FREKANS ATLAMALI DİZİLER

KÜBRA BAYRAKTAR

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ARALIK 2010
ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Ünver KAYNAK
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Prof. Dr. Ömer AKIN
Matematik Anabilim Dalı Başkanı

Kübra BAYRAKTAR tarafından hazırlanan FREKANS ATLAMALI DİZİLER adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

_____

Yrd. Doç. Dr. Zülfükar SAYGI
Tez Danışmanı

Tez Jüri Üyeleri

Başkan : Prof. Dr. Ferruh ÖZBUDAK _____

Üye : Yrd. Doç. Dr. Zülfükar SAYGI _____

Üye : Yrd. Doç. Dr. Çetin ÜRTİŞ _____

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.

(İmza)

(Adı Soyadı)

Üniversitesi : **TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü : **Fen Bilimleri**
Anabilim Dalı : **Matematik**
Tez Danışmanı : **Yrd. Doç. Dr. Zülfükar SAYGI**
Tez Türü ve Tarihi : **Yüksek Lisans – Aralık 2010**

Kübra BAYRAKTAR

FREKANS ATLAMALI DİZİLER

ÖZET

Bu tezin amacı, Elektronik, İletişim ve Bilgisayar Mühendisliği'ndeki kodlarda bilgi iletimi sağlamak için gerekli olan FHS lerin cebirsel yolla oluşturulmasıdır. Bu amaçla bazı makaleler incelenmiş ve FHS üretim metotlarına dayalı detaylı bir anlatım yapılmıştır. Bu anlatımın içeriğinde FHS ve optimal FHS nin tanımı, optimallik kriterleri vardır. Optimallik için alt sınırlara da yer verilmiştir. Ayrıca bu anlatımlardan sonra makalelerdeki optimal FHS oluşturmaya dayalı yöntemleri inceleyip bu yöntemleri iyice anladıktan sonra, hepsinde ortak ve sonlu cisimlerde de uygulaması olan bir yöntem olan, iz fonksiyonu yardımıyla FHS oluşturanlara bakılmıştır. Makalelerde verilen örnekler detaylı bir şekilde anlatılmıştır. Bu anlatımdan sonra da makalelerdeki oluşumları sağlamaya yönelik başka örnekler de MAGMA programı yardımıyla incelenmiştir. Bunun ötesinde makalelerdeki oluşumları sağlamayan parametrelerin neden çalışmadığına dair örnekler de incelenmiştir. Bu sorun net bir yanıt bulamamakla beraber, cevap aramak için teoremlerin ispatlarına bakılmıştır. Bu tezde bu ispatlara yer verilmemiştir, ancak sadece bazı somut örnekler için MAGMA programı sayesinde incelemeler yapılmıştır. Sonuçta ise bu üretim metotları için açıkça bir karşılaştırma yapılmıştır. Birbirini kapsayan ve birinin diğerinin dışında kaldığı parametreler gözlemlenmiş ve tartışılmıştır. Sonuç olarak bu yapılar için bir tablo oluşturulmuş ve bu tablo bize hangi parametrenin nerede olduğuna dair kesin bir sonuç vermiştir. Yeni parametreler ve farklı yöntemler arayışımız devam etmekte olup, başka fonksiyonlar yardımıyla da incelenebilecek olan bu FHS yöntemlerinden, iz fonksiyonu yardımıyla oluşturulmuş olanları için başka yeni parametreler de bulunabilir.

Anahtar Kelimeler: Frekans atlamalı diziler, cebirsel frekans atlamalı dizi yöntemleri, optimal frekans atlamalı diziler, optimal frekans atlamalı dizi çiftleri, optimal frekans atlamalı dizi ailesi.

University : **TOBB Economics and Technology University**
Institute : **Institute of Natural and Applied Sciences**
Science Programme : **Mathematics**
Supervisor : **Assistant Professor Dr. Zülfükar SAYGI**
Degree Awarded and Date : **M.Sc. – December 2010**

Kübra BAYRAKTAR

FREQUENCY HOPPING SEQUENCES

ABSTRACT

Purpose of this thesis is algebraic construction of frequency hopping sequences(FHS) which are needed for securing transmission of information in codes of Electronic, Telecommunication and Computer Engineering. It is studied for this purpose ve there is an detailed expression about constructions of generating FHS. In this expression,there are definitions of FHS, optimal FHS and criterions of optimality. There are also lower bounds for optimality. Algebraic constructions of optimal FHS are analysed in some papers. These constructions are abstracted quite well. Especially it is looked trace functions to form optimal FHS. This trace function is also an application of Finite Fields. The examples given in some papers are analysed too detailed. Some other examples are also analysed by the aid of MAGMA programme. Beyond these analyses, we looked at some other examples that it is not given in the papers. But there is no answer to this. We also looked at the proofs of theorems and lemmas, yet there is no proof in this thesis. We looked at just for some crude examples. In conclusion we did a clear comparison for the constructions. We did the table for distinguishing distinctions among parametres. And this table answered us exactly. One can find other parametres and other functions to construct like these optimal FHS.

Keywords: Frequency hopping sequences, algebraic constructions of optimal frequency hopping sequence, optimal Frequency hopping sequences, optimal Frequency hopping sequence pair, optimal Frequency hopping sequences family.

TEŞEKKÜR

Çalışmalarım boyunca bana yol gösterip katkıda bulunan, beni yönlendiren hocam Yrd. Doç. Dr. Zülfükar SAYGI' ya, Onun değerli yardımlarına, yine kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Matematik Bölümü öğretim üyelerine teşekkür ederim. Ayrıca bu tez Cebirsel Eğriler ve Üssel Toplamlar Kullanarak Bazı Kriptografik Uygulamalar adlı TÜBİTAK projesi kapsamında yürütülmüştür.

Yine çalışmalarım boyunca yazdığı kodlarla tezime katkıda bulunan ve çalışmalarımda her açıdan bana yardım eden ofis ve proje arkadaşım Seda KAHRAMAN' a ve manevi olarak bana destek olan diğer bütün ofis arkadaşlarıma teşekkür ederim.

Son olarak desteklerini benden hiçbir zaman esirgemeyen, beni yetiştirip bugünlere gelmemi sağlayan sevgili anneme, babama, ablama ve minik yeğenim Kayra' ya çok müteşekkirim.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

İÇİNDEKİLER vii

ÇİZELGELERİN LİSTESİ ix

KISALTMALAR x

1. GİRİŞ 1

1.1. Genel Bilgiler 1

1.2. Frekans Atlamalı Diziler (FHS) 3

1.3. Bilinen Optimallik Sınırları 7

2. CEBİRSEL YÖNTEMLER 12

2.1. Genel Üretim Metodu 14

2.1.1. [4] deki Diziler 15

2.1.2. [5] deki Diziler 20

2.1.3. [9] daki Diziler 23

2.1.4. [3] deki Diziler ($p=2$ durumu) 26

2.1.5. [3] deki Diziler ($p \neq 2$ durumu) 29

3. KARŞILAŞTIRMALAR 33

3.1. [4] ile [5] deki Parametrelerin Karşılaştırılması 35

3.2. [4] ile [9] daki Parametrelerin Karşılaştırılması 36

3.3. [5] ile [9] daki Parametrelerin Karşılaştırılması 37

KAYNAKLAR 38

EKLER 40

ÖZGEÇMİŞ 43

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 1.1. *X, Y, Z* dizileri için Hamming korelasyon değerleri 4
Çizelge 3.1. Çizelge 3.1. [4,5,9,3] makalelerindeki dizilerin parametreleri 33

KISALTMALAR

Kısaltmalar Açıklama

FHS	Frekans Atlamalı Diziler (Frequency Hopping Sequence)
FHSS	Frekans Atlamalı Yayılı İzge (Frequency Hopping Spread Spectrum)
DSSS	Dogrudan Sıra Yayılı İzge (Direct Sequence Spread Spectrum)
MA	Çoklu Erişim (Multiple Access)
CDMA	Kod Bölmeli Çoklu Erişim (Code Division Multiple Access)
FHMA	Frekans Atlamalı Çoklu Erişim (Frequency Hopping Multiple Access)
FH-CDMA	Frekans Atlamalı Kod Bölmeli Çoklu Erişim (Frequency Hopping Code Division Multiple Access)
S(n;F)	F alfabesinde, n uzunluklu bütün dizilerin kümesi
H(X)	X dizisinin Hamming oto-korelasyonu
H(X,Y)	X ve Y dizilerinin Hamming kros-korelasyonu
M(U)	U ailesinin Hamming korelasyonu
(n,k,λ)	Eleman sayısı k olan alfabe üzerinde, uzunluğu n olan X dizileri için H(X)= λ iken elde edilen dizi.
$(n,k,\lambda;N)$	Eleman sayısı k olan alfabe üzerinde, uzunluğu n olan X dizileriyle oluşturulan aile için H(X)= λ ve N de ailedeki eleman sayısını göstermektedir.
F_{q^m}	q^m elemanlı sonlu cisim
w(X)	X dizisinin Hamming ağırlığı
$d_H(X,Y)$	X ve Y dizilerinin Hamming uzaklığı

BÖLÜM 1.

1.GİRİŞ

1.1. Genel Bilgiler

Frekans atlamalı yayılı izge (frequency-hopping spread spectrum, FHSS) ve doğrudan sıra yayılı izge (direct sequence spread spektrum, DSSS) temel iki yayılım kodlama teknolojisidir. FHSS, birçok frekans kanalı arasından bir tanesini seçerek radyo sinyallerini iletme yöntemidir. Bu seçimi frekansı ileten ve frekans iletilen kişiler tarafından bilinen rastgele bir diziyi kullanarak yapar. Bu rastgele dizi, temelde bir kurala göre hazırlanmış olmasına rağmen, karmaşıklığı ve ender rastlanmasından dolayı rastgele adını alır. FHSS yöntemi, çoklu erişim metodu olarak frekans atlamalı kod bölmeli çoklu erişim şemasında (frequency-hopping code division multiple access**,** FH-CDMA) kullanılır[20]. Çoklu erişim metodu, bilgisayar iletişimi ağlarında, birden fazla uç noktanın, bir iletim ortamına erişip iletim yapabilmeleri özelliğidir. Bu iletimi merkezi bir zaman bölüşümü ya da frekans bölüşümü olmadan yapar. Çoklu erişim kod bölmeli, zaman bölmeli ya da frekans bölmeli olarak yapılır. FHSS yöntemi için kod bölmeli çoklu erişimden (code division multiple access, CDMA) faydalanılır. DSSS ise, iletişimde kullanılan bir tekniktir. İletilen sinyalin bant genişliği ne kadar fazlaysa o kadar hızlı iletim gerçekleşir. Bu yöntemlerdeki 'Yayılı izge' ise, taşıyıcı sinyallerin bir cihazın iletim frekansı bant genişliği (spektrum) üzerinden gerçekleşir[18]. Daha fazla bilgi için [18], [20] ve [1] e bakılabilir.

