İKİLİ OLMAYAN DİZİLERİN KORELASYON DAĞILIMLARI ÜZERİNE SONUÇLAR

ERNİST TİLENBAEV

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

EYLÜL 2013

ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Necip CAMUŞCU

Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Prof. Dr. Mustafa BAYRAKTAR

Anabilim Dalı Başkanı

ERNİST TİLENBAEV tarafından hazırlanan İKİLİ OLMAYAN DİZİLERİN KORELASYON DAĞILIMLARI ÜZERİNE SONUÇLAR adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Çetin ÜRTİŞ	Yrd. Doç. Dr. Zülfükar SAYGI
1. Tez Danışmanı	2. Tez Danışmanı

Tez Jüri Üyeleri

Başkan : Doç. Dr. Ali DOĞANAKSOY _____

Üye : Yrd. Doç. Dr. Çetin ÜRTİŞ _____

Üye : Doç. Dr. Emrah KILIÇ _____

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Ernist TİLENBAEV

Üniversitesi	:	**TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü	:	**Fen Bilimleri**
Anabilim Dalı	:	**Matematik Bölümü**
1. Tez Danışmanı	:	**Yrd. Doç. Dr. Çetin ÜRTİŞ**
2. Tez Danışmanı	:	**Yrd. Doç. Dr. Zülfükar SAYGI**
Tez Türü ve Tarihi	:	**Yüksek Lisans – Eylül 2013**

Ernist TİLENBAEV

İKİLİ OLMAYAN DİZİLERİN KORELASYON DAĞILIMLARI ÜZERİNE SONUÇLAR

ÖZET

p bir asal sayı, m bir tek tamsayı, $d = (p^m + 1)^2/2(p + 1)$ ve $0 < l < (p^m + 1)/2$ olarak verilsin. Bu çalışmada, $m(t)$ periyodu $p^{2m} - 1$ olan bir p-li m-dizi olmak üzere $m(t)$ ile desime olmuş dizi $m(dt+l)$ nin korelasyon dağılımı ele alınmıştır. [1] çalışmasında bu korelasyonun alabileceği tüm değerler verilmiştir. $p = 3$ olan ilk durumda en fazla 9 tane, $p > 3$ olan ikinci durumda en fazla 11 tane değer olabileceği belirtilmiştir. Bu çalışmada $p = 3, m \leq 5$ ve l nin tüm değerleri için korelasyon dağılım tablolarını elde ettik ve korelasyon değerlerinin en fazla 8 değer aldığını gözlemledik. [1] çalışmasında korelasyon değerlerinin 9 değerli olduğunu belirtmişlerdi. Bu durumda [1] da belirtilen $-1 + ((1 + p)/2)p^m$ adayı mevcut değildir. Ayrıca $p = 3, m = 3$ ve $l = (p^m + 1)/4$ durumu için korelasyon değerlerine bakıldığı zaman toplamda 6 tane farklı değer ortaya çıkmıştır. Bu durum [2] deki $l = 0$ durumunun çalışmasına benzer olmakla beraber dağılım tablosu tamamen farklıdır.

Anahtar Kelimeler: Diziler, Korelasyon, Otokorelasyon, İkili diziler, İkili olmayan diziler, Dağılım.

University	:	**TOBB University of Economics & Technology**
Institute	:	**Institute of Natural and Applied Sciences**
Science Programme	:	**Mathematics**
1st Supervisor	:	**Asst. Prof. Çetin ÜRTİŞ**
2nd Supervisor	:	**Asst. Prof. Zülfükar SAYGI**
Degree Awarded & Date	:	**M.Sc. – September 2013**

Ernist TİLENBAEV

SOME OBSERVATIONS ON DISTRIBUTION OF CROSS CORRELATION OF TWO NONBINARY SEQUENCES

ABSTRACT

Let p be an odd prime, m an odd integer, $d = (p^m + 1)^2/2(p + 1)$ and $0 < l < (p^m+1)/2$. In this study we have considered cross correlation distribution of p-ary m-sequence $m(t)$, with period $p^{2m}-1$, and its decimated sequences $m(dt+l)$. In [1] authors had given possible values of cross correlation, as 9 different values for the case $p = 3$ and 11 different values for the case $p > 3$. For the case $p = 3, m \leq 5$ and all possible values of l we have given complete distribution table and observed that there are 8 different values in total. Note that it was stated in [1], this distribution has at most 9 values, that is we observe that the candidate $-1 + ((1 + p)/2)p^m$ does not occur. Furthermore, for the case $p = 3, m = 3$ and $l = (p^m+1)/4$ we have observed that there are exactly 6 different values. In this case the distribution is different from the case $l = 0$.

Keywords: Sequences, Cross-correlation, Auto-correlation, Binary sequences, Non binary sequences, Distribution.

TEŞEKKÜR

Bu çalışmayı tamamlamamda ve hayatımın diğer birçok aşamasında emeği geçen tez danışmanlarım Çetin ÜRTİŞ ve Zülfükar SAYGI'ya teşekkürlerimi ve saygılarımı sunarım.

Birçok konuda yardımlarını esirgemeyen TOBB ETÜ Matematik Bölümü hocalarıma, asistan arkadaşlarıma teşekkür ederim.

Tüm öğretim hayatım boyunca maddi ve manevi manada en büyük destekçim olan aileme ve eşim Barchynai KİMSANOVA'ya teşekkürü borç bilirim.

Ayrıca yüksek lisans eğtimimdeki maddi desteklerinden dolayı TOBB ETÜ'ye teşekkür ederim.

Bu araştırmada yer alan nümerik hesaplamalar TÜBİTAK ULAKBİM, Yüksek Başarım ve Grid Hesaplama Merkezi'nde (TRUBA Kaynaklarında) gerçekleştirilmiştir.

İçindekiler

Tablo Listesi

1. ÖN BİLGİLER

Bu bölümde, sonraki bölümler için altyapı olacak bazı temel matematiksel ifadeler tanımlanmaktadır. Burada verilen tüm tanımlar, teoremler ve kullanılan notasyonlar genel haliyle verilmiştir ve [9]'den faydalanılmıştır.

1.1 İz fonksiyonu

q bir asalın pozitif kuvveti ve m pozitif bir tam sayı olmak üzere $\mathbb{F}_q$ ile q elemanlı sonlu cisim ve $\mathbb{F}_{q^m}$ ile $\mathbb{F}_q$ nun m. dereceden genişlemesi gösterilecektir.

Tanım 1. *$F = \mathbb{F}_{q^m}$ ve $K = \mathbb{F}_q$ olmak üzere F den K ya* ***iz fonksiyonu***

$$\begin{aligned} Tr_{F/K} : F &\longrightarrow K \\ x &\longmapsto x + x^q + x^{q^2} + \cdots + x^{q^{m-1}} \end{aligned}$$

olarak tanımlanır.

Örnek 2. *$K = \mathbb{F}_2$ ve $F = \mathbb{F}_8 = \mathbb{F}_2(\alpha)$, $\alpha^3 + \alpha^2 + 1 = 0$ olmak üzere*

$$Tr_{F/K}(x) = x + x^3 + x^4$$

olup F nin tüm elemanları için

$$\begin{array}{rccc} Tr_{F/K}: & F & \longrightarrow & K \\ & 0 & \longmapsto & 0 \\ & 1 & \longmapsto & 1 \\ & \alpha & \longmapsto & 1 \\ & \alpha^2 & \longmapsto & 1 \\ & \alpha+1 & \longmapsto & 0 \\ & \alpha^2+1 & \longmapsto & 0 \\ & \alpha^2+\alpha & \longmapsto & 0 \\ & \alpha^2+\alpha+1 & \longmapsto & 1 \end{array}$$

elde edilir.

Örnek 3. *$K=\mathbb{F}_4=\mathbb{F}_2(u)$, $u^2+u+1=0$ ve $F=\mathbb{F}_{16}=\mathbb{F}_4(\beta)$, $\beta^2+\beta+u=0$ olmak üzere $Tr_{F/K}(x)=x+x^4$ olup F nin tüm elemanları için*

$$\begin{array}{rccc} Tr_{F/K}: & F & \longrightarrow & K \\ & 0 & \longmapsto & 0 \\ & 1 & \longmapsto & 0 \\ & u & \longmapsto & 0 \\ & u+1 & \longmapsto & 0 \\ & \beta & \longmapsto & 1 \\ & \beta+1 & \longmapsto & 1 \\ & \beta+u & \longmapsto & 1 \\ & \beta+u+1 & \longmapsto & 1 \\ & u\beta & \longmapsto & u \\ & u\beta+1 & \longmapsto & u \\ & u\beta+u & \longmapsto & u \\ & u\beta+u+1 & \longmapsto & u \\ & u\beta+\beta & \longmapsto & u+1 \\ & u\beta+\beta+1 & \longmapsto & u+1 \\ & u\beta+\beta+u & \longmapsto & u+1 \\ & u\beta+\beta+u+1 & \longmapsto & u+1 \end{array}$$

elde edilir.

