HELLESETH-GONG DİZİLERİNİN KORELASYONLARI ÜZERİNE SONUÇLAR

HASAN DİLEK

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

AĞUSTOS 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

HASAN DİLEK tarafından hazırlanan HELLESETH-GONG DİZİLERİNİN KORELASYONLARI ÜZERİNE SONUÇLAR adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

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

Tez Jüri Üyeleri

Başkan : Doç. Dr. Ali DOĞANAKSOY _____

Üye : Yrd. Doç. Dr. Zülfükar SAYGI _____

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.

Hasan DİLEK

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

Hasan DİLEK

HELLESETH-GONG DİZİLERİNİN KORELASYONLARI ÜZERİNE SONUÇLAR

ÖZET

Diziler şifreleme alanında kullanılan önemli argümanlardır. İyi korelasyona sahip dizilerin günümüzde birçok uygulaması vardır. Bu uygulamaların bazılarında birden fazla kullanıcı tek bir iletişim kanalını kullanmaktadır. Helleseth ve Gong tarafından önerilen dizi ve bu dizinin kaydırılmasıyla elde edilen yeni dizinin korelasyonunun 3 değerli dağılıma sahip olduğu bilinmektedir. Literatürdeki çalışmalar bu kaydırmalı dizilerin özel olarak d (desimasyon) sayısı ile elde edildiğini göstermiştir. Bu tezde Helleseth-Gong dizisinin hangi d değerleri için 3 dağılıma sahip olduğu incelenmiş, farklı d sayıları için dağılımın 3 değerli olduğu gösterilmiştir. Bunlara ilaveten ispatlanması güç olan yeni bir gözlem ortaya konmuş ve SAGE kodu ile belirli boyutlar için doğrulanmıştır. Bu yeni gözlemin ispatı için farklı bir teknik gerekmektedir.

Anahtar Kelimeler: Otokorelasyon, çapraz-korelasyon, m-dizileri, p-li diziler, Walsh dönüşümü, Helleseth-Gong dizileri.

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

Hasan DİLEK

SOME RESULTS ON CORRELATIONS OF HELLESETH-GONG SEQUENCES

ABSTRACT

Sequences are important arguments that uses in coding area however, not all of the sequences, only the sequences which have low correlation distribution have many appliances. In some of these appliances more than one user can connect through the same connection channel. Helleseth and Gong found a sequence with the function which they found and they showed that the decimation numbers' correlation of these sequence have three distributions. Researches in the literature showed that these decimation numbers are found specially with the d (decimation) number. In this thesis, the author analyzed which of the Helleseth-Gong sequence have three valued distributions and proved that the distribution can be three valued distribution for the different d numbers. In addition, a new observation which has a hard proof was found and its correctness proved by written SAGE code. To prove of this observation, a different technique is needed.

Keywords: Autocorrelation, cross-correlation, m-sequences, p-ary sequences, Walsh transform, Helleseth-Gong sequences.

TEŞEKKÜR

Araştırmalarımın her aşamasında değerli bilgi ve yardımlarını esirgemeyen, çalışmalarımı katkılarıyla yönlendiren tez danışmanlarım Yrd. Doç. Dr. Zülfükar SAYGI ve Yrd. Doç. Dr. Çetin ÜRTİŞ' e,

Yüksek lisans eğitimi sırasında kıymetli tecrübelerinden yararlandığım TOBB Ekonomi ve Teknoloji Üniversitesi Matematik Bölümü öğretim üyelerine ve tüm asistan arkadaşlarıma,

Tüm hayatım boyunca maddi manevi hiçbir yardımı esirgemeyen ve bugünlere gelmemi sağlayan aileme teşekkür ederim.

Bu tez "109T344 Cebirsel Eğriler ve Üssel Toplamlar Kullanarak Bazı Kriptografik Uygulamalar" başlıklı proje ile TÜBİTAK tarafından desteklenmiştir. Bu proje ve tezime desteklerinden dolayı TÜBİTAK'a teşekkürü borç bilirim.

İçindekiler

Tablo Listesi

1. GİRİŞ

Bu bölümde, sonraki bölümlerde kullanılacak bazı temel matematiksel ifadeler tanıtılmaktadır. Burada verilen tüm tanımlar, teoremler ve kullanılan notasyonlar için [6] dan faydalanılmıştır. Bu bölümden itibaren

- p ile bir asal sayı,
- q ile p asal sayısının bir pozitif kuvveti,
- $\mathbb{F}_q$ ile q elemanlı sonlu cisim,
- $\mathbb{F}_{q^m}$ ile de $\mathbb{F}_q$ cisminin m. mertebeden bir sonlu genişlemesi ($m \in \mathbb{Z}^+$)

belirtilecektir.

1.1 İz Fonksiyonu

Tanım 1. *[6]* $F = \mathbb{F}_{q^m}$ *ve* $K = \mathbb{F}_q$ *olmak üzere* F *den* K *ya*

$$Tr_{F/K}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}$$

şeklinde tanımlanan $Tr_{F/K}$ *fonksiyonuna* ***iz fonksiyonu*** *denir.*

Örnek 2. *$K = \mathbb{F}_2$ ve $F = \mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\alpha^2 + \alpha + 1 = 0$ olmak üzere $Tr_{F/K}(x) = x + x^2$ olup şu değerleri verir:*

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

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 şu değerleri verir:*

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

Örnek 4. *$K = \mathbb{F}_3$ ve $F = \mathbb{F}_{27} = \mathbb{F}_3(\alpha)$, $\alpha^3+2\alpha+1 = 0$ olmak üzere $Tr_{F/K}(x) = x + x^3 + x^9$ olup şu değerleri verir:*

$$
\begin{array}{rcl}
Tr_{F/K} : F & \longrightarrow & K \\
1 & \longmapsto & 0 \\
\alpha & \longmapsto & 0 \\
\alpha^2 & \longmapsto & 2 \\
\alpha^3 & \longmapsto & 0 \\
\alpha^4 & \longmapsto & 2 \\
\alpha^5 & \longmapsto & 1 \\
\alpha^6 & \longmapsto & 2 \\
\alpha^7 & \longmapsto & 2 \\
\alpha^8 & \longmapsto & 1 \\
\alpha^9 & \longmapsto & 0 \\
\alpha^{10} & \longmapsto & 2 \\
\alpha^{11} & \longmapsto & 2 \\
\alpha^{12} & \longmapsto & 2 \\
\alpha^{13} & \longmapsto & 0 \\
\alpha^{14} & \longmapsto & 0 \\
\alpha^{15} & \longmapsto & 1 \\
\alpha^{16} & \longmapsto & 0 \\
\alpha^{17} & \longmapsto & 1 \\
\alpha^{18} & \longmapsto & 2 \\
\alpha^{19} & \longmapsto & 1 \\
\alpha^{20} & \longmapsto & 1 \\
\alpha^{21} & \longmapsto & 2 \\
\alpha^{22} & \longmapsto & 0 \\
\alpha^{23} & \longmapsto & 1 \\
\alpha^{24} & \longmapsto & 1 \\
\alpha^{25} & \longmapsto & 1
\end{array}
$$

Tanım 5. *[6] İz fonksiyonunda değer kümesi asal cisim olursa, yani $K = F_p$ olursa, iz fonksiyonuna **mutlak iz fonksiyonu** denir.*

Teorem 6. *[6] [İz Fonksiyonunun Temel Özellikleri] $F = \mathbb{F}_{q^m}$ ve $K = \mathbb{F}_q$ olsun. Buna göre*

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

K bir sonlu cisim ve F onun bir sonlu genişlemesi olsun. Her 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 [6].

1.2 Kuadratik Formlar

Tanım 7. *[6] $\mathbb{F}_q[x_1, x_2, ..., x_n]$'de derecesi 2 olan homojen polinoma veya 0 polinomuna $\mathbb{F}_q$ üzerinde n bilinmeyenli **kuadratik form** denir. Eğer q tek ise $\mathbb{F}_q$ üzerindeki herhangi f kuadratik formu için*

$$f(x_1, x_2, ..., x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \quad , \; a_{ij} = a_{ji}$$

sağlanır. Bu durumda f, a_{ij} bileşenlerinden oluşan $n \times n$ tipindeki A matrisiyle ilişkilendirilebilir. Bu A matrisine f'nin katsayılar matrisi denir. Tanımından dolayı $A^T = A$ olur. Yani A simetriktir. Eğer X, $x_1, ..., x_n$ parametrelerinden oluşan sütun vektörü ise f, $X^T AX$ şeklinde tanımlanabilir.

Örnek 8. *[6] $\mathbb{F}_5$ üzerinde iki bilinmeyenli $f(x_1, x_2) = 2x_1^2 + x_1x_2 + x_2^2$ kuadratik form verilsin (ikili kuadratik form). f'nin katsayılar matrisi*

$$A = \begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix}$$

olur. Buradan

$$X^T AX = (x_1\ x_2)\begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 2x_1^2 + x_1x_2 + x_2^2 = f(x_1, x_2)$$

olarak bulunur.

Örnek 9. $\mathbb{F}_7$ *üzerinde tanımlı üç bilinmeyenli*

$$f(x_1, x_2, x_3) = 3x_1^2 + 2x_2^2 + 3x_3^2 - 2x_1x_2 - 2x_2x_3$$

kuadratik form verilsin. f'nin katsayılar matrisi

$$A = \begin{pmatrix} 3 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 3 \end{pmatrix}$$

olur. Buradan

$$\begin{aligned} X^T AX &= (x_1, x_2, x_3)\begin{pmatrix} 3 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 3 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \\ &= 3x_1^2 + 2x_2^2 + 3x_3^2 - 2x_1x_2 - 2x_2x_3 = f(x_1, x_2, x_3) \end{aligned}$$

olarak bulunur. Üstelik A matrisinin rankı 3'dür.

