OPTİMAL FREKANS ATLAMALI DİZİLER

Seda KAHRAMAN

YÜKSEK LİSANS TEZİ

MATEMATİK

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Eylül 2011

ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Ünver KAYNAK

Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Prof. Dr. Ömer AKIN

Anabilim Dalı Başkanı

Seda KAHRAMAN tarafından hazırlanan "OPTİMAL 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.

Seda KAHRAMAN

Üniversitesi : **TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü : **Fen Bilimleri Enstitüsü**
Anabilim Dalı : **Matematik**
Tez Danışmanı : **Yrd. Doç. Dr. Zülfükar SAYGI**
Tez Türü ve Tarihi : **Yüksek Lisans - Eylül 2011**

Seda KAHRAMAN

OPTİMAL FREKANS ATLAMALI DİZİLER

ÖZET

Bu tezin amacı, Frekans Atlamalı Kod Bölüşümlü Çoklu Erişim[1] (FH-CDMA), Bluetooth ve ultra geniş bant gibi popüler sistemlerde kullanılan Optimal Frekans Atlamalı Dizilerin (FHS lerin) oluşturulmasıdır. Literatürde optimalliği belirleyen sınırlar bulunmaktadır. Buradaki optimallik Lempel-Greenberger ve Peng-Fan anlamındadır. Bu tezde, 1974 den bugüne yayımlanmış optimal FHS üretim metodları incelenmiş ve bir tabloda toplanmıştır. Ayrıca Lempel-Greenberger Sınırı nın keskin bir sınır olup olmadığının incelenmesi için 1974 te yayımlamış makalede bulunun optimallik sınırı ve ispatı verilmiştir. FHS lerin oluşturulmasında kullanılan cebirsel, kombinatorik vs. gibi bir çok metod vardır. Bunların içinden cebirsel bir üretim metodu olan İz Fonksiyonu ile üretim yapan 4 makale incelenmiş ve bunların MAGMA ile gerçekleştirimi yapılarak örnekleri incelenmiştir. Ayrıca girilen parametrelere göre FHS oluşturan yeni bir MAGMA kodu yazılmıştır ve yeni optimal dizilerin varlığı incelenmiştir. Sabit parametreler için optimal FHS ler bulunmuştur ancak bunlar henüz bir kurala oturtulamamaktadır. Yeni optimal FHS üretim arayışımız devam etmekte olup ilerleyen çalışmalarımızda, İz Fonksiyonunun yanı sıra diğer üretim metodları için de benzer bir çalışma yürütülebilir.

Anahtar Kelimeler: Frekans atlamalı diziler, optimal frekans atlamalı diziler, frekans atlamalı dizi üretim yöntemleri, optimal frekans atlamalı dizi çiftleri, optimal frekans atlamalı dizi ailesi, Lempel-Greenberger Sınırı.

[1] Frequency Hopping Code Division Multiple Access

University : **TOBB Economics and Technology University**
Institute : **Institute of Natural and Applied Sciences**
Science Programme : **Mathematics**
Supervisor : **Assist. Prof. Dr. Zülfükar SAYGI**
Degree Awarded and Date : **M.Sc. - September 2011**

Seda KAHRAMAN

OPTIMAL FREQUENCY HOPPING SEQUENCES

ABSTRACT

The purpose of this thesis is constructing Optimal Frequency Hopping Sequences (FHSs) which are used in popular systems such as Frequency Hopping-Code Division Multiple Access (FH-CDMA), Bluetooth and Ultra-Wide Band. There are bounds in literature determining optimality. The optimality here is by means of Lempel-Greenberger and Peng-Fan. In this thesis, construction methods of optimal FHSs published since 1974 are analysed and gathered in a table. In addition, so as to examine the sharpness of Lempel-Greenberger Bound, the optimality bound and its proof given in the paper published in 1974 take place. There are several methods for constructing optimal FHSs like algebraic, combinatorial e.t.c.. Four papers giving algebraic construction via trace function are analysed and their examples are builded by implementing construction methods in MAGMA. Additionally, a MAGMA code is implemented in order to construct FHSs for entered parameters and new existing optimal FHSs are searched. There are optimal FHSs for some fixed parameters, but there is not captured any pattern yet. Our search for optimal FHS construction is not finished. In our future study, we are planning to do the same study that we have done for Trace function for other techniques.

Anahtar Kelimeler: Frequency hopping sequences, optimal frequency hopping sequences, construction methods of optimal frequency hopping sequences, optimal frequency hopping sequence pairs, optimal frequency hopping sequence families, Lempel-Greenberger Bound.

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren danışmanım Yrd. Doç. Dr. Zülfükar SAYGI'ya, yine lisans ve yüksek lisans eğitimim boyunca kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Matematik Bölümü öğretim üyelerine,

Hiçbir zaman benden yardımlarını esirgemeyen ofis arkadaşlarım Hande Akkocaoğlu, Esra Erdoğan Karaoğlu ve diğer yüksek lisans arkadaşlarıma,

Beni her zaman destekleyen ve bugünlere gelmemi sağlayan aileme teşekkürü borç bilirim.

Bu tez TÜBİTAK tarafından 109T344 referans numaralı "'Cebirsel Eğriler ve Üssel Toplamlar Kullanarak Bazı Kriptografik Uygulamalar"' başlıklı proje tarafından desteklenmiştir. Eğitimim süresince projedeki desteklerinden dolayı TÜBİTAK'a teşekkürü borç bilirim.

İÇİNDEKİLER

ŞEKİLLERİN LİSTESİ

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

BÖLÜM 1

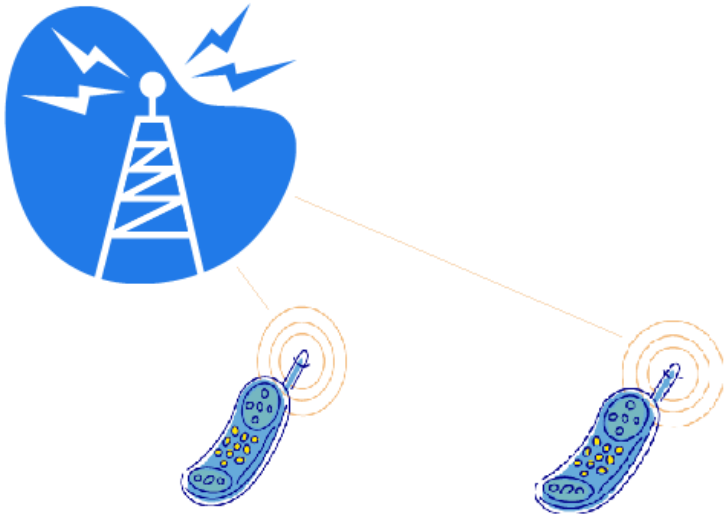
1. Giriş

1.1. Genel Bilgiler

Frekans Atlamalı Yayılı İzge Sistemleri, kısaca FHSS[1], yaygın kullanılan bir dijital modülasyon tekniğidir. Diğer bir digital modülasyon tekniği de Doğrudan Dizi Yayılı İzgedir[2] (kısaca DSSS). Modülasyon terimini biraz açacak olursak, taşıyıcı sinyali denilen yüksek-frekanslı bir dalganın üzerine genellikle bilgi içeren düşük frekanslı bir dalganın bindirilerek taşınmasıdır. Daha açık olarak kablosuz veri gönderme metodudur. Veri iletişimi çağımızda büyük önem taşımaktadır. Özellikle de kablosuz veri iletişimi, hem kurumsal hem askeri hem de kişisel hayatın vazgeçilmezlerindendir. Kablosuz iletim teknolojilerinin daha güvenli ve hatasız olması ve aynı anda çok sayıda kişiye hizmet verebilmesi için modülasyon ve modülasyon teknikleri üzerinde durulması ve geliştirilmesi gereken olgulardır.

FHSS ve DSSS modülasyon tekniklerinin birbirine göre üstün yanları bulunmaktadır [25]. Ancak, FHSS nin geliştirilmesine sebep olan en önemli üstünlüklerinden biri Yakın-Uzak Probleminin etkisini oldukça azaltarak çoklu erişime imkan sağlamasıdır. Yakın-Uzak Problemi şu örnekle anlaşılabilir. Şekil 1.1. de olduğu gibi bir alıcı ve iki verici olduğunu düşünelim. Bu iki verici eş zamanlı olarak aynı güçle veri gönderdiğinde ters kare kuralına göre alıcıya yakın olan vericinin gönderdiği daha güçlü gelecektir. Böylece uzak olanın gönderdiği yakındakinin gürültüsü olacaktır [26]. FHSS tekniğinde vericiler frekanslar arasında atlayarak veri gönderdiği için çakışma olmadığı sürece alıcı problemsiz olarak her ikisinin de gönderdiği veriyi alabilecektir. Çakışma olmaması için de FHSS de kullanılan frekans atlamalı dizilerin optimal olması gerekir. Dizilerin optimal olması ile ilgili ayrıntılı bilgi ilerleyen bölümlerde verilecektir.

[1] Frequency Hopping Spread Spectrum Systems
[2] Direct Sequence Spread Spectrum



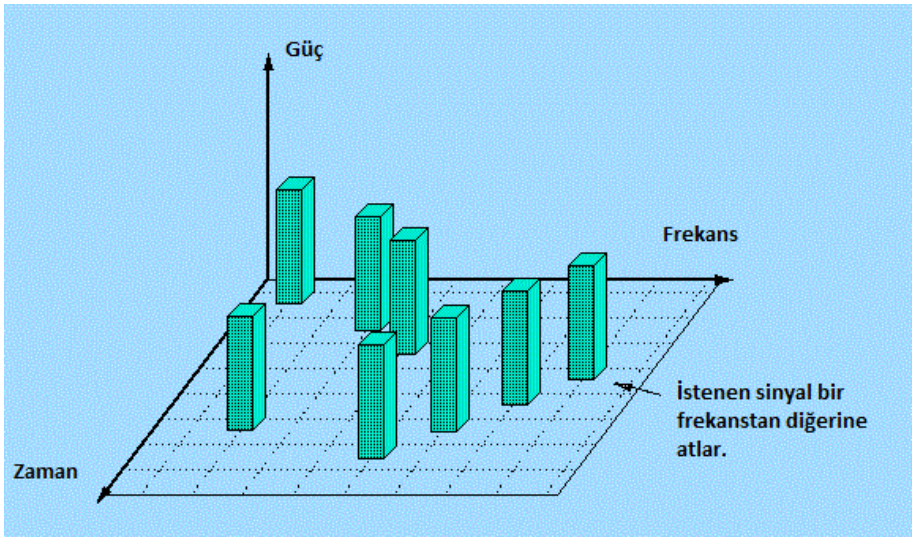
Şekil 1.1. Yakın-Uzak Problemi

Frekans Atlamalı Yayılı İzge Sistemleri, karıştırıcı önleme[3], güvenli ve çoklu erişim sağlama özellikleri ile ordu radyo iletişimi, mobil iletişim, modern radar ve deniz radarı yankı-konum sistemlerinde[4] yaygın olarak kullanılır [7], [14]. Özellikle de, Frekans Atlamalı Kod Bölüşümlü Çoklu Erişim (FH-CDMA), Bluetooth ve ultra geniş bant gibi popüler sistemler kullanım alanları içindedir [10], [19], [23], [24].

Frekans atlamalı sistemlerde verici, taşıyıcı frekansını belli bir örüntüye göre değiştirir. Bu örüntüler frekans atlamalı dizi denilen sözde-rastgele kodlardır. Yani, elemanları frekanslar olan dizi mantığında (elemanların sırası önemli) sıralanmış kodlardır. Elemanların sırası atlanacak frekansların sırasını belirlemektedir. Gönderilecek veri, dizi elemanlarının sırasına göre belli zaman aralıklarında frekanslar üzerinde atlayarak parça parça iletilir. Böylelikle hem üçüncü şahıslar tarafından takip edilmesi zor olmakta hem de bir zaman aralığında sadece bir frekans kullanıldığı için boşta kalan frekanslardan diğer vericiler iletim yapabilmektedir. Böylelikle frekans atlamalı sistemler çoklu erişimi rahatlıkla sağlayabilirler. Şekil 1.2., bir

[3] antijamming
[4] sonar echo-location systems

vericinin belli zaman aralıklarında eşit miktarda güç ile frekanslar arasında atlama grafiğini göstermektedir.



Şekil 1.2. Frekans Atlamalı Sistemler için Zaman-Frekans-Güç Grafiği [27]

1.2. Bazı Tanımlar

Bu bölümde Frekans Atlamalı Diziler ile ilgili literatürdeki bazı tanımlar verilecektir.

Tanım 1.2.0.1. Olabilecek bütün frekans değerlerinden oluşan

$$\mathbb{F} = \{f_0, f_1, \cdots, f_{l-1}\}$$

kümesine *Alfabe* denir.

Örnek 1.2.0.2. Bazı alfabe örnekleri şöyle verilebilir:
$\mathbb{F}_2 = \{0, 1\}$
$\mathbb{F}_{2^2} = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$
$\mathbb{F}_{q^m}$ şeklindeki tüm sonlu cisimler.

Tanım 1.2.0.3 (Frekans Atlamalı Dizi). $\mathbb{F}$ bir alfabe ve *S* kümesi de $\mathbb{F}$ üzerinde uzunluğu v olan bütün dizilerin kümesi olsun. *S* nin herbir elemanına $\mathbb{F}$ üzerinde v-uzunluğunda *Frekans*

Atlamalı Dizi denir. Kısaca FHS ile gösterilir.

Daha önce belirtildiği gibi FHS denilen sözde rastgele kodların hem rastgele hem de çakışmayı mümkün olduğunca azaltan nitelikte olması çok önemlidir [17], [14], [24]. Bu özellikleri sağlayan FHS ler üretmek için literatürde bir çok çalışma yapılmıştır. Bir dizinin optimal olması kendi faz-kaymışlarına olabildiğince az benzemesi anlamına gelmektedir. Örneğin bir FHS üzerinden iletim yapılmaya başlansın. t birim zaman sonra bir başkası aynı FHS ie veri göndermeye başlarsa kullanılan FHS optimal olmadığında t kez kaymış haliyle k tane terimi aynı ise k kez çakışma oluşacaktır. Eğer optimal ise çakışma sayısı k mümkün olduğunca az olacaktır.

Örnek 1.2.0.4. $\mathbb{F}_3$ alfabesi üzerinde uzunluğu $v = 13$ olan X=(0, 0, 1, 1, 2, 2, 0, 0, 1, 1, 2, 2, 0) frekans atlamalı dizisi üzerinden iletim yapıldığını düşünelim. Bir başkasının da t=1 birim zaman sonra iletime başladığını düşünelim. X dizisinin bir birim faz-kaymışı, yani bir birim sola kaymışı X'=(0, 1, 1, 2, 2, 0, 0, 1, 1, 2, 2, 0, 0) dizisidir. Bu iki dizinin çakışmaları aşağıdaki tabloda koyu olarak işaretlenmiştir.

X	**0**	0	**1**	1	**2**	2	**0**	0	**1**	1	**2**	2	**0**
X'	**0**	1	**1**	2	**2**	0	**0**	1	**1**	2	**2**	0	**0**

Tabloda da görüldüğü üzere aynı FHS yi kullanarak farklı zamanlarda iletim yapmaya başlayan bu iki kişi tam 7 kez aynı frekansı kullanmaya çalışacaklardır. Diğer bir deyişle 7 kez çakışma olacak ve iletim düzgün yapılamayacaktır.

Benzer şekilde iki farklı FHS nin ya da bunların faz-kaymışlarının da terimlerinin bir kısmı aynı olacaktır. Dizilerin ne kadar çakışmaya neden olduğunu görmek için Hamming Korelasyonu hesaplanmaktadır. Çünkü Hamming Korelasyonu her bir t faz-kaymışı için çakışmaları sayan bir fonksiyondur. Tanımı şu şekilde verilebilir.