İz fonksiyonunda değer kümesi asal cisim olursa, yani $K = \mathbb{F}_p$ olursa, iz fonksiyonuna **mutlak iz fonksiyonu** denir.

Teorem 4 (İz Fonksiyonunun Temel Özellikleri)**.** *$F = \mathbb{F}_{q^m}$ ve $K = \mathbb{F}_q$ olsun. Buna göre*

1. *Her $\alpha, \beta \in F$ için $Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$ dır.*
2. *Her $\alpha \in F$ ve $c \in K$ için $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha)$ dır.*
3. *İz dönüşümü örtendir.*
4. *Her $a \in K$ için $Tr_{F/K}(a) = ma$ dır.*
5. *Her $\alpha \in F$ için $Tr_{F/K}(\alpha^{q^k}) = Tr_{F/K}(\alpha)$ dır ($k \in \mathbb{N}$).*

K bir sonlu cisim ve F onun bir sonlu genişlemesi olsun, ikisi de K üzerinde vektör uzaylarıdır. Bu teoremde verilen ilk iki özellik de $Tr_{F/K}$ nın F den K ya bir lineer dönüşüm olduğunu söyler. Hatta F den K ya tüm lineer dönüşümler iz fonksiyonu kullanılarak inşa edilebilir. Bu sayede, ileride toplamsal karakterler olarak isimlendirilecek yapılar incelenirken belirli bir karakterizasyon elde edilebilecektir.

Teorem 5. *K bir sonlu cisim ve F onun sonlu bir genişlemesi olsun. Her $\alpha \in F$ için $\beta \in F$ olmak üzere $L_\beta(\alpha) = Tr_{F/K}(\beta\alpha)$ şeklinde tanımlanan fonksiyonlar lineer dönüşümlerdir ve F den K ya tüm lineer dönüşümler bu şekilde elde edilir. Ayrıca $\alpha \neq \beta$ iken $L_\alpha \neq L_\beta$ olur.*

1.2 Karakterler

G değişmeli bir grup ve $U = \{z \in \mathbb{C} : |z| = 1\}$ olsun. U çarpma işlemine göre bir gruptur. χ, G den U ya tanımlanan bir grup homomorfizması (yani her $g, h \in G$ için $\chi(gh) = \chi(g)\chi(h)$) ise χ fonksiyonuna G **nin karakteri** denir.

Örnek 6. *$G = \mathbb{Z}_2 \times \mathbb{Z}_2$ olmak üzere*

$$\begin{array}{rccc} \chi: & G & \longrightarrow & U \\ & (0,0) & \longmapsto & 1 \\ & (0,1) & \longmapsto & -1 \\ & (1,0) & \longmapsto & -1 \\ & (1,1) & \longmapsto & 1 \end{array}$$

şeklinde tanımlanan χ dönüşümü bir karakterdir.

Örnek 7. *$G = \mathbb{Z}_6$ olmak üzere $\chi(k) = e^{2\pi ik/3}$ dönüşümü bir karakterdir.*

Örnek 8. *Bir önceki örnek genelleştirilebilir. G bir sonlu devirli grup, yani $n \in \mathbb{Z}^+$ olmak üzere $G = \mathbb{Z}_n$ olsun. G üzerinde $\chi_j(k) = e^{2\pi ijk/n}$ şeklinde tanımlanan χ_j dönüşümleri birer karakterdir ve $\mathbb{Z}_n$ üzerinde tanımlanan tüm karakterler bu şekildedir.*

Her $g \in G$ için $\chi(g) = 1$ olan karaktere **aşikar karakter** denir ve özel olarak χ_0 ile gösterilir. χ, G nin bir karakteri olmak üzere $\overline{\chi}$ karakteri $\overline{\chi}(g) = \overline{\chi(g)}$ şeklinde tanımlanırsa, bu $\overline{\chi}$ karakterine de χ karakterinin **eşlenik karakteri** denir. G üzerinde tanımlanan tüm karakterlerin kümesi $G\hat{}$ ile gösterilip $G\hat{}$ üzerinde $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$ olacak şekilde bir çarpma işlemi tanımlanır ise $G\hat{}$ bu işleme göre bir grup oluşturur, bu grubun birim elemanı aşikar karakter ve χ karakterinin tersi de χ in eşlenik karakteridir. Ayrıca $|G\hat{}| = |G|$ dir.

Teorem 9. *G bir sonlu değişmeli grup olsun. χ onun üzerinde aşikar olmayan bir karakter ise*

$$\sum_{g \in G} \chi(g) = 0$$

olur. $g \in G$ birim elemandan farklı bir eleman ise

$$\sum_{\chi \in G\hat{}} \chi(g) = 0$$

olur.

Teorem 10 (Karakterlerde Ortogonallik Bağıntıları)**.** *$\chi, \psi \in G\hat{}$ olmak üzere*

$$\tfrac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)} = \begin{cases} 0, & \chi \neq \psi \\ 1, & \chi = \psi \end{cases}$$

ve $g, h \in G$ olmak üzere

$$\frac{1}{|G|}\sum_{\chi\in\hat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} 0, & g \neq h \\ 1, & g = h \end{cases}$$

olur.

Sonlu cisimlerde iki tane grup vardır, biri toplama işlemine göre grup diğeri ise çarpımsal grup. Dolayısıyla bir sonlu cisimden iki tür karakter tanımlanabilir. Bu karakterler de üzerinde tanımlandıkları gruba göre **toplamsal karakter** ve **çarpımsal karakter** diye adlandırılır.

Tr ile $\mathbb{F}_q$ sonlu cisminden tanımlanan mutlak iz fonksiyonu belirtilirse, $\mathbb{F}_q$ üzerinde tanımlanan $\chi_1(x) = e^{2\pi i Tr(x)/p}$ fonksiyonu bir toplamsal karakter olur ve **kanonik toplamsal karakter** ismini alır. Bu karakter yardımıyla Teorem 11 da olduğu gibi tüm toplamsal karakterler inşa edilebilir.

Teorem 11. *$b \in \mathbb{F}_q$ olmak üzere χ_b fonksiyonu $\chi_b(x) = \chi_1(bx)$ şeklinde tanımlansın. χ_b bir toplamsal karakter olur ve $\mathbb{F}_q$ üzerindeki tüm toplamsal karakterler bu yolla elde edilir.*

Örnek 12. *$\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$; $\alpha^2 + \alpha + 1 = 0$ olmak üzere $\mathbb{F}_4$ üzerinde tanımlanan tüm toplamsal karakterleri inceleyelim. Bunun için öncelikle $\mathbb{F}_4$ üzerindeki mutlak iz fonksiyonu*

$$\begin{array}{rccc} Tr_{\mathbb{F}_4/\mathbb{F}_2}: & \mathbb{F}_4 & \longrightarrow & \mathbb{F}_2 \\ & x & \longmapsto & x + x^2 \\ & 0 & \longmapsto & 0 \\ & 1 & \longmapsto & 0 \\ & \alpha & \longmapsto & 1 \\ & \alpha+1 & \longmapsto & 1 \end{array}$$

şeklinde bulunur. $\chi_1(x) = e^{2\pi i Tr(x)/2}$ olduğundan

$$\begin{array}{rccc} \chi_1: & (\mathbb{F}_4, +) & \longrightarrow & \mathbb{U} \\ & 0 & \longmapsto & 1 \\ & 1 & \longmapsto & 1 \\ & \alpha & \longmapsto & -1 \\ & \alpha+1 & \longmapsto & -1 \end{array}$$

elde edilir, diğer karakterler Teorem 11 kullanılarak hesaplanırsa

$(\mathbb{F}_4,+)$	$\xrightarrow{\chi_0}$	$\mathbb{U}$	$(\mathbb{F}_4,+)$	$\xrightarrow{\chi_\alpha}$	$\mathbb{U}$	$(\mathbb{F}_4,+)$	$\xrightarrow{\chi_{\alpha+1}}$	$\mathbb{U}$
0	$\longmapsto$	1	0	$\longmapsto$	1	0	$\longmapsto$	1
1	$\longmapsto$	1	1	$\longmapsto$	-1	1	$\longmapsto$	-1
α	$\longmapsto$	1	α	$\longmapsto$	-1	α	$\longmapsto$	1
$\alpha+1$	$\longmapsto$	1	$\alpha+1$	$\longmapsto$	1	$\alpha+1$	$\longmapsto$	-1

olacak şekilde elde edilir. Bu dört karakter dışında toplamsal karakter yoktur.