2. DİZİLER

2.1 Temel Özellikler

İletişim sistemindeki birçok uygulama için önemli olan ve üzerinde çalışılan problem, iyi korelasyon özellikleri olan diziler bulmaktır. p tek asal sayısı için, periyodu $p^n - 1$ olan birçok $p-$li dizinin iyi korelasyon özelliği olduğu ve büyük lineer karmaşıklığa sahip olduğu gösterilmiştir [11, 12, 13, 14]. Kod-bölünmeli çoklu-erişim sistemlerinde (code-division multiple-access-CDMA) iyi otokorelasyon ve çapraz korelasyon özellikli dizi kümelerine ihtiyaç duyulur. Bu sebeple $p-$li dizi ile m-dizisinin çapraz korelasyonu incelenmiştir [16, 17]. p'nin farklı değerleri için bu korelasyon dağılımının kaç değerli olduğu bulunmuştur [15, 18, 19]. İdeal otokorelasyonlu dizilerin senkronizasyon uygulamaları önemlidir. Örneğin, 3G hücresel iletişimdeki sinyaller, ilerleyen süreçte Gold dizi çiftlerinin çapraz korelasyon özelliği yerine sadece m-dizilerinin Walsh dönüşümünün kullanıldığı "Gold Diziler Çifti" diye adlandırılacak ([8]) özellikli bir çift m-dizisinden oluşur.

Bu tür sinyal seti yapılarında sadece ikinci seviye otokorelasyon dizilerinin Walsh dönüşümünün özellikleri kullanılır. Örneğin kriptolojide, optimal üç değerli Walsh dönüşümlü fonksiyonların iyi kriptolojik özellikleri vardır [1, 3]. Bu tür fonksiyonlar, Bükük(bent) fonksiyonlarının oluşmasında görev alabilir.

İkinci derece tekli otokorelasyon dizilerinde, herhangi bir "n" için [10]'da detayları görülebilecek birçok yapı vardır. Ancak, ikinci derece otokorelasyonlu p-li dizilerinde, alt alandaki yapılar kullanılmadan, herhangi bir tek p değeri için genel tek bir yapı vardır; m-dizileri.

Helleseth ve Gong, üç değerli(ternary) ailede genellenen ideal ikinci seviye otokorelasyonlu herhangi p(tek sayı) değeri için bir p-ary dizi yapısı oluşturmuşlardır [1]. Bu tür dizilerde Helleseth-Gong dizilerine atıf yapılır. m-dizileri ile Helleseth-Gong dizilerinin desimasyonları arasındaki çapraz korelasyon değerleri bazı desimasyon sayıları için üç değerli dağılıma sahiptir. Bu yapılar 3. bölümde detaylı olarak incelenecektir.

Örnek 10. $(u(t)) = (0,0,-1,0,-1,-1,-1,+1,+1,0,-1,+1,-1)$ *dizisi* $F = \{-1,0,1\}$ *alfabesi kullanılarak tanımlanmış bir dizidir.*

Örnek 11. *1'in ilkel 3.dereceden kökü* ω *olmak üzere*

$$(u(t)) = (1,1,\omega^2,1,\omega^2,\omega)$$

dizisi $F = \{1,\omega,\omega^2\}$ *alfabesi kullanılarak tanımlanmış bir dizidir.*

Çoğu zaman ikinci örnekte olduğu gibi diziler

$$(u(t)) = (\omega^{a(t)}) \text{ ve } (v(t)) = (\omega^{b(t)})$$

şeklinde kullanılır. Burada ω, 1'in p. ilkel kökü ve $a(t)$ ile $b(t)$ ise *mod* p'deki tam sayılardır. Bu yüzden bazı durumlarda diziyi $(u(t))$ yerine $(a(t))$ ile gösteririz. Dolayısıyla Örnek 11'de verilen dizimiz $F = \{1,\omega,\omega^2\}$ alfabesi yerine $F' = \{0,1,2\}$ alfabesi kullanılarak $(a(t)) = (0,0,2,0,2,1)$ olarak ifade edilebilir.

Örnek 12. $2-$*li(binary) dizi: Alfabemiz* $\mathbb{F}_2$ *den alınmışsa 2-li veya binary dizi denir.* $(0,1,1,0,0)$ *bir ikili dizi örneğidir.*

Örnek 13. $3-$*lü(ternary) dizi: Alfabemiz* $\mathbb{F}_3$ *ten alınmışsa 3-lü dizi denir.*

$(0,1,2,2,2,1,1,0,2)$ *bir üçlü dizi örneğidir.*

2.2 Dizilerin Korelasyonları

Bu bölüm boyunca periyodu n olan diziler ele alınacaktır. Verilen bir $(u(t))$ dizisinin periyodu her t değeri için

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

şartını sağlayan en küçük pozitif n sayısıdır. Periyodu n olan $u(t)$ dizisi için

$$\begin{aligned} u(t) &= (u_1, u_2, \cdots, u_n) \\ &= (u_1, u_2, \cdots, u_n)^\infty \end{aligned}$$

gösterimleri kullanılacaktır. Burada verilen $u(t)$ dizisi ilk n terim için sonsuz defa kendini tekrar etmektedir. Aksi söylenmediği takdirde bu iki gösterim diziler için eş anlamlı olarak kullanılacaktır.

2.2.1 Çapraz-korelasyon

Tanım 14. *$(u(t))$ ve $(v(t))$ birer n-periyodlu diziler olmak üzere bu iki dizinin τ kaydırmalı çapraz korelasyonu*

$$C_{u,v}(\tau) = \sum_{t=0}^{n-1} u(t+\tau)\,\overline{v(t)}$$

şeklinde tanımlanır.

Örnek 15. *$(u(t)) = (1, 1, \omega^2, 1, \omega^2, \omega)$ ve $(v(t)) = (\omega, \omega^2, 1, 1, \omega, 1)$ ise $\tau = 1$ kaydırmalı korelasyonu aşağıdaki gibidir:*

$$\begin{aligned} C_{u,v}(1) &= \sum_{t=0}^{n-1} u(t+1)\,\overline{v(t)} \\ &= \omega^2 + \omega^3 + 1 + \omega^2 + \omega^2 + \omega^3 = -3\omega \end{aligned}$$

Bazı çalışmalarda işlem kolaylığı açısından Tanım 14 yerine aşağıdaki korelasyon tanımı kullanılır.

Tanım 16. *$\mathbb{F}_p$ üzerinde tanımlı $(a(t))$ ve $(b(t))$ birer n-periyodlu diziler olmak üzere bu iki dizinin τ kaydırmalı çapraz korelasyonu*

$$C_{u,v}(\tau) = \sum_{t=0}^{n-1} \omega^{a(t+\tau)-b(t)}$$

şeklindedir. Burada ω birimin p. ilkel köküdür.

Örnek 17. *Örnek 15'de verilen* $(u(t)) = (1, 1, \omega^2, 1, \omega^2, \omega)$ *yerine* $(a(t)) = (0, 0, 2, 0, 2, 1)$ *ve* $(v(t)) = (\omega, \omega^2, 1, 1, \omega, 1)$ *yerine* $(b(t)) = (1, 2, 0, 0, 1, 0)$ *alınarak* $\tau = 1$ *kaydırmalı çapraz korelasyon değeri*

$$\begin{aligned} C_{a,b}(1) &= \sum_{t=0}^{6-1} \omega^{a(t+1)-b(t)} \\ &= \omega^2 + \omega^3 + 1 + \omega^2 + \omega^2 + \omega^3 \\ &= -3\omega \end{aligned}$$

olarak bulunur.

2.2.2 Otokorelasyon

Tanım 18. *Bir dizinin kendisi ile korelasyonuna otokorelasyon denir ve* $C_{u,u}(\tau)$ *ile gösterilir.* $0 < \tau < n-1$ *olmak üzere her* τ *için* $C_{u,u}(\tau) = -1$ *ise* $(u(t))$ *ideal ikili otokorelasyona sahiptir denir.*

Örnek 19. $(u(t)) = (1, 1, \omega^2, 1, \omega^2, \omega)$ *ise* $0 < \tau < 6$ *olmak üzere* τ *kaydırmalı otokorelasyon değerleri aşağıdaki gibidir:*

$\tau = 1$ *için:*

$$\begin{aligned} C_{u,u}(1) &= \sum_{t=0}^{n-1} u(t+1)\,\overline{u(t)} \\ &= 1 + \omega^2 + \omega + \omega^2 + \omega^2 + \omega^2 \\ &= 4\omega^2 + \omega + 1 \\ &= 3\omega^2 \\ &= -3\omega - 3 \end{aligned}$$

$\tau = 2$ *için:*

$$\begin{aligned} C_{u,u}(2) &= \sum_{t=0}^{6-1} u(t+2)\,\overline{u(t)} \\ &= \omega^2 + 1 + 1 + \omega + \omega + \omega^2 \\ &= 2\omega^2 + 2\omega + 2 \\ &= 0 \end{aligned}$$

$\tau = 3$ *için:*

$$\begin{aligned} C_{u,u}(3) &= \sum_{t=0}^{6-1} u(t+3)\,\overline{u(t)} \\ &= \omega^2 + 1 + 1 + \omega + \omega + \omega^2 \\ &= 2\omega^2 + 2\omega + 2 \\ &= 0 \end{aligned}$$

$\tau = 4$ *için:*

$$\begin{aligned} C_{u,u}(4) &= \sum_{t=0}^{6-1} u(t+4)\,\overline{u(t)} \\ &= \omega^2 + 1 + 1 + \omega + \omega + \omega^2 \\ &= 2\omega^2 + 2\omega + 2 \\ &= 0 \end{aligned}$$

$\tau = 5$ *için:*

$$\begin{aligned} C_{u,u}(5) &= \sum_{t=0}^{6-1} u(t+5)\,\overline{u(t)} \\ &= \omega + 1 + \omega + \omega^2 + \omega + \omega \\ &= \omega^2 + 4\omega + 1 \\ &= 3\omega \end{aligned}$$

elde edilir.

Çoğu uygulamalarda hem otokorelasyonu hem de çapraz korelasyonu "iyi" olan dizi ailelerine ihtiyaç duyulmaktadır. Örneğin $\mathcal{F}$ bir M elemanlı n-periyodlu diziler ailesi olsun:

$$\mathcal{F} = (\{s_i(t)\} : i = 1, 2, ..., M).$$

Bu durumda $\mathcal{F}$ ailesinin "iyi" olması için otokorelasyonun mutlak değerlerinin en büyüğünün değerinin küçük olması, yani

$$maks\,\{C_{i,i}(\tau) : \tau \neq 0\}$$

değerinin küçük olması ve çapraz korelasyonların mutlak değerinin en büyüğünün küçük olmasıdır, yani

$$maks\left\{C_{i,j}\left(\tau\right) : i \neq j\right\}$$

küçük olmasıdır.