FHS ler FH-CDMA iletişim sisteminin tamamlayıcı bir parçasıdır. FHS, FHSS metodu için yararlıdır. Yukarıda bahsedilen sistemlerden biri olan FHMA(frequency hopping multiple access, frekans atlamalı çoklu erişim) sistemleri için veri gönderme tekniğinden faydalanılabilir. Ayrıca birçok iletişim sistemlerinin yayılı izgesinde da FHS etkilidir. Askeri iletişimlerde kullanılan anti sinyal karıştırıcı(antijamming) için, güvenlik ve çoklu erişim yöntemlerinde, ayrıca günümüzde askeri olmayan iletişimlerde de, bluetooth, kablosuz ağ iletişimlerinde (ultra-wide band, UWB) de,

FHS kullanılmaktadır. Bluetooth, temelde FHS leri kullanarak, bilgi alışverişi sağlar. Bluetoothla herhangi bir veriyi bilgisayara ya da cep telefonuna doğru bir şekilde aktarmak için FHS lerden yararlanılmaktadır.

Yukarıda saydığımız çeşitli sistemler için kullanılan FHS lerin, iyi Hamming korelasyonuna sahip olması gerekmektedir.

Bu tezde ise FHS, Hamming korelasyonu ve optimal dizi tanımları anlatılıp, iyi Hamming korelasyonuna sahip olanları incelenecektir. FHS nin çeşitli üretim yolları vardır. Bu yollar çeşitli fonksiyonlarla yapılabilir. Biz burada iz fonksiyonu yardımıyla oluşturulmuş olan cebirsel oluşum yöntemlerini inceleyeceğiz. Bu yöntemlerle bulunan FHS lerin içinde en iyi hamming korelasyona sahip olanları bulmanın bazı kısa yöntemlerine dair alt sınırlar verip, bunların yanı sıra optimal dizi şartlarını sağlayan cebirsel oluşumlardan 5 tanesini detaylı bir şekilde anlatacağız. Bu detayın içinde en iyi olma şartlarını sağlayan/sağlamayan örnekler bulunmaktadır. Ayrıca MAGMA programı tarafından hesaplanan dizilerin korelasyonlarına da bakılıp optimallikle ilgili doğrulukları teyit edilecektir. [5],[4],[9] ve [3] numaralı makalelerde anlatılan iz fonksiyonu kullanılan cebirsel yöntemler, karşılaştırmalı tabloyla beraber ortaya konacak ve parametrelerin teker teker kıyaslaması yapılıp, aradaki farklar/benzerlikler ortaya konup bir tablo hazırlanacaktır. Birbirini içeren, kesişen parametreler açıkça ortaya konacaktır. Böylece FHS lerin cebirsel üretim yöntemlerinden birisi bütün yönleriyle ele alınmış olunacaktır.

1.2. Frekans Atlamalı Diziler(FHS)

Olabilecek bütün frekans değerlerinden oluşan $F = \{f_o, f_1, \cdots, f_{k-1}\}$ kümesine **alfabe** denir. n pozitif bir tam sayı olmak üzere, F kümesindeki elemanlarla oluşturulan n uzunluğundaki bütün dizilerin kümesi $S(n;F)$ ile gösterilir,

$$S(n;F) = \{X = (x_1, \ldots, x_n) : x_i \in F \text{ ve } i = 1, 2, ..., n\}.$$

$S(n;F)$ kümesinden alınan herhangi bir elemana F üzerinde uzunluğu n olan **frekans atlamalı dizi (frequency hopping sequence)**, kısaca **FHS**, denir.

Örnek 1: $F = \mathbf{Z}_3 = \{0, 1, 2\}$ ve $n = 13$ olsun.

$S(13;\mathbf{Z}_3) = \{(a_1, a_2, \ldots, a_{13}) : a_i \in \mathbf{Z}_3$ ve $i=1,2,...,13\}$ kümesinde X, Y ve Z dizileri aşağıdaki gibi tanımlanabilir:

$X = (0, 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1),$

$Y = (0, 1, 1, 1, 2, 1, 1, 0, 0, 1, 2, 0, 2),$

$Z=(1, 1, 1, 0, 2, 2, 2, 0, 1, 1, 2, 2, 1).$

O halde X, Y ve Z dizileri $\mathbf{Z}_3$ üzerinde uzunluğu 13 olan birer FHS olurlar.

İki dizi arasındaki uzaklığı hesaplamak için hamming korelasyonu tanımına ihtiyaç duyarız. FHS ler için Hamming korelasyonu aşağıdaki gibi tanımlanır.

Tanım 1.1: (Hamming Korelasyonu) $S(n;F)$ kümesinden alınan herhangi iki X,Y dizisi, $X=(x_1, x_2, \ldots, x_n)$ $Y=(y_1, y_2, \ldots, y_n)$ için, t zamanda gecikmeyi göstermek üzere, Hamming korelasyonu $H_{X,Y}$,

$$H_{X,Y}(t) = \sum_{i=0}^{n-1} h(x_i, y_{i+t}), \quad 0 \le t < n \ , \tag{1.1}$$

olarak tanımlanır. Burada $h(x,y) = \begin{cases} 1, & x = y \text{ ise} \\ 0, & x \neq y \text{ ise} \end{cases}$ olur ve yer indisi $i+t$ üzerindeki bütün işlemler, dizinin uzunluğu n olduğu için, ($mod\ n$) de hesaplanır.

Örnek 2: Hamming korelasyon hesabını, Örnek1 de verilen *X, Y* ve *Z* dizileri için inceleyelim.

X = (0, 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1),

Y = (0, 1, 1, 1, 2, 1, 1, 0, 0, 1, 2, 0, 2),

Z=(1, 1, 1, 0, 2, 2, 2, 0, 1, 1, 2, 2, 1).

Verilen herhangi iki dizi için Hamming korelasyonu

$$H_{X,Y}(t) = \sum_{i=0}^{12} h(x_i, y_{i+t}),\ 0 \le t<13$$

olduğundan dizilerin korelasyonları için Çizelge 1.1 elde edilir.
Burada dizilerin *i+t* indis değerleri, mod 13 e göre hesaplanır.

Çizelge 1.1. *X, Y, Z* dizileri için Hamming korelasyon değerleri

t	$H_{X,X}(t)$	$H_{Y,Y}(t)$	$H_{Z,Z}(t)$	$H_{X,Y}(t)$	$H_{X,Z}(t)$	$H_{Y,Z}(t)$
0	13	13	13	4	4	6
1	4	4	7	4	4	3
2	4	4	3	4	3	2
3	4	4	2	4	4	4
4	4	4	4	4	7	2
5	4	4	4	4	5	4
6	4	4	6	4	2	6
7	4	4	6	4	1	8
8	4	4	4	4	6	5
9	4	4	4	4	5	6
10	4	4	2	4	6	3
11	4	4	3	4	5	4
12	4	4	7	4	4	6

FHS dizilerinin birbirlerinden ayırt edilebilmesi için olası bütün t değerleri üzerinden Hamming korelasyonlarının maksimum değerleri göz önüne alınır.

Tanım 1.2: $S(n;F)$ kümesinden alınan herhangi iki farklı *X,Y* dizisi için;

$$H(X) \quad = \underset{1\le t<n}{maks}\left\{H_{X,X}(t)\right\} \tag{1.2}$$

$$H(X,Y) = \underset{0\le t<n}{maks}\left\{H_{X,Y}(t)\right\} \tag{1.3}$$

$$M(X,Y) = maks\left\{H(X),H(Y),H(X,Y)\right\} \tag{1.4}$$

olarak tanımlanır. Tanım 1.2 deki (1.2) eşitliği bir dizinin kendisiyle korelasyonu olan, Hamming oto-korelasyonu, (1.3) eşitliği bir dizinin farklı bir diziyle korelasyonu olan, Hamming kros-korelasyonudur.

Tezin bundan sonraki bölümlerinde, eleman sayısı *k* olan bir alfabe üzerinde, *n* uzunluklu bir *X* FHS dizisi için, $\lambda = H(X)$ olmak üzere, (n,k,λ)-FHS gösterimi kullanılacaktır.

Örnek 3: *X = (0, 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1),*

Y = (0, 1, 1, 1, 2, 1, 1, 0, 0, 1, 2, 0, 2),

Z=(1, 1, 1, 0, 2, 2, 2, 0, 1, 1, 2, 2, 1)

olmak üzere Örnek 2 de elde edilen Çizelge 1.1 den

$$H(X) \quad = \underset{1\le t<13}{maks}\left\{H_{X,X}(t)\right\} = 4,$$

$$H(Y) \quad = \underset{1\le t<13}{maks}\left\{H_{Y,Y}(t)\right\} = 4,$$

$$H(Z) \quad = \underset{1\le t<13}{maks}\left\{H_{Z,Z}(t)\right\} = 7$$

olarak bulunur. Benzer şekilde;

$$H(X,Y) = \underset{0\le t<n}{maks}\left\{H_{X,Y}(t)\right\} = 4,$$

$$H(X,Z) = \underset{0\le t<13}{maks}\left\{H_{X,Z}(t)\right\} = 7,$$

$$H(Y,Z) = \underset{0\le t<13}{maks}\left\{H_{Y,Z}(t)\right\} = 8.$$

Yukarıdaki değerler kullanılarak;

M(X, Y)=maks{4, 4, 4) =4,

M(X, Z)=maks{4, 7, 7}=7,

M(Y,Z)=maks{4, 7, 8}=8

elde edilir. Dolayısıyla X dizisi (*13,3,4*)-FHS, Y dizisi (*13,3,4*)-FHS, Z dizisi (*13,3,7*)-FHS olur.