Çarpımsal karakterler ise $\mathbb{F}_q^*$ üzerinden tanımlanacaktır, $\mathbb{F}_q^*$ devirli olduğu için Teorem 13 elde edilir.

Teorem 13. *g, $\mathbb{F}_q$ nun sabit bir ilkel elemanı olsun. Her bir $j = 0, 1, 2, ..., q-2$ için $\psi_j(g^k) = e^{2\pi ijk/(q-1)}$ şeklinde tanımlanan ψ_j fonksiyonları birer çarpımsal karakterdir ve $\mathbb{F}_q^*$ üzerinde tanımlanan tüm karakterler bu şekilde elde edilir.*

Örnek 14. *$\mathbb{F}_7^*$ üzerinde $g = 3$ üreteci dikkate alınırsa, tüm çarpımsal karakterler $j = 0, 1, ..., 6$ olmak üzere $\psi_j(3^k) = e^{2\pi ijk/6}$ şeklinde inşa edilir. Buna göre $\mathbb{F}_7$ de $6 = g^3 = 3^3 \ (mod\ 7)$ olmak üzere $\psi_4(6) = e^{12\pi i/3} = 1$ olur.*

Örnek 15. *q tek olmak üzere $\mathbb{F}_q$ nun $\psi_{(q-1)/2}$ çarpımsal karakterine kuadratik (quadratic) karakter denir. Bu karakter $q = p$ için sayılar teorisindeki Legendre sembolüne denk olur.*

2. GİRİŞ

2.1 Diziler ve Özellikleri

2.1.1 Uygulama Alanları

Modern iletişim sistemlerinde *iyi korelasyona* sahip dizilerin bir çok uygulama alanı mevcuttur. Bunlardan bazıları sinyal senkronizasyonu, navigasyon, radarlar, rasgele sayı üretici, kriptografi ve çoklu-erişmeli iletişim sistemlerinde sinyal belirlemedir.

Kod Bölmeli Çoklu Erişim (Code-division multiple-access, CDMA) sistemlerinde birden fazla kullanıcı aynı kanal üzerinden iletişim kurarlar. Kullanıcılardan gelen sinyalleri ayırt etmek için her kullanıcıya birer imza dizi atanır. Böyle bir sistemde kullanıcıların çakışmaları en az olacak şekilde imza dizileri belirlemek önemlidir. Günümüzde telefon ve kablosuz iletişimde adını çok duyduğumuz 2G ve 3G standartları CDMA sistemlerini kullanmaktadırlar.

Örnek verecek olursak

Örnek 16.

$$\{u(t)\} = \{1111112322111111111\}$$

alfabe kümesi veya kısaca alfabesi {1,2,3} ve uzunluğu 18 olan bir dizidir.

Örnek 17. *ω, 5 inci dereceden ilkel kök olmak üzere*

$$\{u(t)\} = \{1111\omega^2\omega^4\omega^4\omega^3\omega^3\omega^3\}$$

alfabesi $\{1, \omega, \omega^2, \omega^3, \omega^4\}$ olan bir dizi tanımlar. Bu dizi yerine $u(t) = \{\omega^{a(t)}\}$ olmak üzere alfabesi $\{0, 1, 2, 3, 4\}$ olan $a(t) = \{0000244333\}$ dizisi kullanılabilir.

Son örnekte olduğu gibi çoğu durumda, ayrıca bizim çalışmalarımızda da gösterim kolaylığı açısından $u(t)$ dizisi yerine $u(t) = \{\omega^{a(t)}\}$ olarak tanımlanan $a(t)$ dizisi ele alınacaktır.

Tanım 18. *Alfabesi $\mathbb{F}_p$ den olan diziye p-li dizi denir.*

Tanım 19. *$u(t)$ bir dizi olmak üzere her t için*

$$u(t+n) = u(t)$$

olacak şekilde en küçük n pozitif tam sayısına $u(t)$ dizisinin periyodu denir.

Not 20. *Periyodu n olan sonsuz uzunluklu bir dizi için $(u_1u_2...u_n)^\infty$ gösterimini veya $(u_1u_2...u_n)$ gösterimini kullanacağız.*

2.1.2 M-dizileri

Uygulamada ve matematiksel hesap yaparken diğer dizilere göre daha kullanışlı olması açısından maksimal uzunluklu diziler veya matematiksel yazılımı ile m-dizileri çok yaygın kullanılmaktadır ve birçok araştırmacı tarafından çalışılmıştır. Bu kısımda m-dizilerinin tanımı ve özelliklerini verelim.

Tanım 21. *q bir asalın pozitif kuvveti olmak üzere uzunluğu $q^m - 1$ ve alfabesi $\mathbb{F}_q$ olan periyodik diziye maksimal uzunluklu dizi (m-dizisi) denir.*

p-li m-dizilerinin uygulamalarda çok kullanılmasının bir sebebi aşağıdaki lemmada vereceğimiz denklik sayesinde dizilerin korelasyon ve korelasyon dağılımlarının hesabında kolaylık sağlamasıdır.

Lemma 22. *$m(t)$ dizisi periyodu $p^n - 1$ olan bir p-li m-dizisi olsun. α, $\mathbb{F}_{p^n}$ nin bir ilkel elemanı olmak üzere $m(t)$ dizisi aşağıdaki şekilde ifade edilebilir*

$$m(t) = Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}\left(\alpha^t\right)$$

olarak ifade edilebilir.

2.1.3 Desimasyon İle Elde Edilmiş Diziler

p-li m-dizilerinin iz dönüşümü ile tanımını göz önünde bulundurarak bir dizinin alt dizilerine bakacağız. Bunlara literatürdeki ismi ile desimasyon (decimation) diyeceğiz.

Tanım 23. *$m(t)$ herhangi bir periyodik dizi ve $d \in \mathbb{Z}^+$ olmak üzere $m(dt)$ dizisine desimasyon ile elde edilmiş dizi denir. Burada $m(t)$ dizisinin elemanları d atlayarak alınmaktadır ve yine periyodik bir dizi elde edilir.*

Örnek 24. $\{m(t)\} = \{1,2,3,4,5,6,7,8,9\}$ *olsun bu durumda* $\{m(3t)\} = \{1,4,7\}$ *olur.*

Burada dikkat etmemiz gereken dizinin uzunluğu ile desimasyon sayısının *obeb*'idir. Örnek ile bakacak olursak.

Örnek 25. $\{m(t)\} = (1,2,3,4,5,6,7)^\infty$ *olsun bu durumda*

$$\{m(3t)\} = (1,4,7,3,6,2,5)^\infty$$

olur.

Son örnekte dizinin periyodu 7 ve desimasyon katsayımız 3 olup bu iki sayı aralarında asal oldukları için desimasyon dizisinin periyodu da 7 elde edildi.

Örnek 26. $\{u(t)\} = (012001111200121)^\infty$ *alfabesi* $\mathbb{F}_3 = \{0,1,2\}$ *ve periyodu* 15 *olan bir dizi olsun. Bu durumda* $\{u(3t)\} = (00121)^\infty$ *periyodu 5 olan bir dizidir,* $\{u(5t)\} = (010)^\infty$ *ise periyodu 3 olan bir dizidir ve* $\{u(2t)\} = (020110111011202)^\infty$ *de periyodu 15 olan bir dizidir.*

Bazı durumlarda $m(t)$ dizisinin desimasyonlarında başlangıç değerini farklı elde edebilmek için başlangıç noktası l kadar kaydırılabilir.