Tanım 1.2.0.5 (Hamming Korelasyonu). İki frekans atlamalı dizi $X, Y \in S$ verildiğinde, bunlar arasındaki *Hamming Korelasyonu* $H_{X,Y}$ aşağıdaki şekilde tanımlanır:

$$H_{X,Y}(t) = \sum_{i=0}^{v-1} h[x_i, y_{i+t}] \quad , \quad 0 \leq t < v \tag{1.2.1}$$

Burada

$$h[a,b] = \begin{cases} 1 & \text{, eğer } a = b \text{ ise} \\ 0 & \text{, diğer durumlar} \end{cases} \tag{1.2.2}$$

şeklindedir ve indis pozisyonundaki her işlem mod v de yapılır.

Herhangi iki FHS nin $0 \leq t < v$ kaymışı için Hamming korelasyonu tanımlandı. Şimdi bu tanımdan yararlanarak aşağıdaki tanımlar verilebilir.

Tanım 1.2.0.6. Birbirinden farklı $\forall\, X, Y \in S$ FHS leri için:
Hamming Oto-Korelasyonu:

$$H(X) = \max_{1 \leq t < v} \{H_{XX}(t)\}$$

Hamming Çapraz-Korelasyonu:

$$H(X,Y) = \max_{0 \leq t < v} \{H_{XY}(t)\}$$

Dizi çiftleri için Hamming Korelasyonu:

$$M(X,Y) = \max\{H(X), H(Y), H(X,Y)\}$$

Dizi aileleri için Hamming Korelasyonu:

$$M(\mathbb{F}) = \max\{\max_{X \in \mathbb{F}} H(X), \max_{X,Y \in \mathbb{F}, X \neq Y} H(X,Y)\}$$

eşitlikleri ile tanımlanır.

Örnek 1.2.0.7. Örnek 1.2.0.4 deki X dizisinin Hamming Oto-Korelasyonunu hesaplayalım:

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

$H_{X,X}(t)$ değerlerine bakılacak olursa X dizisinin Hamming Oto-Korelasyonu bu değerlerin maksimumu olduğundan $H(X) = 10$ olarak bulunur.

Hamming korelasyonları tanımlarından sonra, optimallik için Hamming Korelasyonu nasıl olmalı sorusuna cevap vermek gerekmektedir. Şimdiye kadar bir kaç kez belirtildiği üzere bunun için çakışmanın mümkün olduğunca az olması gerekir. O halde, Hamming korelasyonu çakışmaları saydığından bir dizinin optimal olması o dizinin Hamming Oto-Korelasyonunun diğer dizilere göre düşük olmasını gerektirir. Benzer tanım dizi çiftleri için de geçerlidir. Bundan yola çıkarak optimallik kriterleri şu şekilde verilebilir.

Optimallik Kriterleri:

O.1 $\forall X^{'} \in S$ için $H(X) \leq H(X^{'})$ sağlanıyorsa $X \in S$ dizisine *Optimal* denir.

O.2 $\forall X^{'}, Y^{'} \in S$, $X^{'} \neq Y^{'}$ için $M(X,Y) \leq M(X^{'}, Y^{'})$ sağlanıyorsa X, Y ayrık dizilerine *Optimal Çift* denir.

O.3 $\mathbb{F}$ deki her ayrık çift optimal çift ise $\mathbb{F} \subset S$ alt kümesine *Optimal Aile* denir.

Optimallik kriterlerine dikkat edilirse optimalliği kontrol etmek özellikle dizinin boyu v büyüdüğünde çok zordur. Çünkü v uzunluğundaki tüm dizilerin (S nin elemanlarının) her t kaymışı için Hamming Korelasyonları hesaplanmalı ve bunların maksimumları alınmalı. Bu işlem v büyüdüğünde zorlaştığı gibi kullanılan frekans alfabesinin büyümesiyle de elle hesaplaması imkansız hale gelebilir. Bu nedenle Hamming Korelasyonları için sınırlar bulunmuştur. Bu tezde literatürde en çok kullanılan iki sınır verilecektir. Sınırların ilki 1974 yılında Lempel ve Greenberger [1] tarafından yayınlanmış olup dizilerin Hamming Oto-Korelasyonu içindir. Bu sınır Lemma 1.2.0.8 de verilmiş olup ilerleyen bölümlerde ayrıntılı olarak ispatı verilecektir. İkinci sınır ise 2004 yılında Peng ve Fan [8] tarafından yayınlanmıştır. Bu sınır ise dizi aileleri için olup $N = 2$ olarak alındığında dizi çiftleri için geçerlidir ve Lemma 1.2.0.10 da verilmiştir. Bu sınırlar sayesinde bir dizinin, dizi çiftinin ya da dizi ailesinin optimalliğine bak-

mak için bütün *S* kümesindeki FHS lerin korelasyonlarını hesaplamaya gerek kalmamaktadır. Eğer korelasyon değeri sınıra eşit ise dizi, dizi çifti veya aileleri için optimaldir denir.

Lemma 1.2.0.8 (Lempel-Greenberger Sınırı(1974)). [1] *$|\mathbb{F}| = q$ olmak üzere her v uzunluğundaki $X \in S$ frekans atlamalı dizisi için, ϵ, $v \equiv \epsilon$ (mod q) denkliğini sağlayan en küçük negatif olmayan tamsayı olmak üzere;*

$$H(X) \geq \left\lceil \frac{(v-\epsilon)(v+\epsilon-q)}{q(v-1)} \right\rceil \tag{1.2.3}$$

eşitsizliği sağlanır.

Örnek 1.2.0.9. $q = 4$ ve $v = 5$ için $v = 5 \equiv 1 = \epsilon$ (mod 4) olduğundan

$$H(X) \geq \left\lceil \frac{(5-1)(5+1-4)}{4(5-1)} \right\rceil = \left\lceil \frac{8}{16} \right\rceil = 1$$

olur.

Lemma 1.2.0.10 (Peng-Fan Sınırı(2004)). [8] *Kabul edelim ki $\mathbb{F} \subset S$, q-boyutlu alfabe üzerinde v-uzunluğundaki N diziden oluşan küme olsun. $I = \lfloor vN/q \rfloor$ olarak tanımlanırsa*

$$M(\mathbb{F}) \geq \left\lceil \frac{(vN-q)v}{(vN-1)q} \right\rceil \tag{1.2.4}$$

ve

$$M(\mathbb{F}) \geq \left\lceil \frac{2IvN-(I+1)Iq}{(vN-1)N} \right\rceil \tag{1.2.5}$$

sağlanır.

Örnek 1.2.0.11. $F = \{X, Y, Z\}$ dizi ailesi verilsin. $N = 3$, $q = 4$ ve $v = 5$ için

$$M(F) \geq \left\lceil \frac{(5 \cdot 3-4)5}{(5 \cdot 3-1)4} \right\rceil = \left\lceil \frac{55}{56} \right\rceil = 1$$

olur.

BÖLÜM 2

2. Lempel-Greenberger Sınırı

Bu bölümde [1] makalesinin II. Bölümü ayrıntılarıyla incelenecektir.

2.1. Optimal Dizilerin Üretilmesi ve Lempel-Greenberger Sınırı

Verilecek olan üretim metodunda ana araç olarak $GF(p)$ üzerinde doğrusal üretilmiş maksimal-uzunluk dizileri[1] (kısaca M-dizileri) kullanılacaktır. Burada p bir asal sayıdır ve GF(p), elemanları basitçe $0, 1, \ldots, p-1$ ile gösterilen ve işlemleri mod-p de çarpma ve toplama olan sonlu cisimdir. GF(p) üzerinde n. dereceden bir $B = b(j)$ M-dizisi, periyodu (uzunluğu) $q = p^n - 1$ olan

$$\sum_{i=0}^{n} f_i b(j-i) = 0$$

doğrusal yineleme ilişkisini sağlayan bir dizidir. Burada yineleme katsayıları olan f_i ler GF(p) üzerindeki $f(z) = \sum_{i=0}^{n} f_i z^i$ ilkel polinomundan alınır.

M-dizileri hakkında çok iyi bilinen bazı özellikler şöyledir:

M.1 Her p asalı ve her pozitif n tamsayısı için, GF(p) üzerinde uzunluğu $q = p^n - 1$ olan bir m-dizisi vardır.

M.2 Kabul edelim ki W, GF(p) üzerindeki tamamı-sıfır olanlar hariç bütün n-lilerin kümesi olsun ve yine kabul edelim ki GF(p) üzerindeki $q = p^n - 1$ uzunluğundaki M-dizisi $B = b(j)$ olsun. Bu taktirde her bir $w \in W$ için $0 \leq j < q$ olacak şekilde bir tek j

[1] Linearly generated maximal-length sequences

indeksi vardır, öyle ki

$$w = b(j), b(j+1), \ldots, b(j+n-1)$$

sağlanır.

M.3 Bir M-dizisinin q devirli faz-kaymışları[2] ve q uzunluğundaki tamamı-sıfır dizisi mod-p de terimsel toplama altında değişmeli grup oluştururlar. Buna M-dizilerinin "kaydır ve topla" özelliği denir.

M-dizilerinin, optimal dizilerin oluşturulmasındaki kullanımını açıklamak için biraz notasyon ve tanım verilecektir. p bir asal, k pozitif bir tamsayı olarak verildiğinde P_k, P üzerindeki bütün k uzunluğundaki kelimeleri (k-lılar) göstermek üzere kabul edelim ki

$$P = \{0, 1, \ldots, p-1\}$$
$$P_k = \{0, 1, \ldots, p^k - 1\}$$

olsun.

$w = (w_0, w_1, \ldots, w_{k-1})$ dizisini $w\sigma = \sum_{i=0}^{k-1} w_i p^i \in P_k$ ile ilişkilendiren P^k dan P_k ya tanımlı doğal birebir bir σ dönüşümü vardır.

Şimdi P üzerinde q uzunluğundaki $X = x(j)$ dizisi verilsin. Kabul edelim ki X(j,k), X in ardışık elemanlarından oluşan j. k uzunluğundaki kelimeyi$(x(j), x(j+1), \ldots, x(j+k-1))$ göstersin. Ayrıca kabul edelim ki $\mu_x(w)$, her bir $w \in P^k$ için $w = X(j,k)$ olacak şekilde X in ayrık j, $0 \leq j < q$, pozisyonlarının sayısını versin. (Genelde olduğu gibi x(q-1) elemanını x(0) takip eder ve pozisyon indisleri mod-q da alınır.) $\mu_x(w)$, w nun X deki görünme sayısını[3] verir. Eğer σ dönüşümü X in ardışık k-lılarına uygulanırsa, P_k üzerinde q uzunluğundaki $Y = y(j)$

[2]The q cyclic phase-shifts
[3]Multiplicity

dizileri elde edilir. Burada

$$y(j) = X(j,k)\sigma = \sum_{i=0}^{k-1} x(j+i)p^i, \quad 0 \leq j < q \tag{2.1.1}$$

olur. Daha kompakt olarak X ile Y arasındaki ilişki

$$Y = X_{\sigma_k}$$

şeklinde verilir ve Y ye X in σ_k-transformu denir.

Örnek 2.1.0.12. [1] p=3, n=3, q=$3^3 - 1$, k=2 olsun.

$$X = 0\,0\,1\,1\,1\,0\,2\,1\,1\,2\,1\,0\,1\,0\,0\,2\,2\,2\,0\,1\,2\,2\,1\,2\,0\,2 \tag{2.1.2}$$

üçlü dizisinin σ_2-transformunu aşağıdaki şekilde bulunur:

$Y(j) = X(j)\sigma_2 = \sum_{i=0}^{2-1} x(j+i)3^i, \qquad 0 \leq j < 3^3 - 1 = 26$ için hesaplanırsa

$$Y(0) = X(0)\sigma_2 = \sum_{i=0}^{1} x(0+i)3^i = X(0).3^0 + X(1).3^1 = 0.1 + 0.3 = 0$$

$$Y(1) = X(1)\sigma_2 = \sum_{i=0}^{1} x(1+i)3^i = X(1).3^0 + X(2).3^1 = 0.1 + 1.3 = 3$$

$$Y(2) = X(2)\sigma_2 = \sum_{i=0}^{1} x(2+i)3^i = X(2).3^0 + X(3).3^1 = 1.1 + 1.3 = 4$$

$$Y(3) = X(3)\sigma_2 = \sum_{i=0}^{1} x(3+i)3^i = X(3).3^0 + X(4).3^1 = 1.1 + 1.3 = 4$$

$$Y(4) = X(4)\sigma_2 = \sum_{i=0}^{1} x(4+i)3^i = X(4).3^0 + X(5).3^1 = 1.1 + 0.3 = 1$$

$$Y(5) = X(5)\sigma_2 = \sum_{i=0}^{1} x(5+i)3^i = X(5).3^0 + X(6).3^1 = 0.1 + 2.3 = 6$$

$$Y(6) = X(6)\sigma_2 = \sum_{i=0}^{1} x(6+i)3^i = X(6).3^0 + X(7).3^1 = 2.1 + 1.3 = 5$$

$$Y(7) = X(7)\sigma_2 = \sum_{i=0}^{1} x(7+i)3^i = X(7).3^0 + X(8).3^1 = 1.1 + 1.3 = 4$$

$$Y(8) = X(8)\sigma_2 = \sum_{i=0}^{1} x(8+i)3^i = X(8).3^0 + X(9).3^1 = 1.1 + 2.3 = 7$$

$$Y(9) = X(9)\sigma_2 = \sum_{i=0}^{1} x(9+i)3^i = X(9).3^0 + X(10).3^1 = 2.1 + 1.3 = 5$$

$$Y(10) = X(10)\sigma_2 = \sum_{i=0}^{1} x(10+i)3^i = X(10).3^0 + X(11).3^1 = 1.1 + 0.3 = 1$$

$$Y(11) = X(11)\sigma_2 = \sum_{i=0}^{1} x(11+i)3^i = X(11).3^0 + X(12).3^1 = 0.1 + 1.3 = 3$$

$$Y(12) = X(12)\sigma_2 = \sum_{i=0}^{1} x(12+i)3^i = X(12).3^0 + X(13).3^1 = 1.1 + 0.3 = 1$$

$$Y(13) = X(13)\sigma_2 = \sum_{i=0}^{1} x(13+i)3^i = X(13).3^0 + X(14).3^1 = 0.1 + 0.3 = 0$$

$$Y(14) = X(14)\sigma_2 = \sum_{i=0}^{1} x(14+i)3^i = X(14).3^0 + X(15).3^1 = 0.1 + 2.3 = 6$$

$$Y(15) = X(15)\sigma_2 = \sum_{i=0}^{1} x(15+i)3^i = X(15).3^0 + X(16).3^1 = 2.1 + 2.3 = 8$$

$$Y(16) = X(16)\sigma_2 = \sum_{i=0}^{1} x(16+i)3^i = X(16).3^0 + X(17).3^1 = 2.1 + 2.3 = 8$$

$$Y(17) = X(17)\sigma_2 = \sum_{i=0}^{1} x(17+i)3^i = X(17).3^0 + X(18).3^1 = 2.1 + 0.3 = 2$$

$$Y(18) = X(18)\sigma_2 = \sum_{i=0}^{1} x(18+i)3^i = X(18).3^0 + X(19).3^1 = 0.1 + 1.3 = 3$$

$$Y(19) = X(19)\sigma_2 = \sum_{i=0}^{1} x(19+i)3^i = X(19).3^0 + X(20).3^1 = 1.1 + 2.3 = 7$$

$$Y(20) = X(20)\sigma_2 = \sum_{i=0}^{1} x(20+i)3^i = X(20).3^0 + X(21).3^1 = 2.1 + 2.3 = 8$$

$$Y(21) = X(21)\sigma_2 = \sum_{i=0}^{1} x(21+i)3^i = X(21).3^0 + X(22).3^1 = 2.1 + 1.3 = 5$$

$$Y(22) = X(22)\sigma_2 = \sum_{i=0}^{1} x(22+i)3^i = X(22).3^0 + X(23).3^1 = 1.1 + 2.3 = 7$$

$$Y(23) = X(23)\sigma_2 = \sum_{i=0}^{1} x(23+i)3^i = X(23).3^0 + X(24).3^1 = 2.1 + 0.3 = 2$$

$$Y(24) = X(24)\sigma_2 = \sum_{i=0}^{1} x(24+i)3^i = X(24).3^0 + X(25).3^1 = 0.1 + 2.3 = 6$$

$$Y(25) = X(25)\sigma_2 = \sum_{i=0}^{1} x(25+i)3^i = X(25).3^0 + X(0).3^1 = 2.1 + 0.3 = 2$$

elde edilir. Sonuç olarak Y dizisi

$$Y = 0\,3\,4\,4\,1\,6\,5\,4\,7\,5\,1\,3\,1\,0\,6\,8\,8\,2\,3\,7\,8\,5\,7\,2\,6\,2 \tag{2.1.3}$$

şeklinde bulunur.