Hamming korelasyon değerlerine bakılarak, dizilerin optimallik kriterleri şu şekilde verilir [11].

1. $X \in S(n;F)$ olmak üzere, eğer her $X' \in S(n;F)$ için $H(X) \le H(X')$ eşitsizliği sağlanırsa X e **optimal dizi** denir.

2. $X, Y \in S(n;F)$ ve $X \neq Y$ olmak üzere, eğer birbirinden farklı herhangi $X', Y' \in S(n;F)$ için $M(X,Y) \le M(X',Y')$ eşitsizliği sağlanırsa X,Y dizilerine **optimal dizi çifti** denir.

3. $S(n;F)$ kümesinin herhangi bir alt kümesi K olsun. K kümesinden alınan herhangi iki farklı dizi, optimal dizi çifti oluşturuyorsa K kümesine **optimal aile** denir.

Uyarı: $S(n;F)$ kümesinde $|F| = k$ olmak üzere; k^n farklı dizi bulunduğundan, bu kümeden alınan herhangi bir X dizisinin optimal olup olmadığına tanım yardımıyla karar vermek güç ve uzun bir süreçtir. Bu nedenle bir sonraki bölümde özetleyeceğimiz sınırlar kullanılabilir.

1.3. Bilinen Optimallik Sınırları

Bir önceki bölümde verilen optimallik kriterlerinin tanımları ışığında, bir dizinin optimal olabilmesi için, en küçük Hamming korelasyonlu dizi optimal olacağından, o dizinin Hamming oto-korelasyonunun, yani (1.2) denkleminin, minimum olması gerekmektedir. Bir dizi çiftinin optimal olabilmesi için o dizi çifti için tanımlanan Hamming oto-korelasyonlarının ve Hamming kros-korelasyonlarının maksimumunun, yani (1.4) denklemindeki ifadenin, minimum olması gerekmektedir. Optimal bir ailenin de optimal dizi çiftlerinden oluşması ve olabildiğince fazla sayıda farklı eleman içermesi gerekmektedir. Dolayısıyla bir dizinin optimal olması için, minimum değerlerine ilişkin, aşağıda verilen Lempel-Greenberger alt sınırı kullanılabilir.

Lemma 1.3: [11] Her X (n,k,λ)-FHS dizisi için, ε, $n \equiv \varepsilon \pmod{k}$ olan en küçük negatif olmayan tam sayı olmak üzere;

$$H(X) \geq \left\lceil \frac{(n-\varepsilon)(n+\varepsilon-k)}{k(n-1)} \right\rceil \tag{1.5}$$

eşitsizliği sağlanır. Burada $\lceil x \rceil$, x ten büyük veya x e eşit olan en küçük tam sayıdır.

Dizilerin optimal olması için, Lemma 1.3 ün sonucu olarak bulunan aşağıdaki alt sınır da kullanılabilir.

Sonuç 1.4: [6] Her X (n,k,λ)-FHS dizisi için, $n=sk+\varepsilon$, $0 \leq \varepsilon < k-1$ olmak üzere;

$$H(X) \geq \begin{cases} s, & n \neq k \text{ ise} \\ 0, & n = k \text{ ise} \end{cases} \tag{1.6}$$

eşitsizliği sağlanır.

Sonuç 1.5: [6] X (n,k,λ)-FHS dizisi için, $n>k$, $n=sk+\varepsilon$, $0\le\varepsilon<k-1$ olmak üzere, $H(X)=\left\lfloor \frac{n}{k} \right\rfloor$=s ise X optimaldir. Burada $\lfloor x \rfloor$, x ten küçük veya x e eşit olan en büyük tam sayıdır.

Örnek 4: Örnek 2 de verilen X, Y ve Z dizileri için $k=3$, $n=13$ olduğundan Lemma 1.3. de kullanılan $n \equiv \varepsilon \pmod{k}$ değeri $\varepsilon \equiv 1 \pmod 3$ olarak bulunur. Buna göre, (1.5) denkleminde sağ taraf $\left\lceil \frac{(13-1)(13+1-3)}{3(13-1)} \right\rceil = 4$ bulunur. O halde X ve Y dizileri için, Örnek 2 den, $H(X)=4$, $H(Y)=4$ ve $H(Z)=7$ olduğundan X ve Y dizileri optimaldir. Z dizisi ise optimal değildir.

Şimdi de Lempel-Greenberger alt sınırı dizi çifti için verilecektir.

Teorem 1.6: [11] Ayrık iki X, Y (n,k,λ)-FHS için;

$$M(X,Y) \ge \frac{\sum_{I=0}^{k-1}(d_i^{\,2}+e_i^{\,2}+d_i e_i)-2n}{3n-2} \tag{1.7}$$

eşitsizliği sağlanır. Burada d_i, e_i, $0 \le$ i $\le$ k-1, X ve Y dizileri için $d_i = \mu_X(f_i)$, $e_i = \mu_Y(f_i)$. Burada $\mu_X(a)$ fonksiyonu X dizisindeki a ların sayısını, $\mu_Y(a)$ fonksiyonu Y dizisindeki a ların sayısını göstermektedir.

Örnek 5: $\mathbf{Z}_3 = \{0,1,2\}$ alfabe kümesi üzerinde tanımlı,

X = (0, 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1),

Y = (0, 1, 1, 1, 2, 1, 1, 0, 0, 1, 2, 0, 2)

dizileri için X dizisindeki 0 ların sayısı 4, yani $d_0 = 4$, 1 lerin sayısı 3, yani $d_1 = 3$, 2 lerin sayısı 6, yani $d_2 = 6$ olduğu görülür. Benzer şekilde Y dizisi için $e_0 = 4$, $e_1 = 6$, $e_2 = 3$ olur. O halde (1.9) denkleminin sağ tarafı

$\frac{4^2+4^2+16+3^2+6^2+18+6^2+3^2+18-2\times13}{3\times13-2}=4$ bulunur. Örnek 3 te *M(X,Y)=4* olduğundan, *X* ve *Y* dizileri optimal bir çift oluşturur.

Alfabedeki eleman sayısı bir asal sayının kuvveti olduğundan aşağıdaki sınır elde edilmiştir.

Lemma 1.7: [11] q bir asal sayının pozitif bir kuvveti olmak üzere, iki farklı X,Y $\left(q^m-1,q,\lambda\right)$-FHS dizisi için;

$$M(X,Y)\geq q^{m-1} \tag{1.8}$$

eşitsizliği sağlanır.

Dizi ailelerinin optimallikleri incelenirken, bu ailelerdeki dizi ve dizi çiftlerinin aldığı Hamming korelasyon değerleri göz önüne alınır.

Tanım 1.8: U, $S(n;F)$ nin N elemanlı bir alt kümesi olsun. U dizi ailesi için Hamming korelasyonu;

$$M(U)=\max\left\{\max_{x\in U}H(X),\max_{X,Y\in U,\,X\neq Y}H(X,Y)\right\} \tag{1.9}$$

olarak verilir.

Bir dizi ailesinin optimal olması için aşağıda verilen alt sınır kullanılabilir.

Lemma 1.9: [13] Eleman sayısı k olan bir F alfabesi üzerinde tanımlı, N elemanlı $U\subseteq S(n;F)$ kümesinde,

$$I=\left\lfloor\frac{nN}{k}\right\rfloor$$

olmak üzere;

$$M(U) \geq \left\lceil \frac{(nN-k)n}{(nN-1)k} \right\rceil \tag{1.10}$$

ve

$$M(U) \geq \left\lceil \frac{2INn-(I+1)kI}{(nN-1)N} \right\rceil \tag{1.11}$$

eşitsizlikleri sağlanır.

Eğer bir dizi ailesi Lemma 1.9 da verilen alt sınırları sağlarsa o dizi ailesine Peng-Fan optimaldir denir.

Örnek 6: Örnek 5 deki X ve Y dizileri için $U=\{X,Y\}$ olsun. $N=2,\ n=13,\ k=3$ olmak üzere Örnek 3 ve Tanım 1.8. den $M(U)=4$ olarak bulunur. (1.10) denkleminde sağ taraf $\left\lceil \frac{(13\times 2-3)13}{(13\times 2-1)3} \right\rceil = 4$ olduğundan U optimal bir aile tanımlar.

Teorem 1.10: [13,14] X,Y ayrık iki (n,k,λ)-FHS olsunlar. $I=\left\lfloor \frac{nN}{k} \right\rfloor$ ve $2n=Ik+r$, $0\leq r<k$ olmak üzere;

$$M(X,Y) \geq \frac{4In-(I+1)Ik}{4n-2} \tag{1.12}$$

eşitsizliği sağlanır.

Teorem 1.11: [10] Her $X,Y \in K \subseteq S(n;F)$ dizisi için, $|F|=k$, $I=\left\lfloor \frac{nN}{k} \right\rfloor$ ve K kümesinin eleman sayısı N olmak üzere, $H(X)$, dizinin oto-korelasyonu (1.2), $H(X,Y)$, dizilerin kros-korelasyonu (1.3) ve $I=\left\lfloor \frac{nN}{k} \right\rfloor$ olmak üzere;

$$(n-1)kH(X)+(N-1)nkH(X,Y) \geq (nN-k)n \tag{1.13}$$

$$(n-1)NH(X)+(N-1)NkH(X,Y)\geq 2InN-(I+1)Ik \tag{1.14}$$

eşitsizlikleri sağlanır.

BÖLÜM 2.

2.CEBİRSEL YÖNTEMLER

Tezin kalan bölümünde FHS lerin üretilmesinde kullanılan özel bir yöntem ele alınacaktır. Bu yöntem kullanılarak [4,5,9,3] çalışmalarında farklı FHS ler elde edilmiştir. Bu yöntemlerin detaylarına geçmeden önce sonlu cisimlerde bilinmesi gereken bazı temel bilgiler verilecektir. Bu konudaki detaylı bilgiler için [12] incelenebilir.

p bir asal sayı ve q, p nin pozitif bir kuvveti olmak üzere, F_q ile q elemanlı sonlu cisim gösterilecektir. Bu cismin elemanları $x^q - x$ polinomunun kökleri olarak görülebilir. $m \geq 1$ pozitif bir tam sayı olmak üzere, F_{q^m} ile F_q nun m. mertebeden genişlemesi gösterilecektir.