Örnek 27. $\{m(t)\} = \{1,2,3,4,5,6,7,8,9\}$ *olsun bu durumda* $\{m(3t+1)\} = \{2,5,8\}$ *olur.*

Örnek 28. $\{u(t)\} = (012001111200121)^{\infty}$ *alfabesi* $\mathbb{F}_3 = \{0,1,2\}$ *ve periyodu* 15 *olan bir dizi olsun. Bu durumda* $\{u(3t+1)\} = (10102)^{\infty}$ *periyodu 5 olan bir dizidir,* $\{u(5t+2)\} = (211^{\infty}$ *ise periyodu 3 olan bir dizidir ve* $\{u(2t+1)\} = (101120202011011)^{\infty}$ *de periyodu 15 olan bir dizidir.*

Not 29. $m(dt)$ *desime edilmiş dizisinin periyodu* $\frac{n}{obeb(n,d)}$ *dir. Benzer şekilde* $l \in \mathbb{Z}^+$ *için* $m(dt+l)$ *desime edilmiş dizisinin periyodu da* $m(dt)$ *ile aynıdır.*

3. KORELASYON DAĞILIMI

3.1 Korelasyon Tanımı ve Temel Teknikler

Özel olarak belirtilmedikçe bu bölümden itibaren aşağıdaki notasyonlar kullanılacaktır.

- p bir tek asal sayı olsun.
- m tek tam sayı, $n = 2m$ ve $d = \dfrac{(p^m+1)^2}{2(p+1)}$ olsun.
- $\mathbb{F}_{p^n}$ mertebesi p^n olan sonlu cisim olsun.
- $\mathbb{F}_{p^n}$ cisminin bir ilkel elemanı α olsun.
- $j \mid i$ olmak üzere $\mathrm{Tr}_{\mathbb{F}_{p^i}/\mathbb{F}_{p^j}} : \mathbb{F}_{p^i} \to \mathbb{F}_{p^j}$ dönüşümü bir iz dönüşümü tanımlar.
- $\omega = \exp\left(2\pi\sqrt{-1}/p\right)$ birimin $p-$inci ilkel kökü olsun.
- $x \in \mathbb{F}_{p^n}$ için $\chi(x) = \omega^{\mathrm{Tr}_{p^n/p}(x)}$ toplamsal karakter olsun.

Tanım 30. *(a_t) ve (b_t) periyodları $p^n - 1$ olan p-li diziler olsun. $0 \le \tau < p^n - 1$ olmak üzere bu iki dizi arasındaki τ kaydırmalı çapraz korelasyon*

$$C_{a,b}(\tau) = \sum_{t=0}^{p^n-2} \omega^{a_{t+\tau} - b_t}$$

olarak tanımlanır.

Lemma 31. *[9]* $f \mid p^m+1$ *ve* $a \in \mathbb{F}_{p^n}^*$ *olmak üzere*

$$\sum_{x\in\mathbb{F}_{p^n}} \omega^{Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(ax^f)} = \begin{cases} (f-1)\,p^m, j\in\mathbb{Z} \text{ olmak üzere } a=\alpha^{h+jf} \text{ ise} \\ -p^m, \text{ diğer türlü} \end{cases}$$

olur. Buradaki h *değeri*

$$h = \begin{cases} 0, & \text{eğer } (p^m+1)/f \text{ çift ise} \\ \frac{f}{2}, & \text{eğer } (p^m+1)/f \text{ tek ise} \end{cases}$$

olarak tanımlıdır.

Önerme 32. *[2]* $n=2m$ *ve* $d=\dfrac{(p^m+1)^2}{2(p+1)}$ *olmak üzere*

- $obeb\,(p^n-1,d)=\dfrac{p^m+1}{2}$
- $d\,(p^{m+1}+1)\equiv p^m+1 \pmod{p^n-1}$

eşitlikleri sağlanır.

Not 33. *Önermedeki ikinci eşitliğin doğruluğunu* $\dfrac{p\,(p^m+1)+p+1}{p+1}$ *sayısının çift olduğunu göz önünde bulundurarak* $d\,(p^{m+1}+1)=(p^n-1)\dfrac{p\,(p^m+1)+p+1}{p+1}+p^m+1)$ *denkliğini ele alarak görebiliriz.*

$m(t)$ bir p-li m-dizisi ve $m(dt+l)$ desime edilmiş dizisi olsun. Bu durumda Lemma 22 deki eşitliği kullanarak

$$\begin{aligned} C_l(\tau) &= \sum_{t=0}^{p^n-2} \omega^{m(t+\tau)-m(dt+l)} \\ &= \sum_{t=0}^{p^n-2} \omega^{\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}\left(\alpha^{t+\tau}-\alpha^{dt+l}\right)} \\ &= \sum_{x\in\mathbb{F}_q^*} \omega^{\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}\left(ax-bx^d\right)} \qquad (a=\alpha^\tau, b=\alpha^l) \\ &= \sum_{x\in\mathbb{F}_{p^n}^*} \chi\left(ax-bx^d\right) \\ &= C(a,b)-1 \end{aligned} \tag{3.1.1}$$

eşitliğini elde ederiz.

Not 34. *(3.1.1) eşitliğindeki* $C(a,b) = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(ax - bx^d\right)$ *fonksiyonu ile* $C_l(\tau)$ *fonksiyonunun değerlerinin dağılımları aynıdır. Dolayısıyla bundan sonra* $C(a,b)$ *fonksiyonunu ele alacağız.*

Şimdi Not 34 de geçen $C(a,b)$ korelasyon fonksiyonunun alabileceği değerleri bulmak için gerekli tanım ve teoremleri verelim.

$C(a,b)$ toplamını biraz da açacak olursak

$$\begin{aligned} 2C(a,b) &= 2\sum_{x\in\mathbb{F}_{p^n}} \chi\left(ax - bx^d\right) \\ &= \sum_{x\in\mathbb{F}_{p^n}} \chi\left(ax^{p^{m+1}+1} - bx^{p^m+1}\right) + \sum_{x\in\mathbb{F}_{p^n}} \chi\left(arx^{p^{m+1}+1} - br^d x^{p^m+1}\right) \\ &= T(a,b) + T\left(ar, br^d\right) \end{aligned} \tag{3.1.2}$$

elde ederiz.

Not 35. *(3.1.2) eşitliğindeki* $T(a,b) = \sum_{x\in\mathbb{F}_{p^n}} \chi\left(ax^{p^{m+1}+1} - bx^{p^m+1}\right)$ *fonksiyonu ileride moment toplamlarında kullanılacaktır.*

Örnek 15 de de bahsettiğimiz gibi $\mathbb{F}_{p^n}$ nin kuadratik karakteri aşağıdaki gibi tanımlanır.

Tanım 36.

$$\eta(x) = \begin{cases} 1, \text{ eğer } x \in \mathbb{F}_{p^n} \text{ sıfırdan farklı kuadratik eleman ise,} \\ -1, \text{ eğer } x \notin \mathbb{F}_{p^n} \text{ kuadratik eleman değil ise,} \\ 0, \text{ eğer } x = 0 \text{ ise.} \end{cases}$$

Bu tanımın yardımı ile ileride kullanacağımız, literatürde Gauss Toplamı olarak da bilinen sonucu vereceğiz.

Teorem 37. *p bir asal ve* η, $\mathbb{F}_p$ *nin bir kuadratik karakteri olmak üzere*

$$\sum_{i=1}^{p-1} \eta(i)\omega^i = \begin{cases} p^{\frac{1}{2}}, \text{ eğer } p \equiv 1 \pmod 4 \text{ ise} \\ jp^{\frac{1}{2}}, \text{ eğer } p \equiv 3 \pmod 4 \text{ ise} \end{cases}$$

dir. Burada ω *birimin* p *inci ilkel kökü ve* $j = \sqrt{-1}$ *dir.*

3.1.1 Kuadratik Form

Korelasyon hesaplamada kullanılan tekniklerin bazıları kuadratik formlara dayanmaktadır ve bizim çalışmalarımızda da kuadratik formlara yer verilmiştir.

Tanım 38. *$\mathbb{F}_p[x_1, x_2, ..., x_n]$ deki ikinci dereceden homojen polinoma $\mathbb{F}_p$ üzerinde n değişkenli kuadratik form denir ve $a_{ij} \in \mathbb{F}_p$ olmak üzere*

$$f(x_1, x_2, ..., x_n) = \sum_{i,j \leq n} a_{ij} x_i x_j$$

olarak gösterilir.

$(\mathbb{F}_p)^n$ ile $\mathbb{F}_p$ üzerinde n boyutlu lineer uzayı belirtelim. $b \in \mathbb{F}_p$ olmak üzere $f(x_1, x_2, ..., x_n) = b$ kuadratik formunun çözümünü bu kuadratik formun rankı ile bağlantılıdır.