Verilecek olan optimal dizi üretimi aşağıdaki sonuca dayandırılacaktır.

Teorem 2.1.0.13. [1] Kabul edelim ki X, GF(p) üzerinde $q = p^n - 1$ uzunluğundaki M-dizisi olsun. Bu takdirde, her bir k için X in σ_k-transformu P_k üzerinde q uzunluğunda bir optimal dizi verir.

Bu sonuç ispatlanırken $k < n$ durumlarına bakılacaktır. Çünkü $k \geq n$ durumunda M-dizilerinin (M.2) özelliğinden k-lıların X içinde görünme sayısı en fazla 1 dir. Daha açık şekilde, X deki k-lıların kümesine W denirse, $k = n$ için $\forall w \in W$ k-lısı (M.2) gereğince X içinde yalnızca bir kez görünür. Dolayısıyla $k > n$ olduğunda da k-lıların ilk n elemanı X içinde yalnız bir kez göründüğünden aynı durum $k > n$ için de geçerli olur. Böylece her k-lı ayrık olduğundan $Y = X\sigma_k$ nın bütün elemanları ayrık olacaktır. Aşağıdaki örnek $k = n$ durumu için verilmiştir.

Örnek 2.1.0.14. [1] Örnek 2.1.0.12 deki

$$X = 0\,0\,1\,1\,1\,0\,2\,1\,1\,2\,1\,0\,1\,0\,0\,2\,2\,2\,0\,1\,2\,2\,1\,2\,0\,2$$

dizisini düşünelim. Bu örnekte n=3 idi. k=3 alarak kontrol edelim.
Çizelge Çizelge 2.1. de görüldüğü üzere görünme sayısı 1 dir. Yani bütün elemanlar ayrıktır.

Y dizisinin her elemanı ayrık olduğundan ve Korelasyon Fonksiyonu her zaman ≥ 0 olduğundan $H_{YY}(\tau) = 0$ olur ve böylece $\forall \tau \neq 0$ için Y (O.1) optimallik kriterini aşikar olarak sağlar.

Çizelge 2.1. X dizisi için k=3 lülerin görünme sıklığı

Sıra No	k=3 lü	Görünme Sayısı	Sıra No	k=3 lü	Görünme Sayısı
1	0 0 1	1	14	0 0 2	1
2	0 1 1	1	15	0 2 2	1
3	1 1 1	1	16	2 2 2	1
4	1 1 0	1	17	2 2 0	1
5	1 0 2	1	18	2 0 1	1
6	0 2 1	1	19	0 1 2	1
7	2 1 1	1	20	1 2 2	1
8	1 1 2	1	21	2 2 1	1
9	1 2 1	1	22	2 1 2	1
10	2 1 0	1	23	1 2 0	1
11	1 0 1	1	24	2 0 2	1
12	0 1 0	1	25	0 2 0	1
13	1 0 0	1	26	2 0 0	1

Şimdi daha ilginç olan $k < n$ durumları için Teorem 2.1.0.13 in ispatını birkaç lemmaya bölünerek verilecektir.

Lemma 2.1.0.15. [1] *Kabul edelim ki X bir M-dizisi olsun ve Y, X in* $1 \leq k \leq n$ *olmak üzere* $q = p^n - 1$ *uzunluğundaki* σ_k*-transformu olsun. Bu takdirde her bir* $v \in P_k$ *için*

$$\mu_Y(v) = \begin{cases} p^{n-k} - 1, & \textit{eğer } v = 0 \\ p^{n-k}, & \textit{eğer } v \neq 0 \end{cases} \tag{2.1.4}$$

olur.

İspat: $w \in P^k$ k-lısı σ-dönüşümü altında $v \in P_k$ elemanına dönüştürülmüş olsun. Yani $w\sigma = \sum_{i=0}^{k-1} w_i p^i = v$ olsun. X ile Y arasındaki ilişkiden dolayı w nun X de görünme sayısının $w\sigma = v$ nin Y de görünme sayısına eşit olduğu aşikardır. Yani

$$\mu_X(w) = \mu_Y(w\sigma) = \mu_Y(v) \tag{2.1.5}$$

sağlanır. $w = (w'_0, w'_1, \ldots, w'_{k-1})$ olacak şekilde p^{n-k} tane ayrık $w' = (w'_0, w'_1, \ldots, w'_{n-1}) \in$

P^n n-lisi vardır. 0^n tamamı-sıfır n-lisini göstermek üzere (M.2) özelliğinden

$$\mu_X(w') = \begin{cases} 0, & \text{eğer } w' = 0^n \\ 1, & \text{eğer } w \neq 0^n \end{cases} \tag{2.1.6}$$

sağlanır. (2.1.6) den

$$\mu_X(w) = \begin{cases} p^{n-k} - 1, & \text{eğer } w = 0^k \\ p^{n-k}, & \text{eğer } w \neq 0^k \end{cases} \tag{2.1.7}$$

olduğu açıktır. (2.1.7) ve (2.1.5) gereğince

$$\mu_Y(v) = \begin{cases} p^{n-k} - 1, & \text{eğer } v = 0 \\ p^{n-k}, & \text{eğer } v \neq 0 \end{cases}$$

elde edilir. Bu da istenilendir. □

Lemma 2.1.0.16. [1] *Kabul edelim ki $X = x(j)$ ve $X' = x'(j)$ P üzerinde q uzunluklu diziler olsun ve kabul edelim ki $Y = y(j)$ ve $Y' = y'(j)$ onların göreli*[4] *σ_k-transformları olsunlar. $Z = X - X'$, X ile X' arasındaki terimsel mod p farkı*[5] *olmak üzere*

$$H_{YY'}(0) = \mu_Z(0^k) \tag{2.1.8}$$

olur.

İspat: Hamming Korelasyonun tanımı gereğince,

$$H_{X,Y}(t) = \sum_{i=0}^{v-1} h[x_i, y_{i+t}] \quad , \quad 0 \leq t < v$$

[4]respective
[5]termwise mod p difference

olduğundan

$$H_{YY'}(0) = \sum_{j=0}^{q-1} h[y(j), y'(j)]$$

sağlanır. (2.1.1) gereğince

$$y(j) = X(j,k)\sigma = \sum_{i=0}^{k-1} x(j+i)p^i, \quad 0 \leq j < q$$

olduğundan

$$y(j) = y'(j) \quad \Longleftrightarrow \quad X(j,k) = X'(j,k)$$

veya

$$y(j) = y'(j) \quad \Longleftrightarrow \quad Z(j,k) = 0^k \tag{2.1.9}$$

olur. (1.2.2) gereğince

$$h[a,b] = \begin{cases} 1, & \text{eğer } a = b \text{ ise} \\ 0, & \text{diğer durumlar} \end{cases}$$

olduğundan ve (2.1.9) ifadesinden

$$H_{YY'}(0) = \mu_Z(0^k)$$

elde edilir. Böylece ispat tamamlanır. □

Lemma 2.1.0.17. [1] *Kabul edelim ki* $Y = y(j)$, $1 \leq k \leq n$ *için* $q = p^n - 1$ *uzunluğundaki*

$X = x(j)$ *M-dizisinin* σ_k*-transformu olsun. Bu taktirde,*

$$H_{YY}(\tau) = \begin{cases} q, & \textit{eğer } \tau = 0 \\ p^{n-k} - 1, & \textit{eğer } \tau \neq 0 \end{cases} \tag{2.1.10}$$

olur.

İspat: $\tau = 0$ durumunda dizinin kendisiyle korelasyonuna bakılacağından çakışma sayısı dizinin uzunluğu olan q değerine eşit olur. Böylece Hamming korelasyonu q olur. Dolayısıyla bu durum aşikardır.

$\tau \neq 0$ durumunu inceleyelim. Kabul edelim ki γ^τ,

$$X_{\gamma^\tau} = \{x(j)\}\,\gamma^\tau = \{x(j+\tau)\} \tag{2.1.11}$$

şeklinde tanımlanan kaydırma operatörü olsun. Açıkça görülüyor ki Y, X in σ_k-transformu ise

$$Y_{\gamma^\tau} = (X_{\gamma^\tau})\sigma_k \tag{2.1.12}$$

olur. Yani Y_{γ^τ} da X_{γ^τ} nun σ_k-transformu olur. $Z = X - X'$ ve

$$X' = \{x'(j)\} = X_{\gamma^\tau}$$

$$Y' = \{y'(j)\} = Y_{\gamma^\tau} \tag{2.1.13}$$

dersek,

$$H_{YY}(\tau) = \sum_{j=0}^{q-1} h[y(j), y(j+\tau)]$$

$$= \sum_{j=0}^{q-1} h[y(j), y'(j)] \tag{2.1.14}$$

$$= H_{YY'}(0) \tag{2.1.15}$$

elde edilir. Lemma 2.1.0.16 gereğince de

$$H_{YY}(0) = \mu_Z(0^k) \tag{2.1.16}$$

elde edilir. $Z = X - X_{\gamma^\tau}$ olduğundan (M.3) özelliği gereğince $\forall \tau \neq 0$ için, Z, X in başka bir devirsel kaymışıdır. 0^k nın görünme sıklığı X in her devirsel kaymışı için aynı olduğundan (2.1.16) ifadesi

$$H_{YY}(0) = \mu_Z(0^k), \quad \tau \neq 0 \tag{2.1.17}$$

ifadesine indirgenir. Sonuç olarak da

$$\mu_Y(v) = \begin{cases} p^{n-k} - 1, & \text{eğer } v = 0 \\ p^{n-k}, & \text{eğer } v \neq 0 \end{cases}$$

olduğundan ve (2.1.17) gereğince

$$H_{YY}(\tau) = p^{n-k} - 1, \quad \tau \neq 0 \tag{2.1.18}$$

elde edilir. Böylece ispat tamamlanır. □

(2.1.2) deki X dizisi GF(3) üzerinde $q = 3^3 - 1 = 26$ uzunluğunda bir M-dizisidir. X in sağladığı doğrusal yineleme[6]

$$x(j) = x(j-1) - x(j-3)$$

şeklindedir. (2.1.3) deki $Y = X_{\sigma_2}$ dizisi için, (2.1.4) gereğince sıfırdan farklı her $v \in P_2$ verildiğinde $\mu_Y(0) = 3^{3-2} - 1 = 2$ ve $\mu_Y(v) = 3^{3-2} = 3$ olduğu ayrıca (2.1.10) gereğince $\tau \neq 0$ için $H_{YY}(\tau) = 3^{3-2} - 1 = 2$ olduğu kolayca kontrol edilebilir.

Teorem (2.1.0.13) ün ispatını tamamlamak için bir lemmaya daha ihtiyaç vardır.

Lemma 2.1.0.18. [1] *$|A| = m$ olacak şekilde bir A alfabesi üzerindeki q uzunluğundaki her $Y = y(j)$ dizisi için b, $q \equiv b$ (mod m) olacak şekildeki en küçük negatif olmayan kalan olmak üzere,*

$$H(Y) \geq \frac{(q-b)(q+b-m)}{m(q-1)} \tag{2.1.19}$$

sağlanır. ($H(Y)$, H_{YY} nin maksimum faz-dışı değeridir.)

İspat: $\overline{H}(Y)$, H_{YY} nin faz-dışı ortalama değeri olmak üzere

$$\sum_{\tau=0}^{q-1} H_{YY}(\tau) = q + \sum_{\tau=1}^{q-1} H_{YY}(\tau) = q + (q-1)\overline{H}(Y) \tag{2.1.20}$$

[6] linear recurrence

olur. Ayrıca

$$\sum_{\tau=0}^{q-1} H_{YY}(\tau) = \sum_{\tau=0}^{q-1}\sum_{j=0}^{q-1} h\left[y(j), y(j+\tau)\right]$$

$$= \sum_{j=0}^{q-1}\sum_{\tau=0}^{q-1} h\left[y(j), y(j+\tau)\right]$$

$$= \sum_{j=0}^{q-1} \mu_Y(y(j))$$

$$= \sum_{w\in A} \left[\mu_Y(w)\right]^2 \tag{2.1.21}$$

sağlanır. (2.1.20) ve (2.1.21) birleştirilirse

$$\overline{H}(Y) = \frac{1}{q-1}(\sum_{w\in A} \left[\mu_Y(w)\right]^2 - q) \tag{2.1.22}$$

bulunur. Kabul edelim ki,

$$\alpha = \min_{\mu_Y} \sum_{w\in A} \left[\mu_Y(w)\right]^2) \tag{2.1.23}$$

olsun. Buradaki minimizasyon, A üzerinde

$$\sum_{w\in A} \mu_Y(w) = q \tag{2.1.24}$$

kısıtını sağlayan bütün negatif olmayan tamsayı değerli μ_Y görünme sıklığı dağılımları üzerindendir. Verilen kısıtlar altında bir μ_Y dağılımının α nın minimum değerini, μ_Y nin mümkün olduğunca düzgün dağılması gerek ve yeter şartı altında aldığını göstermek basit bir integral

programlama alıştırmasıdır. Yani, eğer

$$q = em + f, \quad 0 \leq f < m \tag{2.1.25}$$

ise μ_Y nin en aza indiren dağılım[7] olması için gerek ve yeter şart A nın $m - f$ elemanının görünme sıklığının $\mu_Y(w) = e$ ve kalan f elemanının görünme sıklığının $\mu_Y(w) = e + 1$ olmasıdır. Daha iyi anlamak için şu şekilde bir μ_Y dağılımı düşünün:

$$\exists w_1, w_2 \in A \quad \ni \quad \mu_Y(w_1) - \mu_Y(w_2) > 1$$

ve bu dağılımı w_1 için $\mu'_Y(w_1) = \mu_Y(w_1) - 1$ olan, w_2 için $\mu'_Y(w_2) = \mu_Y(w_2) + 1$ ve w_1 ve w_2 dışındaki $\forall w \in A$ için $\mu'_Y(w) = \mu_Y(w)$ olan μ'_Y dağılımıyla karşılaştırdığımızı düşünün. μ'_Y için amaçlanan fonksiyonun[8] μ_Y için amaçlanandan küçük olduğu kolayca görülür. Böylece α nın değeri

$$\begin{aligned}
\alpha &= (m - f)e^2 + f(e + 1)^2 \\
&= e^2 m - e^2 f + e^2 f + 2ef + f \\
&= e(em + 2f) + f \\
&= \frac{q - f}{m}(m\frac{q - f}{m} + 2f) + b \\
&= \frac{1}{m}\left[(q - f)^2 + 2f(q - f) + mf\right]
\end{aligned} \tag{2.1.26}$$

[7] minimizing distribution
[8] objective function

$$= \frac{1}{m}\left[q^2 - 2qf + f^2 + 2qf - 2f^2 + mf\right]$$

$$= \frac{1}{m}\left[(q^2 - b^2) + mf\right]$$

$$= \frac{1}{m}\left[(q-f)(q+f) + mf\right] \tag{2.1.27}$$

olarak bulunur. (2.1.22) ve (2.1.23) den A üzerinde q uzunluğundaki $\forall Y$ için

$$\overline{H}(Y) \geq \frac{1}{q-1}(\alpha - q) \tag{2.1.28}$$

sağlanır. Ayrıca $\forall Y$ için

$$H(Y) \geq \overline{H}(Y) \tag{2.1.29}$$

olduğundan

$$H(Y) \geq \frac{1}{q-1}(\alpha - q) \tag{2.1.30}$$

olur. (2.1.27) de bulunan α, (2.1.30) da yerine yazılırsa istenen

$$H(Y) \geq \frac{(q-b)(q+b-m)}{m(q-1)}$$

eşitsizliği elde edilir. □

BÖLÜM 3

3. Tablo

Bu bölümde öncelikle literatürde bulunan optimal FHS dizilerinin, çiftlerin ve ailelerinin parametrelerinin bir tablosu verilecektir. Optimal diziler için Lempel-Greenberger Sınırı, optimal aileler için Peng-Fan Sınırı kullanılmıştır.