2.3 M-dizileri

Maksimal uzunluk dizileri veya m-dizileri uygulamalarda ve yeni dizileri oluşturmada önemli rol oynamaktadırlar.

Tanım 20. *m-dizisi periyodu $n = q^m - 1$ ve alfabeleri $\mathbb{F}_q$ cisminden olan lineer dizidir.*

- m-dizisinde ardışık m-lilerin hepsi mevcuttur (hepsi sıfır olan m-li dışında).
- Herhangi bir m-dizisi derecesi m olan bir primitif polinom yardımı ile indirgemeli bir şekilde elde edilebilir.

Örnek 21. *Elemanları $\mathbb{F}_3$'e ait ve periyodu $n = 3^3 - 1 = 26$ olan bir m-dizisi aşağıdaki şekilde tanımlanabilir:*

$\mathbb{F}_3$'te primitif olan $f\left(x\right) = x^3 + 2x + 1$ polinomunu ele alalım ve bu polinomun yardımı ile $\left(s\left(t\right)\right)$ dizisi indirgemeli olarak şu şekilde tanımlayalım

$$s\left(t+3\right) + 2s\left(t+1\right) + s\left(t\right) \equiv 0 \left(\mathrm{mod}\, 3\right)$$

veya

$$s\left(t+3\right) \equiv s\left(t+1\right) + 2s\left(t\right) \left(\mathrm{mod}\, 3\right)$$

alarak ve başlangıç değerlerini de $\left(s\left(0\right), s\left(1\right), s\left(2\right)\right) = \left(0, 0, 2\right)$ seçerek $m-$dizisini elde ederiz:

$$\left(0,0,2,0,2,1,2,2,1,0,2,2,2,0,0,1,0,1,2,1,1,2,0,1,1,1\right)^{\infty}$$

m-dizilerinin tercih edilme sebebi olarak öncelikle aşağıdakiler verilebilir:

- iz dönüşümü ile bilinen başka bir probleme kolayca dönüştürülebilmesi
- çapraz korelasyon ve otokorelasyonunun nispeten daha kolay hesaplanmasıdır.

2.4 Desimasyon İle Elde Edilmiş Diziler

Tanım 22. *Verilen bir* $(m(t))$ *dizisi ve herhangi bir pozitif* d *sayısı için* $(m(dt))$ *olarak tanımlanan dizilere* ***desimasyon ile elde edilmiş diziler*** *denir. Burada verilen* $(m(t))$ *dizisinin elemanları* d *kadar atlanarak alınmış olur.*

Örnek 23. $(s(t)) = (0,0,2,0,2,1,2,2,1,0,2,2,2,0,0,1,0,1,2,1,1,2,0,1,1,1)^{\infty}$ *dizisi için*

- $(s(2t)) = (0,2,2,2,1,2,2,0,0,2,1,0,1)^{\infty}$
- $(s(3t)) = (0,0,2,0,2,1,2,2,1,0,2,2,2,0,0,1,0,1,2,1,1,2,0,1,1,1)^{\infty}$
- $(s(4t)) = (0,2,1,2,0,1,1,2,2,2,0,2,0)^{\infty}$
- $(s(5t)) = (0,1,2,1,1,1,2,0,0,1,1,0,1,0,2,1,2,2,2,1,0,0,2,2,0,2)^{\infty}$
- $(s(6t)) = (0,2,2,2,1,2,2,0,0,2,1,0,1)^{\infty}$
- $(s(7t)) = (0,2,0,2,2,0,0,1,2,2,2,1,2,1,0,0,2,1,1,1,2,1)^{\infty}$
- $(s(8t)) = (0,1,0,1,2,0,0,2,2,1,2,2,2)^{\infty}$
- $(s(9t)) = (0,0,2,0,2,1,2,2,1,0,2,2,2,0,0,1,0,1,2,1,1,2,0,1,1,1)^{\infty}$
- $(s(10t)) = (0,2,1,2,0,1,1,2,2,2,0,2,0)^{\infty}$
- $(s(11t)) = (0,2,0,2,2,0,0,1,2,2,2,1,2,0,1,0,1,1,0,0,2,1,1,1,2,1)^{\infty}$
- $(s(12t)) = (0,2,1,2,0,1,1,2,2,2,0,2,0)^{\infty}$
- $(s(13t)) = (0,0)^{\infty}$ *elde edilir.*

Not 24. *Dizinin periyodu n ile desimasyon değeri d aralarında asal ise elde edien $\{m(dt)\}$ dizisinin periyodu yine n olur. Daha genel olarak $e = obeb(d,n)$ olmak üzere $\{m(dt)\}$ dizisinin periyodu n/e olur. Dolayısıyla $e > 1$ ise desimasyon sonucunda daha kısa periyodlu diziler elde edilmiş olur.*

α, $\mathbb{F}_{p^n}$'nin bir ilkel elemanı olsun. $m(t) = Tr_1^n(\alpha^t)$ periyodu $p^n - 1$ olan bir p-li m-dizisi olsun. Bu durumda $m(dt+k)$ dizisi (d desimasyonuyla elde edilmiş ve k kadar kaydırılmış) ile $m(t)$ nin çapraz korelasyonu şu şekilde verilir:

$$\begin{aligned}
C_l(\tau) &= \sum_{t=0}^{p^n-2} \omega^{m(t+\tau)\overline{\omega^{m(dt+k)}}} \\
&= \sum_{t=0}^{p^n-2} \omega^{m(t+\tau)-m(dt+k)} \\
&= \sum_{t=0}^{p^n-2} \omega^{Tr\left(\alpha^{t+\tau}\right)-Tr\left(\alpha^{dt+k}\right)} \\
&= \sum_{t=0}^{p^n-2} \omega^{Tr\left(\alpha^{t+\tau}-\alpha^{dt+k}\right)} \\
&= \sum_{t=0}^{p^n-2} \omega^{Tr\left(\alpha^t\alpha^\tau-\left(\alpha^t\right)^d\alpha^k\right)} \\
&= \sum_{t=0}^{p^n-2} \omega^{Tr\left(x\alpha^\tau-x^d\alpha^k\right)} \\
&= \sum_{x\in\mathbb{F}_{p^n}} \omega^{Tr\left(xa-x^db\right)} \\
&= S(a,b).
\end{aligned}$$

Yukarıda m-dizilerinin çapraz korelasyon hesabını yaparken

$$S(a,b) = \sum_{x\in\mathbb{F}_q} \omega^{Tr\left(ax-bx^d\right)}$$

gibi bir üstel toplama rastladık.Bu toplamı hesaplamak için literatürde bir çok yöntem vardır. Bu çalışmamız sırasında toplamı hesaplamak için Walsh dönüşümü kullanılacaktır.

2.5 Bir Dizinin Walsh Dönüşümü

Tanım 25. *$\mathbb{F}_{p^n}$'den $\mathbb{F}_p$'ye tanımlı $f(x)$ ve $\lambda \in \mathbb{F}_{p^n}$ için f fonksiyonunun λ'daki Walsh dönüşümü*

$$\hat{f}(\lambda) = \sum_{x \in F_{p^n}} \omega^{f(x)+Tr_n(\lambda x)}$$

şeklinde tanımlanır.

Walsh dönüşümü kriptoloji alanında ve sonlu cisimler üzerindeki dizilerin inşası ve analizinde önemli rol oynamaktadır. İkili ve ikili olmayan diziler için Walsh dönüşümü, $a(t) = f(\alpha^t)$ şeklinde tanımlanan p-li dizi ile $b(t) = Tr_n(\alpha^t)$ şeklindeki m-dizisi arasındaki çapraz-korelasyonu belirler. $\lambda = -\alpha^{-\tau}$ olmak üzere iki dizi arasındaki τ kaydırmalı çapraz-korelasyon şu şekilde bulunur:

$$\begin{aligned} C_{a,b}(\tau) &= \sum_{t=0}^{p^n-2} \omega^{a(t+\tau)-b(t)} \\ &= \sum_{x \in F_{p^n} \setminus \{0\}} \omega^{f(\alpha^\tau \alpha^t)-Tr_n(\alpha^t)} \\ &= \sum_{x \in F_{p^n} \setminus \{0\}} \omega^{f(x)+Tr_n(\lambda x)} \\ &= -\omega^{f(0)} + \hat{f}(\lambda). \end{aligned}$$

Dolayısıyla iki dizinin çapraz-korelasyonu için ilk önce Walsh dönüşümünü bulmak hesaplamada büyük kolaylık sağlamaktadır.

3. HELLESETH-GONG DİZİSİ

3.1 Helleseth-Gong Fonksiyonu

Bu bölümde aşağıdaki notasyonlar kullanılacaktır.

- p tek asal sayı,
- α, $\mathbb{F}_{p^n}$'nin primitif elemanı,
- $n = (2m+1)k$,
- s, $1 \leq s \leq 2m$ ve $obeb(s, 2m+1) = 1$ şartlarını sağlayan bir tam sayı,
- $b_0 = 1$, $i = 1, 2, ..., m$ olmak üzere $b_i = b_{2m+1-i}$ ve $b_{is} = (-1)^i$, (burada b_{is} indisleri mod $2m+1$ de değer almaktadır),
- $u_0 = b_0/2 = (p+1)/2$,
- $i = 1, 2, ..., m$ olmak üzere $u_i = b_{2i}$ olsun.

Tanım 26. $\mathbb{F}_{p^n}$ *üzerinde tanımlanan*

$$f(x) = \sum_{i=0}^{m} u_i x^{(p^{2ki}+1)/2}$$

fonksiyonuna ***Helleseth-Gong fonksiyonu*** *denir.*

Lemma 27. *[3]* $\mathbb{F}_{p^n}$ *üzerinde tanımlanan*

$$f(x) = \sum_{i=0}^{m} u_i x^{(p^{2ki}+1)/2}$$

fonksiyonu için $\mathbb{F}_p$ *üzerinde tanımlı*

$$s(t) = Tr_n(f(\alpha^t))$$

dizisi ideal otokorelasyona sahiptir.

