19)=-1\} \end{aligned} \quad (4.1.1)$$

(19) daki modulo 2 fonksiyonu uygulanırsa;

$$\begin{aligned} H_{(2)\lambda} = \{ & \mu_2(0)=-4+2k, \mu_2(1)=-3+2k, \mu_2(2)=-2+2k, \mu_2(3)=-1+2k, \mu_2(4)=2k, \\ & \mu_2(5)=1+2k, \mu_2(6)=2+2k, \mu_2(7)=-3, \mu_2(8)=-2, \mu_2(9)=-1, \mu_2(10)=0, \\ & \mu_2(11)=1, \mu_2(12)=2, \mu_2(13)=3, \mu_2(14)=-2-2k, \mu_2(15)=-1-2k, \\ & \mu_2(16)=-2k, \mu_2(17)=1-2k, \mu_2(18)=2-2k, \mu_2(19)=3-2k\} \end{aligned} \quad (4.1.2)$$

gibi elde edilmektedir. Elde edilen (4.1.1) ve (4.1.2) kümelerinden normları küçük olan elemanlar seçilerek oluşturulan küme aşağıdaki gibidir.

$$\begin{aligned} H_{\lambda} = \{ & \mu_1(0)=0, \mu_1(1)=1, \mu_1(2)=2, \mu_2(3)=-1+2k, \mu_2(4)=2k, \\ & \mu_2(5)=1+2k, \mu_1(6)=-2k, \mu_1(7)=-1-2k, \mu_2(8)=-2, \mu_2(9)=-1, \mu_2(10)=0, \\ & \mu_2(11)=1, \mu_2(12)=2, \mu_1(13)=-1+2k, \mu_1(14)=2k, \mu_2(15)=-1-2k, \\ & \mu_2(16)=-2k, \mu_2(17)=1-2k, \mu_2(18)=-2, \mu_2(19)=-1\} \end{aligned} \quad (4.1.3)$$

Önerilmiş λ Hurwitz tamsayısının alt kümelerini $H_{\lambda}^{(0)}$ ve $H_{\lambda}^{(1)}$ ile gösterelim. Bu kümeler aşağıdaki gibi elde edilmektedir.

$H_{(1)\lambda}$ kümesinin alt kümeleri

$$H_{(1)\lambda}^{(0)} = \{\mu_1(0)=0, \mu_1(2)=2, \mu_1(4)=-2-2k, \mu_1(6)=-2k, \mu_1(8)=2-2k, \\ \mu_1(10)=-2-4k, \mu_1(12)=-2+2k, \mu_1(14)=2k, \mu_1(16)=2+2k, \mu_1(18)=-2\} \quad (4.1.4)$$

ve

$$H_{(1)\lambda}^{(1)} = \{\mu_1(1)=1, \mu_1(3)=3, \mu_1(5)=-1-2k, \mu_1(7)=1-2k, \mu_1(9)=3-2k, \\ \mu_1(11)=-3+2k, \mu_1(13)=-1+2k, \mu_1(15)=1+2k, \mu_1(17)=-3, \mu_1(19)=-1\} \quad (4.1.5)$$

şeklindedir. $H_{(2)\lambda}$ kümesinin alt kümeleri ise

$$H_{(2)\lambda}^{(0)} = \{\mu_2(0)=-4+2k, \mu_2(2)=-2+2k, \mu_2(4)=2k, \mu_2(6)=2+2k, \mu_2(8)=-2, \\ \mu_2(10)=0, \mu_2(12)=2, \mu_2(14)=-2-2k, \mu_2(16)=-2k, \mu_2(18)=2-2k\} \quad (4.1.6)$$

ve

$$H_{(2)\lambda}^{(1)} = \{\mu_2(1)=-3+2k, \mu_2(3)=-1+2k, \mu_2(5)=1+2k, \mu_2(7)=-3, \mu_2(9)=-1, \\ \mu_2(11)=1, \mu_2(13)=3, \mu_2(15)=-1-2k, \mu_2(17)=1-2k, \mu_2(19)=3-2k\} \quad (4.1.7)$$

şeklindedir. (4.1.4) ile (4.1.6) ve (4.1.5) ile (4.1.7) kümelerinden en küçük norma sahip olan elemanların oluşturduğu kümeler önerilmiş λ Hurwitz tamsayısının $H_{\lambda}^{(0)}$ ve $H_{\lambda}^{(1)}$ ile gösterilen alt kümelerdir. Bu kümeler

$$H_{\lambda}^{(0)} = \{\mu_1(0)=0, \mu_1(2)=2, \mu_2(4)=2k, \mu_1(6)=-2k, \mu_2(8)=-2, \\ \mu_2(10)=0, \mu_2(12)=2, \mu_1(14)=2k, \mu_2(16)=-2k, \mu_2(18)=-2\} \quad (4.1.8)$$

ve

$$H_{\lambda}^{(1)} = \{\mu_1(1)=1, \mu_2(3)=-1+2k, \mu_2(5)=1+2k, \mu_1(7)=-1-2k, \mu_2(9)=-1, \\ \mu_2(11)=1, \mu_1(13)=-1+2k, \mu_2(15)=-1-2k, \mu_2(17)=1-2k, \mu_2(19)=-1\} \quad (4.1.9)$$

