Optimal Frekans Atlamalı Diziler

Seda Kahraman ve Zülfükar Saygı

***Özet*—Bu çalışmanın 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. Bu çalışmada bahsedilen optimallik Lempel-Greenberger ve Peng-Fan anlamındadır. 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 yeni optimal dizilerin ve dizi çiftlerinin varlığı araştırılmıştır.**

***Anahtar Kelimeler*—Frekans atlamalı diziler, Hamming korelasyonu, optimal frekans atlamalı diziler, İz fonksiyonu, optimal frekans atlamalı dizi çiftleri, optimal frekans atlamalı dizi ailesi.**

***Abstract*—The aim of this paper is the constructions of optimal frequency hopping sequences (FHS) that are used in Frequency Hopping Code Division Multiple Access (FH-CDMA) systems, Bluetooth and ultra wide band. There are some bounds in the literature to determine the optimality. The optimality in this work is referred to Lempel-Greenberger and Peng-Fan. There are some constructions techniques for FHSs such that algebraic, combinatorial, etc. We have examined 4 different papers in which the Trace function is used for the constructions and we have implemented the corresponding MAGMA codes. Also new optimal sequences and sequence pairs are investigated.**

***Index Terms*—Frequency hopping sequences, Hamming correlation, optimal frequency hopping sequences, Trace function, optimal FHS pairs, optimal FHS family.**

I. GİRİŞ

FREKANS atlamalı diziler, Frekans Atlamalı Yayılı İzge (FHSS) sistemlerinde kullanılmaktadır. FHSS sistemleri, karıştırıcı önleme[2], güvenli ve çoklu erişim sağlama özellikleri ile ordu radyo iletişimi, mobil iletişim, modern radar ve deniz radarı yankı-konum sistemlerinde[3] yaygın olarak kullanılır [2], [8]. Frekans Atlamalı Kod Bölüşümlü Çoklu Erişim (FH-CDMA), Bluetooth ve ultra geniş bant gibi popüler sistemler en önemli kullanım alanlarıdır [4], [10], [11], [12]. FHSS önemli bir modülasyon tekniğidir. Bu tekniğin geliştirilmesini sağlayan en önemli sebep Yakın-Uzak Probleminin [19] etkisini oldukça azaltarak çoklu erişime imkan sağlamasıdır. Bu teknikte vericiler frekanslar arasında atlayarak veri gönderdiği için aynı anda aynı frekansı kullanmaya çalışmadıkları sürece çakışma olmadan alıcıya veri aktarabileceklerdir. Çakışma olmaması için de FHSS de kullanılan frekans atlamalı dizilerin optimal olması gerekir. Yani iyi bir Hamming Korelasyonuna sahip olmalıdırlar. FHSS sistemlerinde optimalliğin yanısıra diziyi üreten LFSR nin boyu olarak tanımlanan doğrusal karmaşıklığın da büyük olması beklenir [5]. Bu çalışmada incelenen makaleler sadece optimallik üzerinde durmuşlardır. Çalışmalarda kullanılan optimallik Lempel-Greenberger ve Peng-Fan anlamındadır. FHS lerin oluşturulmasında kullanılan cebirsel, kombinatorik vs. gibi bir çok metod vardır. Detaylı bilgi ve referanslar için [17] çalışması incelenebilir. Bunların içinden cebirsel bir üretim metodu olan İz Fonksiyonu ile üretim yapan 4 makale incelenmiş ve bunların MAGMA ile gerçekleştirimi yapılarak örnekleri incelenmiştir. Ayrıca yeni optimal dizilerin varlığı araştırılmıştır.

Gerçek hayat uygulamalarında kullanmak için çeşitli uzunluklarda diziler gerekebilir. Bu nedenle farklı dizi uzunlukları için optimal dizilerin bilinmesi önemlidir. Literatürde farklı metodlarla Lempel-Greenberger sınırına göre optimal dizi üreten çalışmalar (optimal çift ve aile üretenlerden) daha fazladır (bkz. [4], [13], [1], [15], [14]). Bunun yanında optimal aile üreten sadece bir kaç üretim metodu vardır [9].