Lemma 28. *[3]* $\mathbb{F}_{p^n}$ *üzerinde tanımlanan*

$$f(x) = \sum_{i=0}^{m} u_{m-i} x^{(q^{2i}+1)/q+1}$$

fonksiyonu için $\mathbb{F}_p$ *üzerinde tanımlı*

$$s(t) = Tr_n(f(\alpha^t))$$

dizisi ideal otokorelasyona sahiptir.

Yukarıdaki lemmalarda $s = 2$ alınırsa $i = 1, 2, ..., m$ için $b_{2i} = u_i = (-1)^i$ ve $b_0 = 2u_0 = 1$ olur. Burada başlangıç değeri $u_0 = (p+1)/2$'dir.

Sonuç 29. *[3]* $u_0 = (p+1)/2$, $u_i = (-1)^i$, $i = 1, 2, ..., m$ *olsun.* $f(x)$ *Lemma 27 veya Lemma 28 deki gibi tanımlansın. Bu durumda* $\mathbb{F}_p$ *üzerinde tanımlanan*

$$s(t) = Tr_n(f(\alpha^t))$$

dizisi ideal otokorelasyona sahiptir.

Lemma 27 ve Lemma 28 kullanılarak aşağıda verilen ideal otokorelasyona sahip diziler elde edilebilir.

Tablo 3.1: İdeal Otokorelasyona Sahip Bazı Diziler [2]

p	n	m	$u_0u_1...u_m$	s
3	5	2	2 1 2	1
3	5	2	2 2 1	2
3	7	3	2 1 2 2	1
3	7	3	2 2 1 2	2
3	7	3	2 2 2 1	3
3	9	4	2 1 1 2 2	1
3	9	4	2 2 1 2 1	2
3	9	4	2 1 2 2 1	4
3	11	5	2 1 1 2 2 2	1
3	11	5	2 2 1 2 1 2	2
3	11	5	2 2 2 1 2 1	3
3	11	5	2 2 2 1 1 2	4
3	11	5	2 1 2 2 2 1	5
5	5	2	3 1 4	1
5	5	2	3 4 1	2
5	7	3	3 1 4 4	1
5	7	3	3 4 1 4	2
5	7	3	3 4 4 1	3
7	5	2	4 1 6	1
7	5	2	4 6 1	2

3.2 Helleseth-Gong Fonksiyonunun 3 Değerli Dağılıma Sahip Walsh Dönüşümü

Bu bölümdeki sonuçlar ve ispatlar [1] ve [2] makalelerinden alınmış olup, ispatlarda verilmeyen bazı geçişler daha açık hale getirilmiştir.

Teorem 30. *[1]* $u_0 = (p+1)/2$, $u_i = (-1)^i$, $i = 1, 2, ..., m$, *ve* $d \in \left\{1, \frac{p^n+1}{p^k+1}\right\}$ *olsun. Bu durumda*

$$h(x) = Tr_n\left(\sum_{i=0}^{m} u_i x^{\frac{p^{2ki}+1}{2}d}\right)$$

şeklinde tanımlanan fonksiyonun

$$\hat{h}(\lambda) = \sum_{x\in\mathbb{F}_{p^n}} \omega^{h(x)+Tr_n(\lambda x)}$$

Walsh dönüşümü $\left\{0, \pm p^{\frac{n+k}{2}}\right\}$ *değerlerini alır.* λ *değeri* $\mathbb{F}_{p^n}$ *sonlu cismini gezerken* $\hat{h}(\lambda)$*'nin dağılımı aşağıdaki gibidir:*

$$\begin{array}{lll} 0 & \textit{değeri} & p^n - p^{n-k} \quad \textit{defa} \\ -p^{(n+k)/2} & \textit{değeri} & (p^{n-k} - p^{(n-k)/2})/2 \quad \textit{defa} \\ p^{(n+k)/2} & \textit{değeri} & (p^{n-k} + p^{(n-k)/2})/2 \quad \textit{defa.} \end{array}$$

Teoremin ispatı için aşağıdaki tanım ve lemmalara ihtiyaç duyulacaktır.

İlk önce $d = \frac{p^n+1}{p^k+1}$ durumunu ispatlayalım. Daha sonra bu ispatı kullanarak $d = 1$ durumu ispatlanabilir.

$\mathbb{F}_{p^n}$'den $\mathbb{F}_{p^k}$'ya tanımlanan $F(x)$ için

$$\begin{aligned} F(x) &= Tr_k^n(f(x^d) + \lambda x) \\ &= Tr_k^n\left(\sum_{i=0}^{m} u_i x^{\frac{p^{2ki}+1}{2}\frac{p^n+1}{p^k+1}} + \lambda x\right) \end{aligned}$$

olur ve

$$\begin{aligned} h(x) + Tr_n(\lambda x) &= Tr_k\left(Tr_k^n(f(x^d) + \lambda x)\right) \\ &= Tr_k\left(F(x)\right) \end{aligned}$$

sağlanır. Böylece

$$\begin{aligned} \frac{p^{2ki}+1}{2} \cdot \frac{p^n+1}{p^k+1} &\equiv \left(\frac{p^{2ki}-1}{2} + 1\right) \cdot \left(\frac{p^n - p^k}{p^k+1} + 1\right) \\ &\equiv 1 \cdot 1 \\ &\equiv 1 \ (\ mod\ p^k - 1). \end{aligned}$$

olduğundan $r \in \mathbb{F}_{p^k}$ için

$$F(rx) = rF(x)$$

sağlanır. Ayrıca n/k tek olduğundan $\text{obeb}\left(\frac{p^n+1}{p^k+1}, p^n-1\right) = 1$ olur. Üstelik

$$\begin{aligned}\frac{p^{2ki}+1}{2}\cdot(p^n+1) &\equiv \frac{p^{2ki}+1}{2}\cdot 2 \\ &\equiv p^{2ki}+1 \ \ (\ mod\ p^n-1)\end{aligned}$$

olduğundan

$$F(y^{p^k+1}) = Tr_k^n\left(\sum_{i=0}^{m} u_i y^{p^{2ki}+1} + \lambda y^{p^k+1}\right)$$

sağlanır. Şimdi $q = p^k$ olsun ve $Q_\lambda(y)$ aşağıdaki gibi tanımlansın. Bu takdirde

$$\begin{aligned}Q_\lambda(y) &= F(y^{q+1}) \\ &= Tr_k^n\left(\sum_{i=0}^{m} u_i y^{q^{2i}+1} + \lambda y^{q+1}\right)\end{aligned}$$

olur. $y = \sum_{i=1}^{n/k} y_i\alpha_i$ olarak tanımlayalım. Burada $\alpha_1,\ \alpha_2, ...,\ \alpha_{n/k}$ $\mathbb{F}_{p^n}$ 'nin $\mathbb{F}_{p^k}$ üzerindeki tabanıdır. İz dönüşüm fonksiyonunun özelliğinden $a_{i,j}^{(\lambda)} \in \mathbb{F}_{p^k}$ olmak üzere $Q_\lambda(y) = \sum_{i,j} a_{i,j}^{(\lambda)} y_i y_j$ yazılabilir. Bu bilgiler kullanılarak aşağıdaki lemma verilebilir.

Lemma 31. *[1, 3, 4] $k\,|n$ ve $q = p^k$ olmak üzere $Q(y)$, $\mathbb{F}_q$ üzerinde tanımlı bir kuadratik form olsun. $q = p^k$, ρ n/k değişkenli rank ve r, $\mathbb{F}_q$ 'da karesel olmayan bir eleman olsun. Bu durumda*

$$S = \frac{1}{2}\left(\sum_{y\in\mathbb{F}_{p^n}} \omega^{Tr_k(Q(y))} + \sum_{y\in\mathbb{F}_{p^n}} \omega^{Tr_k(rQ(y))}\right)$$

şeklinde tanımlanırsa

$$S = \begin{cases} 0 & eğer\ \rho\ tek\ ise \\ \pm\, \rho^{\frac{n}{k}-\frac{\rho}{2}} & eğer\ \rho\ çift\ ise \end{cases}$$

olur.

Lemma 32. *[1] $\mathbb{F}_q$ üzerinde $Q_\lambda(y)$ kuadratik formun n/k değişkenli rankı ρ, sadece n/k, $n/k-1$ veya $n/k-2$ değerlerini alabilir.*

İspat. $Q_\lambda(y)$'nin ρ rankı hesabında $z \in \mathbb{F}_{q^{n/k}} = \mathbb{F}_{q^{2m+1}}$ ve her $y \in \mathbb{F}_{q^{2m+1}}$ için

$$Q_\lambda(y+z) = Q_\lambda(y)$$

denkleminin çözüm sayısının $q^{n/k-\rho}$ olduğunu belirlemeliyiz.