$\mathrm{F}_{q^m} \setminus \{0\}$ çarpımsal bir gruptur ve bu grubun devirli olduğu bilinmektedir.

$\mathrm{F}_{q^m} \setminus \{0\} = \langle \alpha \rangle = \{\alpha^i : 0 \leq i \leq q^{m-2}\}$ olmak üzere, α ya F_{q^m} nin primitif (ilkel) elemanı denir. $\beta = \alpha^j$ ve $ebob(j, q^m - 1) = 1$ şartını sağlayan tüm β elemanları da primitif olur.

F_{q^m} den F_q ya tanımlı ve bir çok uygulamada karşımıza çıkan iz (Trace, Tr) fonksiyonu aşağıdaki gibi tanımlanır.

$$Tr : \mathrm{F}_{q^m} \to \mathrm{F}_q$$
$$\alpha \mapsto Tr_{q^m/q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

Fonksiyonun özelliği herhangi bir α elemanını, q eşleniklerinin toplamına götürmesidir. Bu fonksiyon kullanılarak bir çok özelliğe sahip dizi ve dizi aileleri elde edilmiştir ve uygulamalarda kullanılmaktadır.

Verilen bir X dizisinin sıfırdan farklı elemanlarının sayısına o dizinin **Hamming ağırlığı** denir ve *w(X)* şeklinde gösterilir.

Aynı uzunluktaki *X, Y* dizileri için aynı indeks değerindeki farklı elemanların sayısına **X ile Y nin Hamming uzaklığı** denir ve $d_H(X,Y)$ ile gösterilir. Dizilerin uzunluğu n olmak üzere, $d_H(X,Y)$=*w(X-Y)* olduğu açıktır.

2.1. Genel Üretim Metodu

p bir asal sayı ve q, p nin pozitif bir kuvveti olsun. m pozitif tam sayısı için l, q^m-1 in pozitif bir böleni ve $n=\dfrac{q^m-1}{l}$ olarak tanımlansın. F_{q^m} nin herhangi bir primitif elemanı α olmak üzere $\beta=\alpha^l$ olarak alalım.
Her $0\le i\le q^m-2$ için n uzunluğundaki c_i dizileri;

$$c_i=\left(Tr_{q^m/q}(\alpha^i),Tr_{q^m/q}(\alpha^i\beta),\ldots,Tr_{q^m/q}(\alpha^i\beta^{n-1})\right) \tag{2.1}$$

olarak tanımlansın.

Burada seçilen özel p, q, m ve l değerlerine bağlı olarak optimal FHS dizilerinin, optimal FHS dizi çiftlerinin ve optimal FHS ailelerinin nasıl elde edilebileceğini inceleyeceğiz. Göz önüne aldığımız FHS dizileri [4,5,9,3] da elde edilen dizilerdir.

Dizilerin Hamming Korelasyonlarını hesaplayabilmek için aşağıdaki üssel toplamı hesaplamak gereklidir. Bu toplamı hesaplamak için [4,5,9,3] de farklı teknikler kullanılmıştır. c_i dizisinin ağırlığı $w(c_i)$ olmak üzere

$$\begin{aligned} n-w(c_i) &= \sum_{j=0}^{n-1}\frac{1}{q}\sum_{c\in \mathrm{F}_q}\xi^{Tr_{q/p}\left(cTr_{q^m/q}\left(\alpha^i\beta^j\right)\right)} \\ &= \frac{1}{q}\left(n+\sum_{c\in \mathrm{F}_q^*}\sum_{j=0}^{n-1}\xi^{Tr_{q/p}\left(Tr_{q^m/q}\left(\alpha^i c\beta^j\right)\right)}\right) \\ &= \frac{1}{q}\left(n+\sum_{c\in \mathrm{F}_q^*}\sum_{j=0}^{n-1}\xi^{Tr_{q^m/p}\left(\alpha^i c\alpha^{lj}\right)}\right) \end{aligned}$$

olur, burada $\xi=e^{i\frac{2\pi}{p}}$ olarak alınır.

2.1.1. [4] deki diziler

Bu bölümde (2.1) de verilen dizilerin parametrelerinin aşağıdaki gibi alınması sonucu ortaya çıkan FHS dizileri incelenecektir

$$\begin{cases} p: & 2 \text{ den farklı bir asal sayı} \\ q: & p \text{ nin pozitif bir kuvveti} \\ m: & 3\text{'den büyük veya 3'e eşit tek bir tamsayı} \\ l: & 2 \\ n: & \dfrac{q^m-1}{2} \end{cases}$$

Lemma 2.1 [4]: $m \geq 3$ tek bir tam sayı ve $0 \leq i \leq q^m - 2$ olmak üzere c_i dizisinin Hamming ağırlığı:

$$w(c_i) = \frac{q^m - q^{m-1}}{2} \tag{2.2}$$

olur.

c_i dizilerinin Hamming korelasyonları

$$H(c_i) = H_{c_i,c_i}(t) = n - d_H(c_i, c_{i\beta^t}) = \frac{q^m\text{-}1}{2} - w\left(c_{i-i\beta^t}\right)$$

olduğundan dolayı aşağıdaki şekilde elde edilir. Burada $1 \leq t < n$ olmak üzere her t için

$$c_{i\beta^t} = \left(Tr_{q^m/q}\left(\alpha^i\beta^t\right), Tr_{q^m/q}\left(\alpha^i\beta^{t+1}\right), \ldots, Tr_{q^m/q}\left(\alpha^i\beta^{t+n-1}\right)\right)$$

$$c_{i-i\beta^t} = \left(Tr_{q^m/q}\left(\alpha^i(1-\beta^t)\right), Tr_{q^m/q}\left(\alpha^i\beta(1-\beta^t)\right), \ldots, Tr_{q^m/q}\left(\alpha^i\beta^{n-1}(1-\beta^t)\right)\right)$$ olarak tanımlanır.

Lemma 2.2 [4]: $m \geq 3$ tek bir tam sayı ve $0 \leq i \leq q^m - 2$ olmak üzere;

$$H(c_i) = \frac{q^{m-1} - 1}{2} \tag{2.3}$$

olur.

Örnek 7: *p=3, q=3, m=3, l=2,* $n = \frac{q^m - 1}{2} = \frac{3^3 - 1}{2} = 13$ olmak üzere

c_0 = (0, 2, 1, 2, 0, 1, 1, 2, 2, 2, 0, 2, 0)

olarak bulunur. Lemma 2.2. den $H(c_0) = \frac{q^{m-1} - 1}{2} = \frac{3^{3-1} - 1}{2} = 4$ olacağından c_0 bir *(13,3,4)*-FHS olur. Lemma 1.3. den (13,3,4)-FHS dizileri için $H(X) \geq \left\lceil \frac{(n-\varepsilon)(n+\varepsilon-k)}{k(n-1)} \right\rceil = \left\lceil \frac{(13-1)(13+1-3)}{3(13-1)} \right\rceil = 4$ olduğundan c_0 ın optimal bir (13,3,4)-FHS dizisi olduğu görülür.

Örnek 8: *p=5, q=5, m=3, l=2,* $n = \frac{q^m - 1}{2} = \frac{5^3 - 1}{2} = 62$ olmak üzere (MAGMA yardımıyla)

c_0 = (3, 4, 3, 3, 1, 4, 4, 4, 1, 4, 3, 0, 4, 3, 1, 3, 0, 2, 0, 2, 1, 1, 3, 2, 0, 4, 4, 0, 0, 1, 4, 2, 1, 2, 2, 4, 1, 1, 1, 4, 1, 2, 0, 1, 2, 4, 2, 0, 3, 0, 3, 4, 4, 2, 3, 0, 1, 1, 0, 0, 4, 1)

olarak bulunur ve $H(c_0) = 12$ elde edilir. Bu durumda c_0 bir (62,5,12)-FHS olur. Lemma 1.3. den (62,5,12)-FHS dizileri için $H(X) \geq \left\lceil \frac{(62-1)(62+1-5)}{5(62-1)} \right\rceil = 12$ olduğundan c_0 ın optimal bir (62,5,12)-FHS dizisi olduğu görülür.

Teorem 2.3 [4]: $m \geq 3$ tek bir tam sayı ve $0 \leq i \leq q^m - 2$ olmak üzere; c_i bir optimal $\left(\frac{q^m - 1}{2}, q, \frac{q^{m-1} - 1}{2} \right)$-FHS oluşturur.

Teorem 2.4 [4]: $m \geq 3$ tek bir tam sayı, $a = \alpha^j$; $0 \leq \mathrm{j} \leq \mathrm{q}^m - 2$, $F_{q^m} \setminus \{0\}$ da karesel bir eleman, yani $a \in F_{q^m} \setminus \{0\}$ ve bir $c \in F_{q^m}$ için $a = c^2$, ve $b = \alpha^k$; $0 \leq \mathrm{k} \leq \mathrm{q}^m - 2$, $F_{q^m} \setminus \{0\}$ de karesel olmayan bir eleman, yani $b \in F_{q^m} \setminus \{0\}$ ve her $c \in F_{q^m}$ için $b \neq c^2$ olsun. Bu durumda c_j ve c_k optimal bir dizi çifti olurlar.

Örnek 9: *p=3, q=3, m=3, l=2,* $n = \frac{q^m - 1}{2} = \frac{3^3 - 1}{2} = 13$ olmak üzere

c_1 = *(0, 2, 2, 1, 1, 1, 0, 1, 0, 0, 1, 2, 1),*

c_2 = *(2, 2, 0, 2, 0, 0, 2, 1, 2, 0, 1, 1, 2)*

olarak bulunur.

MAGMA yardımıyla $H(c_1)=4$, $H(c_2)=4$, $H(c_1, c_2)=4$, dolayısıyla $M(c_1, c_2)=4$ elde edilir. Lemma 1.9 (1.10) ve (1.11) den (*13,3,4)*-FHS dizileri için

$$M(X,Y) \geq \left\lceil \frac{(nN-k)n}{(nN-1)k} \right\rceil = \left\lceil \frac{(13\times 2-3)13}{(13\times 2-1)3} \right\rceil = 4 \qquad \text{ve}$$

$$M(X,Y) \geq \left\lceil \frac{2INn-(I+1)kI}{(nN-1)N} \right\rceil = 4$$

olduğundan c_1 ve c_2 dizilerinin optimal bir çift olduğu görülür.