A. Genel Bilgiler ve Tanımlar

Olabilecek bütün frekans değerlerinden oluşan $\mathbb{F} = \{f_0, f_1, \cdots, f_{l-1}\}$ kümesine *Alfabe* denir. $\mathbb{F}$ 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.

Tanım 1 (Hamming Korelasyonu). $X = (x_0, x_1, \ldots, x_{v-1})$ ve $Y = (y_0, y_1, \ldots, y_{v-1})$ şeklinde iki frekans atlamalı $X, Y \in S$ dizisi verildiğinde, bunlar arasındaki *Hamming Korelas- yonu* $H_{X,Y}$ aşağıdaki şekilde tanımlanır:

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

Burada

$$h[a,b] = \begin{cases} 1 & \text{, eğer } a = b \text{ ise} \\ 0 & \text{, diğer durumlar} \end{cases} \tag{2}$$

şeklindedir ve indis pozisyonundaki her işlem mod v de yapılır.

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

Tanım 2. Birbirinden farklı her $X, Y \in S$ FHS leri için:
Hamming Oto-Korelasyonu:

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

Hamming Çapraz-Korelasyonu:

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

S. Kahraman, Matematik Bölümü, TOBB Ekonomi ve Teknoloji Üniversitesi.
Z. Saygı, Matematik Bölümü, TOBB Ekonomi ve Teknoloji Üniversitesi.

[1] Frequency Hopping Code Division Multiple Access
[2] antijamming
[3] sonar echo-location systems

Dizi çiftleri için Hamming Korelasyonu:

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

Dizi aileleri için Hamming Korelasyonu:

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

eşitlikleri ile tanımlanır.

Hamming korelasyonu çakışmaları sayan bir fonksiyondur. İletişimdeki problemlerin mümkün olduğunca az olması için çakışma sayısının mümkün olduğunca az olması gerekmektedir. Bu nedenle aşağıdaki optimallik kriterleri belirlenmiştir.

Optimallik Kriterleri:

O.1 Her $X' \in S$ için $H(X) \leq H(X')$ sağlanıyorsa $X \in S$ dizisine *Optimal* denir

O.2 Her $X', Y' \in S$, $X' \neq Y'$ 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. Bu nedenle Hamming Korelasyonları için sınırlar bulunmuştur. Bu çalışmada literatürde en çok kullanılan iki sınır kullanılmıştır. Eğer Hamming korelasyon değeri sınıra eşit ise dizi, dizi çifti veya aileleri için optimaldir denir.

Buradan itibaren uzunluğu v, alfabe boyu q ve hamming oto korelasyonu $\lambda = H(X)$ olan dizileri (v, q, λ) ile, q elemanlı alfabe üzerinde tanımlı v uzunluğunda N diziden oluşan ve hamming korelasyonu $\lambda = M(F)$ olan dizi ailesini $(v, N, \lambda : q)$ ile göstereceğiz.

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

$$H(X) \geq \left\lceil \frac{(v-\epsilon)(v+\epsilon-q)}{q(v-1)} \right\rceil \tag{3}$$

eşitsizliği sağlanır.

Lemma 2 (Peng-Fan Sınırı(2004)). [3] *$F \subset S$, q boyutlu alfabe üzerinde tanımlı v uzunluğundaki N diziden oluşan dizi ailesi olsun. $I = \lfloor vN/q \rfloor$ olarak tanımlanırsa*

$$M(F) \geq \left\lceil \frac{(vN-q)v}{(vN-1)q} \right\rceil \tag{4}$$

ve

$$M(F) \geq \left\lceil \frac{2IvN-(I+1)Iq}{(vN-1)N} \right\rceil \tag{5}$$

sağlanır.