şeklindedir. Önerilmiş λ Hurwitz tamsayısının enerjisi $E_\lambda = \frac{1}{N(\lambda)} \cdot \sum_{z \in H_\lambda} N(z)$ formülüyle bulunmaktadır. Bu enerji hesaplanırken önerilmiş λ Hurwitz tamsayısının $H_{\lambda}^{(0)}$ altkümesi kullanılacaktır. Çünkü önerilmiş λ Hurwitz tamsayısının $H_{\lambda}^{(0)}$ altkümesi, bu kümenin eleman sayısını norm kabul eden başka bir λ_1 Hurwitz tamsayısı alınarak karşılaştırma yapılacaktır. $H_{\lambda}^{(0)}$ altkümesinin eleman sayısı aynı zamanda $N(\lambda)$ 'ya eşittir. Yani $N(\lambda)=10$ dur. $H_{\lambda}^{(0)}$

altkümesinin herbir elemanın normlarının toplamı 32 dir. Buradan $E_\lambda = \frac{32}{10} = 3,2$ olarak hesaplanmaktadır. δ_λ^2, önerilmiş λ Hurwitz tamsayısının minimum kare öklidyen uzaklığıdır. Bu uzaklık kümenin sıfırdan farklı en küçük normuna eşittir. $H_\lambda^{(0)}$ altkümesinin minimum kare öklidyen uzaklığı $\delta_\lambda^2 = 4$ tür. Önerilmiş λ Hurwitz tamsayısının CFM 'si (constellation figure of merit), M Hurwitz tamsayısının boyutu olmak üzere $CFM(\lambda) = \frac{M \cdot \delta_\lambda^2}{2 \cdot E_\lambda}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla $H_\lambda^{(0)}$ altkümesinin CFM 'si $CFM(\lambda) = \frac{4 \cdot 4}{2 \cdot (3,2)} = 2,5$ olarak hesaplanmaktadır. Önerilmiş λ Hurwitz tamsayısının $H_\lambda^{(0)}$ altkümesinin eleman sayısını norm kabul eden Hurwitz tamsayısı $\lambda_1 = 2 + 2i + 1 + k$ dır. λ_1 Hurwitz tamsayısının normu $N(\lambda_1) = 10$ dur. λ_1 Hurwitz tamsayısına sırasıyla (18) deki modulo 1 fonksiyonu uygulanırsa $H_{(1)\lambda_1}$ kümesinin elemanları

$$H_{(1)\lambda_1} = \{\mu_1(0) = 0, \mu_1(1) = 1, \mu_1(2) = 2, \mu_1(3) = -1-2k, \mu_1(4) = -2k, \\ \mu_1(5) = 1-2k, \mu_1(6) = 2k, \mu_1(7) = 1+2k, \mu_1(8) = -2, \mu_1(9) = -1\} \quad (4.1.10)$$

ve (19) daki modulo 2 fonksiyonu uygulanırsa $H_{(2)\lambda_1}$ kümesinin elemanları

$$H_{(2)\lambda_1} = \{\mu_2(0) = -3+k, \mu_2(1) = -2+k, \mu_2(2) = -1+k, \mu_2(3) = k, \mu_2(4) = 1+k, \\ \mu_2(5) = -2-k, \mu_2(6) = -1-k, \mu_2(7) = -k, \mu_2(8) = 1-k, \mu_2(9) = 2-k\} \quad (4.1.11)$$

şeklindedir. (4.1.10) ve (4.1.11) kümelerinden normu en küçük olan elemanların oluşturduğu küme

$$H_{\lambda_1} = \{\mu_1(0) = 0, \mu_1(1) = 1, \mu_2(2) = -1+k, \mu_2(3) = k, \mu_2(4) = 1+k, \\ \mu_2(5) = -2-k, \mu_2(6) = -1-k, \mu_2(7) = -k, \mu_2(8) = 1-k, \mu_1(9) = -1\} \quad (4.1.12)$$

şeklindedir. λ_1 Hurwitz tamsayısının enerjisi $E_{\lambda_1}=\frac{1}{N(\lambda_1)}\cdot\sum_{z\in H_{\lambda_1}}N(z)$ formülüyle bulunmaktadır. (4.1.12) kümesinin eleman sayısı aynı zamanda normu $N(\lambda_1)=10$ ve elemanlarının normları toplamı 17 dir. Buradan λ_1 Hurwitz tamsayısının enerjisi $E_{\lambda_1}=\frac{17}{10}=1,7$ bulunmaktadır. (4.1.12) kümesinin sıfırdan farklı en küçük elemanı yani minimum kare öklidyen uzaklığı $\delta^2_{\lambda_1}=1$ dir. λ_1 Hurwitz tamsayısının CFM 'si (constellation figure of merit), M Hurwitz tamsayısının boyutu olmak üzere $CFM(\lambda_1)=\frac{M\cdot\delta^2_{\lambda_1}}{2\cdot E_{\lambda_1}}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla H_{λ_1} kümesinin CFM 'si $CFM(\lambda_1)=\frac{4\cdot 1}{2\cdot(1,7)}=1,1765$ olarak hesaplanmaktadır. λ_1 Hurwitz tamsayısına karşılık gelen Gauss tamsayısı G_{3+i} dir. G_{3+i} Gauss tamsayısına (18) deki modulo 1 fonksiyonu uygulanırsa G_{3+i} Gauss tamsayısının kümesi

$$G_{3+i}=\{\mu(0)=0,\mu(1)=1,\mu(2)=-1-i,\mu(3)=-i,\mu(4)=1-i,\\ \mu(5)=-1-2i,\mu(6)=-1+i,\mu(7)=i,\mu(8)=1+i,\mu(9)=-1\} \quad (4.1.13)$$

şeklinde oluşmaktadır. G_{3+i} Gauss tamsayısının enerjisi $E_\lambda=\frac{1}{N(\lambda)}\cdot\sum_{z\in G_\lambda}N(z)$ formülüyle bulunmaktadır. (4.1.13) kümesinin eleman sayısı aynı zamanda normu $N(\lambda)=10$ ve elemanlarının normları toplamı 17 dir. Buradan λ_1 Hurwitz tamsayısının enerjisi $E_{\lambda_1}=\frac{17}{10}=1,7$ bulunmaktadır. (4.1.13) kümesinin sıfırdan farklı en küçük elemanı yani minimum kare öklidyen uzaklığı $\delta^2_{\lambda_1}=1$ dir. G_{3+i} Gauss tamsayısının CFM 'si (constellation figure of merit), M Gauss tamsayısının boyutu olmak üzere $CFM(\lambda)=\frac{M\cdot\delta^2_{\lambda}}{2\cdot E_{\lambda}}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla G_{3+i} kümesinin CFM 'si $CFM(\lambda)=\frac{2\cdot 1}{2\cdot(1,7)}=0.5882$ olarak hesaplanmaktadır.