Bunun için aşağıdaki gözlemi yapabiliriz.

$$Q_\lambda(y+z) = Q_\lambda(y) \Leftrightarrow$$
$$Tr_k^n\left(\sum_{i=0}^{m} u_i(y+z)^{q^{2i}+1} + \lambda(y+z)^{q+1}\right) = Tr_k^n\left(\sum_{i=0}^{m} u_i y^{q^{2i}+1} + \lambda y^{q+1}\right).$$

Bu ifade

$$Tr_k^n\left(\sum_{i=0}^{m} u_i(y^{q^{2i}}z + yz^{q^{2i}}) + \lambda(y^q z + yz^q) + \sum_{i=0}^{m} u_i z^{q^{2i}+1} + \lambda z^{q+1}\right) = 0$$

eşitliğine denktir. Buradan

$$Tr_k^n\left(y\left(\sum_{i=0}^{m} u_i(z^{q^{-2i}} + z^{q^{2i}}) + \lambda^{q^{-1}} z^{q^{-1}} + \lambda z^q\right) + \sum_{i=0}^{m} u_i z^{q^{2i}+1} + \lambda z^{q+1}\right) = 0$$

elde edilir. Eğer bu eşitlik her $y \in \mathbb{F}_{q^{2m+1}}$ için sağlanırsa

$$\begin{aligned} L(z) &= \sum_{i=0}^{m} u_i(z^{q^{-2i}} + z^{q^{2i}}) + \lambda^{q^{-1}} z^{q^{-1}} + \lambda z^q \\ &= 0 \end{aligned}$$

ve

$$Tr_k^n\left(\sum_{i=0}^{m} u_i z^{q^{2i}+1} + \lambda z^{q+1}\right) = 0$$

olmalıdır. Burada 2. denklem, 1. denklemin $Tr_k^n(zL(z))$ dönüşümüyle elde edilir. Dahası 1. denklemi kullanarak,

$$\begin{aligned} L(z) + (L(z))^{q^2} &= \sum_{i=0}^{m} u_i(z^{q^{-2i}} + z^{q^{2i}}) + \lambda^{q^{-1}} z^{q^{-1}} + \lambda z^q \\ &\quad + \sum_{i=0}^{m} u_i(z^{q^{-2i+2}} + z^{q^{2i+2}}) + \lambda^q z^q + \lambda^{q^2} z^{q^3} \\ &= \sum_{i=1}^{m}(u_i + u_{i-1}) z^{q^{2i}} + u_0 z + u_m z^{q^{2m+2}} + \lambda^{q^{-1}} z^{q^{-1}} + \lambda z^q \\ &\quad + \sum_{i=1}^{m-1}(u_i + u_{i+1}) z^{q^{-2i}} + u_m z^{q^{-2m}} + u_0 z^{q^2} + \lambda^q z^q + \lambda^{q^2} z^{q^3} \\ &= (u_1 + u_0) z^{q^2} + u_0 z + u_m z^{q^{2m+2}} + \lambda^{q^{-1}} z^{q^{-1}} + \lambda z^q \\ &\quad + (u_1 + u_0) z + u_m z^{q^{-2m}} + u_0 z^{q^2} + \lambda^q z^q + \lambda^{q^2} z^{q^3} \end{aligned}$$

elde edilir. Bu eşitlik $2u_0 + u_1 = 0$ ve her $z \in \mathbb{F}_{q^{2m+1}}$ için $z^{q^{2m+1}} = z$ olduğundan

$$\begin{aligned} &= \lambda^{q^{-1}} z^{q^{-1}} + (2u_0 + u_1)(z + z^{q^2}) + (2u_m + \lambda + \lambda^q) z^q + \lambda^{q^2} z^{q^3} \\ &= \lambda^{q^{-1}} z^{q^{-1}} + (2u_m + \lambda + \lambda^q) z^q + \lambda^{q^2} z^{q^3} \end{aligned}$$

haline dönüşür. Bu yüzden $L(z)$'nin sıfırları ile

$$\begin{aligned} P(z) &= L(z)^q + (L(z))^{q^3} \\ &= \lambda z + (2u_m + \lambda^q + \lambda^{q^2}) z^{q^2} + \lambda^{q^3} z^{q^4} \end{aligned}$$

denkleminin sıfırları aynıdır. Bu $P(z)$'nin sıfırları $\mathbb{F}_{q^2}$'de boyutu en fazla 2 olan bir vektör uzayıdır. n/k tek olduğundan, $P(z)$'nin çözüm uzayının $\mathbb{F}_q$'daki boyutu da en fazla 2'dir (Trachtenberg [4]). Böylece $n/k - \rho \leq 2$ olur ve $Q_\lambda(y)$ kuadratik formun ρ rankı, sadece n/k, $n/k - 1$ veya $n/k - 2$ değerlerini alabilir. ■

Lemma 33. *[10]* $\mathbb{F}_{p^n}$*'den* $\mathbb{F}_p$ *'ye tanımlı herhangi bir* $f(x)$ *ve* $\lambda \in \mathbb{F}_{p^n}$ *için* f *fonksiyonunun* λ'*daki Walsh dönüşümü*

$$\hat{f}(\lambda) = \sum_{x \in F_{p^n}} \omega^{f(x)+Tr_n(\lambda x)}$$

olmak üzere

$$\sum_{x \in F_{p^n}} \hat{f}(\lambda) = p^n$$

ve

$$\sum_{x \in F_{p^n}} \left|\hat{f}(\lambda)\right|^2 = p^{2n}$$

eşitlikleri sağlanır.

Teorem 30'un ispatı. $r, \mathbb{F}_{p^k}$ 'da karesel olmayan bir eleman olsun. Bu durumda n/k tek olduğundan r, $\mathbb{F}_q$ 'da karesel olmayan bir eleman olur. $Q(y)$, $\mathbb{F}_q$ üzerinde tanımlı bir quadratik form olsun. $q = p^k$, $\rho \;\; n/k$ değişkenli rank ve r, $\mathbb{F}_{p^n}$ 'da da karesel olmayan bir elemandır.

$$obeb(q+1, q^{n/k}-1) = 2$$

olduğundan y, $\mathbb{F}_{p^n}$'i gezerken, y^{q+1} ve ry^{q+1}, $\mathbb{F}_{p^n}$'i iki defa gezer.

$$F(rx) = rF(x)$$

olduğundan

$$\begin{aligned}\hat{h}(\lambda) &= \sum_{x\in\mathbb{F}_{p^n}} \omega^{h(x)+Tr_n(\lambda x)} \\ &= \sum_{x\in\mathbb{F}_{p^n}} \omega^{Tr_k(F(x))} \\ &= \frac{1}{2}\left(\sum_{y\in\mathbb{F}_{p^n}} \omega^{Tr_k(F(y^{q+1}))} + \sum_{y\in\mathbb{F}_{p^n}} \omega^{Tr_k(F(ry^{q+1}))}\right) \\ &= \frac{1}{2}\left(\sum_{y\in\mathbb{F}_{p^n}} \omega^{Tr_k(Q(y))} + \sum_{y\in\mathbb{F}_{p^n}} \omega^{Tr_k(rQ(y))}\right)\end{aligned}$$

sonucu elde edilir. Lemma 32'den $Q_\lambda(y)$ kuadratik formun ρ rankı, sadece n/k, $n/k-1$ veya $n/k-2$ değerlerini alabiliyordu. Bu yüzden Lemma 33'den $\hat{h}(\lambda)$, $\left\{0, \pm p^{\frac{n+k}{2}}\right\}$ değerlerini alır.

Böylece Lemma 31'i kullanarak ispat tamamlanır.

$d=1$ ve $s=2$ durumu için üstte yaptığımız ispatta

$$\begin{aligned}F(x) &= Tr_k^n(f(x)+\lambda x) \\ Q_\lambda(y) &= F(y^2) \\ &= Tr_k^n\left(\sum_{i=0}^{m} u_i y^{q^{2i}+1} + \lambda y^2\right)\end{aligned}$$

değişikliklerini yapmamız yeterli olacaktır. Buradaki $Q_\lambda(y)$ kuadratik formun rankını bulmak için

$$\lambda^q z^{q^2} + (-1)^m z^q + \lambda z = 0$$

denkleminin $\mathbb{F}_{q^{n/k}}$'daki çözümlerin sayısını bulmamız gerekir. Buradan da rankın en fazla 2 olduğunu elde ederiz. Böylece teorem $d=1$ içinde doğrudur. ■

Aşağıdaki tabloda Helleseth ve Gong Teorem 30'daki buldukları desimasyon sayılarına ilave olarak, deneysel olarak elde ettikleri 3 dağılıma sahip Walsh dönüşümü veren desimasyon sayıları vermişlerdir.

Tablo 3.2: Deneysel Sonuçlar [1]

Sonlu Cisim	s	d
$\mathbb{F}_{3^5}$	1	$1, 49, 61$
	2	$7, 23, 35, 49$
$\mathbb{F}_{3^7}$	1	$1, 391$
	2	$61, 169$
	3	$1, 439$
$\mathbb{F}_{3^9}$	1	$1, 3361$
	2	$547, 1667$
	4	$1, 3937$
$\mathbb{F}_{3^{11}}$	1	$1, 29767$
	2	$4921, 14641$
	3	$1, 34571$
	4	$1, 35431$
	5	$1, 31639$
$\mathbb{F}_{3^{13}}$	1	$1, 266449$
	2	$44287, 133103$
	3	$1, 307105$
	4	$1, 318865$
	5	$1, 311105$
	6	$1, 284701$
$\mathbb{F}_{3^{15}}$	1	$1, 2393671$
	2	$398581, 1194649$
	4	$1, 2869783$
	7	$1, 2449831$

Takip eden iki teoremde Tablo 3.2 de verilen bazı desimasyon sayıları için ispat yapılmıştır [2].