Bu bölümde verilen diziler üretilirken *m* nin tek sayı olarak seçilme şartı vardı. Aşağıdaki 4 örnekte *m* değeri çift sayı alınarak farklı parametrelerde diziler üretilmiştir. Örneklerin sonucunda optimal diziler elde edilemediği gözlenmiştir.

Örnek 10: *p=3, q=3, m=2, l=2,* $n = \frac{q^m - 1}{2} = \frac{3^2 - 1}{2} = 4$ olmak üzere (MAGMA yardımıyla)

c_0 = (2, 0, 1, 0)

c_1 =(1, 1, 2, 2)

c_2 =(0, 1, 0, 2)

c_3 =(1, 2, 2, 1)

c_4 =(1, 0, 2, 0)

c_5 =(2, 2, 1, 1)

c_6 =(0, 2, 0, 1)

c_7 =(2, 1, 1, 2)

olarak bulunur ve her $0 \le i \le 7$ için H(c_i)=2 elde edilir. Bu durumda her $0 \le i \le 7$ için c_i ler birer (4,3,2)-FHS olurlar. Lemma 1.3 den (n,k, λ)=(4,3, λ) dizileri için $H(X) \ge \left\lceil \frac{(n-\varepsilon)(n+\varepsilon-k)}{k(n-1)} \right\rceil = \left\lceil \frac{(4-1)(4+1-3)}{3(4-1)} \right\rceil = 1$ olduğundan yukarıdaki dizilerin sınırda verilen eşitliğe ulaşamadıkları gözlenmiştir.

Örnek 11: p=3, q=3, m=4, l=2, $n = \frac{q^m - 1}{2} = \frac{3^4 - 1}{2} = 40$ olmak üzere (MAGMA yardımıyla)
c_1 =(1, 1, 0, 2, 1, 1, 0, 0, 2, 1, 2, 1, 0, 1, 2, 0, 1, 0, 0, 0, 2, 2, 0, 1, 2, 2,
0, 0, 1, 2, 1, 2, 0, 2, 1, 0, 2, 0, 0, 0)
olarak bulunur ve H(c_1)=40 elde edilir. Bu durumda c_1 dizisi bir (40,3,40)-FHS olur. Lemma 1.3 den (n,k, λ)=(40,3, λ) dizileri için $H(X) \ge \left\lceil \frac{(n-\varepsilon)(n+\varepsilon-k)}{k(n-1)} \right\rceil = \left\lceil \frac{(40-1)(40+1-3)}{3(40-1)} \right\rceil = 13$ olduğundan c_1 dizisinin, sınırda verilen eşitliğe ulaşamadığı gözlenmiştir.

Örnek 12: p=5, q=5, m=2, l=2, $n = \frac{q^m - 1}{2} = \frac{5^2 - 1}{2} = 12$ olmak üzere(MAGMA yardımıyla)
c_0 = (2, 2, 1, 4, 4, 2, 3, 3, 4, 1, 1, 3)
olarak bulunur ve H(c_0)=4 elde edilir. Bu durumda c_0 bir (12,5,4)-FHS olur. Lemma 1.3 den (n,k, λ)=(12,5, λ)-FHS dizileri için $H(X) \ge \left\lceil \frac{(n-\varepsilon)(n+\varepsilon-k)}{k(n-1)} \right\rceil = \left\lceil \frac{(12-2)(12+2-5)}{5(12-1)} \right\rceil = 12$ olduğundan c_0 dizisinin sınırda verilen eşitliğe ulaşamadığı gözlenmiştir.

Örnek 13: p=3, q=9, m=2, l=2, $n = \frac{q^m - 1}{2} = \frac{9^2 - 1}{2} = 40$

i=0 için, v, $p(x) = x^2 + 2x + 2$ polinomunun kökü olmak üzere, (MAGMA yardımıyla)

c_0 = (2, 2, v^5, 2, v, v^7, v^7, 1, v^7, 2, v^2, v^2, v^3, v^2, v^7, v^5, v^5, v^6, v^5, v^2, 1, 1, v, 1, v^5, v^3, v^3, 2, v^3, 1, v^6, v^6, v^7, v^6, v^3, v, v, v^2, v, v^6)

olarak bulunur ve H(c_0)=40 elde edilir. Lemma 1.3 ten (n,k, λ)=(40,9, λ)-FHS dizileri için $H(X) \geq \left\lceil \frac{(n-\varepsilon)(n+\varepsilon-k)}{k(n-1)} \right\rceil = \left\lceil \frac{(40-4)(40+4-9)}{9(40-1)} \right\rceil = 4$ olduğundan c_0 dizisinin sınırda verilen eşitliğe ulaşamadığı gözlenmiştir.

2.1.2. [5] deki diziler

Bu bölümde (2.1) de verilen dizilerin parametrelerinin aşağıdaki gibi alınması sonucu ortaya çıkan FHS dizileri incelenecektir

$$\begin{cases} p: & \text{bir asal sayı} \\ q: & p \text{ nin pozitif bir kuvveti} \\ m: & \text{pozitif bir tamsayı} \\ l: & q-1 \\ n: & \dfrac{q^m-1}{q-1} \end{cases}$$

Burada c_i dizileri indeks değerleri, $0 \le i \le q-2$ olarak alınmıştır.

Aşağıdaki lemma Teorem 6 [5] in ispatından elde edilmiştir.

Lemma 2.5: $0 \le i \le l-1$ ve $ebob\left(q-1, \sum_{i=0}^{m-1} q^i\right) = 1$ olmak üzere c_i dizisinin Hamming ağırlığı:

$$w(c_i) = q^{m-1} = \frac{q^m - q^{m-1}}{q-1} \tag{2.4}$$

olur.

c_i dizilerinin Hamming korelasyonları

$$H(c_i) = H_{c_i,c_i}(t) = n - d_H(c_i, c_{i\beta^t}) = \frac{q^m\text{-}1}{l} - w\left(c_{i-i\beta^t}\right)$$

olduğundan dolayı aşağıdaki şekilde elde edilir.

Lemma 2.6: $0 \le i \le l-1$ ve $ebob\left(q-1, \sum_{i=0}^{m-1} q^i\right) = 1$ olmak üzere;

$$H(c_i) = \frac{q^{m-1}-1}{q-1} \tag{2.5}$$

olur.

Teorem 2.7 [5]: $0 \le i \le l-1$ ve $ebob\left(q-1, \sum_{i=0}^{m-1} q^i\right) = 1$ olmak üzere; her bir i için c_i optimal bir $\left(\frac{q^m-1}{q-1}, q, \frac{q^{m-1}-1}{q-1}\right)$-FHS oluşturur.

Örnek 14: *p=5, q=5, m=3, l=4,* $n = \frac{q^m-1}{q-1} = \frac{5^3-1}{5-1} = 31$ olmak üzere (MAGMA yardımıyla)

X=(4, 3, 4, 4, 4, 0, 3, 3, 2, 2, 1, 2, 4, 0, 1, 2, 2, 4, 1, 4, 2, 1, 4, 0, 0, 4, 2, 0, 1, 0, 1)

olarak bulunur ve H(X)=6 elde edilir. Lemma 1.3. den (31,5,6)-FHS dizileri için $H(X) \ge \left\lceil \frac{(n-\varepsilon)(n+\varepsilon-k)}{k(n-1)} \right\rceil = \left\lceil \frac{(31-1)(31+1-5)}{5(31-1)} \right\rceil = 6$ olduğundan c_0 ın optimal bir (31,5,6)-FHS dizisi olduğu görülür.

Örnek 15: *p=5, q=5, m=3, l=4,* $n = \frac{q^m-1}{q-1} = \frac{5^3-1}{5-1} = 31$ olmak üzere (MAGMA yardımıyla)

X=(4, 3, 4, 4, 4, 0, 3, 3, 2, 2, 1, 2, 4, 0, 1, 2, 2, 4, 1, 4, 2, 1, 4, 0, 0, 4, 2, 0, 1, 0, 1)

Y=(0, 0, 3, 4, 0, 2, 0, 2, 3, 1, 3, 3, 3, 0, 1, 1, 4, 4, 2, 4, 3, 0, 2, 4, 4, 3, 2, 3, 4, 2, 3)

olarak bulunur ve *H(X)=6, H(Y)=6, H(X,Y)=6,* dolayısıyla *M(X,Y)=6* elde edilir. Lemma 1.9 (1.10) (1.11) den (31,5,6)-FHS dizileri için

$$M(X,Y) \ge \left\lceil \frac{(nN-k)n}{(nN-1)k} \right\rceil = \left\lceil \frac{(31\times 2-5)31}{(31\times 2-1)5} \right\rceil = 6 \quad \text{ve}$$

$$M(X,Y) \ge \left\lceil \frac{2INn-(I+1)kI}{(nN-1)N} \right\rceil = 6$$

olduğundan X ve Y dizilerinin optimal bir çift olduğu görülür.

Teorem 2.8 [5]: $ebob\left(q-1,\sum_{i=0}^{m-1}q^i\right)=1$ ise $S_i=\{c_i:0\le i\le l-1\}$ kümesini göstermek üzere S_i kümesi bir optimal $\left(\frac{q^m-1}{q-1},q,\frac{q^{m-1}-1}{q-1};q-1\right)$-FHS ailesi olur.

Örnek 16: p=5, q=5,m=3,l=4, $n=\frac{q^m-1}{q-1}=\frac{5^3-1}{5-1}=31$ olmak üzere, (MAGMA yardımıyla)

X=(0, 0, 3, 4, 0, 2, 0, 2, 3, 1, 3, 3, 3, 0, 1, 1, 4, 4, 2, 4, 3, 0, 2, 4, 4, 3, 2, 3, 4, 2, 3),

Y=(4, 3, 4, 4, 4, 0, 3, 3, 2, 2, 1, 2, 4, 0, 1, 2, 2, 4, 1, 4, 2, 1, 4, 0, 0, 4, 2, 0, 1, 0, 1),

Z=(1, 1, 3, 1, 2, 0, 3, 1, 1, 2, 3, 2, 1, 3, 2, 0, 0, 2, 1, 0, 3, 0, 3, 2, 4, 2, 2, 2, 0, 4, 4),

T=(3, 1, 4, 1, 3, 4, 1, 0, 0, 1, 3, 0, 4, 0, 4, 1, 2, 1, 1, 1, 0, 2, 2, 3, 3, 4, 3, 1, 0, 4, 3)

olarak bulunur. *U={X,Y,Z,T}* alındığında *M(U)=6* olarak elde edilir. Lemma 1.9 (1.10) ve (1.11) den $M(U)\ge\left\lceil\frac{(nN-k)n}{(nN-1)k}\right\rceil=\left\lceil\frac{(31\times4-5)31}{(31\times4-1)5}\right\rceil=6$ ve $M(U)\ge\left\lceil\frac{2INn-(I+1)kI}{(nN-1)N}\right\rceil=6$ olduğundan dolayı U ailesinin (31,5,6;4) optimal bir aile olduğu görülür.