Önerilmiş Hurwitz (Lipschitz) Tamsayısı	CFM Hurwitz	CFM Lipschitz	Hurwitz Tamsayısı	CFM	Lipschitz Tamsayısı	CFM	Gauss Tamsayısı	CFM
$3+3i+j+k$	$2,5$	1,1765	$2+2i+j+k$	1,1765	$2+2i+j+k$	0,6061	$3+i$	0,5883

Örnek 2: $\lambda = 4+3i+2j+k$ önerilmiş Hurwitz tamsayısı olsun. Bu önerilmiş λ Hurwitz sayısının normu $N(\lambda)=30$ dur. Önerilmiş λ Hurwitz tamsayısı herbiri 10 elemanlı 3 farklı kümeye ayrıştırılabilir. Önerilmiş λ Hurwitz tamsayısının enerjisi $E_\lambda = \frac{1}{N(\lambda)} \cdot \sum_{z \in H_\lambda} N(z)$ formülüyle bulunmaktadır. Bu enerji hesaplanırken önerilmiş λ Hurwitz tamsayısının $H_\lambda^{(0)}$ altkümesi kullanılacaktır. Çünkü önerilmiş λ Hurwitz tamsayısının $H_\lambda^{(0)}$ altkümesi, bu kümenin eleman sayısını norm kabul eden başka bir λ_1 Hurwitz tamsayısı alınarak karşılaştırma yapılacaktır. $H_\lambda^{(0)}$ altkümesinin eleman sayısı aynı zamanda $N(\lambda)$ 'ya eşittir. Yani $N(\lambda)=10$ dur. $H_\lambda^{(0)}$ altkümesinin herbir elemanın normlarının toplamı 75 dir. Buradan $E_\lambda = \frac{75}{10} = 7,5$ olarak hesaplanmaktadır. δ_λ^2, önerilmiş λ Hurwitz tamsayısının minimum kare öklidyen uzaklığıdır. Bu uzaklık kümenin sıfırdan farklı en küçük normuna eşittir. $H_\lambda^{(0)}$ altkümesinin minimum kare öklidyen uzaklığı $\delta_\lambda^2 = 6$ tür. Önerilmiş λ Hurwitz tamsayısının CFM 'si (constellation figure of merit), M Hurwitz tamsayısının boyutu olmak üzere $CFM(\lambda) = \frac{M \cdot \delta_\lambda^2}{2 \cdot E_\lambda}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla $H_\lambda^{(0)}$ altkümesinin CFM 'si $CFM(\lambda) = \frac{4 \cdot 6}{2 \cdot (7,5)} = 1,6$ olarak hesaplanmaktadır. Önerilmiş λ Hurwitz tamsayısının $H_\lambda^{(0)}$ altkümesinin eleman sayısını norm kabul eden Hurwitz tamsayısı $\lambda_1 = 2+2i+1+k$ dır. λ_1 Hurwitz tamsayısının normu $N(\lambda_1)=10$ dur. λ_1 Hurwitz tamsayısının enerjisi $E_{\lambda_1} = \frac{1}{N(\lambda_1)} \cdot \sum_{z \in H_{\lambda_1}} N(z)$ formülüyle bulunmaktadır. H_{λ_1} kümesinin

eleman sayısı aynı zamanda normu $N(\lambda_1)=10$ ve elemanlarının normları toplamı 17 dir. Buradan λ_1 Hurwitz tamsayısının enerjisi $E_{\lambda_1}=\frac{17}{10}=1,7$ bulunmaktadır. H_{λ_1} kümesinin sıfırdan farklı en küçük elemanı yani minimum kare öklidyen uzaklığı $\delta^2_{\lambda_1}=1$ dir. λ_1 Hurwitz tamsayısının CFM 'si (constellation figure of merit), M Hurwitz tamsayısının boyutu olmak üzere $CFM(\lambda_1)=\frac{M\cdot\delta^2_{\lambda_1}}{2\cdot E_{\lambda_1}}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla H_{λ_1} kümesinin CFM 'si $CFM(\lambda_1)=\frac{4\cdot 1}{2\cdot(1,7)}=1,1765$ olarak hesaplanmaktadır. λ_1 Hurwitz tamsayısına karşılık gelen Gauss tamsayısı G_{3+i} dir.

G_{3+i} Gauss tamsayısının enerjisi $E_\lambda=\frac{1}{N(\lambda)}\cdot\sum_{z\in G_\lambda}N(z)$ formülüyle bulunmaktadır. G_{3+i} kümesinin eleman sayısı aynı zamanda normu $N(\lambda)=10$ ve elemanlarının normları toplamı 17 dir. Buradan G_{3+i} Gauss tamsayısının enerjisi $E_{\lambda_1}=\frac{17}{10}=1,7$ bulunmaktadır. G_{3+i} kümesinin sıfırdan farklı en küçük elemanı yani minimum kare öklidyen uzaklığı $\delta^2_{\lambda_1}=1$ dir. G_{3+i} Gauss tamsayısının CFM 'si (constellation figure of merit), M Gauss tamsayısının boyutu olmak üzere $CFM(\lambda)=\frac{M\cdot\delta^2_{\lambda}}{2\cdot E_{\lambda}}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla G_{3+i} kümesinin CFM 'si $CFM(\lambda)=\frac{2\cdot 1}{2\cdot(1,7)}=0.5882$ olarak hesaplanmaktadır.