Çizelge 3.1. BİLİNEN OPTİMAL FHS PARAMETRELERİ

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
1.	$p^m - 1$	p^k	$p^{m-k} - 1$	p^k	$0 < k \leq m$	[1]	M-dizileri
2.	p^2	p	p	p		[2]	Genelleştirilmiş Bent Fonksiyonu
3.	$q^m - 1$	q	q^{m-1}	q		[3]	M-dizileri
4.	$q^m - 1$	q^k	q^{m-k}	q^k		[6]	M-dizileri, Genelleştirilmiş GMW
5.	$p^{mn} - 1$	$p^{m(n-t)}$	$p^{mn} - 1$	1	$1 \leq t \leq n, 1 \leq m$	[9]	Partition type difference packing with uniform block size (direct construction)
6.	$3(6f + 1)$	p	k	1	$f \in \mathbb{Z}^+$	[9]	Partition type difference packing with uniform block size (direct construction)

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
7.	$4(12f+1)$	p	k	1	f tek tamsayı	[9]	Partition type difference packing with uniform block size (direct construction)
8.	$5(20f+1)$	p	k	1	$f \in \mathbb{Z}^+$, f pozitif tamsayı[a]	[9]	Partition type difference packing with uniform block size (direct construction)
9.	$7(42f+1)$	p	k	1	$f \in \mathbb{Z}^+$, f pozitif tamsayı[b]	[9]	Partition type difference packing with uniform block size (direct construction)
10.	$3m$	m	3	1	$m \equiv 1$ (mod 6)	[9]	Partition type difference packing with uniform block size (direct construction)

[a] f, [4] Teorem 2.1 deki şartı sağlayacak
[b] f, [5] Teorem 12 deki şartı sağlayacak

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
11.	p_1p_2	p_2	p_1	1	$p_1 \equiv 3$ (mod 4), p_1, p_2 tek asal, $p_1 < p_2$	[9]	Partition type difference packing with uniform block size (direct construction)
12.	p_1p_2	p_2	p_1	1	$p_1 \equiv 1$ (mod 4), p_1, p_2 tek asal, $g(p_2) \geq \frac{p_1-1}{4}$, g fonksiyonu[a]	[9]	Partition type difference packing with uniform block size (direct construction)
13.	p_1p_2	p_2	p_1	1	$p_2 \equiv 3$ (mod 4), p_1, p_2 tek asal, $p_1 < p_2$, ($p_2 \equiv 7, 11, 15$(mod 16) olduğunda $p_2 = p_1 + 2$ olma durumu hariç)	[9]	Partition type difference packing with uniform block size (direct construction)
14.	$3p$	p	3	1	$p > 3\, asal$	[9]	Partition type difference packing with uniform block size (direct construction)

[a] g fonksiyonu [9] daki (4.3) ifadesindeki gibi tanımlıdır.

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
15.	$5p$	p	5	1	$p > 5$ $asal$	[9]	Partition type difference packing with uniform block size (direct construction)
16.	m	$\frac{m-1}{2}$	2	1	$m \equiv 1, 3$ (mod 6), $m \in \mathbb{Z}^+$	[9]	Partition type difference packing with uniform block size (direct construction)
17.	p	$\frac{p-1}{k-1}$	$k-1$	1	$p \equiv 1$ (mod $k(k-1)$) asal, $k = 4, 5, 6$, $k = 6$ iken $p \neq 61$	[9]	Partition type difference packing with uniform block size (direct construction)
18.	p	e	k	1	$p = ke+1$ asal, k tek tamsayı	[9]	Partition type difference packing with uniform block size (direct construction)

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
19.	$p(k+1)$	mk^2+1	$k-1$	1	$p = mk(k-1)+1$, p tek asal, $k = 4, 5, 6$, $m \in \mathbb{Z}^+$, $k = 6$ iken $p \neq 61$	[9]	Partition type difference packing with a hole (recursive)
20.	$p_1 p_2$	$ep_2 + mk$	$k-1$	1	$p_1 = ke+1$ tek asal, $p_2 = mk(k-1)+1$, $k = 4, 5, 6$, $m \in \mathbb{Z}^+$, $k = 6$ iken $p_2 \neq 61$	[9]	Partition type difference packing with a hole (recursive)
21.	p	$e+1$	$f-1$	e	$p = ef+1$ tek asal, $f \geq 2$, $e \geq 3f$	[10]	Cyclotomic
22.	p	e	f	1	$p = ef+1$ asal, e çift tamsayı, f tek tamsayı	[10]	Cyclotomic
23.	p	$e+1$	$f-1$	1	$p = ef+1$ asal, $2 \leq f \leq e+2$	[10]	Cyclotomic

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
24.	n	l	k	1	l ve k tamsayılar olmak üzere $n = lk$	[11]	Perfect nonlinear function
25.	$\frac{q^m-1}{2}$	q	$\frac{q^{m-1}-1}{2}$	1	$m \geq 3$ tek tamsayı, $ebob(2, m) = 1$	[11]	İz fonksiyonu, İz kodları
26.	$\frac{q^m-1}{2}$	q	$\frac{q^{m-1}-1}{2}$	2	$m \geq 3$ tek tamsayı, $ebob(2, m) = 1$	[11]	İz fonksiyonu, İz kodları
27.	$q^m - 1$	q	$q^{m-1} - 1$	1	$m \geq 1$, $q = p^r$, $r \in \mathbb{Z}^+$, $1 \leq s \leq q - 2$, $ebob(sm - 1, q - 1) = 1$	[11]	Norm fonksiyonu, İz kodları
28.	$q^m - 1$	q	q^{m-1}	q	$m \geq 1$, $q = p^r$, $r \in \mathbb{Z}^+$, $1 \leq s \leq q - 2$, $ebob(sm - 1, q - 1) = 1$	[11]	Norm fonksiyonu, İz kodları
29.	ef	e	f	1	$q = ef + 1$ bir asalın kuvveti	[12]	Cyclotomy, Discrete logarithm function

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
30.	ef	$e+1$	$f-1$	1	$q = ef + 1$ bir asalın kuvveti	[12]	Cyclotomy, Discrete logarithm function
31.	ef	$e+1$	f	e	$q = ef + 1$ bir asalın kuvveti	[12]	Cyclotomy, Discrete logarithm function
32.	$\frac{q^m-1}{q-1}$	q	$\frac{q^{m-1}-1}{q-1}$	$q-1$	$ebob(q-1, m) = 1$	[12]	İz fonksiyonu, İz kodları
33.	$6t+2$	$2t+1$	2	1	$t \geq 0$,	[13]	Difference packing, Difference family (Kombinatorik)
34.	$2p$	$\frac{2p+1}{3}$	2	1	$p \equiv 1 \pmod 6$,	[13]	Difference packing, Difference family (Kombinatorik)
35.	$8p$	$\frac{8p+1}{3}$	2	1	$p \equiv 7,\ 13 \pmod{18}$,	[13]	Difference packing, Difference family (Kombinatorik)

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
36.	$\frac{q^m-1}{e}$	q	$\frac{q^{m-1}-1}{e}$	1	$e \mid (q^m-1)$, $ebob(e, \frac{q^m-1}{q-1}) = 1$	[13]	İz fonksiyonu, İz kodları
37.	$\frac{q^m-1}{e}$	q	$\frac{q^{m-1}-1}{e}$	2	$e \mid (q^m-1)$, $ebob(e, \frac{q^m-1}{q-1}) = 1$	[13]	İz fonksiyonu, İz kodları
38.	$\frac{q^m-1}{e}$	q	$\frac{q^{m-1}-1}{e}$	e	$e \mid (q^m-1)$, $ebob(e, \frac{q^m-1}{q-1}) = 1$	[13]	İz fonksiyonu, İz kodları
39.	q^m-1	q	$q^{m-1}-1$	1	$m \geq 1$, $q = p^r$, $r \in \mathbb{Z}^+$, $1 \leq s \leq q-2$, $ebob(1-sg(m), q-1) = 1$, g fonksiyonu[a]	[13]	Gama fonksiyonu, İz kodları
40.	q^m-1	q	$q^{m-1}-1$	q^m-1	$m \geq 1$, $q = p^r$, $r \in \mathbb{Z}^+$, $1 \leq s \leq q-2$, $ebob(1-sg(m), q-1) = 1$, g fonksiyonu[b]	[13]	Gama fonksiyonu, İz kodları

[a] g fonksiyonu [13] ün B bölümünde anlatıldığı gibi bir fonksiyon.
[b] g fonksiyonu [13] ün B bölümünde anlatıldığı gibi bir fonksiyon.

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
41.	$2(2^m-1)$	$e+1$	$2f$	$\lfloor \frac{e}{2} \rfloor$	$2(2^m-1)=2ef, e \geq 2f+2,$ $f \geq 2$	[14]	Cyclotomy, Çinli kalan teoremi
42.	q^2+1	q	$q+1$	q^2-1	$q=2^k$, k tamsayı	[15]	İz fonksiyonu, İz kodları
43.	$\frac{q+1}{2}$	q	1	$2(q-1)$	$q \equiv 1$ (mod 4)	[15]	İz fonksiyonu, İz kodları
44.	$q-1$	q	$k-1$	$\frac{q^k-1}{q-1}$	q-1 asal	[15]	İz fonksiyonu, İz kodları
45.	$\frac{q^m-1}{q-1}$	q	$k-3$	$\frac{q^{k-m}-q}{k}$	$ebob(m, q-1)=1$	[15]	İz fonksiyonu, İz kodları
46.	$\frac{q^m-1}{N}$	q	$\frac{q^m-q+(q-1)\sqrt{q^m}}{qN}$	N	N çift tamsayı, $ebob(N, \frac{q^m-1}{N}) = 1,$ $q-1 \equiv \frac{N}{2} \ (mod \ N),$ $ebob(\frac{r-1}{q-1} \ (mod \ N), N) = 2,$ $N > \frac{q-1}{q}\sqrt{r}$	[15]	İz fonksiyonu, İz kodları

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
47.	$q-1$	e	f	e	$q = ef + 1$, f veya q çift tamsayı	[16]	Cyclotomic
48.	$q-1$	e	f	1	$q = ef + 1$, f ve q tek tamsayı	[16]	Cyclotomic
49.	ef	$e+1$	f	1	$e + 1 \geq f$	[16]	Cyclotomic
50.	kN	N	k	1	$N \geq 3$, $N = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, $2 \leq p_1 < p_2 < p_r$ asal, $r \geq 1$ $e_i \geq 1 \forall i = 1, 2, \ldots, r$, $2 \leq k \leq p_1 - 1$	[17]	Interleaving
51.	$2N$	N	2	1	$N > 1$ tek tamsayı $N = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, $2 \leq p_1 < p_2 < p_r$ asal, $r \geq 1$ $e_i \geq 1 \forall i = 1, 2, \ldots, r$,	[17]	Interleaving

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
52.	$3N$	N	3	1	$N \geq 5$ $n \equiv 1, 5$ (mod 6) $N = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, $2\, p_1 < p_2 < p_r$ asal, $r \geq 1$ $e_i \geq 1 \forall i = 1, 2, \ldots, r$,	[17]	Interleaving
53.	kN	N	k	1	$N = p$ asal $2 \leq k \leq p - 1$	[17]	Interleaving
54.	kN	N	k	1	$N = 2^{2m+1} - 1$ $m \geq 1$ $N = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, $2 \leq p_1 < p_2 < p_r$ asal, $r \geq 1$ $e_i \geq 1 \forall i = 1, 2, \ldots, r$, $k = 3$ veya 4	[17]	Interleaving
55.	$2N$	N	2	1	N çift tamsayı $N = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, $2 \leq p_1 < p_2 < p_r$ asal, $r \geq 1$ $e_i \geq 1 \forall i = 1, 2, \ldots, r$,	[17]	Interleaving

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
56.	N^2	N	N	N	$N = p$ asal	[17]	Interleaving
57.	$2p$	M	$2f + 1$	$\frac{M}{2}$	$p = Mf + 1$ tek asal $M \geq 4$, f tek tamsayı	[17]	Cyclotomy
58.	kp	p	k	$\lfloor \frac{p-1}{k} \rfloor$	p tek asal $2 \geq k \geq p - 1$	[17]	Cyclotomy
59.	kp	p	k	$\lfloor \frac{p-1}{k} \rfloor$	p tek asal $2 \geq k \geq p - 1$	[17]	Cyclotomy
60.	$q^m - 1$	q^k	q^{m-k}	q^k	$0 < k \leq m$	[18]	Difference balanced function, İz kodları
61.	p	L	$2g$	1	$p = 2Lg + 1$ tek asal $p \equiv 3$ (mod 4)	[19]	Cyclotomy
62.	p	$L + 1$	$2g - 1$	1	$p = 2Lg + 1$ tek asal $p \equiv 3$ (mod 4) $3 \leq g \leq \frac{L+3}{2}$ tek tamsayı	[19]	Cyclotomy

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
63.	kp	p	k	1	p tek asal, $2 \geq k \geq p-1$	[19]	Quadratic Residue
64.	$2M-2m-1$	M	1	1	$M \geq 4$ tamsayı, $0 \leq m \leq \frac{M}{2}-1$	[19]	$\mathbb{Z}_m$ üzerinde permütasyonlar
65.	$2M-2m$	M	1	1	$M \geq 3$ tamsayı, $0 \leq m \leq \frac{M-1}{2}$	[19]	$\mathbb{Z}_m$ üzerinde permütasyonlar
66.	$2M$	M	2	1	$M \geq 3$ tek tamsayı	[19]	$\mathbb{Z}_m$ üzerinde permütasyonlar
67.	$2M$	M	2	1	$M \geq 2$ tamsayı	[19]	$\mathbb{Z}_m$ üzerinde permütasyonlar
68.	$2M+1$	M	2	1	$M \geq 3$ tamsayı	[19]	$\mathbb{Z}_m$ üzerinde permütasyonlar

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
69.	p	$\frac{p-1}{2}$	2	1	$p \geq 13$ tamsayı $p \equiv 1$ (mod 4)	[19]	$\mathbb{Z}_m$ üzerinde permütasyonlar
70.	$2M+3$	M	2	1	$M \geq 8$ tamsayı	[19]	$\mathbb{Z}_m$ üzerinde permütasyonlar
71.	$2M+5$	M	2	1	$M \geq 10$ tamsayı	[19]	$\mathbb{Z}_m$ üzerinde permütasyonlar
72.	$\frac{q^m-1}{2}$	q	$\frac{q^{m-1}-1}{2}$	q	$m \geq 3$ tek tamsayı, $ebob(2,m)=1$	[20]	İz fonksiyonu, İz kodları
73.	$\frac{q^m-1}{e}$	q	$\frac{q^{m-1}-1}{e}$	e	$e \mid (q^m-1)$, $ebob(e, \frac{q^m-1}{q-1})=1$	[20]	İz fonksiyonu, İz kodları