Lemma 39. *$f \in \mathbb{F}_p[x_1, x_2, ..., x_n]$ bir kuadratik form ve Z aşağıdaki gibi tanımlansın*

$$Z := \{z \in (\mathbb{F}_p)^n : f(x+z) - f(x) = 0, \forall x \in (\mathbb{F}_p)^n\}.$$

Bu durumda Z, $(\mathbb{F}_p)^n$ nin bir altuzayıdır ve f nin rankı $rank(f) = n - boyut(Z)$ şeklinde hesap edilmektedir.

Sonlu cisimlerde sonlu genişlemenin de bir lineer uzay gibi düşünürsek $\mathbb{F}_{p^n}$ de $\mathbb{F}_p$ üzerinde bir lineer uzaydır. Buradan yola çıkarak son verdiğimiz lemmayı farklı biçimde yazabiliriz.

Sonuç 40. *$\mathbb{F}_{p^n}$ den $\mathbb{F}_p$ ye tanımlanan bir kuadratik formun rankı ρ olmak üzere aşağıdaki eşitlik geçerlidir*

$$p^{n-\rho} = \#\{z \in \mathbb{F}_{p^n} : f(x+z) = f(x), \forall x \in \mathbb{F}_{p^n}\}.$$

3.1.2 Korelasyon Fonksiyon Değerleri

Teorem 41. *[1] $d = \frac{(p^m+1)^2}{2(p+1)}$ olmak üzere $C_l(\tau)$ korelasyon fonksiyonunun alabileceği değerler aşağıdaki gibidir.*

i) $p = 3$ *için toplam 9 tane farklı değer vardır ve bunlar aşağıdaki gibidir:*

$$\{-1, -1 \pm p^m, \ -1 \pm \frac{1+i\sqrt{p}}{2}p^m, \\ -1 \pm \frac{1-i\sqrt{p}}{2}p^m, -1 \pm \frac{1+p}{2}p^m\Big\}.$$

ii) $p \equiv 3 \pmod 4 \, (\neq 3)$ *için toplam 11 tane farklı değer vardır ve bunlar aşağıdaki gibidir:*

$$\Big\{-1, -1 \pm p^m, -1 \pm \frac{1+i\sqrt{p}}{2}p^m, -1 \pm \frac{1-i\sqrt{p}}{2}p^m, \\ -1 \pm \frac{1+p}{2}p^m, -1 \pm \frac{1-p}{2}p^m\Big\}.$$

iii) $p \equiv 1 \pmod 4$ *için toplam 11 tane farklı değer vardır ve bunlar aşağıdaki gibidir:*

$$\Big\{-1, -1 \pm p^m, -1 \pm \frac{1+\sqrt{p}}{2}p^m, -1 \pm \frac{1-\sqrt{p}}{2}p^m, \\ -1 \pm \frac{1+p}{2}p^m, -1 \pm \frac{1-p}{2}p^m\Big\}.$$

4. ÇALIŞMALARIMIZ

4.1 Problem Tanımı

p bir tek asal sayı ve m tek tamsayı olmak üzere [1] çalışmalarında $m(t)$ p-li m-dizisi ile $m(dt + l)$ dizilerinin korelasyonunun alabileceği tüm değerleri ele almışlardır. [2] çalışmasında ise $l = 0$ durumu için korelasyon dağılımını vermişlerdir.

Bizim çalımamızda ise [2]'nun çalışmasını bir adım daha ilerleterek $l \neq 0$ durumları için problemi ele aldık. Nümerik hesaplar dışında tüm dağılımı elde etmek için gerek olan moment toplamları hesapladık.

Problem 42. *p tek asal sayı, m tek tamsayı, $0 < l < (p^m + 1)/2$ ve $d = \frac{(p^m+1)^2}{2(p+1)}$ olmak üzere $m(t)$ p-li m-dizisi ile bu dizinin desimasyonu $m(dt+l)$ nin korelasyon dağılımı nedir?*

4.2 Moment Toplamları

Not 34 ve Not 35 de verdiğimiz gibi moment toplamlarında kullanacağımız fonksiyonların tanımını verelim.

Tanım 43. *p bir asal, m tek tam sayı, $n = 2m$ ve $a, b \in \mathbb{F}_{p^n}^*$ olmak üzere $C(a, b)$*

ve $T(a,b)$ *fonksiyonları*

$$C(a,b) = \sum_{x \in \mathbb{F}_{p^n}} \chi\left(ax - bx^d\right)$$

ve

$$T(a,b) = \sum_{x \in \mathbb{F}_{p^n}} \chi\left(ax^{p^m+1+1} - bx^{p^m+1}\right)$$

şeklinde tanımlanır.

[1], [2] ve [3]'deki gibi özellikleri ve teknikleri kullanarak aşağıdaki moment toplamları elde edilebilir. Bu eşitlikler korelasyon dağılımını hesaplamak için gereklidir.

Lemma 44. *p bir asal, m tek tam sayı,* $n = 2m$ *ve* $b \in \mathbb{F}_{p^n}^*$ *olmak üzere aşağıdaki eşitlikler sağlanır:*

i) $\sum_{a \in \mathbb{F}_{p^n}} C(a,b) = p^n.$

ii) $N = \begin{cases} \frac{(p^n - p^m)}{2}, j \in \mathbb{Z} \text{ için } -2b = \alpha^{\frac{p^m+1}{2}j} \text{ ise} \\ -p^m, \text{ diğer türlü} \end{cases}$

olmak üzere

$$\sum_{a \in \mathbb{F}_{p^n}} C^2(a,b) = \begin{cases} p^n N, \text{ eğer } p \equiv 3 \pmod 4 \text{ ise} \\ p^{2n}, \text{ eğer } p \equiv 1 \pmod 4 \text{ ise} \end{cases}$$

dir.

iii) $\sum_{a \in \mathbb{F}_{p^n}} T(a,b) = q.$

iv) $N_2 = \begin{cases} p^n, \ j \in \mathbb{Z} \text{ için } -2b = \alpha^{\frac{p^m+1}{2}+j(p^m+1)} \text{ ise} \\ -p^m, \text{ diğer türlü} \end{cases}$

olmak üzere

$$\sum_{a \in \mathbb{F}_{p^n}} T^2(a,b) = \begin{cases} p^{2n}, & \text{eğer } p \equiv 1 \pmod 4 \\ p^n N_2 & \text{eğer } p \equiv 3 \pmod 4 \end{cases}$$

dir.

İspat:

i) Teorem 9 i kullanarak $\sum_{a\in\mathbb{F}_{p^n}} \chi(ax) = \begin{cases} p^n, & x=0 \text{ iken} \\ 0, & x\neq 0 \text{ iken} \end{cases}$ elde ederiz. Bu eşitliği kullanarak,

$$\begin{aligned}\sum_{a\in\mathbb{F}_{p^n}} C(a,b) &= \sum_{a\in\mathbb{F}_{p^n}} \sum_{x\in\mathbb{F}_{p^n}} \chi\left(ax-bx^d\right) \\ &= \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-bx^d\right) \sum_{a\in\mathbb{F}_{p^n}} \chi(ax) \\ &= p^n\end{aligned}$$

elde ederiz.

ii) Önerme 32 teki özellik gereği $p\equiv 1 \pmod 4$ iken d tek ve $p\equiv 3 \pmod 4$ iken d çift olduğunu göz önünde bulundurarak

$$\begin{aligned}\sum_{a\in\mathbb{F}_{p^n}} C^2(a,b) &= \sum_{a\in\mathbb{F}_{p^n}} \sum_{x\in\mathbb{F}_{p^n}} \chi\left(ax-bx^d\right) \sum_{y\in\mathbb{F}_{p^n}} \chi\left(ay-by^d\right) \\ &= \sum_{x,y\in\mathbb{F}_{p^n}} \chi\left(-b\left(x^d+y^d\right)\right) \sum_{a\in\mathbb{F}_{p^n}} \chi\left(a(x+y)\right) \qquad (4.2.1) \\ &= p^n \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-b\left(x^d+(-x)^d\right)\right) \qquad (4.2.2) \\ &= \begin{cases} p^{2n}, & p\equiv 1 \pmod 4 \text{ iken} \\ p^n N & p\equiv 3 \pmod 4 \text{ iken} \end{cases}\end{aligned}$$

elde ederiz. Burada r karesel olmayan eleman olmak üzere

$$\begin{aligned}N &= \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^d\right) \\ &= \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^{\frac{p^m+1}{2}}\right) \\ &= \frac{1}{2}\sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^{p^m+1}\right) + \frac{1}{2}\sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2br^{\frac{p^m+1}{2}}x^{p^m+1}\right) \\ &= \begin{cases} \frac{1}{2}\left(p^n-p^m\right), & j\in\mathbb{Z} \text{ için } -2b=\alpha^{\frac{p^m+1}{2}j} \text{ ise} \\ -p^m, & \text{diğer türlü} \end{cases}\end{aligned}$$

eşitliğini sağlar. Ayrıca (4.2.1) eşitliğinden (4.2.2) eşitliğine geçiş sırasında karakter toplamlarındaki Teorem 9 kullanılarak

$$\sum_{a\in\mathbb{F}_{p^n}} \chi\left(a\left(x+y\right)\right) = \begin{cases} p^n,\ x+y=0 \text{ iken} \\ 0,\ x+y\neq 0 \text{ iken} \end{cases}$$

elde edilmiştir.