Teorem 34. *[2] p tek asal sayı, $q = p^k$, $b_0 = 1$, $i = 1, 2, ..., m$ olmak üzere $b_i = b_{2m+1-i}$ ve $b_{is} = (-1)^i$ olsun. Burada b_{is} indisleri* $\bmod 2m+1$ *de değer almaktadır. $u_0 = b_0/2 = (p+1)/2$ ve $i = 1, 2, ..., m$ olmak üzere $u_i = b_{2i}$ olsun. Bu durumda*

$$h(x) = Tr_n\left(\sum_{i=0}^{m} u_i x^{\frac{p^{2ki}+1}{2}d}\right)$$

şeklinde tanımlanan fonksiyonun

$$\hat{h}(\lambda) = \sum_{x\in\mathbb{F}_{p^n}} \omega^{h(x)+Tr_n(\lambda x)}$$

Walsh dönüşümü $\left\{0, \pm p^{\frac{n+k}{2}}\right\}$ *değerlerini alır. λ değeri $\mathbb{F}_{p^n}$ sonlu cismini gezerken $\hat{h}(\lambda)$'nin dağılımı aşağıdaki gibidir:*

0	*değeri*	$p^n - p^{n-k}$	*defa*
$-p^{(n+k)/2}$	*değeri*	$(p^{n-k} - p^{(n-k)/2})/2$	*defa*
$p^{(n+k)/2}$	*değeri*	$(p^{n-k} + p^{(n-k)/2})/2$	*defa.*

Teorem 35. *[2] p tek asal sayı, $q = p^k$, $b_0 = 1$, $i = 1, 2, ..., m$ olmak üzere $b_i = b_{2m+1-i}$ ve $b_{is} = (-1)^i$ olsun. Burada b_{is} indisleri* $\bmod 2m+1$ *de değer almaktadır. $u_0 = b_0/2 = (p+1)/2$ ve $i = 1, 2, ..., m$ olmak üzere $u_i = b_{2i}$ olsun. Bu durumda*

$$f(x) = \sum_{i=0}^{m} u_i x^{(q^{2i}+1)/2}$$

$1 < d < q^{2m+1} - 1$ eşitsizliğindeki d sayısı aşağıdaki özellikleri sağlasın.

$$(q^{(m+1)s} + 1)d \equiv 2q^h \pmod{q^{2m+1s} - 1} \quad , 0 \le h < 2m+1$$

$g(x) = f(x^d)$ 'nin Walsh dönüşümü $\left\{0, \pm p^{\frac{n+k}{2}}\right\}$ *değerlerini alır. λ değeri $\mathbb{F}_{p^n}$ sonlu cismini gezerken $\hat{g}(\lambda)$'nin dağılımı aşağıdaki gibidir:*

0	*değeri*	$p^n - p^{n-k}$	*defa*
$-p^{(n+k)/2}$	*değeri*	$(p^{n-k} - p^{(n-k)/2})/2$	*defa*
$p^{(n+k)/2}$	*değeri*	$(p^{n-k} + p^{(n-k)/2})/2$	*defa.*

Böylece Teorem 34 ve Teorem 35 ile Tablo 3.2'deki bazı desimasyon sayıları da ispatlanmıştır. Fakat aşağıda verilen desimasyon sayıları ve bu değerlerle hesaplanan çapraz-korelasyon değerlerinin ispatı henüz verilmemiştir. Bu yüzden diğer bölümde, Tablo 3.2'deki bazı desimasyon değerleri genelleştirilmeye çalışılacak ve bazıları içinde yeni bir gözlem verilecektir.

Tablo 3.3: Henüz İspatlanmayan Desimasyon Sayıları

Sonlu Cisim	s	d
$\mathbb{F}_{3^5}$	2	$7, 23, 35, 49$
$\mathbb{F}_{3^7}$	2	$61, 169$
$\mathbb{F}_{3^9}$	2	$547, 1667$
$\mathbb{F}_{3^{11}}$	2	$4921, 14641$
$\mathbb{F}_{3^{13}}$	2	$44287, 133103$
$\mathbb{F}_{3^{15}}$	2	$398581, 1194649$

4. ÇALIŞMALARIMIZ

4.1 $d = 481$ durumu

Helleseth-Gong dizisi ve desimasyon ile elde edilmiş dizinin korelasyon dağılımını bulmak için SAGE kodu [22] kullanılmıştır. Söz konusu korelasyon değerleri Tablo-3.3'den kolaylıkla elde edilebilir. Araştırmalarımızda $p = 3$ için Tablo-3.2'deki desimasyon değerlerini doğruladık. Buna ek olarak $p = 5$, $k = 1$, $n = 5$ ve $s = 2$ iken $d = 481$ desimasyon değerinin üç haneli bir Walsh dönüşümüne sahip olduğunu gözlemledik.

$d = 481$ desimasyon değeri [1] ve [2] nolu çalışmalarda yer almamaktadır. Aşağıda bu sayısal gözlemin teknik ispatı yapılmıştır. Bunun yanı sıra Tablo-3.3 ve SAGE kodu [22] kullanılarak $p = 3$ durumunda yeni bir sonuç Gözlem 37'de sunulmuştur.

Teorem 36. *$p = 5$, $k = 1$, $n = 5$, $s = 2$ ve $d = 481$ olsun. $i = 0, 1, 2, ..., m$ için $u_i = (-1)^i$ ve $u_0 = (p+1)/2$ olsun. Bu durumda*

$$h(x) = Tr_n\left(\sum_{i=0}^{2} u_i x^{\frac{5^{2i}+1}{2}481}\right)$$

fonksiyonunun

$$\hat{h}(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} \omega^{h(x)+Tr_n(\lambda x)}$$

Walsh dönüşümü $\{0, \pm 5^3\}$ *değerlerini alır.* λ *değeri* $\mathbb{F}_{5^5}$ *sonlu cismini gezerken* $\hat{h}(\lambda)$*'nin dağılımı aşağıdaki gibidir:*

$$\begin{array}{rlll} 0 & \textit{değeri} & 5^5 - 5^4 & = 2500 \quad \textit{defa} \\ -5^3 & \textit{değeri} & (5^4 - 5^2)/2 & = 300 \quad \textit{defa} \\ 5^3 & \textit{değeri} & (5^4 + 5^2)/2 & = 325 \quad \textit{defa.} \end{array}$$

İspat. $\mathbb{F}_{5^5}$ den $\mathbb{F}_5$'e tanımlanan $F(x)$ için

$$F(x) = Tr_5(f(x^{481}) + \lambda x) = Tr_5\left(\sum_{i=0}^{2} u_i x^{\frac{5^{2i}+1}{2}481} + \lambda x\right)$$

olur. Buradan

$$h(x) + Tr_5(\lambda x) = Tr_5(f(x^{481}) + \lambda x) = F(x)$$

sağlanır. Böylece

$$\frac{5^{2i}+1}{2} \cdot 481 = 1 \cdot 1 = 1 \pmod 4$$

olduğundan $r \in \mathbb{F}_5$ için

$$F(rx) = rF(x)$$

sağlanır. Üstelik

$$\begin{aligned} F(x) &= Tr_5(u_0 x^{481} + u_1 x^{13 \cdot 481} + u_2 x^{313 \cdot 481} + \lambda x) \\ &= Tr_5(u_0 x^{481} + u_1 x^5 + u_2 x^{601} + \lambda x) \end{aligned}$$

olur. x'in $5^4 + 5 = 630$uncu kuvvetini alırsak,

$$\begin{aligned} F(x^{630}) &= Tr_5(u_0 x^2 + u_1 x^{26} + u_2 x^{626} + \lambda x^{630}) \\ &= Tr_5(u_0 x^{5^0+1} + u_1 x^{5^2+1} + u_2 x^{5^4+1} + \lambda x^{5^4+5}) \end{aligned}$$

elde edilir.

$F(x^{630})$, $\mathbb{F}_5$ üzerinde bir kuadratik formdur. Lemma 31, Lemma 32 ve Lemma 33 kullanılarak ispat tamamlanır. ■

Bu teknik Trachtenberg [6], Helleseth ve Gong [1]'un çalışmaları sonucunda elde edilmiştir.

4.2 Gözlem

Gözlem 37. *SAGE kodu [22] kullanarak $p = 3$ için aşağıdaki gözlem elde edilmiştir.*

$n = 2m + 1$, $n \geq 5$, $u_0 = (p+1)/2$ ve $i = 1, 2, ..., m$, olmak üzere $u_i = (-1)^i$ ve $d = \frac{p^{n-2}+1}{p+1}$ olsun. Bu durumda

$$h(x) = Tr_n\left(\sum_{i=0}^{m} u_i x^{\frac{p^{2ki}+1}{2}d}\right)$$

şeklinde tanımlanan fonksiyonun

$$\hat{h}(\lambda) = \sum_{x\in\mathbb{F}_{p^n}} \omega^{h(x)+Tr_n(\lambda x)}$$

Walsh dönüşümü $\left\{0, \pm p^{\frac{n+k}{2}}\right\}$ değerlerini alır. λ değeri $\mathbb{F}_{p^n}$ sonlu cismini gezerken $\hat{h}(\lambda)$'nin dağılımı aşağıdaki gibidir:

0	*değeri*	$p^n - p^{n-k}$	*defa*
$-p^{(n+k)/2}$	*değeri*	$(p^{n-k} - p^{(n-k)/2})/2$	*defa*
$p^{(n+k)/2}$	*değeri*	$(p^{n-k} + p^{(n-k)/2})/2$	*defa.*

Not 38. *[1] ve [2]'deki teknikleri kullanarak bu gözlemi ispatlamaya çalıştık. İspata devam ederken elde edilen polinomun kuadratik form değil daha yüksek dereceli bir polinom olduğunu gördük. [1] ve [2]'de Walsh dönüşümünün dağılımının hesaplanması kuadratik formlara dayanmaktadır. Bu yüzden* $p = 5$, $n = 5$ *ve* $d = 481$ *durumu için ispat verilmiş ama buradaki yeni gözlemin ispatı tamamlanamamıştır.*

Örnek 39. $p = 3$, $n = 5$, $s = 2$ *ve* $k = 1$ *alalım.* $d = \frac{p^{n-2}+1}{p^k+1} = \frac{28}{4} = 7$ *durumunu inceleyelim. Bu durumda* $\mathbb{F}_{3^5}$*'den* $\mathbb{F}_3$*'e tanımlanan* $F(x)$ *için*

$$\begin{aligned} F(x) &= Tr_k^n(f(x^7) + \lambda x) \\ &= Tr_k^n\left(\sum_{i=0}^{m} u_i x^{\frac{p^{2i}+1}{2}7} + \lambda x\right) \end{aligned}$$

olur. $n = (2m+1)k$ *ve* $n = 5$ *olduğundan* $m = 2$ *bulunur. Ayrıca*

$$\begin{aligned} h(x) + Tr_n(\lambda x) &= Tr_k\left(Tr_k^n(f(x^7) + \lambda x)\right) \\ &= Tr_k\left(F(x)\right) \end{aligned}$$

sağlanır. Böylece

$$\begin{aligned} \frac{p^{2i}+1}{2} \cdot \frac{p^{n-2}+1}{p^k+1} &= \left(\frac{p^{2i}+1}{2}\right) \cdot (7)\,, \ i = 0, 1, 2 \\ &= 1 \ (\ mod\ 3-1) \end{aligned}$$

olur.

$$\frac{p^{2ki}+1}{2} \cdot \left(\frac{p^{n-2}+1}{p^k+1}\right) t = p^{2ki} + 1 \quad (\ mod\ 3^5 - 1)$$

denkleminin

$$\begin{aligned} i = 0 \ için \qquad & 7t \equiv 2 \qquad (\ mod\ 242) \\ i = 1 \ için \qquad & 35t \equiv 10 \qquad (\ mod\ 242) \\ i = 2 \ için \qquad & 287t \equiv 82 \qquad (\ mod\ 242) \end{aligned}$$

şartlarını sağlayan t *sayısı* 104*'tür. Fakat* $t = 104 = 3^4 + 2 \cdot 3^2 + 3^1 + 2 \cdot 3^0$ *olduğundan* λx^{104} *ifadesi kuadratik değildir.*

5. SONUÇ

Gong, Helleseth ve Hu; Helleseth-Gong dizisinin alt sınıfı olan ve kaydırılarak elde edilen yeni dizinin Walsh dönüşümü üzerine çalışmışlardır. Bu dizinin Walsh dönüşümünün dolayısıyla çapraz-korelasyonun 3 değerli olduğunu göstermiş ve henüz ispatlanamamış olan birçok desimasyon sayısı bulmuşlardır.