	Dizi Boyu	*Alfabe Boyu*	H_{maks}	*FHS Sayısı*	*Kısıtlar*	*Ref.*	*Teknik*
74.	N	$\frac{N-1}{n}-1$	n	m_1	$N = p_1p_2\dots p_m$, $p_i = m_in+1$, $1 \leq i \leq m$	[21]	k-fold cyclotomic numbers
75.	$\frac{q+1}{k}$	q	1	$k(q-1)$	$k \mid (q+1)$, $q+1 \equiv k$ (mod $2k$)	[22]	Irreducible cyclic codes
76.	$\frac{q^m-1}{e}$	q^k	$\frac{q^{m-k}-1}{e}$	e	$0 < k \leq m$, $e \mid (q-1)$, $ebob(e,m) = 1$	[24]	d–form function with difference balanced function
77.	q^m-1	q^k	q^{m-k}	q^k	$0 < k \leq m$	[24]	d–form function with difference balanced function

BÖLÜM 4

4. Nümerik Çalışmalar

Bu bölümde İz Fonksiyonu ile yaptığımız nümerik çalışmalar anlatılacaktır. Çalışmalarımızda öncelikle [11], [12], [13], ve [15] makalelerinde bulunan iz fonksiyonu kullanarak optimal dizi üreten cebirsel metodlar incelenmiş ve bunların MAGMA ile gerçekleştirimi yapılmıştır. Gerçekleştirimlere ait MAGMA kodları ekler bölümünde bulunmaktadır. Daha sonra ise girilen parametrelere göre FHS üreten bir kod yazılarak yeni parametreler için optimallik araştırması yapılmıştı. Bazı parametreler için optimal FHS ler bulunmuş olup bunlar henüz bir kurala oturtulamamıştır. Konuyla ilgili nümerik çalışmalarımız devam etmektedir. Şimdi yukarıda bahsi geçen dört makaledeki beş cebirsel üretim metodu ve örnekleri, ardından da yaptığımız çalışmalar verilecektir. Bu bölüm boyunca, uzunluğu v, alfabe boyu $|\mathbb{F}| = q$ ve hamming otokorelasyonu $H(X) = \lambda$ olan frekans atlamalı dizileri (v, q, λ)-FHS notasyonuyla, uzunluğu v, alfabe boyu $|\mathbb{F}| = q$ ve dizi aileleri için hamming korelasyonu $M(F) = \lambda$ olan frekans atlamalı dizilerden oluşan N elemanlı F kümesini ise $(v, q, \lambda; N)$ ile göstereceğiz.

4.1. [11] Makalesindeki Üretim Metodu

Kabul edelim ki p bir tek asal sayı ve r pozitif tamsayı olmak üzere $q = p^r$ olsun. Ayrıca kabul edelim ki, $m \geq 3$ pozitif tek tamsayısı verilsin ve α, $\mathbb{F}_{q^m}$ nin ilkel elemanı olmak üzere $\beta = \alpha^{2s}$ olsun. Burada s, $ebob(s, q^m - 1) = 1$ özelliğini sağlayan bir pozitif tamsayıdır. $Tr_{q^m/q}$, $\mathbb{F}_{q^m}$ den $\mathbb{F}_q$ ya tanımlanan iz fonksiyonu olmak üzere $\forall a \in \mathbb{F}_{q^m}^*$ için

$$c_a = \left(Tr_{q^m/q}(a), Tr_{q^m/q}(a\beta), \cdots, Tr_{q^m/q}(a\beta^{n-1}))\right)$$

dizileri Lemma 1.2.0.8 daki Lempel-Greenberger Sınırına göre optimal $(\frac{q^m-1}{2}, q, \frac{q^{m-1}-1}{2})$-FHS lerdir.

Örnek 4.1.0.19. $p = 5$, $r = 1$ olsun. O halde $q = 5^1 = 5$ olarak bulunur. $m = 3$ olarak alalım ve $ebob(s, q^m - 1) = ebob(1, 5^3 - 1) = 1$olduğundan s=1 olarak alalım. Bölüm E.1 de bulunan MAGMA kodunun dizi oluşturan bölümü çalıştırıldığında elde edilen dizilerden bazıları aşağıdaki gibidir:

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

(1, 1, 0, 0, 4, 1, 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)

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

(1, 0, 0, 4, 1, 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)

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

Örnek 4.1.0.20. $p = 3$, $r = 2$ olsun. O halde $q = 3^2 = 9$ olarak bulunur. $m = 3$ olarak alalım ve $ebob(s, q^m - 1) = ebob(1, 9^3 - 1) = 1$ olduğundan $s = 1$ olarak alalım. Bölüm E.1 de bulunan MAGMA kodunun dizi oluşturan bölümü çalıştırıldığında elde edilen dizilerden bazıları t, $\mathbb{F}_3$ üzerinde 2. dereceden x^2+2x+2 ilkel polinomunun kökü olmak üzere aşağıdaki gibidir:

(t, 2, t^5, t^6, t^6, 1, t^2, t^7, 2, t^5, 0, 1, t^2, t, t^6, 2, t^2, t, t^2, t^5, 1, t^2, 1, t^5, t, 1, t^3, t^2, t^6, t^7, t^6, 2, t^6, t^6, t^3, t^6, t^2, t^2, t^6, 0, t^5, t, t^7, 0, t^3, t^3, t^6, t^6, t^5, 2, 2, 0, t, 0, t, 1, 0, t, t^2, t^6, t^2, 2, t^5, t^2, t, t^3, t^7, 2, 2, 2, t^5, t^3, 2, t^6, 0, 0, 2, t, t^3, t^6, t^3, 0, t^5, t^3, t^3, t, t^5, 1, t^6, t, 0, t^7, t^2, t^3, 2, 2, t^6, 1, t^5, t^2, t^3, 0, t^6, 1, t^7, 2, t^2, 1, t^7, 1, t^3, t^6, 1, t^6, t^3, t^7, t^6, t, 1, 2, t^5, 2, t^2, 2, 2, t, 2, 1, 1, 2, 0, t^3, t^7, t^5, 0, t, t, 2, 2, t^3, t^2, t^2, 0, t^7, 0, t^7, t^6, 0, t^7, 1, 2, 1, t^2, t^3, 1, t^7, t, t^5, t^2, t^2, t^2, t^3, t, t^2, 2, 0, 0, t^2, t^7, t, 2, t, 0, t^3, t, t, t^7, t^3, t^6, 2, t^7, 0, t^5, 1, t, t^2, t^2, 2, t^6, t^3, 1, t, 0, 2, t^6, t^5, t^2, 1, t^6, t^5, t^6, t,

$2, t^6, 2, t, t^5, 2, t^7, t^6, t^2, t^3, t^2, 1, t^2, t^2, t^7, t^2, t^6, t^6, t^2, 0, t, t^5, t^3, 0, t^7, t^7, t^2, t^2, t, 1, 1, 0, t^5,$
$0, t^5, 2, 0, t^5, t^6, t^2, t^6, 1, t, t^6, t^5, t^7, t^3, 1, 1, 1, t, t^7, 1, t^2, 0, 0, 1, t^5, t^7, t^2, t^7, 0, t, t^7, t^7, t^5, t,$
$2, t^2, t^5, 0, t^3, t^6, t^7, 1, 1, t^2, 2, t, t^6, t^7, 0, t^2, 2, t^3, 1, t^6, 2, t^3, 2, t^7, t^2, 2, t^2, t^7, t^3, t^2, t^5, 2, 1,$
$t, 1, t^6, 1, 1, t^5, 1, 2, 2, 1, 0, t^7, t^3, t, 0, t^5, t^5, 1, 1, t^7, t^6, t^6, 0, t^3, 0, t^3, t^2, 0, t^3, 2, 1, 2, t^6, t^7,$
$2, t^3, t^5, t, t^6, t^6, t^6, t^7, t^5, t^6, 1, 0, 0, t^6, t^3, t^5, 1, t^5, 0, t^7, t^5, t^5, t^3, t^7, t^2, 1, t^3, 0)$

$(\ t^3, t^3, t^2, t, t, 0, t^6, 0, t^6, t^5, 0, t^6, t^7, t^3, t^7, t, t^2, t^7, t^6, 1, 2, t, t, t, t^2, 1, t, t^3, 0, 0, t, t^6, 1, t^3,$
$1, 0, t^2, 1, 1, t^6, t^2, t^5, t^3, t^6, 0, 2, t^7, 1, t, t, t^3, t^5, t^2, t^7, 1, 0, t^3, t^5, 2, t, t^7, t^5, 2, t^5, 1, t^3, t^5,$
$t^3, 1, 2, t^3, t^6, t^5, t, t^2, t, t^7, t, t, t^6, t, t^5, t^5, t, 0, 1, 2, t^2, 0, t^6, t^6, t, t, 1, t^7, t^7, 0, 2, 0, 2, t^3, 0,$
$2, t^5, t, t^5, t^7, 1, t^5, 2, t^6, t^2, t^7, t^7, t^7, 1, t^6, t^7, t, 0, 0, t^7, 2, t^6, t, t^6, 0, 1, t^6, t^6, 2, 1, t^3, t, 2, 0,$
$t^2, t^5, t^6, t^7, t^7, t, t^3, 1, t^5, t^6, 0, t, t^3, t^2, t^7, t^5, t^3, t^2, t^3, t^6, t, t^3, t, t^6, t^2, t, 2, t^3, t^7, 1, t^7, t^5,$
$t^7, t^7, 2, t^7, t^3, t^3, t^7, 0, t^6, t^2, 1, 0, 2, 2, t^7, t^7, t^6, t^5, t^5, 0, t^2, 0, t^2, t, 0, t^2, t^3, t^7, t^3, t^5, t^6, t^3,$
$t^2, 2, 1, t^5, t^5, t^5, t^6, 2, t^5, t^7, 0, 0, t^5, t^2, 2, t^7, 2, 0, t^6, 2, 2, t^2, t^6, t, t^7, t^2, 0, 1, t^3, 2, t^5, t^5, t^7,$
$t, t^6, t^3, 2, 0, t^7, t, 1, t^5, t^3, t, 1, t, 2, t^7, t, t^7, 2, 1, t^7, t^2, t, t^5, t^6, t^5, t^3, t^5, t^5, t^2, t^5, t, t, t^5, 0,$
$2, 1, t^6, 0, t^2, t^2, t^5, t^5, 2, t^3, t^3, 0, 1, 0, 1, t^7, 0, 1, t, t^5, t, t^3, 2, t, 1, t^2, t^6, t^3, t^3, t^3, 2, t^2, t^3, t^5,$
$0, 0, t^3, 1, t^2, t^5, t^2, 0, 2, t^2, t^2, 1, 2, t^7, t^5, 1, 0, t^6, t, t^2, t^3, t^3, t^5, t^7, 2, t, t^2, 0, t^5, t^7, t^6, t^3, t,$
$t^7, t^6, t^7, t^2, t^5, t^7, t^5, t^2, t^6, t^5, 1, t^7, t^3, 2, t^3, t, t^3, t^3, 1, t^3, t^7, t^7, t^3, 0, t^2, t^6, 2, 0, 1, 1)$

4.2. [12] Makalesindeki Üretim Metodu

Kabul edelim ki q bir asalın kuvveti ve m bir pozitif tamsayı olsun. Ayrıca kabul edelim ki g, $\mathbb{F}_{q^m}^*$ nin bir üreteci olsun. $\alpha = g^{q-1}$ ve dizinin uzunluğu $v = \frac{q^m-1}{q-1}$ olarak tanımlansın. $Tr_{q^m/q}$, $\mathbb{F}_{q^m}$ den $\mathbb{F}_q$ ya tanımlanan iz fonksiyonu olmak üzere $\forall\ 0 \leq i \leq q-2$ için,

$$S_i^{m,q} = Tr_{q^m/q}(g^i \alpha^t), \quad 0 \leq t \leq v-1$$

dizisini tanımlayalım. Her bir $S_i^{m,q}$, $\mathbb{F}_q$ alfabesi üzerinde v uzunluğunda dizidir. Şimdi

$$S^{m,q} = S_i^{m,q} :\ 0 \leq i \leq q-2$$

tanımlansın. Eğer $ebob(q-1, \sum_{i=0}^{m-1} q^i) = 1$ sağlanırsa $S^{m,q}$, Lemma 1.2.0.10 daki Peng-Fan Sınırına göre optimal $(\frac{q^m-1}{q-1}, q, \frac{q^{m-1}-1}{q-1}; q-1)$ FHS ailesi elde edilir. Ayrıca bu ailenin her bir elemanı Lemma 1.2.0.8 daki Lempel-Greenberger Sınırına göre optimaldir.

Örnek 4.2.0.21. $q = 2$, $m = 4$ olsun. O halde $q^m = 2^4$ olarak bulunur. $ebob(q-1, \sum_{i=0}^{m-1} q^i) = ebob(1, \sum_{i=0}^{m-1} 2^i) = 1$ olduğundan Bölüm E.2 de bulunan MAGMA kodunun dizi oluşturan bölümü çalıştırıldığında elde edilen optimal (15,2,7;1) FHS ailesi aşağıdaki gibidir ($q - 1 = 2 - 1 = 1$ tane dizi oluşur):

(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)

Örnek 4.2.0.22. $q = 4$, $m = 2$ olsun. O halde $q^m = 4^2$ olarak bulunur. $ebob(q-1, \sum_{i=0}^{m-1} q^i) = ebob(3, \sum_{i=0}^{m-1} q^i = \frac{q^m-1}{q-1} = \frac{4^2-1}{4-1} = 5) = 1$ olduğundan Bölüm E.2 de bulunan MAGMA kodunun dizi oluşturan bölümü çalıştırıldığında elde edilen optimal (5,4,1;3) FHS ailesi t, $\mathbb{F}_2$ üzerinde 2. dereceden $x^2 + x + 1$ ilkel polinomun kökü olmak üzere aşağıdaki gibidir:

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

(1, 0, 1, t, t)

(t, t^2, t^2, t, 0)

4.3. [13] Makalesindeki Üretim Metodu

Kabul edelim ki p bir asal sayı ve r pozitif tamsayı olmak üzere $q = p^r$ ve m, l, $l \mid (q-1)$ ve $ebob(\frac{q^m-1}{q-1}, l) = 1$ özelliklerini sağlayan pozitif tamsayılar olsun. Yine kabul edelim ki α, $\mathbb{F}_{q^m}$ nin ilkel elemanı, s, $ebob(s, q^m - 1) = 1$ özelliğini sağlayan bir pozitif tamsayı ve $\beta = \alpha^{ls}$ olsun. $n = \frac{q^m-1}{l}$ ve $Tr_{q^m/q}$, $\mathbb{F}_{q^m}$ den $\mathbb{F}_q$ ya tanımlanan iz fonksiyonu olmak üzere $\forall\ g \in \mathbb{F}_{q^m}^*$ için

$$c_g = \left(Tr_{q^m/q}(g), Tr_{q^m/q}(g\beta), \cdots, Tr_{q^m/q}(g\beta^{n-1}))\right)$$

dizileri Lemma 1.2.0.8 daki Lempel-Greenberger Sınırına göre optimal $(\frac{q^m-1}{l}, q, \frac{q^{m-1}-1}{l})$-FHS dizileridir.