iii) Teorem 9 karakter toplamları özelliği gereği

$$\begin{aligned} \sum_{a\in\mathbb{F}_{p^n}} T\left(a,b\right) &= \sum_{a\in\mathbb{F}_{p^n}} \sum_{x\in\mathbb{F}_{p^n}} \chi\left(ax^{p^{m+1}+1} - bx^{p^m+1}\right) \\ &= \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-bx^{p^m+1}\right) \sum_{a\in\mathbb{F}_{p^n}} \chi\left(ax^{p^{m+1}+1}\right) \\ &= p^n \end{aligned}$$

olarak elde edilir. Son adımda $\sum\limits_{a\in\mathbb{F}_{p^n}} \chi\left(ax^{p^{m+1}+1}\right)$ toplamının $x=0$ için p^n ye ve $x\neq 0$ için sıfıra eşit olduğunu kullandık.

iv) Lemma 31 gereği

$$\begin{aligned} N_2 &= \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-2bx^{p^m+1}\right) \\ &= \begin{cases} p^n,\ j\in\mathbb{Z} \text{ için } -2b = \alpha^{\frac{p^m+1}{2}+j(p^m+1)} \text{ ise} \\ -p^m,\ \text{diğer türlü} \end{cases} \end{aligned}$$

olarak elde ederiz.

Ayrıca $g(x,y) = x^{p^{m+1}+1} + y^{p^{m+1}+1}$ olmak üzere

$$\begin{aligned}
\sum_{a\in\mathbb{F}_{p^n}} T^2(a,b) &= \sum_{a,x,y\in\mathbb{F}_{p^n}} \chi\left(a\cdot g(x,y) - b\left(x^{p^m+1}+y^{p^m+1}\right)\right) \\
&= \sum_{x,y\in\mathbb{F}_{p^n}} \chi\left(-b\left(x^{p^m+1}+y^{p^m+1}\right)\right) \sum_{a\in\mathbb{F}_{p^n}} \chi\left(a\left(g(x,y)\right)\right) \\
&= p^n \sum_{\substack{x,y\in\mathbb{F}_{p^n},\\ g(x,y)=0}\}} \chi\left(-b\left(x^{p^m+1}+y^{p^m+1}\right)\right) \\
&= p^n \sum_{\substack{x,y\in\mathbb{F}_{p^n},\\ x^2+y^2=0}\}} \chi\left(-b\left(x^{p^m+1}+y^{p^m+1}\right)\right) \\
&= p^n \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-b\left(x^{p^m+1}+\left(-x^2\right)^{\frac{p^m+1}{2}}\right)\right) \\
&= p^n \sum_{x\in\mathbb{F}_{p^n}} \chi\left(-b\left(x^{p^m+1}+(-1)^{\frac{p^m+1}{2}}\, x^{p^m+1}\right)\right) \\
&= \begin{cases} p^{2n}, & p\equiv 1 \pmod 4 \text{ iken} \\ p^n N_2, & p\equiv 3 \pmod 4 \text{ iken} \end{cases}
\end{aligned}$$

eşitliğini elde ederiz. ■

4.3 Deneysel Sonuçlar

Bu kısımda nümerik hesaplara ve bu hesaplardan yola çıkarak elde ettiğimiz sonuçlara yer verilmiştir. Tüm hesaplamalar SAGE programını kullanarak TÜBİTAK Grid Hesaplama bilgisayarlarında yapılmıştır. Bu kodlardan bazıları Ekler kısmında bulunmaktadır.

Aşağıdaki örneklerde $m(t)$ ile $m(dt+l)$ dizilerinin korelasyon dağılımı hesaplanmıştır ve l sabit olmak üzere τ değiştikçe bu değerlerin kaç defa tekrarlandığı $\#C_l(\tau)$ ile gösterilmiştir.

$l = 0$ durumu [2] de çalışılmıştır ve $C_l(\tau)$ fonksiyonunun dağılımının tamamı hesaplanmıştır. $l > 0$ durumu ise bu çalışmada ele alınmıştır.

Not 45. *Aşağıda vereceğimiz örneklerde satır ve sütunların açıklaması Tablo*

4.1 daki gibidir. Tabloda görüldüğü gibi l sabit iken τ değiştikçe $C_l(\tau)$ değerinin kaç defa tekrar ettiği hesaplanmıştır ve aynı dağılıma sahip olan l değerleri tek sütunda verilmiştir.

Tablo 4.1: örneklerin açıklaması

	$l = l_0$	$l = l_1, l_2$
$C_l(\tau)$ *değerleri*	$\#C_l(\tau)$	$\#C_l(\tau)$
C_1	C_1 *in* l_0 *iken tekrar sayısı*	C_1 *in* l_1 *iken tekrar sayısı*
C_2	C_2 *in* l_0 *iken tekrar sayısı*	C_2 *in* l_1 *iken tekrar sayısı*
C_3	C_3 *in* l_0 *iken tekrar sayısı*	C_3 *in* l_1 *iken tekrar sayısı*

Şimdi deneysel sonuçları örneklerde verelim.

Örnek 46. *$p = 3, m = 1$ ve $0 \leq l < (p^m+1)/2$ olmak üzere $m(t)$ ile $m(dt+l)$'nin korelasyon dağılımı Tablo 4.2'daki gibi verilmiştir. Bu tabloda $l = 0$ durumunu ayrı bir sütunda gösterdik çünkü bu durum [2] da çalışılmıştı. Bizim verilerimiz de bu çalışma ile örtüşmektedir. İkinci sütun ise bu çalışmada yer alan değerdir.*

Bu örnekte dizinin alfabesi $\mathbb{F}_3$ ve uzunluğu 8 olup

$$\{m(t)\} = (21011202)^\infty$$

şeklinde verilmektedir. Ayrıca $l = 1$ durumu için $m(dt + l)$ dizisi ise

$$\{m(dt + l)\} = (1122)^\infty$$

şeklindedir.

Tablo 4.2: $p = 3, m = 1$ durumu

	$l = 0$	$l = 1$
$C_l(\tau)$ *değerleri*	$\#C_l(\tau)$	$\#C_l(\tau)$
$-1 + p^m$	4	4
$-1 - \frac{1+i\sqrt{p}}{2}p^m$	2	4
$-1 - \frac{1-i\sqrt{p}}{2}p^m$	2	-

Örnek 47. *$p = 3, m = 3$ ve $0 \leq l < (p^m+1)/2$ olmak üzere $m(t)$ ile $m(dt+l)$'nin korelasyon dağılımı Tablo 4.3'daki gibi verilmiştir. Bu tabloda $l = 0$ durumunu*

Tablo 4.3: $p = 3, m = 3$ durumu

	$l = 0$	$l = 1, 2, 3, 4,$ $5, 6, 8, 9, 10,$ $11, 12, 13$	$l = 7$
$C_l(\tau)$ *değerleri*	$\#C_l(\tau)$	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	252	84	-
$-1 + p^m$	196	84	168
$-1 - p^m$	-	28	56
$-1 + \frac{1-i\sqrt{p}}{2} p^m$	-	140	84
$-1 + \frac{1+i\sqrt{p}}{2} p^m$	-	140	84
$-1 - \frac{1-i\sqrt{p}}{2} p^m$	126	112	168
$-1 - \frac{1+i\sqrt{p}}{2} p^m$	126	112	168
$-1 - \frac{1+p}{2} p^m$	28	28	-

ayrı bir sütunda gösterdik çünkü bu durum [2] da çalışılmıştı. Diğer sütunlar ise bu çalışmada yer alan durumlardır.