Önerilmiş Hurwitz (Lipschitz) Tamsayısı	CFM Hurwitz	CFM Lipschitz	Hurwitz Tamsayısı	CFM	Lipschitz Tamsayısı	CFM	Gauss Tamsayısı	CFM
$4+3i+2j+k$	$1,6$	1,8182	$2+2i+j+k$	1,1765	$2+2i+j+k$	0,6061	$3+i$	0,5883

Örnek 3: $\lambda=5+3i+2j+k$ önerilmiş Hurwitz tamsayısı olsun. Bu önerilmiş λ Hurwitz sayısının normu $N(\lambda)=39$ dur. Önerilmiş λ Hurwitz tamsayısı herbiri 13 elemanlı 3 farklı

kümeye ayrıştırılabilir. Önerilmiş λ Hurwitz tamsayısının enerjisi $E_\lambda = \frac{1}{N(\lambda)} \cdot \sum_{z \in H_\lambda} N(z)$ formülüyle bulunmaktadır. $H_\lambda^{(0)}$ altkümesinin eleman sayısı aynı zamanda $N(\lambda)$ 'ya eşittir. Yani $N(\lambda) = 13$ dur. $H_\lambda^{(0)}$ altkümesinin herbir elemanın normlarının toplamı 108 dir. Buradan $E_\lambda = \frac{108}{13} = 8,3077$ olarak hesaplanmaktadır. δ_λ^2, önerilmiş λ Hurwitz tamsayısının minimum kare öklidyen uzaklığıdır. Bu uzaklık kümenin sıfırdan farklı en küçük normuna eşittir. $H_\lambda^{(0)}$ altkümesinin minimum kare öklidyen uzaklığı $\delta_\lambda^2 = 9$ tür. Önerilmiş λ Hurwitz tamsayısının CFM 'si (constellation figure of merit), M Hurwitz tamsayısının boyutu olmak üzere $CFM(\lambda) = \frac{M \cdot \delta_\lambda^2}{2 \cdot E_\lambda}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla $H_\lambda^{(0)}$ altkümesinin CFM 'si $CFM(\lambda) = \frac{4 \cdot 9}{2 \cdot (8,3077)} = 2,1667$ olarak hesaplanmaktadır. Önerilmiş λ Hurwitz tamsayısının $H_\lambda^{(0)}$ altkümesinin eleman sayısını norm kabul eden Hurwitz tamsayısı $\lambda_1 = 2 + 2i + 2j + k$ dır. λ_1 Hurwitz tamsayısının normu $N(\lambda_1) = 13$ dur. λ_1 Hurwitz tamsayısının enerjisi $E_{\lambda_1} = \frac{1}{N(\lambda_1)} \cdot \sum_{z \in H_{\lambda_1}} N(z)$ formülüyle bulunmaktadır. H_{λ_1} kümesinin eleman sayısı aynı zamanda normu $N(\lambda_1) = 13$ ve elemanlarının normları toplamı 24 dir. Buradan λ_1 Hurwitz tamsayısının enerjisi $E_{\lambda_1} = \frac{24}{13} = 1,8462$ bulunmaktadır. H_{λ_1} kümesinin sıfırdan farklı en küçük elemanı yani minimum kare öklidyen uzaklığı $\delta_{\lambda_1}^2 = 1$ dir. λ_1 Hurwitz tamsayısının CFM 'si (constellation figure of merit), M Hurwitz tamsayısının boyutu olmak üzere $CFM(\lambda_1) = \frac{M \cdot \delta_{\lambda_1}^2}{2 \cdot E_{\lambda_1}}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla H_{λ_1} kümesinin CFM 'si $CFM(\lambda_1) = \frac{4 \cdot 1}{2 \cdot (1,8462)} = 1,0833$ olarak hesaplanmaktadır. λ_1 Hurwitz tamsayısına karşılık gelen Gauss tamsayısı G_{3+2i} dir.

G_{3+2i} Gauss tamsayısının enerjisi $E_\lambda = \frac{1}{N(\lambda)} \cdot \sum_{z \in G_\lambda} N(z)$ formülüyle bulunmaktadır. G_{3+2i} kümesinin eleman sayısı aynı zamanda normu $N(\lambda) = 13$ ve elemanlarının normları toplamı

28 dir. Buradan G_{3+2i} Gauss tamsayısının enerjisi $E_{\lambda_1}=\frac{28}{13}=2,1538$ bulunmaktadır. G_{3+2i} kümesinin sıfırdan farklı en küçük elemanı yani minimum kare öklidyen uzaklığı $\delta_{\lambda_1}^2=1$ dir. G_{3+2i} Gauss tamsayısının CFM 'si (constellation figure of merit), M Gauss tamsayısının boyutu olmak üzere $CFM(\lambda)=\frac{M\cdot\delta_\lambda^2}{2\cdot E_\lambda}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla G_{3+2i} kümesinin CFM 'si $CFM(\lambda)=\frac{2\cdot 1}{2\cdot(2,1538)}=0.4643$ olarak hesaplanmaktadır.

Önerilmiş Hurwitz (Lipschitz) Tamsayısı	CFM Hurwitz	CFM Lipschitz	Hurwitz Tamsayısı	CFM	Lipschitz Tamsayısı	CFM	Gauss Tamsayısı	CFM
$5+3i+2j+k$	2,1667	1,3929	$2+2i+2j+k$	1,0833	$2+2i+2j+k$	0,4643	$3+2i$	0,4643