Örnek 4.3.0.23. $q = 8$, $m = 2$ olsun. O halde $q^m = 8^2$ olarak bulunur. $l = 7$ olarak şeçilirse $7 \mid (8-1)$ ve $ebob(\frac{8^2-1}{8-1}, 7) = 1$ sağlandığından Bölüm E.3 de bulunan MAGMA kodunun dizi oluşturan bölümü çalıştırıldığında elde edilen optimal (9,8,1)-FHS dizilerinden bazıları v, $\mathbb{F}_2$ üzerinde 3. dereceden $x^3 + x + 1$ ilkel polinomun kökü olmak üzere aşağıdaki gibidir:

(1, v^5, v^2, v^2, v^5, 1, v^6, 0, v^6)

(v^2, v^4, v^3, 0, v^3, v^4, v^2, v^6, v^6)

(1, v, v^6, v^3, v^3, v^6, v, 1, 0)

(1, v^3, v^5, v^4, 0, v^4, v^5, v^3, 1)

(0, v, v^2, 1, v^4, v^4, 1, v^2, v)

4.4. [15] Makalesindeki Üretim Metodu

4.4.1 I. Metod

Kabul edelim ki $p = 2$, s pozitif bir tamsayı olmak üzere $q = p^s$ ve $r = q^4$ olsun. $N = q^2 - 1$ ve $n = q^2+1$ olarak tanımlansın. α, GF(r)* ın bir üreteci olsun ve $g = \alpha^N$ olarak tanımlansın. $Tr_{r/q}$, $\mathbb{F}_r$ den $\mathbb{F}_q$ ya tanımlı iz fonksiyonu olmak üzere $\forall\ 0 \leq i \leq N-2$ için

$$S_i^q = Tr_{r/q}(\alpha^i g^t), \quad 0 \leq t \leq n-1$$

dizileri tanımlansın. Her bir S_i^q, GF(q) üzerinde n uzunluğunda dizilerdir.

$$S^q = S_i^q :\ 0 \leq i \leq N-1$$

olarak tanımlanırsa, S^q kümesi, Lemma 1.2.0.10 daki Peng-Fan Sınırına göre optimal $(q^2 + 1, q, q + 1; q^2 - 1)$ FHS ailesi oluşturur.

Örnek 4.4.1.1. $p = 2$, $s = 3$ olarak alınırsa $q = p^s = 2^3$ ve $r = 8^4$ olur. Böylece $N = 8^2 - 1 = 63$ ve $n = 8^2 + 1 = 65$ olarak bulunur. Bu takdirde Bölüm E.4 da bulunan 1. üretim metodundaki MAGMA kodunun dizi oluşturan bölümü çalıştırıldığında elde edilen optimal (65,8,9;63) FHS ailesinin dizilerinden bazıları t, $\mathbb{F}_2$ üzerinde 3. dereceden $x^3 + x + 1$ ilkel polinomun kökü olmak üzere aşağıdaki gibidir:

(t^4, 0, t^3, t^4, t^6, 0, t, t, t^6, t^3, t^5, t^2, t^6, 1, t^5, t^6, t^2, t^3, 0, 1, t^3, t^2, t, t, t^4, t^4, t^6, 1, 1, t^6, t^4, t^4, t, t, t^2, t^3, 1, 0, t^3, t^2, t^6, t^5, 1, t^6, t^2, t^5, t^3, t^6, t, t, 0, t^6, t^4, t^3, 0, t^4, t^6, t, t^4, 0, 0, 0, t^4, t, t^6)

(t^3, 1, t^2, t^2, t^6, t, t^6, t^3, 0, 0, t^2, t^4, t^5, t^3, t^3, t, 0, t^6, t^5, t^6, t^2, t^5, t^6, t^5, t^5, t^2, 0, t^4, 0, t^4, 0, t^2, t^5, t^5, t^6, t^5, t^2, t^6, t^5, t^6, 0, t, t^3, t^3, t^5, t^4, t^2, 0, 0, t^3, t^6, t, t^6, t^2, t^2, 1, t^3, t^4, 1, t^2, t, t, t^2, 1, t^4)

(t^5, t^4, t^3, t^6, t^5, 0, t^2, t^2, t^5, t^2, 0, t^6, 1, 1, t^3, t^2, t^3, t^2, t, t^5, t^6, t^2, 0, 1, t^4, 0, t^2, t^4, 1, 1, t^4, t^2, 0, t^4, 1, 0, t^2, t^6, t^5, t, t^2, t^3, t^2, t^3, 1, 1, t^6, 0, t^2, t^5, t^2, t^2, 0, t^5, t^6, t^3, t^4, t^5, t, t, t, 0, t, t, t)

(t, t^3, 0, t^6, 0, 0, t^3, t^2, t^2, 1, t^6, t^2, t^2, t, t, 1, t, t^2, t^4, 1, t^3, 1, t^5, t, t^4, 0, t, t^5, t^6, 0, t^6, t^5, t, 0, t^4, t, t^5, 1, t^3, 1, t^4, t^2, t, 1, t, t, t^2, t^2, t^6, 1, t^2, t^2, t^3, 0, 0, t^6, 0, t^3, t, t^3, t^5, 1, 1, t^5, t^3)

(0, t^2, 0, t^4, t^5, t, 1, t^3, t^5, 1, t, t^4, t^2, 1, t^3, t^2, t^4, t^5, 0, t, t^6, t^3, t^6, t^3, t^4, t^3, t^5, t^2, t^4, 0, 0, t^4, t^2, t^5, t^3, t^4, t^3, t^6, t^3, t^6, t, 0, t^5, t^4, t^2, t^3, 1, t^2, t^4, t, 1, t^5, t^3, 1, t, t^5, t^4, 0, t^2, 0, t^3, t^2, 0, t^2, t^3)

(t^2, t^3, 0, t, t, t^3, 1, t, t, t^6, t, 1, 0, t^2, 1, t, t^2, 0, t^3, t^4, t^5, t^5, 1, 0, t^6, t, t^6, t^5, t^6, t^4, 0, t^4, t^6, t^5, t^6, t, t^6, 0, 1, t^5, t^5, t^4, t^3, 0, t^2, t, 1, t^2, 0, 1, t, t^6, t, t, 1, t^3, t, t, 0, t^3, t^2, t^4, t^4, t^4, t^4)

(t, t^2, t^4, t^5, 1, t^2, 1, t, t^6, t^4, t^5, t^5, t^5, t, 0, t^2, t^6, t^2, t^3, t^3, 0, t^2, t^5, t, t^4, t^6, 1, t^6, 0, 0, t, t, 0, 0, t^6, 1, t^6, t^4, t, t^5, t^2, 0, t^3, t^3, t^2, t^6, t^2, 0, t, t^5, t^5, t^5, t^4, t^6, t, 1, t^2, 1, t^5, t^4, t^2, t, t^5, 0, t^5)

(t, t^6, t, t^4, t^2, t^6, t^4, t, t, t^5, t, t^4, t^3, t^3, 0, t^4, 0, 1, t^2, t^6, 0, t^5, t^3, 0, t^6, t^6, t^3, 1, 1, t^2, t^4, 0, t^4,

t^2, 1, 1, t^3, t^6, t^6, 0, t^3, t^5, 0, t^6, t^2, 1, 0, t^4, 0, t^3, t^3, t^4, t, t^5, t, t, t^4, t^6, t^2, t^4, t, t^6, t, t^6, t^6)

4.4.2 II. Metod

Kabul edelim ki p bir tek asal, s ve m pozitif tamsayılar olmak üzere $q = p^s$ ve $r = q^m$ olsun. Ayrıca kabul edelim ki N, $r-1$ in pozitif çift tamsayı böleni ve $n = \frac{r-1}{N}$ olsun. α, GF(r)* ın bir üreteci olsun ve $g = \alpha^N$ olarak tanımlansın. $Tr_{r/q}$, $\mathbb{F}_r$ den $\mathbb{F}_q$ ya tanımlı iz fonksiyonu olmak üzere $\forall\ 0 \leq i \leq N-2$ için

$$S_i^{q,m} = Tr_{r/q}(\alpha^i g^t), \quad 0 \leq t \leq n-1$$

dizileri tanımlansın. Her bir S_i^q, GF(q) üzerinde n uzunluğunda dizilerdir.

$$S^{q,m} = S_i^{q,m} :\ 0 \leq i \leq N-1$$

olarak tanımlandığında, $S^{q,m}$ kümesi, $ebob(n, N) = 1$, $q-1 \equiv \frac{N}{2}$ (mod N), $ebob(\frac{r-1}{q-1}\ (mod\ N),$ $N) = 2$ ve $N > \frac{q-1}{q}\sqrt{r}$ şartları sağlanırsa Lemma 1.2.0.10 daki Peng-Fan Sınırına göre optimal $\left(\frac{r-1}{N}, q, \frac{(r-q+(q-1)\sqrt{r})}{qN}; N\right)$ FHS ailesi oluşturur.

Örnek 4.4.2.1. $p = 3$, $s = 2$ olmak üzere $p^s = 3^2 = 9$ alınırsa $m = 2$ için $r = 9^2$ bulunur. $N = 16 \mid (9^2 - 1)$ seçilirse $n = \frac{81-1}{16} = 5$ olur. $ebob(n, N) = ebob(5, 16) = 1$, $9 - 1 = 8 \equiv \frac{18}{2} = 8$ (mod 16), $ebob\left((\frac{81-1}{9-1} = 10\ (mod\ 16), 16)\right) = 2$ ve $N = 16 > \frac{8}{9}\sqrt{9} = 8$ sağlandığından parametre seçimimiz doğrudur. Bu takdirde Bölüm E.4 da bulunan 2. üretim metodundaki MAGMA kodunun dizi oluşturan bölümü çalıştırıldığında elde edilen optimal (5,9,1;16) FHS ailesinin dizileri t, $\mathbb{F}_3$ üzerinde 2. dereceden $x^2 + 2x + 2$ ilkel polinomun kökü olmak üzere aşağıdaki gibidir:

(2, t^7, t^5, t^5, t^7)

(t, 1, 2, t^5, 0)

(2, 2, t^6, t^3, t^6)

(t^3, 2, 0, 1, t^7)

(t^5, t^2, t^5, t^3, t^3)

(0, t^7, t^6, t^2, t^3)

(2, t^2, t^2, 2, t)

(t^5, t, t^2, 0, t^6)

(t, t^3, 1, t^3, t)

(t, 0, t^5, 2, 1)

(t^7, t^2, 1, 1, t^2)

(2, t^3, t^7, 1, 0)

(t^7, t^7, t, t^6, t)

(t^6, t^7, 0, t^3, t^2)

(1, t^5, 1, t^6, t^6)

(0, t^2, t, t^5, t^6)

4.5. Çalışmalarımız

Bu bölümde yaptığımız optimal dizi üretme çalışmalarından bir örnek verilecek, sonrasında ise çalıştığımız parametreler tablo şeklinde aktarılacaktır. Üretim metodumuz için kabul edelim ki p bir asal sayı ve r pozitif tamsayı olmak üzere $q = p^r$ olsun. Ayrıca kabul edelim ki, m pozitif tamsayı olmak üzere $\mathbb{F}_{q^m}$ olsun ve α, $\mathbb{F}_{q^m}$ nin bir ilkel elemanı olmak üzere $\beta = \alpha^{ls}$ olsun. Burada s, $ebob(s, q^m - 1) = 1$ özelliğini sağlayan bir pozitif tamsayı, l ise $q^m - 1$ in pozitif

bir tamsayı bölenidir. Oluşturduğumuz MAGMA kodu $Tr_{q^m/q}$, $\mathbb{F}_{q^m}$ den $\mathbb{F}_q$ ya tanımlanan iz fonksiyonu olmak üzere $\forall a \in \mathbb{F}^*_{q^m}$ için

$$\left(Tr_{q^m/q}(a), Tr_{q^m/q}(a\beta), \cdots, Tr_{q^m/q}(a\beta^{n-1})\right) \tag{4.5.1}$$

dizileri oluşturulup bunların Hamming Korelasyonlarını Tanım 1.2.0.5 ve 1.2.0.6 ya göre hesap-

lar ve sınırlarla karşılaştırarak optimalliğine karar verir.