2.1.3. [9]daki diziler

Bu bölümde (2.1) de verilen dizilerin parametrelerinin aşağıdaki gibi alınması sonucu ortaya çıkan FHS dizileri incelenecektir

$$\begin{cases} p: & \text{bir asal sayı} \\ q: & p \text{ nin pozitif bir kuvveti} \\ m: & \text{pozitif bir tamsayı} \\ l: & q-1 \text{ in bir böleni ve ebob}\left(\dfrac{q^m-1}{q-1}, l\right)=1 \\ n: & \dfrac{q^m-1}{l} \end{cases}$$

Lemma 2.9 [9]: Her $0 \le i \le q^m - 2$ için c_i dizisinin Hamming ağırlığı:

$$w(c_i) = \frac{q^m - q^{m-1}}{l} \tag{2.6}$$

olarak verilir.

c_i dizilerinin Hamming korelasyonları

$$H(c_i) = H_{c_i,c_i}(t) = n - d_H(c_i, c_{i\beta^t}) = \frac{q^m\text{-}1}{l} - w\left(c_{i-i\beta^t}\right)$$

olduğundan dolayı aşağıdaki şekilde elde edilir.

Lemma 2.10 [9]: Her $0 \le i \le q^m - 2$ için c_i dizisinin Hamming korelasyonu

$$H(c_i) = \frac{q^{m-1} - 1}{l} \tag{2.7}$$

olur.

Teorem 2.11 [9]: Her $0 \le i \le q^m - 2$ için c_i optimal bir $\left(\dfrac{q^m-1}{l}, q, \dfrac{q^{m-1}-1}{l}\right)$-FHS dizisi oluşturur.

Örnek 17: *p=7, q=7, m=2, l=3,* $n=\frac{q^m-1}{l}=\frac{7^2-1}{3}=16$ olmak üzere (MAGMA yardımıyla)

X=(1, 4, 6, 1, 2, 0, 2, 6, 6, 3, 1, 6, 5, 0, 5, 1)

olarak bulunur. Lemma 2.10. den $H(c_0)=\frac{q^{m-1}-1}{l}=\frac{7^{2-1}-1}{3}=2$ olacağından X bir (16,7,2)-FHS olur. Lemma 1.3. den (16,7,2)-FHS dizileri için $H(X)\geq\left\lceil\frac{(n-\varepsilon)(n+\varepsilon-k)}{k(n-1)}\right\rceil=\left\lceil\frac{(16-2)(16+2-7)}{7(16-1)}\right\rceil=2$ olduğundan X in optimal bir (16,7,2)-FHS dizisi olduğu görülür.

Teorem 2.12 [9]: c_i ve c_j F_{q^m} de mertebesi *l* olan ayrık sayklotomi sınıflarına ait olsunlar, bu durumda c_i ve c_j optimal çift olurlar.

Örnek 18: *p=7, q=7, m=2,* $n=\frac{q^m-1}{l}=\frac{7^2-1}{3}=16$ olmak üzere (MAGMA yardımıyla)

X=(2, 2, 1, 5, 2, 4, 0, 4, 5, 5, 6, 2, 5, 3, 0, 3)

Y=(1, 4, 6, 1, 2, 0, 2, 6, 6, 3, 1, 6, 5, 0, 5, 1)

olarak bulunur ve *H(X)=2, H(Y)=2, H(X,Y)=2,* dolayısıyla *M(X,Y)=2* elde edilir. Lemma 1.9 (1.10) (1.11) den (16,7,2)-FHS dizileri için

$$M(X,Y)\geq\left\lceil\frac{(nN-k)n}{(nN-1)k}\right\rceil=\left\lceil\frac{(16\times2-7)16}{(16\times2-1)7}\right\rceil=2$$ ve

$$M(X,Y)\geq\left\lceil\frac{2INn-(I+1)kI}{(nN-1)N}\right\rceil=2$$

olduğundan c_1 ve c_2 dizilerinin optimal bir çift olduğu görülür.

Not: Burada $U=\{c_i,c_j\}$ olarak alınırsa *U* eleman sayısı *2* olan bir optimal aile olur.

Teorem 2.13 [9]: $\{a_0, a_1, \ldots\}$ F_{q^m} de mertebesi l olan sayklotomi sınıfları için temsilcilerin bütün kümesinin bir alt kümesi olsun. Bu takdirde $\{c_{a_0}, c_{a_1}, \ldots\}$ optimal bir aile oluşturur.

Yukarıdaki teorem özetlenirse temel sonuç bulunur.

Teorem 2.14 [9]: $\{a_0, a_1, \ldots, a_{l-1}\}$, F_{q^m} de mertebesi l olan sayklotomi sınıf temsilcileri kümesi olsun. $S = \{c_{a_0}, c_{a_1}, \ldots, c_{a_{l-1}}\}$ optimal bir aile oluşturur.

Teorem 2.15 [9]: *q,* bir asalın pozitif bir kuvveti, *m* ve *l* pozitif tam sayılar olmak üzere $l \mid q^m - 1$ ve $\text{ebob}\left(\frac{q^m-1}{q-1}, l\right) = 1$ şartları altında bir $\left(\frac{q^m-1}{l}, q, \frac{q^{m-1}-1}{l}; l\right)$ optimal aile vardır. Aynı zamanda bu ailenin her alt kümesi de optimal bir ailedir.

2.1.4. [3] teki diziler ($p=2$ durumu)

Bu bölümde (2.1) de verilen dizilerin parametrelerinin aşağıdaki gibi alınması sonucu ortaya çıkan FHS dizileri incelenecektir

$$\begin{cases} p: & 2 \\ q: & p \text{ nin pozitif bir kuvveti} \\ m: & 4 \\ l: & q^2-1 \\ n: & \dfrac{q^4-1}{q^2-1}=q^2+1 \end{cases}$$

Burada c_i dizileri, indeks değerleri, $0 \le i \le l-1$ olarak alınmıştır.

Aşağıdaki sonuç Teorem 9 [3] un ispatından elde edilmiştir.

Lemma 2.16: Her $0 \le i \le l-1$ için c_i dizisinin Hamming ağırlığı

$$w(c_i)=q^2-q=\left\lfloor \frac{q^4-q^{4-1}}{q^2-1} \right\rfloor \tag{2.8}$$

olarak verilir.

c_i dizilerinin Hamming korelasyonları

$$H(c_i)=H_{c_i,c_i}(t)=n-d_H(c_i,c_{i\beta^t})=\frac{q^m\text{-}1}{q^2-1}-w\left(c_{i-i\beta^t}\right)$$

olduğundan dolayı aşağıdaki şekilde elde edilir.

Lemma 2.17: Her $0 \le i \le l-1$ için c_i dizisinin Hamming korelasyonu :

$$H(c_i)=q+1=\left\lceil \frac{q^{4-1}-1}{q^2-1} \right\rceil \tag{2.9}$$

olur.

Teorem 2.18 [3]: $S_i=\{c_i : 0 \le i \le l-1\}$ olmak üzere S_i bir optimal $(q^2+1, q, q+1; q^2-1)$ -FHS ailesi olur.

Örnek 19: *p=2, q=4, l= 15,* $n = n = q^2 + 1 = 17$ olmak üzere (MAGMA yardımıyla)

X= (0, t, t^2, 1, t, 1, 1, 1, t^2, t^2, 1, 1, 1, t, 1, t^2, t)

olarak bulunur ve H(X)=5 elde edilir. Lemma 2.17 den $H(X) = q + 1 = 5$ olacağından X bir (17,4,5)-FHS olur. Lemma 1.3. den (17,4,5)-FHS dizileri için $H(X) \geq \left\lceil \frac{(n-\varepsilon)(n+\varepsilon-k)}{k(n-1)} \right\rceil = \left\lceil \frac{(17-1)(17+1-4)}{4(17-1)} \right\rceil = 5$ olduğundan X dizisi optimal bir (17,4,5)-FHS olur.

Örnek 20: *p=2, q=4, l= 15,* $n = q^2 + 1 = 17$ ve t, $p(x) = x^2 + x + 1$ in kökü olmak üzere

X_1 =(0, t, t^2, 1, t, 1, 1, 1, t^2, t^2, 1, 1, 1, t, 1, t^2, t),

X_2 = (1, 1, 1, 0, t, 0, t^2, t, t, 0, t, t, t^2, 0, t, 0, 1),

X_3 = (1, 0, 1, t^2, 1, t^2, 0, t, t^2, 0, 0, t^2, t, 0, t^2, 1, t^2),

X_4 = (1, t, t, 1, t, t^2, t^2, 0, 0, t, 0, t, 0, 0, t^2, t^2, t),

X_5 = (1, 0, 0, 0, 1, t, t, t^2, 1, 0, t, t, 0, 1, t^2, t, t),

X_6 = (t, t, 1, 1, t, t, t, t^2, t, 1, t^2, 0, t^2, 1, t, t^2, t),

X_7 = (1, t^2, t^2, 0, t^2, t^2, 1, 0, t^2, 0, t, t, t, t, 0, t^2, 0),

X_8 = (0, t^2, 1, 0, 0, 1, t^2, 0, 1, t, 1, t, 0, t, 1, t, 1),

X_9 = (1, 0, 0, t^2, 0, t^2, 0, 0, 1, 1, t^2, t, t^2, t^2, t, t^2, 1),

X_{10} = (t^2, 1, t, 0, t^2, t^2, 0, t, 1, t^2, t^2, t, 0, 0, 0, t, t^2),

X_{11} = (t^2, 1, t^2, t, 1, 0, 1, t, t^2, 1, t^2, t^2, t^2, t, t, t^2, t^2)

X_{12} = (t, 0, 1, 0, t^2, t^2, t^2, t^2, 0, 1, 0, t, 1, 1, 0, 1, 1),

X_{13} = (1, 0, t, t^2, t, t^2, 0, t^2, t, t^2, t, 0, 1, t, 0, 0, t),

X_{14} = *(0, 0, t, t, 1,* t^2*, 1, 1,* t^2*, 1, t, t, 0, 0, 1, 0, 1),*

X_{15} = *(0,* t^2*, t, 1, 1,* t^2*, 0, 0, 0,* t^2*, 1, 1, t,* t^2*, 0, 1, 1)*

dizileri bulunur ve $U = \{X_1, X_2, \ldots, X_{15}\}$ olarak alındığında *M(U)=5* olarak elde edilir. Lemma 1.9 (1.10) ve (1.11) den $M(U) \geq \left\lceil \frac{(nN-k)n}{(nN-1)k} \right\rceil = \left\lceil \frac{(17\times 15-4)17}{(17\times 15-1)4} \right\rceil = 5$ ve $M(U) \geq \left\lceil \frac{2INn-(I+1)kI}{(nN-1)N} \right\rceil = 5$ olduğundan dolayı U ailesinin (17,4,5;15) optimal bir aile olduğu görülür.