Örnek 4: $\lambda=6+4i+3j+2k$ önerilmiş Hurwitz tamsayısı olsun. Bu önerilmiş λ Hurwitz sayısının normu $N(\lambda)=65$ dur. Önerilmiş λ Hurwitz tamsayısı herbiri 13 elemanlı 5 farklı kümeye ayrıştırılabilir. Önerilmiş λ Hurwitz tamsayısının enerjisi $E_\lambda=\frac{1}{N(\lambda)}\cdot\sum_{z\in H_\lambda}N(z)$ formülüyle bulunmaktadır. $H_\lambda^{(0)}$ altkümesinin eleman sayısı aynı zamanda $N(\lambda)$ 'ya eşittir. Yani $N(\lambda)=13$ dur. $H_\lambda^{(0)}$ altkümesinin herbir elemanın normlarının toplamı 180 dir. Buradan $E_\lambda=\frac{180}{13}=13,8462$ olarak hesaplanmaktadır. δ_λ^2, önerilmiş λ Hurwitz tamsayısının minimum kare öklidyen uzaklığıdır. Bu uzaklık kümenin sıfırdan farklı en küçük normuna eşittir. $H_\lambda^{(0)}$ altkümesinin minimum kare öklidyen uzaklığı $\delta_\lambda^2=15$ tür. Önerilmiş λ Hurwitz tamsayısının CFM 'si (constellation figure of merit), M Hurwitz tamsayısının boyutu olmak üzere $CFM(\lambda)=\frac{M\cdot\delta_\lambda^2}{2\cdot E_\lambda}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla $H_\lambda^{(0)}$ altkümesinin CFM 'si $CFM(\lambda)=\frac{4\cdot 15}{2\cdot(13,8462)}=2,1667$ olarak hesaplanmaktadır. Önerilmiş λ Hurwitz tamsayısının $H_\lambda^{(0)}$ altkümesinin eleman sayısını norm kabul eden Hurwitz

tamsayısı $\lambda_1 = 2 + 2i + 2j + k$ dır. λ_1 Hurwitz tamsayısının normu $N(\lambda_1) = 13$ dur. λ_1 Hurwitz tamsayısının enerjisi $E_{\lambda_1} = \frac{1}{N(\lambda_1)} \cdot \sum_{z \in H_{\lambda_1}} N(z)$ formülüyle bulunmaktadır. H_{λ_1} kümesinin eleman sayısı aynı zamanda normu $N(\lambda_1) = 13$ ve elemanlarının normları toplamı 24 dir. Buradan λ_1 Hurwitz tamsayısının enerjisi $E_{\lambda_1} = \frac{24}{13} = 1,8462$ bulunmaktadır. H_{λ_1} kümesinin sıfırdan farklı en küçük elemanı yani minimum kare öklidyen uzaklığı $\delta^2_{\lambda_1} = 1$ dir. λ_1 Hurwitz tamsayısının CFM 'si (constellation figure of merit), M Hurwitz tamsayısının boyutu olmak üzere $CFM(\lambda_1) = \frac{M \cdot \delta^2_{\lambda_1}}{2 \cdot E_{\lambda_1}}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla H_{λ_1} kümesinin CFM 'si $CFM(\lambda_1) = \frac{4 \cdot 1}{2 \cdot (1,8462)} = 1,0833$ olarak hesaplanmaktadır. λ_1 Hurwitz tamsayısına karşılık gelen Gauss tamsayısı G_{3+2i} dir.

G_{3+2i} Gauss tamsayısının enerjisi $E_{\lambda} = \frac{1}{N(\lambda)} \cdot \sum_{z \in G_{\lambda}} N(z)$ formülüyle bulunmaktadır. G_{3+2i} kümesinin eleman sayısı aynı zamanda normu $N(\lambda) = 13$ ve elemanlarının normları toplamı 28 dir. Buradan G_{3+2i} Gauss tamsayısının enerjisi $E_{\lambda_1} = \frac{28}{13} = 2,1538$ bulunmaktadır. G_{3+2i} kümesinin sıfırdan farklı en küçük elemanı yani minimum kare öklidyen uzaklığı $\delta^2_{\lambda_1} = 1$ dir. G_{3+2i} Gauss tamsayısının CFM 'si (constellation figure of merit), M Gauss tamsayısının boyutu olmak üzere $CFM(\lambda) = \frac{M \cdot \delta^2_{\lambda}}{2 \cdot E_{\lambda}}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla G_{3+2i} kümesinin CFM 'si $CFM(\lambda) = \frac{2 \cdot 1}{2 \cdot (2,1538)} = 0.4643$ olarak hesaplanmaktadır.

Önerilmiş Hurwitz (Lipschitz) Tamsayısı	CFM Hurwitz	CFM Lipschitz	Hurwitz Tamsayısı	CFM	Lipschitz Tamsayısı	CFM	Gauss Tamsayısı	CFM
$6+4i+3j+2k$	$2,1667$	1,3929	$2+2i+2j+k$	1,0833	$2+2i+2j+k$	0,4643	$3+2i$	0,4643