Örnek 4.5.0.2. Ekler kısmında bulunan Bölüm E.5 deki kod $p = 3$, $q = 3$ ve $q^m = 3^3$ için çalıştırıldığında $q^m - 1$ in tüm bölenleri için diziler oluşturur ve bu dizilerin optimalliğini inceler. Yaptığı hesaplar sonucu oluşturduğu dizileri, optimal dizileri ve çiftleri bir dosya oluşturup aşağıdaki şekilde kaydeder. Burada $q^m - 1 = 3^3 - 1 = 26$ olduğundan program 26 nın bölenleri olan $l = 2$ ve $l = 13$ için diziler oluşturup, $l = 2$ için hem optimal dizi hem optimal çiftler elde edilirken $l = 13$ için sadece optimal diziler bulunmuştur. Buradan anlaşılıyor ki (4.5.1) şeklinde oluşturulan diziler $l = 13 \mid (3^3 - 1)$ için optimal çift oluşturmamaktadır.

```
p=
3
q=
3
q^m=
27
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
l=
2
 ICIN diziler-------------

z
 icin dizi
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]

z^2
 icin dizi
[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]

z^3
 icin dizi
```

```
[ 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1, 0 ]

z^4
 icin dizi
[ 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0, 2 ]

z^5
 icin dizi
[ 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1, 0, 0 ]

z^6
 icin dizi
[ 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0, 2, 2 ]

z^7
 icin dizi
[ 2, 0, 2, 0, 1, 1, 1, 2, 1, 1, 0, 0, 1 ]

z^8
 icin dizi
[ 1, 2, 2, 0, 0, 2, 1, 0, 1, 0, 2, 2, 2 ]

z^9
 icin dizi
[ 0, 2, 0, 1, 1, 1, 2, 1, 1, 0, 0, 1, 2 ]

z^10
 icin dizi
[ 2, 2, 0, 0, 2, 1, 0, 1, 0, 2, 2, 2, 1 ]

z^11
 icin dizi
[ 2, 0, 1, 1, 1, 2, 1, 1, 0, 0, 1, 2, 0 ]

z^12
 icin dizi
[ 2, 0, 0, 2, 1, 0, 1, 0, 2, 2, 2, 1, 2 ]

2
 icin dizi
[ 0, 1, 1, 1, 2, 1, 1, 0, 0, 1, 2, 0, 2 ]

z^14
 icin dizi
[ 0, 0, 2, 1, 0, 1, 0, 2, 2, 2, 1, 2, 2 ]
```

```
z^15
 icin dizi
[ 1, 1, 1, 2, 1, 1, 0, 0, 1, 2, 0, 2, 0 ]

z^16
 icin dizi
[ 0, 2, 1, 0, 1, 0, 2, 2, 2, 1, 2, 2, 0 ]

z^17
 icin dizi
[ 1, 1, 2, 1, 1, 0, 0, 1, 2, 0, 2, 0, 1 ]

z^18
 icin dizi
[ 2, 1, 0, 1, 0, 2, 2, 2, 1, 2, 2, 0, 0 ]

z^19
 icin dizi
[ 1, 2, 1, 1, 0, 0, 1, 2, 0, 2, 0, 1, 1 ]

z^20
 icin dizi
[ 1, 0, 1, 0, 2, 2, 2, 1, 2, 2, 0, 0, 2 ]

z^21
 icin dizi
[ 2, 1, 1, 0, 0, 1, 2, 0, 2, 0, 1, 1, 1 ]

z^22
 icin dizi
[ 0, 1, 0, 2, 2, 2, 1, 2, 2, 0, 0, 2, 1 ]

z^23
 icin dizi
[ 1, 1, 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2 ]

z^24
 icin dizi
[ 1, 0, 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0 ]

z^25
 icin dizi
[ 1, 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1 ]
```

```
1
 icin dizi
[ 0, 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1 ]

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
```

```
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
```

```
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
OPTIMAL CIFTTIR

[ 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1 ]
dizisi optimal

[ 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0 ]
dizisi optimal

[ 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1, 0 ]
dizisi optimal

[ 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0, 2 ]
dizisi optimal

[ 1, 2, 0, 2, 0, 1, 1, 1, 2, 1, 1, 0, 0 ]
dizisi optimal

[ 2, 1, 2, 2, 0, 0, 2, 1, 0, 1, 0, 2, 2 ]
dizisi optimal

[ 2, 0, 2, 0, 1, 1, 1, 2, 1, 1, 0, 0, 1 ]
dizisi optimal

[ 1, 2, 2, 0, 0, 2, 1, 0, 1, 0, 2, 2, 2 ]
dizisi optimal

[ 0, 2, 0, 1, 1, 1, 2, 1, 1, 0, 0, 1, 2 ]
dizisi optimal

[ 2, 2, 0, 0, 2, 1, 0, 1, 0, 2, 2, 2, 1 ]
dizisi optimal

[ 2, 0, 1, 1, 1, 2, 1, 1, 0, 0, 1, 2, 0 ]
```

```
dizisi optimal

[ 2, 0, 0, 2, 1, 0, 1, 0, 2, 2, 2, 1, 2 ]
dizisi optimal

[ 0, 1, 1, 1, 2, 1, 1, 0, 0, 1, 2, 0, 2 ]
dizisi optimal

[ 0, 0, 2, 1, 0, 1, 0, 2, 2, 2, 1, 2, 2 ]
dizisi optimal

[ 1, 1, 1, 2, 1, 1, 0, 0, 1, 2, 0, 2, 0 ]
dizisi optimal

[ 0, 2, 1, 0, 1, 0, 2, 2, 2, 1, 2, 2, 0 ]
dizisi optimal

[ 1, 1, 2, 1, 1, 0, 0, 1, 2, 0, 2, 0, 1 ]
dizisi optimal

[ 2, 1, 0, 1, 0, 2, 2, 2, 1, 2, 2, 0, 0 ]
dizisi optimal

[ 1, 2, 1, 1, 0, 0, 1, 2, 0, 2, 0, 1, 1 ]
dizisi optimal

[ 1, 0, 1, 0, 2, 2, 2, 1, 2, 2, 0, 0, 2 ]
dizisi optimal

[ 2, 1, 1, 0, 0, 1, 2, 0, 2, 0, 1, 1, 1 ]
dizisi optimal

[ 0, 1, 0, 2, 2, 2, 1, 2, 2, 0, 0, 2, 1 ]
dizisi optimal

[ 1, 1, 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2 ]
dizisi optimal

[ 1, 0, 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0 ]
dizisi optimal

[ 1, 0, 0, 1, 2, 0, 2, 0, 1, 1, 1, 2, 1 ]
dizisi optimal

[ 0, 2, 2, 2, 1, 2, 2, 0, 0, 2, 1, 0, 1 ]
```

```
dizisi optimal

Optimallik siniri:
4
Optimal cift siniri:
4
Optimal aile siniri:
4

oto-korelasyonlar:
[ 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4 ]

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
l=
13
 ICIN diziler-------------

z
 icin dizi
[ 0, 0 ]

z^2
 icin dizi
[ 2, 1 ]

z^3
 icin dizi
[ 0, 0 ]

z^4
 icin dizi
[ 2, 1 ]

z^5
 icin dizi
[ 1, 2 ]

z^6
 icin dizi
[ 2, 1 ]

z^7
 icin dizi
[ 2, 1 ]
```

```
z^8
 icin dizi
[ 1, 2 ]

z^9
 icin dizi
[ 0, 0 ]

z^10
 icin dizi
[ 2, 1 ]

z^11
 icin dizi
[ 2, 1 ]

z^12
 icin dizi
[ 2, 1 ]

2
 icin dizi
[ 0, 0 ]

z^14
 icin dizi
[ 0, 0 ]

z^15
 icin dizi
[ 1, 2 ]

z^16
 icin dizi
[ 0, 0 ]

z^17
 icin dizi
[ 1, 2 ]

z^18
 icin dizi
[ 2, 1 ]

z^19
```

```
 icin dizi
[ 1, 2 ]

z^20
 icin dizi
[ 1, 2 ]

z^21
 icin dizi
[ 2, 1 ]

z^22
 icin dizi
[ 0, 0 ]

z^23
 icin dizi
[ 1, 2 ]

z^24
 icin dizi
[ 1, 2 ]

z^25
 icin dizi
[ 1, 2 ]

1
 icin dizi
[ 0, 0 ]

[ 2, 1 ]
dizisi optimal

[ 2, 1 ]
dizisi optimal

[ 1, 2 ]
dizisi optimal

[ 2, 1 ]
dizisi optimal

[ 2, 1 ]
dizisi optimal
```

```
[ 1, 2 ]
dizisi optimal

[ 2, 1 ]
dizisi optimal

[ 2, 1 ]
dizisi optimal

[ 2, 1 ]
dizisi optimal

[ 1, 2 ]
dizisi optimal

[ 1, 2 ]
dizisi optimal

[ 2, 1 ]
dizisi optimal

[ 1, 2 ]
dizisi optimal

[ 1, 2 ]
dizisi optimal

[ 2, 1 ]
dizisi optimal

[ 1, 2 ]
dizisi optimal

[ 1, 2 ]
dizisi optimal

[ 1, 2 ]
dizisi optimal

Optimallik siniri:
0
Optimal cift siniri:
1
Optimal aile siniri:
```

```
1

oto-korelasyonlar:
[ 2, 0, 2, 0, 0, 0, 0, 0, 2, 0, 0, 0, 2, 2, 0, 2, 0, 0, 0, 0, 0, 2, 0, 0, 0, 2 ]

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Bölüm 4.1., 4.2., 4.3. ve 4.4. de verdiğimiz üretim metodlarının anlatıldığı dört makalede sırasıyla $l = 2$, $l = q - 1$, $l \mid (q - 1)$ ve $l = q^2 - 1$ için optimal dizi üretimi yapılmaktadır. Biz ise çalışmalarımızda tüm $l \mid (q^m - 1)$ değerleri için diziler oluşturarak optimalliklerini inceledik. Böylelikle, günümüz kişisel bilgisayarlarının hesaplama gücünün ve veri depolama kapasitesinin elverdiği şekilde hem makaleleri doğrulamış olduk hem optimal dizi ya da çift vermeyen bazı parametreleri görmüş olduk hem de optimal dizi, çift veya her ikisini birden veren yeni parametreler elde etmiş olduk. Çalışmalarımız p tek asal ve $p = 2$ olmak üzere iki ayrı kısmı içermektedir. Çizelge 4.5., Çizelge 4.2. ve 4.5. p tek asal için yaptığımız çalışmaları, Çizelge 4.5. ise $p = 2$ için yaptığımız çalışmaları içermektedir. Tablolarda p bir asal, q bir asalın kuvveti, m genişlemesinin mertebesi olmak üzere l, $(q^m - 1)$ i bölen bir tamsayıdır ($\frac{q^m-1}{l}$ dizilerin boyunu verir). Referans kolonunda ise, eğer parametreler [11], [12], [13] ve [15] makalelerinde işlenmiş ise referansı verilmektedir. Ayrıca, dizilerde dizi uzunluğu $= \frac{q^m-1}{l} \leq q$, dizi çiftlerinde dizinin uzunluğu $= \frac{q^m-1}{l} \leq \frac{q}{2}$ olacak şekilde veren parametreleri *aşikar* olarak nitelendirdik. Bunların dışındaki optimal dizi veya çift oluşturan parametreleri de *yeni* olarak nitelendirdik.

Çizelge 4.1. Parametre Listesi (p tek asal)

p	q	m	l	Optimal Dizi	Optimal Çift	Referans
3	3	2	2	yok	yok	
			4	var	yok	aşikar
3	3	3	2	var	var	[11], [13]
			13	var	yok	aşikar
3	3	4	2	yok	yok	
			4	yok	yok	
			5	yok	yok	
			8	yok	yok	
			10	var	yok	yeni
			16	yok	yok	
			20	yok	yok	
			40	var	yok	aşikar
3	9	2	2	yok	yok	
			4	yok	yok	
			5	yok	yok	
			8	yok	yok	
			10	var	yok	aşikar
			16	yok	yok	
			20	var	var	aşikar
			40	var	var	aşikar
5	5	2	2	yok	yok	
			3	yok	yok	
			4	yok	yok	
			6	var	yok	aşikar
			8	var	var	yeni
			12	var	var	aşikar
5	5	3	2	var	var	[11], [13]
			4	var	var	[12], [13]
			31	var	yok	yeni
			62	var	yok	aşikar
7	7	2	2	yok	yok	
			3	var	var	[13]
			4	yok	yok	
			6	yok	yok	
			8	var	yok	aşikar
			12	var	yok	
			16	var	var	aşikar
			24	var	var	aşikar

Çizelge 4.2. Parametre Listesi (p tek asal)

p	q	m	l	Optimal Dizi	Optimal Çift	Referans
7	7	3	2	var	var	[11], [13]
			3	yok	yok	
			6	yok	yok	
			9	yok	yok	
			18	yok	yok	
			19	yok	yok	
			38	yok	yok	
			57	var	yok	aşikar
			114	var	var	aşikar
			171	var	var	aşikar
11	11	2	2	yok	yok	
			3	yok	yok	
			4	yok	yok	
			5	var	var	[13]
			6	yok	yok	
			8	yok	yok	
			10	yok	yok	
			12	var	yok	aşikar
			15	yok	yok	
			20	var	yok	aşikar
			24	var	var	aşikar
			30	var	var	aşikar
			40	var	var	aşikar
			60	var	var	aşikar
13	13	2	2	yok	yok	
			3	var	var	[13]
			4	yok	yok	
			6	yok	yok	
			7	yok	yok	
			8	yok	yok	
			12	yok	yok	
			14	var	yok	aşikar
			21	var	yok	aşikar
			24	var	var	[15]
			28	var	var	aşikar
			42	var	var	aşikar
			56	var	var	aşikar
			84	var	var	aşikar

Çizelge 4.3. Parametre Listesi (p tek asal)

p	q	m	l	Optimal Dizi	Optimal Çift	Referans
17	17	2	2	yok	yok	
			3	yok	yok	
			4	yok	yok	
			6	yok	yok	
			8	yok	yok	
			9	yok	yok	
			12	yok	yok	
			16	yok	yok	
			18	var	yok	aşikar
			24	var	yok	aşikar
			32	var	var	yeni
			36	var	var	aşikar
			48	var	var	aşikar
			72	var	var	aşikar
			96	var	var	aşikar
			144	var	var	aşikar
19	19	2	2	yok	yok	
			3	var	var	[13]
			4	yok	yok	
			5	yok	yok	
			6	yok	yok	
			8	yok	yok	
			9	var	var	[13]
			10	yok	yok	
			12	yok	yok	
			15	yok	yok	
			18	yok	yok	
			20	var	yok	aşikar
			24	yok	yok	
			30	var	yok	aşikar
			36	var	yok	aşikar
			40	var	var	aşikar
			45	var	yok	aşikar
			60	var	var	aşikar
			72	var	var	aşikar
			90	var	var	aşikar
			120	var	var	aşikar
			180	var	var	aşikar

Çizelge 4.4. Parametre Listesi (p=2)

p	q	m	l	Optimal Dizi	Optimal Çift	Referans
2	4	2	3	var	var	[12],[13]
			5	var	yok	aşikar
2	4	3	3	yok	yok	
			7	yok	yok	
			9	var	yok	yeni
			21	var	yok	aşikar
2	4	4	3	var	var	[12],[13]
			5	yok	yok	
			15	yok	yok	
			17	var	yok	yeni
			51	var	var	yeni
			85	var	yok	aşikar
2	8	2	3	yok	yok	
			7	var	var	[12],[13]
			9	var	yok	aşikar
			21	var	var	aşikar
2	8	3	7	var	var	[12],[13]
			73	var	yok	aşikar
2	16	2	3	var	var	[12],[13]
			5	var	var	[12],[13]
			15	var	var	[12],[13]
			17	var	yok	aşikar
			51	var	var	aşikar
			85	var	var	aşikar

Referanslar

[1] Lempel A., Greenberger H. *Families of Sequences with Optimal Hamming Correlation Properties*, IEEE Trans.Inf. Theory, vol.IT-20 , pp 90-94, 1974.

[2] Kumar P.V. *Frequency-hopping code sequence designs having large linear span*, IEEE Trans.Inf. Theory, vol. 34, no. 1, pp 146-151, January 1988.

[3] Komo J. J., Liu S. C. *Maximal length sequences for frequency hopping*, IEEE Journal of Selected Areas in Communications, vol. 8, no. 5, pp 819-822, June 1990.

[4] Buratti M. *Improving two theorems of Bose on difference families*, J. Combin. Des., vol.3, pp 15-24, 1995.

[5] Buratti M. *On simple radical difference families*, J. Combin. Des., vol.3, pp 161-168, 1995.

[6] Udaya P., Siddiqi M. U. *Optimal large linear span frequency hopping patterns derived from polynomial residue class rings*, IEEE Trans. Inf. Theory, vol. 44, no. 4, pp 1492-1503, April 1998.

[7] Wenhua M., Yixian Y. *Families of FH sequences based on pseudorandom sequences over GF(p)*, International Conference on Communication Technologies (ICCT ’00), vol. 1, Paper S33.4, pp 536-538, August 2000.

[8] Peng D., Fan P. *Lower Bounds on the Hamming Auto- and Cross Correlations of Frequency-Hopping Sequences*, IEEE Trans. Inf. Theory, vol. 50, no. 9, pp 2149-2154, September 2004.

[9] Fuji-Hara R., Miao Y., Mishima M. *Optimal Frequency Hopping Sequences:A Combinatorial Approach*, IEEE Trans. Inf. Theory, vol. 50, no. 10, pp 2408-2420, October 2004.

[10] Chu W., Colbourn C.J. *Optimal frequency-hopping sequences via cyclotomy*, IEEE Trans.Inf. Theory, vol. 51, no. 3, pp 1139-1141, March 2005.

[11] Ding C., Miosio M.J., Yuan J. *Algebraic Constructions of Optimal Frequency Hopping Sequences*, IEEE Trans. Inf. Theory, vol. 53, no. 7, pp 2606-2610, July 2007.

[12] Ding C., Yin J. *Sets of Optimal Frequency Hopping Sequences*, IEEE Trans. Inf. Theory, vol. IT-54, no. 8, pp 3741-3745, August 2008.

[13] Ge G., Miao Y., Yao Z. *Optimal Frequency Hopping Sequences: Auto- and Cross-Correlation Properties*, IEEE Trans. Inf. Theory, vol. 55, no. 2, pp 867-879, February 2009.

[14] Zhang Y., Ke P., Zhang S. *Optimal Frequency-Hopping Sequences Based on Cyclotomy*, First International Workshop on Education Technology and Computer Science (ETCS '09), vol. 1, pp 1122-1126, March 2009.

[15] Ding C., Fuji-Hara R., Fujiwara Y., Jimbo M., Mishima M.*Sets of Frequency Hopping Sequences: Bounds and Optimal Constructions*, IEEE Trans.Inf. Theory, vol.55, no.7, pp 3297-3304, July 2009 .

[16] Han Y. K., Yang K. *On the Sidel'nikov Sequences as Frequency-Hopping Sequences*, IEEE Trans. Inf. Theory, vol. 55, no. 9, pp 4279-4285, September 2009.

[17] Chung J.,Han Y. K., Yang K. *New Classes of Optimal Frequency-Hopping Sequences by Interleaving Techniques*, IEEE Trans.Inf. Theory, vol. 55, No. 12, pp 5783-5791, December 2009.

[18] Zhou Z., Tang X. *A New Construction of Optimal Frequency Hopping Sequence Sets*, IEEE Proceedings of IWSDA'09, 2009.

[19] Chung J., Yang K. *Optimal Frequency-Hopping Sequences With New Parameters*, IEEE Trans.Inf. Theory, vol. 56, No. 4, pp 1685-1693, April 2010.

[20] Wang Q. *Optimal Sets of Frequency Hopping Sequences With Large Linear Spans*, IEEE Trans.Inf. Theory, vol.56, no.4, pp 1729-1736, April 2010 .

[21] Chung J., Yang K. *k-Fold Cyclotomic Numbers and Their Applications to Frequency-Hopping Sequences*, IEEE ISIT 2010, Austin, Texas, U.S.A., pp 1282-1284, June 13 - 18 2010.

[22] Ding C., Yang Y., Tang X.*Optimal Sets of Frequency Hopping Sequences From Linear Cyclic Codes*, IEEE Trans.Inf. Theory, vol.56, no.7, pp 3605-3612, July 2010 .

[23] Juntao G., Yupu H., Xuelian L. *The Linear Span of a Class of Optimal Frequency Hopping Sequences*, Natural Science Foundation of China, pp. 147-151, March 2011.

[24] Zhou Z., Tang X., Peng D., Parampalli U. *New Constructions for Optimal Sets of Frequency-Hopping Sequences*, IEEE Trans.Inf. Theory, vol. 57, No. 6, pp 3831-3840, June 2011.

[25] Schwartz S. M. *Frequency Hopping Spread Spectrum vs Direct Sequence Spread Spectrum in Broadband Wireless Access and Wireless LAN*, sorin m. schwartz seminar, 'http://sorin-schwartz.com/white_papers/fhvsds.pdf'.

[26] Wikipedia, 'http://www.wikipedia.org'.

[27] Glass J. *Frequency Hopping*, 'http://www.wirelesscommunication.nl/reference/chaptr05/spreadsp/fh.htm'.

[28] Computational Algebra Group, MAGMA Computational Algebra System(V2.10-22). 'http://magma.maths.usyd.edu.au/magma/'.

BÖLÜM 5

5. EKLER

E.1 [11] Makalesinin Gerçekleştirimi