2.1.5. [3] teki diziler ($p \neq 2$ durumu)

Bu bölümde (2.1) de verilen dizilerin parametrelerinin aşağıdaki gibi alınması sonucu ortaya çıkan FHS dizileri incelenecektir

$$\begin{cases} p: & \text{tek bir asal sayı} \\ q: & p \text{ nin pozitif bir kuvveti} \\ m: & \text{pozitif bir tam sayı} \\ l: & q^m - 1 \text{ in pozitif bir böleni} \\ n: & \dfrac{q^m - 1}{l} \end{cases}$$

Aşağıdaki sonuç Teorem 10 [3] un ispatından elde edilmiştir.

Lemma 2.19: Her $0 \le i \le l-1$ ve l çift ve $ebob(n,l)=1$, $q\text{-}1 \equiv \dfrac{l}{2} \pmod{l}$ ve $ebob\left(\dfrac{q^m-1}{q-1} \pmod{l}, l\right) = 2$ olmak üzere, c_i dizisinin Hamming ağırlığı:

$$w(c_i) = \frac{(q-1)\left(q^m \pm \sqrt{q^m}\right)}{q \times l} \tag{2.10}$$

olarak verilir.

c_i dizilerinin Hamming korelasyonları

$$H(c_i) = H_{c_i,c_i}(t) = n - d_H(c_i, c_{i\beta^t}) = \frac{q^m\text{-}1}{2} - w\left(c_{i-i\beta^t}\right)$$

olduğundan dolayı aşağıdaki şekilde elde edilir.

Lemma 2.20: Her $0 \le i \le l-1$ l çift ve $ebob(n,l)=1$, $q\text{-}1 \equiv \dfrac{l}{2} \pmod{l}$ ve $ebob\left(\dfrac{q^m-1}{q-1} \pmod{l}, l\right) = 2$ olmak üzere, c_i dizisinin Hamming korelasyonu :

$$H(c_i) = \frac{q^m - q + (q-1)\sqrt{q^m}}{q \times l} \tag{2.11}$$

olur.

Örnek 21: *p=13, q=13, m=2, l=24,* $n=\frac{q^m-1}{l}=\frac{13^2-1}{24}=7$ olmak üzere (MAGMA yardımıyla)

X=(10, 10, 12, 6, 9, 6, 12)

Y=(1, 4, 0, 9, 12, 7, 6)

olarak bulunur ve *H(X)=1, H(Y)=0, H(X,Y)=1,* dolayısıyla *M(X,Y)=1* elde edilir. Lemma 1.9 (1.10) dan (7,13,1)FHS dizileri için

$$M(X,Y)\geq\left\lceil\frac{(nN-k)n}{(nN-1)k}\right\rceil=\left\lceil\frac{(7\times2-13)7}{(7\times2-1)13}\right\rceil=1 \quad \text{ve } M(X,Y)\geq\left\lceil\frac{2INn-(I+1)kI}{(nN-1)N}\right\rceil=1$$

olduğundan X ve Y dizilerinin optimal bir çift olduğu görülür.

Teorem 2.22 [3]: l çift ve $ebob(n,l)=1$, $q-1\equiv\frac{l}{2} \pmod{l}$

$ebob\left(\frac{q^m-1}{q-1}(\text{mod } l),l\right)=2$ ve $l>\frac{q-1}{q}\sqrt{q^m}$ olmak üzere $S_i=\{c_i:0\leq i\leq l-1\}$ kümesi bir optimal $\left(\frac{q^m-1}{l},q,\frac{q^m-q+(q-1)\sqrt{q^m}}{q\times l};l\right)$-FHS ailesi olur.

Örnek 22: *p=13, q=13, m=2, l=24,* $n=\frac{q^m-1}{l}=\frac{13^2-1}{24}=7$ olmak üzere

X_1=(2, 10, 7, 8, 8, 7, 10)

X_2= (1, 4, 0, 9, 12, 7, 6)

X_3= (10, 10, 12, 6, 9, 6, 12)

X_4= (8, 2, 12, 1, 11, 5, 0)

$X_5 = (1, 8, 1, 2, 6, 6, 2)$

$X_6 = (11, 4, 3, 0, 10, 9, 2)$

$X_7 = (9, 1, 1, 9, 11, 10, 11)$

$X_8 = (0, 6, 8, 9, 4, 5, 7)$

$X_9 = (8, 4, 6, 4, 8, 11, 11)$

$X_{10} = (8, 5, 3, 12, 0, 1, 10)$

$X_{11} = (5, 10, 4, 4, 10, 5, 1)$

$X_{12} = (2, 0, 11, 6, 10, 3, 7)$

$X_{13} = (5, 6, 3, 11, 3, 6, 5)$

$X_{14} = (1, 6, 7, 12, 9, 0, 4)$

$X_{15} = (4, 7, 1, 3, 3, 1, 7)$

$X_{16} = (2, 8, 0, 5, 11, 1, 12)$

$X_{17} = (7, 7, 11, 12, 5, 12, 11)$

$X_{18} = (3, 4, 11, 2, 9, 10, 0)$

X_{19} = (2, 3, 2, 4, 12, 12, 4)

X_{20} = (9, 8, 6, 0, 7, 5, 4)

X_{21} = (5, 2, 2, 5, 9, 7, 9)

X_{22} = (0, 12, 3, 5, 8, 10, 1)

X_{23} = (3, 8, 12, 8, 3, 9, 9)

X_{24} = (3, 10, 6, 11, 0, 2, 7)

olarak bulunur ve $U = \{X_1, X_2, \ldots, X_{24}\}$ olarak alındığında *M(U)=1* olarak elde edilir. Lemma 1.9 (1.10) ve (1.11) den $M(U) \geq \left\lceil \frac{(nN-k)n}{(nN-1)k} \right\rceil = \left\lceil \frac{(7\times 24-13)7}{(7\times 24-1)13} \right\rceil = 1$ ve $M(U) \geq \left\lceil \frac{2INn-(I+1)kI}{(nN-1)N} \right\rceil = 1$ olduğundan dolayı U ailesinin (7,13,1;24) optimal bir aile olduğu görülür.

BÖLÜM 3.

3.KARŞILAŞTIRMALAR

Bu bölümde bölüm 2 de ayrıntıları verilen üretim yöntemlerinin birbirleriyle olan karşılaştırmaları verilecektir.

Öncelikle Çizelge 3.1. de parametreler ve parametreler üzerindeki şartlar özetlenecektir. Daha sonraki bölümlerde ise optimal dizi elde etmek için kullanılan şartlar da göz önüne alınarak karşılaştırılabilen parametreler hakkında elde edilen sonuçlar verilecektir.

Çizelge 3.1. [4,5,9,3] makalelerindeki dizilerin parametreleri

	[4] daki diziler	**[5] deki diziler**	**[9] teki diziler**	**[3] teki diziler**	**[3]teki diziler**
p	asal, $\neq 2$	bir asal sayı	bir asal sayı	$p=2$	asal, $\neq 2$
q	P nin pozitif bir kuvveti	p nin pozitif bir kuvveti	p nin pozitif bir kuvveti	p nin pozitif bir kuvveti	p nin pozitif bir kuvveti
m	$m \geq 3$ tek bir tam sayı.	pozitif bir tam sayı	pozitif bir tam sayı	4	pozitif bir tam sayı
l	2	$q-1$	$q-1$ in pozitif bir böleni	q^2-1	q^m-1 in pozitif bir böleni.
*		$ebob\left(q-1, \frac{q^m-1}{q-1}\right)=1$	$ebob\left(\frac{q^m-1}{q-1}, l\right)=1$		l çift ve $ebob(n,l)=1$, $q-1 \equiv \frac{l}{2} \pmod{l}$ $ebob\left(\frac{q^m-1}{q-1} \pmod{l}, l\right)=2$ ve $l > \frac{q-1}{q}\sqrt{q^m}$

n	$\frac{q^m - 1}{l}$
α	F_{q^m} nin bir primitif elemanı.
β	α^l
c_i	$\left(Tr_{q^m/q}(\alpha^i), Tr_{q^m/q}(\alpha^i\beta), \ldots, Tr_{q^m/q}(\alpha^i\beta^{n-1})\right)$

* optimallik için l nin seçimi üzerindeki şartlar

3.1. [4] ile [5] deki Parametrelerin Karşılaştırılması

A: Bölüm 2.1.1. de anlatılan [4] daki dizilerin parametreleri

B: Bölüm 2.1.2. de anlatılan [5] deki dizilerin parametreleri

olmak üzere aşağıdaki sonuçlar elde edilmiştir.