Bu örnekte dizinin alfabesi $\mathbb{F}_3$ *ve uzunluğu* 728 *olup*

$$\{m(t)\} = (00201221001011020221111102100212200112010102122102121122$$

$$11121121101201000112111100110222111012212000100021011212120021200$$

$$11100012221120222222110002202122200122110201201101110102220100112$$

$$21210110101210120201012202200001212012220110212011210100001111011$$

$$20202022212111201111210201002102101222210020210001020110010012201$$

$$22002100111202121220112202001002200102210000010100102112002022010$$

$$11222220120012110022102020121120121221122212212202102000221222200$$

$$22011122202112100020001202212121001210022200021112210111111220001$$

$$10121110021122010210220222020111020022112120220202120210102021101$$

$$10000212102111022012102212020000222022101010111212221022221201 02$$

$$00120120211112001012000201022002002110211001200222101212110221101$$

$$00200110020112000002 02)^{\infty}$$

şeklinde verilmektedir. $l = 1$ *durumu için* $m(dt + l)$ *dizisi ise*

$$\{m(dt + l)\} = (00221210102112022201222001001121202012210111021110 02)^{\infty}$$

şeklinde ve $l = 7$ *durumu için* $m(dt + l)$ *dizisi ise*

$$\{m(dt + l)\} = (11202121102002110111120100221012122010012202222102 00)^{\infty}$$

şeklindedir.

Örnek 48. $p = 3, m = 5$ *ve* $0 \leq l < (p^m+1)/2$ *olmak üzere* $m(t)$ *ile* $m(dt+l)$*'nin korelasyon dağılımı Tablo 4.4'daki gibi verilmiştir. Bu tabloda* $l = 0$ *durumunu ayrı bir sütunda gösterdik çünkü bu durum [2] da çalışılmıştı. Diğer sütunlar ise bu çalışmada yer alan durumlardır. Tabloda görüldü gibi* $l = 0$ *dışında üç farklı sütün vardır ve bunların dağılımları birbirinden farklıdır. Bu örnekte dizinin alfabesi* $\mathbb{F}_3$ *ve uzunluğu* 59048 *dir.*

Tablo 4.4: $p = 3, m = 5$ *durumu*

	$l = 0$	$l = 1, 2, 3, 5, 6, 9,$ $10, 13, 15, 18, 20,$ $26, 27, 30, 32, 34,$ $39, 40, 41, 44, 45,$ $52, 54, 58, 60, 62,$ $64, 68, 70, 77, 78,$ $81, 82, 83, 88, 90,$ $92, 95, 96, 102,$ $104, 107, 109, 112,$ $113, 116, 117, 119,$ $120, 121$	$l = 8, 11, 17,$ $19, 23, 24, 25,$ $28, 29, 31, 33,$ $35, 37, 38, 47,$ $49, 50, 51, 53,$ $57, 65, 69, 71,$ $73, 75, 84, 85,$ $87, 89, 91, 93,$ $94, 97, 98, 99,$ $103, 105, 111,$ 114	$l = 4, 7, 12,$ $14, 16, 21, 22,$ $36, 42, 43, 46,$ $48, 55, 56, 59,$ $61, 63, 66, 67,$ $74, 76, 79, 80,$ $86, 100, 101,$ $106, 108, 110,$ $115, 118$
$C_l(\tau)$ *değerleri*	$\#C_l(\tau)$	$\#C_l(\tau)$	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	21960	6588	8052	7320
$-1 + p^m$	14884	8052	6588	7320
$-1 - p^m$	-	2684	2196	2440
$-1 + \frac{1-i\sqrt{p}}{2}p^m$	-	9516	10492	10004
$-1 + \frac{1+i\sqrt{p}}{2}p^m$	-	9516	10492	10004
$-1 - \frac{1-i\sqrt{p}}{2}p^m$	9882	10248	9272	9760
$-1 - \frac{1+i\sqrt{p}}{2}p^m$	9882	10248	9272	9760
$-1 - \frac{1+p}{2}p^m$	2440	2196	2684	2440

Örnek 49. *$p = 5, m = 1$ ve $0 \leq l < (p^m+1)/2$ olmak üzere $m(t)$ ile $m(dt+l)$'nin korelasyon dağılımı Tablo 4.5'daki gibi verilmiştir. Bu tabloda $l = 0$ durumunu ayrı bir sütunda gösterdik çünkü bu durum [2] da çalışılmıştı. Diğer sütunlar ise bu çalışmada yer alan durumlardır.*

Bu örnekte dizinin alfabesi $\mathbb{F}_5$ ve uzunluğu 24 olup

$$\{m(t)\} = (212011424022343044131033)^{\infty}$$

olarak verilmiştir. Ayrıca $l = 1$ durumu için $m(dt + l)$ dizisi

$$\{m(dt + l)\} = (11224433)^{\infty}$$

şeklinde ve $l = 2$ durumu için $m(dt + l)$ dizisi

$$\{m(dt + l)\} = (22443311)^{\infty}$$

şeklindedir.

Tablo 4.5: $p = 5, m = 1$ durumu

	$l = 0$	$l = 1, 2$
$C_l(\tau)$ *değerleri*	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	6	6
$-1 + p^m$	6	–
$-1 - p^m$	6	6
$-1 + \frac{1-\sqrt{p}}{2}p^m$	3	3
$-1 + \frac{1+\sqrt{p}}{2}p^m$	3	3
$-1 - \frac{1-\sqrt{p}}{2}p^m$	–	112
$-1 - \frac{1+\sqrt{p}}{2}p^m$	–	112
$-1 - \frac{1+p}{2}p^m$	–	–

Örnek 50. *$p = 5, m = 3$ ve $0 \leq l < (p^m+1)/2$ olmak üzere $m(t)$ ile $m(dt+l)$'nin korelasyon dağılımı Tablo 4.6'daki gibi verilmiştir. Bu tabloda da $l = 0$ sütununu ayrı yazdık çünkü bu durum [2] da çalışılmıştı. İkinci sütün ise bizim çalıştığımız durumdur.*

Bu örnekte dizinin alfabesi $\mathbb{F}_5$ ve dizinin uzunluğu 15624 tür. Ayrıca $d = 1323$ olup $m(dt + l)$ dizilerinin uzunluğu 248 dir.

Tablo 4.6: $p = 5, m = 3$ durumu

	$l = 0$	$l = 1, 5, 16, 17, 22, 25, 38, 41, 46, 47, 58, 62$
$C_l(\tau)$ *değerleri*	$\#C_l(\tau)$	$\#C_l(\tau)$
-1	5796	4536
$-1 + p^m$	2646	2520
$-1 - p^m$	3906	2016
$-1 - \frac{1-\sqrt{p}}{2} p^m$	–	1449
$-1 - \frac{1+\sqrt{p}}{2} p^m$	–	1449
$-1 + \frac{1-\sqrt{p}}{2} p^m$	1575	1701
$-1 + \frac{1+\sqrt{p}}{2} p^m$	1575	1701
$-1 + \frac{1-p}{2} p^m$	126	126
$-1 - \frac{1+p}{2} p^m$	–	126

Yukarıdaki tablolardan elde edilen gözlemleri şu şekilde sıralayabiliriz:

1. Tablo 4.3 de $l = 0$ dan farklı iki sütun vardır. İlk sütunda 8 farklı değer gözükmektedir ve burada [1] da belirtilen $-1 - \frac{1-p}{2} p^m$ değeri gözükmemektedir. Ayrıca iki tane çift değerler birbirine eşlenik olup bunların tekrar sayıları da birbirine eşittir.

   İkinci sütunda ise 6 farklı değer gözükmektedir ve dağılımı $l = 0$ durumundan farklı çıkmıştır.

2. Tablo 4.4 te ise $l = 0$ durumundan farklı üç tane sütun bulunmaktadır ve bunların dağılımları birbirinden farklıdır. Ayrıca eşlenik değerlerin tekrar sayıları eşit olduğu gözlenmektedir. Burada da bir önceki durumda olduğu gibi [1] da belirtilen $-1 - \frac{1-p}{2} p^m$ değeri gözükmemektedir.

3. Tablo 4.5 te $l = 0$ durumundan farklı bir tane sütun mevcuttur ve dağılımı 6 değerli olmasına rağmen ilk sütundan farklıdır.