Örnek 5: $\lambda = \frac{13}{2} + \frac{9}{2}i + \frac{3}{2}j + \frac{1}{2}k$ önerilmiş Hurwitz tamsayısı olsun. Bu önerilmiş λ Hurwitz sayısının normu $N(\lambda) = 65$ dur. Önerilmiş λ Hurwitz tamsayısı herbiri 13 elemanlı 5 farklı kümeye ayrıştırılabilir. Önerilmiş λ Hurwitz tamsayısının enerjisi $E_\lambda = \frac{1}{N(\lambda)} \cdot \sum_{z \in H_\lambda} N(z)$ formülüyle bulunmaktadır. $H_\lambda^{(0)}$ altkümesinin eleman sayısı aynı zamanda $N(\lambda)$ 'ya eşittir. Yani $N(\lambda) = 13$ dur. $H_\lambda^{(0)}$ altkümesinin herbir elemanın normlarının toplamı 210 dir. Buradan $E_\lambda = \frac{210}{13} = 16,1538$ olarak hesaplanmaktadır. δ_λ^2, önerilmiş λ Hurwitz tamsayısının minimum kare öklidyen uzaklığıdır. Bu uzaklık kümenin sıfırdan farklı en küçük normuna eşittir. $H_\lambda^{(0)}$ altkümesinin minimum kare öklidyen uzaklığı $\delta_\lambda^2 = 10$ tür. Önerilmiş λ Hurwitz tamsayısının CFM 'si (constellation figure of merit), M Hurwitz tamsayısının boyutu olmak üzere $CFM(\lambda) = \frac{M \cdot \delta_\lambda^2}{2 \cdot E_\lambda}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla $H_\lambda^{(0)}$ altkümesinin CFM 'si $CFM(\lambda) = \frac{4 \cdot 10}{2 \cdot (16,1538)} = 1,2381$ olarak hesaplanmaktadır. Önerilmiş λ Hurwitz tamsayısının $H_\lambda^{(0)}$ altkümesinin eleman sayısını norm kabul eden Hurwitz tamsayısı $\lambda_1 = \frac{5}{2} + \frac{3}{2}i + \frac{3}{2}j + \frac{3}{2}k$ dır. λ_1 Hurwitz tamsayısının normu $N(\lambda_1) = 13$ dur. λ_1 Hurwitz tamsayısının enerjisi $E_{\lambda_1} = \frac{1}{N(\lambda_1)} \cdot \sum_{z \in H_{\lambda_1}} N(z)$ formülüyle bulunmaktadır. H_{λ_1} kümesinin eleman sayısı aynı zamanda normu $N(\lambda_1) = 13$ ve elemanlarının normları toplamı 24 dir. Buradan λ_1 Hurwitz tamsayısının enerjisi $E_{\lambda_1} = \frac{24}{13} = 1,8462$ bulunmaktadır. H_{λ_1} kümesinin sıfırdan farklı en küçük elemanı yani minimum kare öklidyen uzaklığı $\delta_{\lambda_1}^2 = 1$ dir. λ_1 Hurwitz tamsayısının CFM 'si (constellation figure of merit), M Hurwitz tamsayısının boyutu olmak üzere $CFM(\lambda_1) = \frac{M \cdot \delta_{\lambda_1}^2}{2 \cdot E_{\lambda_1}}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla H_{λ_1} kümesinin CFM 'si $CFM(\lambda_1) = \frac{4 \cdot 1}{2 \cdot (1,8462)} = 1,0833$ olarak hesaplanmaktadır. λ_1 Hurwitz tamsayısına karşılık gelen Gauss tamsayısı G_{3+2i} dir.

G_{3+2i} Gauss tamsayısının enerjisi $E_\lambda = \frac{1}{N(\lambda)} \cdot \sum_{z \in G_\lambda} N(z)$ formülüyle bulunmaktadır. G_{3+2i} kümesinin eleman sayısı aynı zamanda normu $N(\lambda) = 13$ ve elemanlarının normları toplamı 28 dir. Buradan G_{3+2i} Gauss tamsayısının enerjisi $E_{\lambda_1} = \frac{28}{13} = 2,1538$ bulunmaktadır. G_{3+2i} kümesinin sıfırdan farklı en küçük elemanı yani minimum kare öklidyen uzaklığı $\delta_{\lambda_1}^2 = 1$ dir. G_{3+2i} Gauss tamsayısının CFM 'si (constellation figure of merit), M Gauss tamsayısının boyutu olmak üzere $CFM(\lambda) = \frac{M \cdot \delta_\lambda^2}{2 \cdot E_\lambda}$ formülüyle hesaplanmaktadır. Bu formül yardımıyla G_{3+2i} kümesinin CFM 'si $CFM(\lambda) = \frac{2 \cdot 1}{2 \cdot (2,1538)} = 0.4643$ olarak hesaplanmaktadır.

Önerilmiş Hurwitz (Lipschitz) Tamsayısı	CFM Hurwitz	CFM Lipschitz	Hurwitz Tamsayısı	CFM	Lipschitz Tamsayısı	CFM	Gauss Tamsayısı	CFM
$\frac{13}{2}+\frac{9}{2}i+\frac{3}{2}j+\frac{1}{2}k$ $6+4i+3j+2k$	$1,2381$	1,3929	$\frac{5}{2}+\frac{3}{2}i+\frac{3}{2}j+\frac{3}{2}k$	1,0833	$2+2i+2j+k$	0,4643	$3+2i$	0,4643

Aşağıdaki tabloda önerilmiş Hurwitz sayıları için bölüntüler ve yeni yıldız kümelerinin kod kazancı gösterilmektedir.

$N = \lambda$ Superset in Normu
$c =$ Küme Sayısı
$d =$ Kümenin Eleman Sayısı
$E_\lambda = \frac{1}{N(\lambda)} \sum_{z \in G_\lambda} N(z)$ Enerji, Normlar Toplamının d ile bölümünden elde edilmektedir.
$CFM(\lambda) = \frac{M \delta_\lambda^2}{2E_\lambda}$ CFM, Boyut ile En Küçük Normun Çarpımının Enerjinin 2 Katına Bölünmesiyle elde edilmektedir.
$SNR = 10 \cdot \log_{10}\left(\frac{CFM\ \ddot{O}nerilmiş\ Hurwitz\ Tamsayısı}{CFM\ Hurwitz\ Tamsayısı}\right)$

Tablo 10: Hurwitz sayıları üzerinde yeni yıldız kümeleri ve yeni blok kodlar

N	c	d	λ SUPERSET	δ^2 EN KÜÇÜK NORM	NORMLAR TOPLAMI	BOYUT	ENERJİ	CFM ÖNERİLMİŞ YILDIZKÜMESİ	SNR [dB]
30	3	10	$4+3i+2j+k$	6	75	4	7,5	1,6	1.34
39	3	13	$5+3i+2j+k$	9	108	4	8,3077	2,1667	3.01
150	6	25	$10+5i+4j+3k$	18	792	4	31,68	1,1364	4.21
156	6	26	$9+7i+5j+k$	36	864	4	33,2308	2,1667	6.72
238	7	34	$11+8i+7j+2k$	21	1799	4	52,9118	0,7938	4.49
222	6	37	$11+8i+6j+k$	18	1824	4	49,2973	0,7303	2.64
350	7	50	$13+9i+8j+6k$	35	3703	4	74,06	0,9452	5.96
371	7	53	$12+11i+9j+5k$	35	4228	4	79,7736	0,8775	6.45
522	9	58	$17+14i+6j+k$	45	6417	4	110,6379	0,8135	6.42
549	9	61	$17+12i+10j+4k$	45	7164	4	117,4426	0,7663	6.36
585	9	65	$15+14i+10j+8k$	45	8064	4	124,0615	0.7254	6.85
657	9	73	$16+14i+13j+6k$	63	10512	4	144	0.875	7.72
740	10	74	$19+17i+9j+3k$	100	11520	4	155,6757	1,2847	10.3
902	11	82	$28+9i+6j+k$	66	15675	4	191,1585	0.6905	7.22
850	10	85	$20+19i+8j+5k$	50	15400	4	181,1765	0,5519	6.38
979	11	89	$29+8i+7j+5k$	77	18832	4	211,5955	0,7278	7.90
1261	13	97	$27+18i+12j+8k$	91	26000	4	268,0412	0.6790	7.89