$A \cap B$	p: 3 q: 3 m: 3 ten büyük veya 3 e eşit bir tek tam sayı l: 2 n: $\frac{q^m - 1}{2}$
$A \setminus B$	p: 2 ve 3 ten farklı bir asal sayı q: p nin pozitif bir kuvveti m: 3 ten büyük veya 3 e eşit bir tek tam sayı l: 2 n: $\frac{q^m - 1}{2}$
$B \setminus A$	p: asal sayı q: 3 ten farklı olmak üzere, p nin pozitif bir kuvveti m: pozitif bir tam sayı l: $q-1$ ve $ebob\left(q-1, \frac{q^m-1}{q-1}\right) = 1$ n: $\frac{q^m - 1}{q-1}$

3.2. [4] ile [9] deki Parametrelerin Karşılaştırılması

A: Bölüm 2.1.1. de anlatılan [4] daki dizilerin parametreleri

B: Bölüm 2.1.3. de anlatılan [9] deki dizilerin parametreleri

olmak üzere aşağıdaki sonuçlar elde edilmiştir.

$A \cap B$	p : 2 den farklı bir asal sayı q : p nin bir kuvveti m : 3 ten büyük veya 3 e eşit bir tek tam sayı l : 2 ve $ebob\left(\frac{q^m-1}{2}, 2\right)=1$ n : $\frac{q^m-1}{2}$
$A \setminus B$	p : 2 den farklı bir asal sayı q : p nin pozitif bir kuvveti m : 3 ten büyük veya 3 e eşit bir tek tam sayı l : 2 ve $ebob\left(\frac{q^m-1}{2}, 2\right)\neq 1$ n : $\frac{q^m-1}{2}$
$B \setminus A$	p : bir asal sayı q : p nin pozitif bir kuvveti m : pozitif bir tam sayı l : $q-1$ in 2 den farklı bir böleni ve $ebob\left(\frac{q^m-1}{q-1}, l\right)=1$ n : $\frac{q^m-1}{l}$

3.3. [5] ile [9] deki Parametrelerin Karşılaştırılması

A: Bölüm 2.1.2. de anlatılan [5] daki dizilerin parametreleri

B: Bölüm 2.1.3. de anlatılan [9] deki dizilerin parametreleri

olmak üzere aşağıdaki sonuçlar elde edilmiştir.

$A \cap B$	p : bir asal sayı q : p nin bir kuvveti m : pozitif bir tam sayı l : $q-1$ ve $ebob\left(q-1, \frac{q^m-1}{q-1}\right)=1$ n : $\frac{q^m-1}{l}$
$A \setminus B$	$\varnothing$
$B \setminus A$	p : bir asal sayı q : p nin pozitif bir kuvveti m : pozitif bir tam sayı l : $q-1$ in kendinden farklı bir böleni ve $ebob\left(\frac{q^m-1}{q-1}, l\right)=1$ n : $\frac{q^m-1}{l}$

KAYNAKLAR

[1] Ayvalık, A., 2007, Frekans atlamalı haberleşmenin karıştırılması, *Yüksek Lisans Tezi, Hacettepe Üniversitesi,* Fen Bilimleri Enstitüsü, Ankara.

[2] Chu, W., Colbourn, C.J., Optimal frequency-hopping sequences via cyclotomy, IEEE Transaction On Information Theory, 51,1139-1141, 2005.

[3] Ding, C., Fuji-Hara, R., Fujiwara, Y., Jimbo, M., Mishima, M., Sets of Frequency Hopping Sequences: Bounds and Optimal Constructions IEEE Transaction On Information Theory, 55(7), 3297-3304, 2009.

[4] Ding, C., Miosio, M., Yuan, J., Algebraic constructions of optimal frequency hopping sequences, IEEE Transaction On Information Theory, 53(7), 2606-2610, 2007.

[5] Ding, C., Yin, J., Sets of optimal frequency hopping sequences, IEEE Transaction On Information Theory, 54(8), 3741-3745, 2008.

[6] Fuji-Hara, R., Miao, Y., Mishima M., Optimal frequency hopping sequences: A combinatorial approach, IEEE Transaction On Information Theory, 50, 2408-2420, 2004.

[7] Fujiwara, Y., Fuji-Hara, R., Frequency hopping sequences with optimal auto- and cross-correlation properties and related codes, Proc. 10th International Workshop on Algebraic Combinat. Coding Theory, 83-96, Zvenigorod, Russia, Eylül 2006.

[8] Ge, G., Fuji-Hara, R., Miao, Y., Further combinatorial constructions for optimal frequency hopping sequences, Journal of Combinatorial Theory Series A, 113(8), 1699-1718, 2006.

[9] Ge, G., Miao, Y., Yao, Z., Optimal Frequency Hopping Sequences: Auto- and Cross-Correlation Properties IEEE Transaction On Information Theory, 55(2), 867-879, 2009.

[10] Kumar, P.V., Frequency-hopping code sequence designs having large linear span, IEEE Transactions On Information Theory, 34(1), 146-151, 1988.

[11] Lempel, A., Greenberger, H., Families of sequences with optimal Hamming correlation properties, IEEE Transaction On Information Theory, 20, 90-94, 1974.

[12] Lidl, R., Niederreiter, L., Finite Fields, *Cambridge University Press,* Cambridge, U.K., 1997.

[13] Peng, D., Fan, P., Lower bounds on the Hamming auto- and cross correlations

of frequency-hopping sequences, IEEE Transaction On Information Theory, 50, 2149-2154, 2004.

[14] Sarwate, D.V., Reed-Solomon codes and the design of sequences for spread-spectrum multiple-access communications, *IEEE Press*, 1994.

[15] Sarwate, D. V., Comments on Lower bounds on the Hamming auto and cross correlations of frequency-hopping sequences, IEEE Transaction On Information Theory, 51, 1615, 2005.

[16] Simon, M.K., Omura, J.K., Scholtz, R.A., Levitt, B.K., Spread spectrum communications handbook, *McGraw-Hill*, New York, 2002.

[17] Scholtz, R.A., Kumar, P.V., Corrada-Bravo, C.J., Signal design for ultra-wideband radio, *Springer*, London, U.K., 2001.

[18] NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management.

[19] ”Specification of the Bluetooth System Core. Bluetooth resmi web sitesi erişim adresi:

http://www.bluetooth.com/ , erişim tarihi: 25 Kasım 2010.

[20] Kozaczuk, W., Enigma: how the german machine cipher was broken, and how it was read by the allies in World War Two, *University Publications of America*, America, 1984.

EKLER

(2.1) dizileri için MAGMA kodu [Bu kod Seda Kahraman tarafından yazılmıştır.]

Bu kod [4] deki Trace fonksiyonu ile p=3, q=3, m=3 ve l=2 optimal dizi oluşturmasını gerçeklemektedir.

```
p:= 3;       //tek bir asal p:= 3;       //tek bir asal
r:= 1;       //genişlemenin boyutu

K:=FiniteField(p);                    //asal cisim
if r ne 1 then
        p1:=PrimitivePolynomial(K,r);
        M<t>:=ext< K|p1>;    //alt cisim
else
        M<t>:=K;                //alt cisim
end if;

q:= p^r;     //alt cismin boyu
m:= 3;       //tek tamsayı
l:=2;        //atlamanın mertebesi
n:=((q^m)-1) div l;              //dizinin boyu
s:=1;             //gcd(s,q^m-1)=1 olacak şekilde

if m ne 1 then
        p2:=PrimitivePolynomial(M,m);
        F<z>:=ext< M|p2>;             //alt cismin genişlemesi ilkel elemanı z yani alfa
else
        F<z>:=M;
end if;
```

```
t:=z^(l*s);    //beta
Dizi:=[M| ];    //optimal dizi

index1:={} ;
for i:=1 to ((q^m)-1) do
        index1 join:={i};
end for;
index2:={} ;
for j:=1 to n do
        index2 join:={j};
end for;

D_ailesi:=[Dizi : x in index1];    //Optimal dizilerin oluşturduğu dizi

for i in index1 do
        print "  ";
        print "  ";
        print z^i," icin dizi";
        for j in index2 do
                Dizi[j]:=Trace((z^i)*(t^(j-1)));
        end for;
        Dizi;
        D_ailesi[i]:=Dizi;
end for;

//Buradan itibaren Hamming Korelasyonu hesaplanmaktadır.

D1:=[x: x in index2];   //H. Korelasyonu için 1. dizi
D2:=[x: x in index2]; //H. Korelasyonu için 2. dizi
korelasyon:=[0: x in index2];
h_korelasyon:=0;
for i in index1 do
```

```
        D1:=D_ailesi[i];
        print i, ". dizi icin Cross veya auto Korelasyon";
        for j in index1 do
                print j,". dizi ile korelasyonlar:";
                D2:=D_ailesi[j];
                D2 cat:= D2;
                for k in index2 do

                        for l in index2 do
                                if D1[l] eq D2[(l+k-1)] then
                                        korelasyon[k] +:=1;
                                end if;
                        end for;

                end for;
                korelasyon;
                korelasyon:=[0: x in index2];

        end for;

end for;
```

ÖZGEÇMİŞ

Kişisel bilgiler

Adı Soyadı :KÜBRA BAYRAKTAR
Doğum yeri ve tarihi :ANKARA/08.11.1985

Eğitim bilgileri

	Tarih	Yer
İlkokul:	1991-1996	Abidinpaşa İlköğretim Okulu
Ortaokul:	1996-1999	Abidinpaşa İlköğretim Okulu
Lise:	1999-2003	Başkent Lisesi (Y.D.A.)
Üniversite:	2004-2008	Ankara Üniversitesi Matematik Bölümü(Lisans)
Yüksek Lisans:	2008-2010	TOBB ETÜ Matematik Bölümü(Burslu)

İş deneyimi

TOBB Ekonomi ve Teknoloji Üniversitesi'nde Verilen Uygulama Dersleri:
2008-2009 Güz Dönemi MAT 309 Cebir (Emrah Kılıç)
2008-2009 Bahar Dönemi MAT 102 Genel Matematik-II (Haydar Eş)
2008-2009 Yaz Dönemi MAT 102 Genel Matematik-II (Zülfükar Saygı)
2009-2010 GüzDönemi MAT 103 Matematik-I (Arif Sabuncuoğlu)
2009-2010 Bahar Dönemi MAT 103 Matematik-I (Mustafa Bayraktar)
2010-2011 Güz Dönemi MAT 101 Genel Matematik-I (Çetin Ürtiş)

İlgi Alanları:

Kriptoloji, Sayılar Teorisi, Topoloji.

İngilizce Bilgisi:

Konuşma: İyi.
Yazma: İyi.
Dinleme: Orta.