5. SONUÇ

Bu çalışmada $m(t)$ p-li m-dizisi ile $m(dt+l)$ desime edilmiş dizisinin korelasyon dağılımı ele alındı. Dağılımın tamamını hesap etmek için gerek olan moment toplamları [2], [3] çalışmalarına benzer teknikler kullanılarak hesaplandı. Ayrıca nümerik hesaplamalarımız sonucu $p = 3$ ve $l \neq 0, (p^m + 1)/4$ iken korelasyon değerlerinin en fazla 8 farklı değer alabileceğini ve $l = (p^m + 1)/4$ iken en fazla 6 değer alabileceğini gözlemledik.

Benzer teknikler kullanılarak $p = 3$, $l = (p^m + 1)/4$ durumu için tüm korelasyon dağılımı verilebilir.

$p = 3$, $l \neq 0, (p^m + 1)/4$ iken bilinen mevcut tekniklerle tüm dağılımının hesabı zor gözüküyor ve ileriye dönük çalışma olarak bırakılmıştır.

Kaynakça

[1] S.T.Choi, T.Lim, J.S.No ve H.Chung, On the cross-correlation of a p-ary m-sequence of period $p^{2m}-1$ and its decimated sequences by $\left(p^m+1\right)^2/2\left(p+1\right)$, IEEE Trans. Inf. Theory, vol. 58, no. 3, March 2012.

[2] J.Luo, T.Helleseth ve A.Kholosha, Two nonbinary sequences with six-valued cross correlation, Proceedings of IWSDA 2011.

[3] E.Y.Seo, Y.S.Kim, J.S.No ve D.J.Shin, Cross-correlation distribution of p-ary m-sequences of period p^{4k-1} and its decimated sequences by $\left(\frac{p^{2k}+1}{2}\right)^2$, IEEE Trans. Inf. Theory, vol. 54, no. 7, July 2008.

[4] T.Helleseth, L.Hu, A.Kholosha, X.Zeng, N.Li ve W.Jiang, Period-different m-sequences with at most four-valued cross correlation, IEEE Trans. Inf. Theory, vol. 55, no. 7, July 2009.

[5] G.J.Ness ve T.Helleseth, Cross correlation of m-sequences of different length, IEEE Trans. Inf. Theory, vol. 52, no. 4, April 2006.

[6] T.Helleseth, A.Kholosha ve A.Johanssen, m-Sequences of different lengths with four-valued cross correlation, ISIT, July 2008.

[7] A.Johanssen, T.Helleseth ve A.Kholosha, Further results on m-sequences with five-valued cross correlation, IEEE Trans. Inf. Theory, vol. 55, no. 12, December 2009.

[8] T.Helleseth, Some results about the cross-correlation function between two maximal linear sequences, Discrete Math. 16, 209-232, 1976.

[9] R.Lidl ve H.Niederreiter, Finite Fields. Cambridge University Press, 1997.

[10] G.J.Ness, T.Helleseth ve A.Kholosha, On the Correlation Distribution of the Coulter–Matthews Decimation, IEEE Trans. Inf. Theory, vol. 52, no. 5, May 2006.

[11] S.T.Choi, T.Lim, J.S.No ve H.Chung, Evaluation of Cross-Correlation Values of p-ary m-Sequence and its Decimated Sequence by $\frac{p^n+1}{p+1} + \frac{p^n-1}{2}$, IEEE Int. Symposium on Inf. Theory Proceedings, 2011.

EKLER

A. Sage Kodları

A.1 $p = 3$ ve $m = 3$ iken dağılımı hesap etmek için kullandığımız kod

```
import os, inspect;
path = os.path.dirname(os.path.abspath
(inspect.getfile(inspect.currentframe())));
num = os.path.basename(path);
num = coerce(int, num);



p = 3;
m = 3;
n = 2*m;
q = p^n;
k = 1;
d = (p^m+1)^2/(2*(p+1));
Fq.<a> = GF(q,'a');

""" Defining variables"""
def chi(x,al,be):
    y = ( al * x - be * x^d ).trace();
    y = coerce( int, coerce(str,y) );
    return exp( 2*pi*I*y / p );
```

```
"""Defining C(alpha, beta)..."""
def C(al,be):
    sum = 0;
    for x in Fq:
        sum = sum + chi(x, al, be);
    return sum-1;

""" 2.234-2352e-10*I tipindeki sayiyi
            duzenlemek icin kullanilan kod"""
def correct(value):
    value = coerce( complex,value );
    value = round( value.real, 4) + round( value.imag, 4)*I;
    return value;


for t in range( q-1 ):
    value = numerical_approx(C(a^t, a^1));
    value = correct(value);
    f = open("/m=3,k=1/{0}/
    values.txt".format(num), "a");
    f.write( coerce(str, value) );
    f.write("\n");
    f.close();

    f = open("/m=3,k=1/{0}/
    hesaplanan_son_deger.txt".format(num), "w");
    f.write( coerce(str, t) );
    f.close();
```

A.2 $p = 5$ ve $m = 3$ iken dağılımı hesap etmek için kullandığımız kod

```
"""Defining variables..."""
#import time;

m=3;
p=5;
n=2*m;
q=p^n;
d=(p^m+1)^2/(2*(p+1));
Fq.<a>=GF(q,'a');
omega = exp(2*pi*I/p);


""" 2.234235-235235235e-10*I tipindeki sayiyi
                  duzenlemek icin kullanilan kod """
def correct(value):
    value = coerce( complex,value );
    value = round( value.real, 4) + round( value.imag, 4)*I;
    return value;


def deger(x):
    return [x.count(0), x.count(1),
            x.count(2), x.count(3), x.count(4)];

def corr(x,y,tao):
    c_t = [];
    for i in range(q-1):
        c_t.append( (x[(i+tao)%(q-1)]-y[i])%p );
    return c_t;
```

```
a_t = [];
for i in range(q-1):
    a_t.append( (a^i).trace() );

l=5;

a_dt_plus_l = [];
for i in range(q-1):
    a_dt_plus_l.append( a_t[(d*i+l) % (q-1)] );

C_values = [];
for i in range(q-1):
    #start = time.clock();
    C_values.append(deger(corr(a_t, a_dt_plus_l, i)));
    #end = time.clock();
    #print "elapsed time is: ", end-start, " seconds.";

Unique_C_values = [];
for i in C_values:
    if i not in Unique_C_values:
        Unique_C_values.append(i);


Table = [];
for i in Unique_C_values:
    Table.append( ( i, C_values.count(i) ) );

f = open("/m=3,k=1/tablo.txt", "a");
f.write("\n\nl={0}\n".format(l));
for e in Table:
    f.write("{0:27} : {1:6}\n".format(correct(
        numerical_approx(e[0][0] +
```

```
            e[0][1]*omega + e[0][2]*omega^2 +
            e[0][3]*omega^3 +
            e[0][4]*omega^4) ), e[1]));
f.close();
```

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: TİLENBAEV, Ernist
Uyruğu	: KIRGIZİSTAN
Doğum tarihi ve yeri	: 1988, Narın/KIRGIZİSTAN
Medeni hali	: Evli
Telefon	: +90 312 2924328
e-mail	: etilenbaev@etu.edu.tr

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Y. Lisans	TOBB Ekonomi ve Teknoloji Üniversitesi, Matematik Bölümü	Eylül, 2013
Lisans	TOBB Ekonomi ve Teknoloji Üniversitesi, Matematik Bölümü	Eylül, 2010

İş Deneyimi

Yıl	**Yer**	**Görev**
2011-2013	TOBB Ekonomi ve Teknoloji Üniversitesi	Araştırma Görevlisi

Yabancı Dil

Kırgızca (anadili), Rusça (ikinci anadili), Türkçe (İleri düzeyde),
İngilizce (İleri düzeyde), İspanyolca (Başlangıç düzeyde)

Yayınlar

1. E.Tilenbaev, H.Dilek, Z. Saygı ve Ç. Ürtiş, "Some Observations on Distribution of Cross Correlation of Two Nonbinary Sequences", ISCTURKEY 2013, 6th International Conference on Information Security and Cryptology, 20-21 Sept. 2013, Ankara, Turkey.

2. H.Dilek, E.Tilenbaev, Z. Saygı, Ç. Ürtiş, "Some Results On Three-Valued Walsh Transforms from Decimations of Helleseth-Gong Sequences", ISCTURKEY 2013 6th International Conference on Information Security and Cryptology, 20-21 Sept. 2013, Ankara, Turkey.