11. SONUÇLAR

Bu projenin amacı; Lipschitz, Hurwitz ve R_2 gibi halkalar üzerinde klasik ve kuantum kodları geliştirmek olarak belirlenmişti. Bu amaç için aşağıdaki hedefler yakalanmaya çalışılmıştır.

1. Lipschitz, Hurwitz ve R_2 halkalarında klasik kodların karakterize edilmesi,
2. Bu kodların simülasyonlarının yapılması,
3. Bu kodlardan 1-hata düzeltebilen mükemmel olanlarının karakterize edilmesi,
4. Bu kodlardan yararlanılarak kuantum kodların inşa edilmesi,
5. Proje kapsamında elde edilecek kodların BPSK, QPSK ve QAM modülasyon türleri kullanılarak literatürdeki kodlarla karşılaştırılması sonucu daha elverişli kodların geliştirilmesi,
6. Bu halkalar üzerindeki kendine-dik ve kendine-ortogonal klasik kodların karakterize edilmesi,
7. Bu kodlar yardımı ile kuantum kodların inşa edilmesidi.

Bu hedeflerin tümüne erişilmiştir. Projenin amacı doğrultusunda bugüne kadar 6 makale yazılmıştır. 3 Makale ise yazım aşamasındadır. Bu makalelerden 3 tanesi çeşitli dergilerde yayınlanmıştır. Yapılan çalışmaları uluslararası platformlarda tanıtmak amacı ile 6 sempozyuma katılınmıştır. Ayrıca 4 sempozyuma gitmek için gerekli çalışmalarımız hazırdır. Bu çalışmaların tümünde TÜBİTAK desteği proje numarası ile belirtilmiştir. Proje kapsamında bir yüksek lisans öğrencisi tezini hazırlamış ve mezun durumuna gelmiştir. Ayrıca bu proje bir doktora ve iki yüksek lisans öğrencimizin bilimsel çalışması için gerekli altyapıyı sağlamıştır.

Kaynaklar

[1] Huber, K., 1994, Codes over Gaussian integers, IEEE Trans. Inform. Theory 40.

[2] Neto, T.P.de N., Interlando, J.C., Favareto, O.M., Elia, M., Palazzo, R., 2001, Lattice Constallations and Codes From Quadratic Number Fields, Transactions on Information Theory.

[3] Hamming, R.W., 1950, Error Detecting and Error Correcting Codes, Bell System Technical Journal 29.

[4] Lee, C.Y., 1958, Some properties of non-binary error correcting codes, IEEE Trans. Inform. Theory 4.

[5] Güzeltepe, M., 2013, Codes over Hurwitz integers, Discrete Mathematics.

[6] Roman, S., 1992, Coding and Information Theory , Graduate Text in Mathematics, Springer Verlag.

[7] Güzeltepe, M., 2017, On Perfect Codes Over $A_p[w]$, Journal of Applied Mathematics and Computation.

[8] Martinez, C., Beivide, R., Gabidulin, E., 2007. Perfect Codes for Metrics Induced by Circulant Graphs , IEEE Trans Inf. Theory, Vol. 53 No:9, 3042-3052.

[9] Ceyhun, Y., Çizge Kuramının Temelleri 1, ÜDK :513.83.

[10] Seker, S. E., 2015. Çizge Teorisi (Graph Theory), YBS Ansiklopedi, Vol. 2, is.2, pp. 17-29.

[11] Özen, M., Güzeltepe, M., 2011. Cyclic codes over some finite quaternion integer rings, Journal of the Franklin Institute 348 (7), 1312-1317.

[12] Martinez, C., Beivide, R., Gabidulin, E. M., 2009. Perfect Codes From Cayley Graphs Over Lipschitz Integers , IEEE Trans Inf. Theory, Vol. 55 No:8, 3552-3562.

[13] Güzeltepe, M., Heden, O., 2014. Perfect Mannheim, Lipschitz and Hurwitz weight codes, Math. Commun. 19 (2), 253-276.

[14] Güzeltepe, M., Heden O., 2016. Perfect 1-error-corecting Lipschitz weight codes, Math. Commun. 21 (1), 23-30.

[15] Güzeltepe, M., Altınel, A., 2017. Perfect 1-error-corecting Hurwitz weight codes, Math. Commun., 265-272.

[16] Coan, B., Perng, C., 2012. Factorization of Hurwitz Quaternions, International Mathematical Forum, Vol. 7, No:43, 2143-2156.