```
 /* BU KOD C.DING 2007 HAZIRAN MAKALESINDEKI IZ FONKSIYONU
  ILE OPTIMAL DIZI OLUSTURMA FONKSIYONUNU GERCEKLEMEKTEDIR*/
p:= 3;        //tek bir asal
r:= 1;        //genislemenin boyutu

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

q:= p^r;      //altcismin boyu
m:= 3;        //tek tamsayi
n:=((q^m)-1) div 2;  //dizinin boyu
s:=1;    //gcd(s,q^m-1)=1 olacak sekilde
if m ne 1 then
p2:=PrimitivePolynomial(M,m);
F<z>:=ext< M|p2>;   //altcismin genislemesi ilkel elemani z yani alfa
else
F<z>:=M;
end if;

t:=z^(2*s);    //beta
Dizi:=[M| ];    //optimal dizi

index1:={} ;        //Fq^m* sonlu cismindeki elemanların sayısı
for i:=1 to ((q^m)-1) do
index1 join:={i};
end for;
index2:={} ;     //dizilerin elemanlarının sayısı
for j:=1 to n do
index2 join:={j};
```

```
end for;

D_ailesi:=[Dizi : x in index1];    //Optimal dizilerin olusturdugu dizi
index3:=[1,3,5,7];
for i in index3 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 hesaplanmaktadir

D1:=[x: x in index2];   //H. Korelasyonu icin 1. dizi
D2:=[x: x in index2]; //H. Korelasyonu icin 2. dizi
korelasyon:=[0: x in index2];
h_korelasyon:=0;
for i in index3 do
D1:=D_ailesi[i];
print i, ". dizi icin Cross veya auto Korelasyon";
for j in index3 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;
```

E.2 [12] Makalesinin Gerçekleştirimi

```
   /* BU KOD C.DING 2008 AGUSTOS MAKALESINDEKI IZ FONKSIYONU ILE OPTIMAL DIZI
OLUSTURMA FONKSIYONUNU GERCEKLEMEKTEDIR*/
p:= 3;        //bir asal
r:= 1;        //genislemenin boyutu

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

q:= p^r;      //altcismin boyu
m:= 3;        //pozitif tamsayi
n:=((q^m)-1) div (q-1);                 //dizinin boyu (makalede v ile gösterilmis)
if m ne 1 then
        p2:=PrimitivePolynomial(M,m);
        F<z>:=ext< M|p2>;                   //altcismin genislemesi ilkel elemani z yani alfa
else
        F<z>:=M;
end if;

t:=z^(q-1);    //makaledeki alfa
Dizi:=[M|];    //optimal dizi

index1:={} ;
for j:=1 to (q-1) do
        index1 join:={j};
end for;

index2:={} ;
for i:=1 to n do
        index2 join:={i};
end for;

D_ailesi:=[Dizi : x in index1];    //Optimal dizi ailesi
for i in index1 do
        print "  ";
        print "  ";
        print "S",i,"(",m,",",q,") icin dizi";
```

```
        for j in index2 do
                Dizi[j]:=Trace((z^i)*(t^(j-1)));
         end for;
        Dizi;
        D_ailesi[i]:=Dizi;
end for;

print (q-1)," ELEMANLI OPTIMAL DIZI AILESININ ELEMANLARI: ",D_ailesi;


//Buradan itibaren Hamming Korelasyonu hesaplanmaktadir

D1:=[x: x in index2];   //H. Korelasyonu icin 1. dizi
D2:=[x: x in index2];        //H. Korelasyonu icin 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;
```

E.3 [13] Makalesinin Gerçekleştirimi

```
 /* BU KOD GE 2009 Subat MAKALESINDEKI IZ FONKSIYONU ILE OPTIMAL
 DIZI OLUSTURMA FONKSIYONUNU GERCEKLEMEKTEDIR*/
p:= 2;        // bir asal
r:= 3;        //genislemenin boyutu
q:=p^r; //olusturulacak alt cismin boyu
K:=FiniteField(p);  //asal cisim
if r ne 1 then
p1:=PrimitivePolynomial(K,r);
M<v>:=ext< K|p1>;  //altcisim
else
M<v>:=K; //altcisim
end if;
m:= 2;        //tamsayi
l:= 3; //((q^m)-1)/(q-1) ile arasında asal ve (q^m)-1) i bolen bir tamsayi
n:=((q^m)-1) div l;  //dizinin boyu
s:=1;    //gcd(s,q^m-1)=1 olacak sekilde
if m ne 1 then
p2:=PrimitivePolynomial(M,m);
F<z>:=ext< M|p2>;   //altcismin genislemesi ilkel elemani 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 olusturdugu 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 hesaplanmaktadir

D1:=[x: x in index2];   //H. Korelasyonu icin 1. dizi
D2:=[x: x in index2]; //H. Korelasyonu icin 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;
```

E.4 [15] Makalesinin Gerçekleştirimi

E.4.1 1. Üretim Metodu

```
  /* BU KOD C.DING 2009 TEMMUZ MAKALESINDEKI ILK METOD OLAN IZ
 FONKSIYONU ILE OPTIMAL DIZI OLUSTURMA FONKSIYONUNU GERCEKLEMEKTEDIR*/
p:= 2;        //sabit
r:= 2;        //genislemenin boyutu pozitif tamsayi(makaledeki s parametresi)

K:=FiniteField(p);                        //asal cisim

if r ne 1 then
        p1:=PrimitivePolynomial(K,r);
        M<t>:=ext< K|p1>;         //altcisim
else
        M<t>:=K;                //altcisim
end if;

q:= p^r;      //altcismin boyu
m:= 4;        //sabit

N:=q^2-1; //Dizi sayisini verir

n:=q^2+1;                 //dizinin boyu

if m ne 1 then
        p2:=PrimitivePolynomial(M,m);
        F<z>:=ext< M|p2>;                 //altcismin genislemesi ilkel elemani z yani alfa
else
        F<z>:=M;
end if;

g:=z^N;    //diger makaledeki beta

Dizi:=[M|];    //optimal dizi

index1:={} ;  //dizi sayisi
for i:=1 to N do
        index1 join:={i};
end for;

index2:={} ; //dizideki eleman sayisi
for j:=1 to n do
```

```
        index2 join:={j};
end for;

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

print N," ELEMANLI OPTIMAL DIZI AILESININ ELEMANLARI: ",D_ailesi;

//Buradan itibaren Hamming Korelasyonu hesaplanmaktadir

D1:=[x: x in index2];   //H. Korelasyonu icin 1. dizi
D2:=[x: x in index2]; //H. Korelasyonu icin 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;
```

E.4.2 2. Üretim Metodu

```
 /* BU KOD C.DING 2009 TEMMUZ MAKALESINDEKI IKINCI METODU OLAN IZ FONKSIYONU
 ILE OPTIMAL DIZI AILESIOLUSTURMA FONKSIYONUNU GERCEKLEMEKTEDIR*/
p:= 3;        //tek asal
r:= 2;        //genislemenin boyutu pozitif tamsayi(makaledeki s parametresi)

K:=FiniteField(p);                        //asal cisim

if r ne 1 then
        p1:=PrimitivePolynomial(K,r);
        M<t>:=ext< K|p1>;         //altcisim
else
        M<t>:=K;               //altcisim
end if;

q:= p^r;      //altcismin boyu
m:= 2;        //pozitif tamsayi

N:=2; //q^m-1 in pozitif böleni.Dizi sayisini verir

n:=(q^m-1) div N;                //dizinin boyu

if m ne 1 then
        p2:=PrimitivePolynomial(M,m);
        F<z>:=ext< M|p2>;                 //altcismin genislemesi ilkel elemani z yani alfa
else
        F<z>:=M;
end if;

g:=z^N;    //diger makaledeki beta

Dizi:=[M|];    //optimal dizi

index1:={} ;  //dizi sayisi
for i:=1 to N do
        index1 join:={i};
end for;

index2:={} ; //dizideki eleman sayisi
```

```
for j:=1 to n do
        index2 join:={j};
end for;

D_ailesi:=[Dizi : x in index1];
for i in index1 do
        print "  ";
        print "  ";
        print "S",(i-1),"(",q,") icin dizi";
        for j in index2 do
            Dizi[j]:=Trace((z^(i-1))*(g^(j-1)));
        end for;
        Dizi;
        D_ailesi[i]:=Dizi;
end for;
print n," ELEMANLI OPTIMAL DIZI AILESININ ELEMANLARI: ",D_ailesi;

//Buradan itibaren Hamming Korelasyonu hesaplanmaktadir

D1:=[x: x in index2];   //H. Korelasyonu icin 1. dizi
D2:=[x: x in index2]; //H. Korelasyonu icin 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;
```

E.5 Verilen Parametrelere Göre Dizi Üreten Program

```
 /**/
 clear;

optimal:= function(p,r,m)     //p bir asal,r ilk genislemenin boyutu, m ikinci genislemenin boyutu
q:=p^r; //olusturulacak alt cismin boyu
K:=FiniteField(p);  //asal cisim
if r ne 1 then
p1:=PrimitivePolynomial(K,r);
M<v>:=ext< K|p1>;  //altcisim
else
M<v>:=K; //altcisim
end if;
PrintFile("D:/deneme.txt","p= ");
PrintFile("D:/deneme.txt",p);
PrintFile("D:/deneme.txt","q= ");
PrintFile("D:/deneme.txt",q);
PrintFile("D:/deneme.txt","q^m= ");
PrintFile("D:/deneme.txt",q^m);
PrintFile("D:/deneme.txt","%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%");
sayac:=2;
for k:=1 to (((q^m-1) div 2)+1 )do
if (q^m-1) mod sayac eq 0  then  // and (q-1) mod sayac ne 0
l:=sayac ; //(q-1) ile arasında asal ve (q^m)-1) i bolen bir tamsayi
PrintFile("D:/deneme.txt","l= ");
PrintFile("D:/deneme.txt",l);
PrintFile("D:/deneme.txt"," ICIN diziler-------------");

n:=((q^m)-1) div l;  //dizinin boyu
s:=1;    //gcd(s,q^m-1)=1 olacak sekilde
if m ne 1 then
p2:=PrimitivePolynomial(M,m);
F<z>:=ext< M|p2>;   //altcismin genislemesi ilkel elemani 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 olusturdugu dizi
index3:=[1,3,5,7];
for i in index1 do
PrintFile("D:/deneme.txt","     ");
PrintFile("D:/deneme.txt",z^i);
PrintFile("D:/deneme.txt"," icin dizi");

for j in index2 do
Dizi[j]:=Trace((z^i)*(t^(j-1)));
end for;
PrintFile("D:/deneme.txt",Dizi);
D_ailesi[i]:=Dizi;
end for;


//Buradan itibaren Hamming Korelasyonu hesaplanmaktadir

D1:=[x: x in index2];   //H. Korelasyonu icin 1. dizi

D2:=[x: x in index2]; //H. Korelasyonu icin 2. dizi
korelasyonlar:=[0: x in index2];
h_korelasyonlar:=[0: x in index1];
auto_korelasyon:=[0: x in index1];
for i in index1 do
D1:=D_ailesi[i];

for j in index1 do

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
korelasyonlar[k] +:=1;
end if;
end for;
end for;
if i eq j then   // dizinin kendi ile korelasyonunu göz ardı etmek icin
```

```
korelasyonlar[1]:=0;
end if;
h_korelasyonlar[j]:=Maximum(korelasyonlar);
if i eq j then   //auto korelasyonları bir dizide topluyoruz
auto_korelasyon[j]:=h_korelasyonlar[j];
end if;


//ASAGIDA OPTIMAL CIFTLER BELIRTILMEKTEDIR
opc_bound:=Ceiling(((2*n-q)*n)/((2*n-1)*q));
opf_bound:=Ceiling(((l*n-q)*n)/((l*n-1)*q));
if j gt 1 and i gt 1 then
for b:=(i-1) to 1 do
mxy1:=Maximum(auto_korelasyon[i-b],auto_korelasyon[i]);
mxy:=Maximum(mxy1,korelasyonlar[i-b]);
//PrintFile("D:/deneme.txt","   ");
//PrintFile("D:/deneme.txt",mxy);
if mxy eq opc_bound then
PrintFile("D:/deneme.txt","     ");
PrintFile("D:/deneme.txt",D_ailesi[i]);
PrintFile("D:/deneme.txt",D_ailesi[i-b]);
PrintFile("D:/deneme.txt","OPTIMAL CIFTTIR");
end if;
end for;
end if;


korelasyonlar:=[0: x in index2];
end for;
//PrintFile("D:/deneme.txt",h_korelasyonlar);
end for;

//ASAGIDA OPTIMAL DIZILER BELIRTILMEKTEDIR
epsilon:=n mod q;
op_bound:=Ceiling(((n-epsilon)*(n+epsilon-q)) / (q*(n-1)));

for v in index1 do
if auto_korelasyon[v] eq op_bound then
PrintFile("D:/deneme.txt","     ");
PrintFile("D:/deneme.txt",D_ailesi[v]);
PrintFile("D:/deneme.txt","dizisi optimal");
end if;
end for;
PrintFile("D:/deneme.txt","");
PrintFile("D:/deneme.txt","Optimallik siniri:");
```

```
PrintFile("D:/deneme.txt",op_bound);
PrintFile("D:/deneme.txt","Optimal cift siniri:");
PrintFile("D:/deneme.txt",opc_bound);
PrintFile("D:/deneme.txt","Optimal aile siniri:");
PrintFile("D:/deneme.txt",opf_bound);
PrintFile("D:/deneme.txt","");
PrintFile("D:/deneme.txt","oto-korelasyonlar:");
PrintFile("D:/deneme.txt",auto_korelasyon);
PrintFile("D:/deneme.txt","");

PrintFile("D:/deneme.txt","%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%");

end if;
sayac:=sayac+1;
end for;
return "bitti";
end function;
optimal(3,1,3);
```

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı,Adı	: Kahraman, Seda
Uyruğu	: Türkiye Cumhuriyeti
Doğum tarihi ve yeri	: 13.10.1986 Antalya
Medeni hali	: Bekar
Telefon	: 0 (242) 321 90 19
e-mail	: sedakahraman@gmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Lisans	TOBB ETÜ	2009

İş Deneyimi

Yıl	**Yer**	**Görev**
2009-2011	TOBB ETÜ	Araştırma Görevlisi

Yabancı Dil

İngilizce