Biz de bu tezde bazı sayısal hesaplamalar yaptık ve bunların sonucuna bağlı olarak ispatlanması için başka bazı tekniklerin gerekli olduğunu görerek bir tahmin sunduk. Buna göre, $d = 481$ desimasyon sayısı için $p = 5$, $k = 1$, $n = 5$ ve $s = 2$ iken bu dağılımın 3 değerli olduğu ispatlanmıştır. Helleseth ve Gong'un makalesinde verilen ispatı henüz bulunmayan desimasyon sayıları ve farklı sonlu cisimlerdeki farklı k, n ve s değerleri için d değerleri bulmak ve dağılımlarını hesaplamak gelecek çalışmaları oluşturacaktır.

Kaynakça

[1] Gong G., Helleseth T. and Hu H., "A three-valued Walsh transform from decimations of Helleseth-Gong sequences," IEEE Trans. Inf. Theory, vol. 58, no. 2, pp. 1158-1162, Feb. 2012.

[2] Gong G., Helleseth T., Hu H. and Li C., "New three valued walsh transforms from decimations of Helleseth-Gong sequences," Proceeding of International Conference on Sequences and Their Applications SETA 2012, LNCS 7280, pp. 327-337, Sep. 2012.

[3] Helleseth T. and Gong G., "New nonbinary sequences with ideal two-level autocorrelation," IEEE Trans. Inf. Theory, vol. 48, no. 11, pp. 2868-2872, Nov. 2002.

[4] Trachtenberg H., "On the cross-correlation functions of maximal linear sequences, " Ph.D. thesis, Univ. Southern California, Los Angeles, CA, 1970.

[5] Helleseth T., "Some results about the cross-correlation function between two maximal linear sequences," Discr. Math., vol.48, no. 11, pp. 209-232, Nov. 1976.

[6] Lidl R. and Niederreiter H., Finite Fields. Cambridge University Press, Cambridge, 2nd edition, 1997.

[7] Dobbertin H., Helleseth T., Kumar P. and Martinsen H., "Ternary m-sequences with three-valued cross-correlation function: New decimations of Welch and Niho type," IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1473-1481, Apr. 2001.

[8] Gold R., "Maximal recursive sequences with 3-valued recursive cross-correlation functions," IEEE Trans. Inf. Theory, vol. 14, no. 1, pp. 154-156, Jan. 1968.

[9] Helleseth T., Kumar P. and Martinsen H., "A new family of ternary sequences with ideal two-level autocorrelation," Des., Codes, Cryptogr., vol. 23, no. 2, pp. 157-166, Jul. 2001.

[10] Golomb S. and Gong G., Signal design for goog correlation for wireless communication, crypography, and radar. Cambridge University Press, 2005.

[11] Jang J., Kim Y., No J., and Helleseth T., "New family of p-ary sequences with optimal correlation property and large linear span," IEEE Trans. Inf. Theory, vol. 50, no. 8, pp. 1839-1844, 2004.

[12] Tang X., Udaya P. and Fan P., "A new family of nonbinary sequences with three-level correlation property and large linear span," IEEE Trans. Inf. Theory, vol. 51, no. 8, pp. 2906-2914, 2005.

[13] Tang X., Udaya P. and Fan P., "New families of p-ary sequences from quadratic form with low correlation and large linear span," Proceeding of International Conference on Sequences and Their Applications SETA 2004, LNCS vol. 3486, pp. 255-265, Springer. 2004.

[14] Li C. and Helleseth T., "New nonbinary sequences families with low correlation and large linear span," Proceeding of IEEE International Symposium on Information Theory ISIT 2012, vol., pp. 1411-1415, 2012.

[15] Luo J. and Helleseth T., "Binary niho sequences with four valued cross-correlations," Proceeding of IEEE International Symposium on Information Theory ISIT 2012, vol., pp. 1216-1220, 2012.

[16] Ness G. and Helleseth T., "Cross-correlation of m-sequences of different lenghts," IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1637-1648, Apr. 2006.

[17] Ness G. and Helleseth T., "A new three valued cross-correlation between m-sequences of different lenghts," IEEE Trans. Inf. Theory, vol. 52, no. 10, pp. 4695-4701, Oct. 2006.

[18] Ness G. and Helleseth T., "A new family of four valued cross-correlation between m-sequences of different lenghts," IEEE Trans. Inf. Theory, vol. 53, no. 11, pp. 4308-4313 Nov. 2007.

[19] Johansen A. and Helleseth T., "A family of m-sequences with five valued cross-correlation," IEEE Trans. Inf. Theory, vol. 55, no. 2, pp. 880-887 Feb. 2009.

[20] Dilek H., Tilenbaev E., Saygı Z. and Ürtiş Ç., 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.

[21] Tilenbaev E., Dilek H., Saygı Z. and Ürtiş Ç., 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.

[22] The new SageMathCloud is in Beta Test, "http://www.sagemath.org/index.html".

EKLER

A. Algoritma

A.1 p=3 için

```
"""Defining variables..."""
import fractions;

m=5;
p=3;
k=1;
n=(2*m+1)*k;
q=p^n;

Fq.<a>=GF(q,'a');

"2.234 - 23523e-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 u(i):
    if i==0:
        return coerce(int, (p+1)/2);
    return (-1)^i;
```

```
d_degerleri = [];
d_karaliste = [];

f = open("/home_palamut2/etilenbaev/hasan/3/degerler.txt", "r");
for line in f:
    try:
        d = coerce(int, line);
        d_degerleri.append(d);
    except:
        print "degerler except";
f.close();

f = open("/home_palamut2/etilenbaev/hasan/3/karaliste.txt", "r");
for line in f:
    try:
        d = coerce(int, line);
        d_karaliste.append(d);
    except:
        print "karaliste except";
f.close();

f = open("/home_palamut2/etilenbaev/hasan/3/d_son_hali.txt", "r");
try:
    d = f.readline();
    d = coerce(int, d);
except:
    d = 1;
f.close();

if (d==1):
    z = 1;
    d_degerleri.append(d);
```

```
    f = open("/home_palamut2/etilenbaev/hasan/3/degerler.txt", "w");
    f.write( coerce(str,d) );
    f.write("\n");
    while (d*p^z %(q-1) != d):
        d_degerleri.append(d*p^z%(q-1));
        f.write( coerce(str, d*p^z%(q-1)) );
        f.write("\n");
        z = z+1;
    f.close();

    d = (p^n+1)/(p^k+1);
    z = 1;
    d_degerleri.append(d);
    f = open("/home_palamut2/etilenbaev/hasan/3/degerler.txt", "a");
    f.write( coerce(str,d) );
    f.write("\n");
    while (d*p^z %(q-1) != d):
        d_degerleri.append(d*p^z%(q-1));
        f.write( coerce(str, d*p^z%(q-1)) );
        f.write("\n");
        z = z+1;
    f.close();
    d=2;

while (d<q):
 if (fractions.gcd(d,q-1)!=1) or
                 (d in d_degerleri) or (d in d_karaliste):
        d = d + 1;
        continue;
   print "d = ",d, "durumu:\n";
   f = open("/home_palamut2/etilenbaev/hasan/3/d_son_hali.txt", "w");
   f.write( coerce(str, d) );
   f.close();
```

```
"""Defining h(x)..."""
def h(x):
     sum = 0;
     for i in range(m+1):
         sum = sum + u(i)*x^( (p^(2*k*i)+1)*d/2 );
     return sum.trace();

 """defining walsh transform"""
 def h_head(lam):
     sum = 0;
     for x in Fq:
         y = h(x)+(lam*x).trace();
         y = coerce( int, coerce(str,y) );
         sum = sum + exp(2*pi*I*( y )/p);
     return sum;

 print "\n tum degerler...\n";
 h_head_values = [];
 Unique_h_values = [];

 for x in range(12):
     value = h_head(a^x);
     value = numerical_approx( value );
     value = correct( value );
     print value;
     h_head_values.append(value);
     for i in h_head_values:
         if i not in Unique_h_values:
             Unique_h_values.append(i);
   if len(Unique_h_values)>3:
     f = open("/home_palamut2/etilenbaev/hasan/3/karaliste.txt", "a");
     f.write( coerce(str, d) );
     f.write("\n");
```

```
        d_karaliste.append(d);
        z = 1;
        while (d*p^z % (q-1) != d ):
                f.write( coerce(str, d*p^z % (q-1)) );
                f.write("\n");
                d_karaliste.append(d*p^z % (q-1));
                z = z + 1;
            f.close();
            break;

   else:
     d_degerleri.append(d);
     f = open("/home_palamut2/etilenbaev/hasan/3/degerler.txt", "a");
     f.write( coerce(str, d) );
     f.write("\n");

        z = 1;
        while (d*p^z % (q-1) != d ):
            d_degerleri.append(d*p^z % (q-1));
            f.write( coerce(str, d*p^z%(q-1)) );
            f.write( "\n" );
            z = z + 1;
        f.close();
    while (d in d_karaliste) or (d in d_degerleri):
        d = d + 1;
```