TÜBİTAK
PROJE ÖZET BİLGİ FORMU

Proje Yürütücüsü:	Doç. Dr. MURAT GÜZELTEPE
Proje No:	116F318
Proje Başlığı:	Çeşitli Halkalar Üzerinde Klasik Kodların Ve Stabilizer Kuantum Kodların Geliştirilmesi
Proje Türü:	3001 - Başlangıç AR-GE
Proje Süresi:	24
Araştırmacılar:	MUSTAFA ERÖZ, GÖKÇEN ÇETİNEL, NÜKHET SAZAK
Danışmanlar:	
Projenin Yürütüldüğü Kuruluş ve Adresi:	SAKARYA Ü. FEN-EDEBİYAT F. MATEMATİK B.
Projenin Başlangıç ve Bitiş Tarihleri:	01/04/2017 - 01/04/2019
Onaylanan Bütçe:	101200.0
Harcanan Bütçe:	62422.39
Öz:	Bu projenin amacı; Lipschitz, Hurwitz gibi çeşitli halkalar üzerinde bant genişliği, veri aktarım hızı ve ortalama enerji tüketimi bakımından daha elverişli klasik kodların üretilmesi, bu kodların simülasyonlarının yapılması, bu kodlardan 1-hata düzeltebilen mükemmel olanlarının karakterize edilmesi ve bu kodlardan yararlanılarak kuantum kodların inşa edilmesidir. Bu proje kapsamında elde edilecek kodlar literatürdeki kodlarla karşılaştırılacaktır. Bu amaçla karşılaştırmalar BPSK (Binary Phase Shift Keying-İkili Faz Kaydırmalı Anahtarlama), QPSK (Quadrature Phase Shift Keying-Dördül Faz Kaydırmalı Anahtarlama) ve QAM (Quadrature Amplitude Modulation-Dördül Genlik Modülasyonu) kullanılarak yapılacaktır. Bu proje kapsamında elde edilecek kodlar ile literatürdeki kodların minimum enerji açısından karşılaştırılması için hata olasılığı-SNR (bir iletim sırasında sinyal gürültü oranı) grafikleri kullanılacaktır. Proje kapsamında elde edilecek kodların, literatürdeki kodlar ile bahsedilen modülasyon türleri açısından kıyaslandığında daha iyi olması hedeflenmektedir. Ayrıca proje kapsamında kuantum kodlar da çalışılacaktır. Bilindiği gibi kendine-dik (self-dual) kodlar ve kendine-ortogonal (self-orthogonal) klasik kodlar kullanılarak kuantum kod elde edilmektedir. Klasik kodlar için klasik devreler ve mantık kapıları olduğu gibi kuantum kodlar için de kuantum devre ve kuantum mantık kapıları vardır. Devreler mantık kapıları kullanılarak elde edilmektedir. Kuantum mantık kapıları Pauli spin matrisleri kullanılarak tanımlanır. Proje kapsamında kullanılacak halkalar için Pauli spin matrisleri ve Hadamard mantık kapısı gibi kuantum mantık kapıları da oluşturulacaktır. Bu mantık kapıları ile kuantum bilgi kodlanacak ve bu bilgi bir kuantum devresi kullanılarak dekodlanacaktır. Kodlama teorisi bilgi aktarımında (CD, DVD, internet?) yoğun olarak kullanılmaktadır. Kodlama teorisinin günümüzün önemli konularından biri olması, bu alandaki çalışmaların güncel olması ve hızla ilerlemesi konunun seçiminin başlıca sebebidir. Projede geliştirilecek klasik kodlar, lineer kodlar ve devirli kodlar yönünden ele alınacaktır. Lineer kodlar bir vektör uzayın alt uzayı veya bir modülün alt modülü olarak ele alınmaktadır. Devirli kodlar ise bir halkanın ideali olarak düşünülebilir. Bu projede çeşitli halkalar üzerinde sonlu modüller kullanılarak lineer kodlar elde edilecektir. Bu halkalar üzerinde polinom parçalanışları kullanılarak veya bu halkaların idealleri kullanılarak devirli kodlar oluşturulacaktır. Lineer ve devirli kod inşaları teorik olarak yapılacaktır. Diğer yandan, kendine-dik ve kendine-ortogonal klasik kodlar yardımı ile kuantum kod elde edilmektedir. Projede elde edeceğimiz lineer ve devirli kodların kendine-dik ve kendine-ortogonal olanları kuantum kod inşa etmek için incelenecektir. Ayrıca Hurwitz sayıları üzerinde kuantum kod çalışılmamış olması ve Hurwitz sayıları üzerinde 1-hata düzeltebilen mükemmel kodların karakterize edilmemiş olması da projenin bir diğer özgün yönüdür. Önerilen proje tamamlandığında, çalışılan halkalar üzerinde klasik kodlar ve kuantum kodlar geliştirilmiş olacaktır. Bu halkalar üzerinde klasik ve kuantum kodların inşa edilmesi kodlama alanında çalışan birçok akademisyenin bu halkalar üzerine odaklanmasını sağlayacaktır.

TÜBİTAK

Anahtar Kelimeler:	Kuantum kod, Hurwitz sayıları, Klasik kod, Blok kod, Kuaterniyon sayıları
Fikri Ürün Bildirim Formu Sunuldu Mu?:	Hayır
Projeden Yapılan Yayınlar:	1- On Some Perfect Codes over Hurwitz Integers (Makale - Diğer Hakemli Makale), 2- On Perfect Codes Over $A_p[w]$ (Makale - Diğer Hakemli Makale), 3- Perfect 1-error-correcting Hurwitz weight codes (Makale - İndeksli Makale), 4- Lattice constellations and codes from Lipschitz Integers (Bildiri - Uluslararası Bildiri - Sözlü Sunum), 5- Classical and quantum codes over Guzeltepe ring with respect to the Ankara Metric" (Bildiri - Uluslararası Bildiri - Sözlü Sunum), 6- Quantum codes from cyclic codes over the ring R (Bildiri - Uluslararası Bildiri - Sözlü Sunum), 7- Perfect 1-error-correcting Hurwitz weight codes (Bildiri - Uluslararası Bildiri - Sözlü Sunum), 8- Perfect Codes over Hurwitz Integers Induced by Circulant Graphs (Bildiri - Uluslararası Bildiri - Sözlü Sunum), 9- On some perfect codes over Hurwitz integers (Bildiri - Uluslararası Bildiri - Sözlü Sunum), 10- Quantum codes from cyclic codes over the ring R (Bildiri - Uluslararası Bildiri - Sözlü Sunum), 11- FEN VE MATEMATİK BİLİMLERİNDEGÜNCEL AKADEMİK ÇALIŞMALAR (Kitap - Kitapta Bölüm),

TÜBİTAK