A.2 p=5 için

```
"""Defining variables..."""
import fractions;
```

```
m=2;
p=5;
k=1;
n=(2*m+1)*k;
q=p^n;

Fq.<a>=GF(q,'a');

"2.234-23523e-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 u(i):
    if i==0:
        return coerce(int, (p+1)/2);
    return (-1)^i;

d_degerleri = [];
d_karaliste = [];

f =open("/home_palamut2/hasan/5/m=2/degerler.txt", "r");
for line in f:
    try:
        d = coerce(int, line);
        d_degerleri.append(d);
    except:
        print "degerler except";
f.close();

f =open("/home_palamut2/hasan/5/m=2/karaliste.txt", "r");
```

```
for line in f:
    try:
       d = coerce(int, line);
       d_karaliste.append(d);
    except:
       print "karaliste except";
f.close();

f =open("/home_palamut2/hasan/5/m=2/d_son_hali.txt", "r");
try:
   d = f.readline();
   d = coerce(int, d);
except:
    d = 1;
f.close();

if (d==1):
   z = 1;
   d_degerleri.append(d);
   f = open("/home_palamut2/hasan/5/m=2/degerler.txt", "w");
   f.write( coerce(str,d) );
   f.write("\n");
   while (d*p^z %(q-1) != d):
        d_degerleri.append(d*p^z%(q-1));
        f.write( coerce(str, d*p^z%(q-1)) );
        f.write("\n");
        z = z+1;
   f.close();

   d = (p^n+1)/(p^k+1);
   z = 1;
   d_degerleri.append(d);
   f = open("/home_palamut2/hasan/5/m=2/degerler.txt", "a");
```

```
   f.write( coerce(str,d) );
   f.write("\n");
   while (d*p^z %(q-1) != d):
        d_degerleri.append(d*p^z%(q-1));
        f.write( coerce(str, d*p^z%(q-1)) );
        f.write("\n");
        z = z+1;
    f.close();
    d=2;

while (d<q):
if (fractions.gcd(d,q-1)!=1) or
               (d in d_degerleri) or (d in d_karaliste):
        d = d + 1;
        continue;
   print "d = ",d, "durumu:\n";
   f = open("/home_palamut2/hasan/5/m=2/d_son_hali.txt", "w");
   f.write( coerce(str, d) );
   f.close();
   """Defining h(x)..."""
   def h(x):
        sum = 0;
        for i in range(m+1):
            sum = sum + u(i)*x^( (p^(2*k*i)+1)*d/2 );
        return sum.trace();

    """defining walsh transform"""
    def h_head(lam):
        sum = 0;
        for x in Fq:
            y = h(x)+(lam*x).trace();
            y = coerce( int, coerce(str,y) );
            sum = sum + exp(2*pi*I*( y )/p);
```

```
    return sum;

print "\n tum degerler...\n";
h_head_values = [];
Unique_h_values = [];

for x in range(12):
    value = h_head(a^x);
    value = numerical_approx( value );
    value = correct( value );
    print value;
    h_head_values.append(value);
    for i in h_head_values:
        if i not in Unique_h_values:
            Unique_h_values.append(i);
    if len(Unique_h_values)>3:
      f = open("/home_palamut2/hasan/5/m=2/karaliste.txt", "a");
      f.write( coerce(str, d) );
      f.write("\n");
      d_karaliste.append(d);
      z = 1;
      while (d*p^z % (q-1) != d ):
            f.write( coerce(str, d*p^z % (q-1)) );
            f.write("\n");
            d_karaliste.append(d*p^z % (q-1));
            z = z + 1;
        f.close();
        break;

else:
  d_degerleri.append(d);
  f = open("/home_palamut2/hasan/5/m=2/degerler.txt", "a");
  f.write( coerce(str, d) );
```

```
      f.write("\n");

        z = 1;
        while (d*p^z % (q-1) != d ):
            d_degerleri.append(d*p^z % (q-1));
            f.write( coerce(str, d*p^z%(q-1)) );
            f.write( "\n" );
            z = z + 1;
        f.close();
    while (d in d_karaliste) or (d in d_degerleri):
        d = d + 1;
```

A.3 p=7 için

```
"""Defining variables..."""
import fractions;

m=3;
p=7;
k=1;
n=(2*m+1)*k;
q=p^n;
Fq.<a>=GF(q,'a');
"2.234-23523e-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 u(i):
    if i==0:
        return coerce(int, (p+1)/2);
    return (-1)^i;
```

```
d_degerleri = [];
d_karaliste = [];

f = open("/home_palamut2/hasan/7/degerler.txt", "r");
for line in f:
    try:
        d = coerce(int, line);
        d_degerleri.append(d);
    except:
        print "degerler except";
f.close();

f = open("/home_palamut2/hasan/7/karaliste.txt", "r");
for line in f:
    try:
        d = coerce(int, line);
        d_karaliste.append(d);
    except:
        print "karaliste except";
f.close();
f = open("/home_palamut2/hasan/7/d_son_hali.txt", "r");
try:
    d = f.readline();
    d = coerce(int, d);
except:
    d = 1;
f.close();
if (d==1):
  z = 1;
  d_degerleri.append(d);
  f = open("/home_palamut2/hasan/7/degerler.txt", "w");
  f.write( coerce(str,d) );
  f.write("\n");
```

```
  while (d*p^z %(q-1) != d):
        d_degerleri.append(d*p^z%(q-1));
        f.write( coerce(str, d*p^z%(q-1)) );
        f.write("\n");
        z = z+1;
  f.close();
  d = (p^n+1)/(p^k+1);
  z = 1;
  d_degerleri.append(d);
  f = open("/home_palamut2/hasan/7/degerler.txt", "a");
  f.write( coerce(str,d) );
  f.write("\n");
  while (d*p^z %(q-1) != d):
        d_degerleri.append(d*p^z%(q-1));
        f.write( coerce(str, d*p^z%(q-1)) );
        f.write("\n");
        z = z+1;
    f.close();
    d=2;
while (d<q):
if (fractions.gcd(d,q-1)!=1) or
                (d in d_degerleri) or (d in d_karaliste):
        d = d + 1;
        continue;
  print "d = ",d, "durumu:\n";
  f = open("/home_palamut2/hasan/7/d_son_hali.txt", "w");
  f.write( coerce(str, d) );
  f.close();
  """Defining h(x)..."""
    def h(x):
        sum = 0;
        for i in range(m+1):
            sum = sum + u(i)*x^( (p^(2*k*i)+1)*d/2 );
```

```
    return sum.trace();
"""defining walsh transform"""
def h_head(lam):
    sum = 0;
    for x in Fq:
        y = h(x)+(lam*x).trace();
        y = coerce( int, coerce(str,y) );
        sum = sum + exp(2*pi*I*( y )/p);
    return sum;

print "\n tum degerler...\n";
h_head_values = [];
Unique_h_values = [];

for x in range(12):
    value = h_head(a^x);
    value = numerical_approx( value );
    value = correct( value );
    print value;
    h_head_values.append(value);
    for i in h_head_values:
        if i not in Unique_h_values:
            Unique_h_values.append(i);
if len(Unique_h_values)>3:
  f = open("/home_palamut2/hasan/7/karaliste.txt", "a");
    f.write( coerce(str, d) );
    f.write("\n");
    d_karaliste.append(d);
    z = 1;
    while (d*p^z % (q-1) != d ):
            f.write( coerce(str, d*p^z % (q-1)) );
            f.write("\n");
            d_karaliste.append(d*p^z % (q-1));
```

```
                z = z + 1;
            f.close();
            break;
  else:
    d_degerleri.append(d);
    f = open("/home_palamut2/hasan/7/degerler.txt", "a");
    f.write( coerce(str, d) );
    f.write("\n");
        z = 1;
        while (d*p^z % (q-1) != d ):
            d_degerleri.append(d*p^z % (q-1));
            f.write( coerce(str, d*p^z%(q-1)) );
            f.write( "\n" );
            z = z + 1;
        f.close();
    while (d in d_karaliste) or (d in d_degerleri):
        d = d + 1;
```

A.4 d=481 için

```
"""Defining variables..."""
import fractions;

m=2;
p=5;
k=1;
n=(2*m+1)*k;
q=p^n;

Fq.<a>=GF(q,'a');
```

```
"2.234-23523e-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 u(i):
    if i==0:
        return coerce(int, (p+1)/2);
    return (-1)^i;

d_degerleri = [];
d_karaliste = [];


d = 481;

"""Defining h(x)..."""
def h(x):
    sum = 0;
    for i in range(m+1):
        sum = sum + u(i)*x^( (p^(2*k*i)+1)*d/2 );
    return sum.trace();

"""defining walsh transform"""
def h_head(lam):
    sum = 0;
    for x in Fq:
        y = h(x)+(lam*x).trace();
        y = coerce( int, coerce(str,y) );
        sum = sum + exp(2*pi*I*( y )/p);
    return sum;
```

```
print "\n tum degerler...\n";
h_head_values = [];
Unique_h_values = [];

for x in range(q-1):
    value = h_head(a^x);
    value = numerical_approx( value );
    value = correct( value );
    print value;
    h_head_values.append(value);
    for i in h_head_values:
        if i not in Unique_h_values:
            Unique_h_values.append(i);
    if len(Unique_h_values)>3:
        d_karaliste.append(d);
        z = 1;
        while (d*p^z % (q-1) != d ):
            d_karaliste.append(d*p^z % (q-1));
            z = z + 1;
        break;

else:
    d_degerleri.append(d);
    z = 1;
    while (d*p^z % (q-1) != d ):
        d_degerleri.append(d*p^z % (q-1));
        z = z + 1;
```

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: DİLEK, Hasan
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 1988, Muğla
Medeni hali	: Bekar
Telefon	: +90 555 8451147
e-mail	: hdilek@etu.edu.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Y. Lisans	TOBB Ekonomi ve Teknoloji Üniversitesi	2013
Lisans	Hacettepe Üniversitesi	2011

Yabancı Dil

İngilizce (iyi)

Yayınlar

1) Dilek H., Tilenbaev E., Saygı Z. and Ürtiş Ç., 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.

2) Tilenbaev E., Dilek H., Saygı Z. and Ürtiş Ç., 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.