Tanım 3. $\mathbb{F}_q$, q elemanlı cisim ve $\mathbb{F}_{q^m}$ onun sonlu genişlemesi olsun. $\alpha \in \mathbb{F}_{q^m}$ olmak üzere $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ iz fonksiyonu

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}$$

şeklinde tanımlanır.

II. Literatürde İz Fonksiyonu ile Üretilen FHS ler

Bu bölümde [5], [6], [7] ve [9] makalelerinde iz fonksiyonu yardımıyla oluşturulan FHS ler incelenecektir. Bu makalelerdeki üretim metodlarında sırasıyla $l = 2, l = q-1, l \mid (q-1)$ ve $l = q^2 - 1$ alınarak uzunlukları $v = \frac{q^m-1}{l}$ olan optimal FHS ler elde edilmiştir. Bu FHS lerin karşılaştırılmaları detaylı olarak [18] çalışmasında incelenmiştir. Uygulamalarda kullanılacak dizi uzunluğuna bağlı olarak bu yöntemlerden uygun olanı seçilebilir.

A. [5] Makalesindeki Üretim Metodu

p bir tek asal sayı ve r pozitif tamsayı olmak üzere $q = p^r$ olsun. $m \geq 3$ 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. Her $a \in \mathbb{F}_{q^m}^*$ için

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

dizileri Lemma 1 deki Lempel-Greenberger Sınırına göre optimal $(\frac{q^m-1}{2}, q, \frac{q^{m-1}-1}{2})$-FHS lerdir. Ayrıca $a \in \mathbb{F}_{q^m}^*$ bir karesel eleman, $a' \in \mathbb{F}_{q^m}^*$ bir karesel olmayan eleman olmak üzere c_a ve $c_{a'}$ optimal çifttir.

Örnek 1. $p = 5$, $r = 1$ olsun. O halde $q = 5^1 = 5$ olarak bulunur. $m = 3$ olsun ve $\mathbb{F}_{5^3}^*$ cismini oluşturmak için $x^3 + 3x + 3$ ilkel polinomunu alalım. $ebob(s, q^m - 1) = ebob(1, 5^3 - 1) = 1$ olduğundan $s = 1$ olarak alalım. MAGMA gerçekleştirimi ile elde edilen $(62, 5, 12)$ dizilerinden $a = 1$ ve $a' = -1$ için diziler aşağıdaki gibidir:

c_1 = (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, 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)

c_{-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, 1, 0, 0, 4, 1).

1 karesel eleman olduğundan -1 karesel olmayan eleman olduğundan $\{c_1, c_{-1}\}$ optimal çift verir.

B. [6] Makalesindeki Üretim Metodu

q bir asalın kuvveti ve m bir pozitif tamsayı olsun. 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.Her $0 \leq i \leq q-2$ 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 $ebob\left(q-1, \sum_{i=0}^{m-1} q^i\right) = 1$ sağlanırsa $S^{m,q}$, Lemma 2 daki Peng-Fan Sınırına göre optimal

$\left(\frac{q^m-1}{q-1}, q-1, \frac{q^{m-1}-1}{q-1}; q\right)$ FHS ailesi elde edilir. Ayrıca bu ailenin her bir elemanı Lemma 1 daki Lempel-Greenberger Sınırına göre optimaldir.

Örnek 2. $q = 4$, $m = 2$ olsun. O halde $q^m = 4^2$ olarak bulunur. $\mathbb{F}_{4^2}^*$ cismini oluşturmak için $x^2 + x + t^2$ ilkel polinomunu alalım. $ebob\left(q-1, \sum_{i=0}^{m-1} q^i\right) = ebob\left(3, \sum_{i=0}^{m-1} q^i = \frac{q^m-1}{q-1} = \frac{4^2-1}{4-1} = 5\right) = 1$ olduğundan MAGMA gerçekleştirimi ile elde edilen optimal (5,3,1;4) FHS ailesi t, $\mathbb{F}_2$ üzerinde 2. dereceden $x^2 + x + 1$ ilkel polinomun kökü olmak üzere aşağıdaki gibidir:

$S_0^{2,8} = (0,\ t,\ t^2,\ t^2,\ t)$

$S_1^{2,8} = (1,\ 1,\ t^2,\ 0,\ t^2)$

$S_2^{2,8} = (1,\ 0,\ 1,\ t,\ t)$

C. [7] Makalesindeki Üretim Metodu

p bir asal sayı ve r pozitif tamsayı olmak üzere $q = p^r$ ve $m,\ l,\ l \mid (q-1)$ ve $ebob\left(\frac{q^m-1}{q-1}, l\right) = 1$ 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. $v = \frac{q^m-1}{l}$ olmak üzere her $g \in \mathbb{F}_{q^m}^*$ için

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

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

Örnek 3. $p = 2$ ve $r = 3$ olsun. $\mathbb{F}_2$ üzerinde 3. dereceden $x^3 + x + 1$ ilkel polinomunun kökü v ile $\mathbb{F}_q = \mathbb{F}_8$ cismini oluşturalım. $m = 2$ alınırsa $q^m = 8^2$ olarak bulunur. $\mathbb{F}_{8^2}$ cismini oluşturmak için x^2+vx+v ilkel polinomunu alalım ve α bu polinomun kökü olsun. $l = 7$ olarak şeçilirse $7 \mid (8-1)$ ve $ebob\left(\frac{8^2-1}{8-1}, 7\right) = 1$ sağlanır. MAGMA gerçekleştirimi ile elde edilen optimal (9,8,1)-FHS dizilerinden bazıları aşağıdaki gibidir:

$c_\alpha = (v,\ 0,\ v,\ v^5,\ v^4,\ v^6,\ v^6,\ v^4,\ v^5)$

$c_{\alpha^2} = (v^2,\ v^5,\ 0,\ v^5,\ v^2,\ v,\ v^3,\ v^3,\ v)$

$c_{\alpha^3} = (v^5,\ v^6,\ v^2,\ 0,\ v^2,\ v^6,\ v^5,\ 1,\ 1)$

$c_{\alpha^4} = (v^4,\ v^2,\ v^3,\ v^6,\ 0,\ v^6,\ v^3,\ v^2,\ v^4)$

$c_{\alpha^5} = (v,\ v,\ v^6,\ 1,\ v^3,\ 0,\ v^3,\ 1,\ v^6)$

D. [9] Makalesindeki I. Üretim Metodu

$p = 2$, s pozitif bir tamsayı olmak üzere $q = p^s$ ve $r = q^4$ olsun. $N = q^2 - 1$ ve $v = q^2 + 1$ olarak tanımlansın. α, $\mathbb{F}_r^*$ ın bir üreteci olsun ve $g = \alpha^N$ olarak tanımlansın.Her $0 \le i \le N-2$ için

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

dizileri tanımlansın. Her bir S_i^q, $\mathbb{F}_q$ üzerinde n uzunluğunda dizilerdir.

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

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

Örnek 4. $p = 2$, $s = 3$ olsun. $\mathbb{F}_2$ üzerinde 3. dereceden $x^3 + x + 1$ ilkel polinomunun kökü t ile $\mathbb{F}_8$ cismini oluşturalım. $r = 8^4$ olacağından $\mathbb{F}_{8^4}$ cismini oluşturmak için $x^4 + t^4x^3 + t^5x^2 + x + t$ ilkel polinomunu alalım. $N = 8^2 - 1 = 63$ ve $v = 8^2 + 1 = 65$ olur. MAGMA gerçekleştirimi ile elde edilen optimal (65,63,9;8) FHS ailesinin dizilerinden bazıları aşağıdaki gibidir:

$S_0^8 = (0,\ t^4,\ t,\ t^3,\ t^2,\ t^6,\ t^6,\ t^4,\ t^4,\ t^4,\ t^5,\ t,\ t^5,\ 1,\ t,\ t^5,\ t,\ t^6,\ t,\ t^2,\ t^3,\ t^4,\ t^2,\ t,\ t^3,\ t^6,\ 1,\ t^4,\ t^2,\ t^2,\ t^3,\ t^5,\ t^2,\ t^2,\ t^5,\ t^3,\ t^2,\ t^2,\ t^4,\ 1,\ t^6,\ t^3,\ t,\ t^2,\ t^4,\ t^3,\ t^2,\ t,\ t^6,\ t,\ t^5,\ t,\ 1,\ t^5,\ t,\ t^5,\ t^4,\ t^4,\ t^4,\ t^6,\ t^6,\ t^2,\ t^3,\ t,\ t^4)$

$S_1^8 = (t^4,\ t^4,\ t^3,\ t,\ t,\ t^5,\ t^5,\ t^6,\ 1,\ t^4,\ 0,\ 1,\ t^6,\ t^3,\ t^2,\ t^4,\ t^3,\ t^6,\ t^2,\ 1,\ t^3,\ t^5,\ t^5,\ 0,\ t^3,\ t,\ 1,\ 0,\ t,\ t^3,\ t^5,\ t,\ 0,\ 0,\ 0,\ t,\ t^5,\ t^3,\ t,\ 0,\ 1,\ t,\ t^3,\ 0,\ t^5,\ t^5,\ t^3,\ 1,\ t^2,\ t^6,\ t^3,\ t^4,\ t^2,\ t^3,\ t^6,\ 1,0,\ t^4,\ 1,\ t^6,\ t^5,\ t^5,\ t,\ t,\ t^3)$

$S_2^8 = (t,\ 0,\ t,\ 0,\ t^6,\ t^2,\ t^2,\ t^3,\ t^2,\ t^6,\ t^3,\ t^2,\ t^3,\ 0,\ t^5,\ 1,\ 1,\ t^2,\ t,t^6,\ 0,\ 0,\ 1,\ t^3,\ t^5,\ t^3,\ t^6,\ t^6,\ t^4,\ 1,\ t,\ t^4,\ t^6,\ t^5,\ t^5,\ t^6,\ t^4,\ t,\ 1,\ t^4,\ t^6,\ t^6,\ t^3,\ t^5,\ t^3,\ 1,\ 0,\ 0,\ t^6,\ t,\ t^2,\ 1,\ 1,\ t^5,\ 0,\ t^3,\ t^2,\ t^3,\ t^6,\ t^2,\ t^3,\ t^2,\ t^2,\ t^6,\ 0)$

$S_3^8 = (t,\ t^4,\ t^4,\ t,\ t^6,\ 0,\ t,\ t^4,\ 0,\ t^6,\ t^3,\ t^2,\ t^5,\ t^6,\ 1,\ t^6,\ 1,\ t^4,\ t^4,\ t^3,\ 0,\ t^6,\ t^2,\ t^6,\ t^6,\ 0,\ t^2,\ t^3,\ 1,\ t,\ t^2,\ t^5,\ t^5,\ t^5,\ 0,\ t^5,\ t^5,\ t^5,\ t^2,\ t,\ 1,\ t^3,\ t^2,\ 0,\ t^6,\ t^6,\ t^2,\ t^6,\ 0,\ t^3,\ t^4,\ t^4,\ 1,\ t^6,\ 1,\ t^6,\ t^5,\ t^2,\ t^3,\ t^6,\ 0,\ t^4,\ t,\ 0,\ t^6)$

$S_4^8 = (t^2,\ t^3,\ 0,\ t^3,\ t^2,\ t^5,\ 0,\ t,\ t^5,\ t^2,\ t^4,\ 1,\ t^4,\ t,\ t^6,\ t^5,\ t^4,\ t^5,\ t^5,\ t^6,\ t^6,\ t^3,\ t^4,\ t^6,\ t^6,\ 1,\ 0,\ 0,\ t^3,\ 0,\ 1,\ t^5,\ 1,\ t^2,\ t^4,\ t^4,\ t^2,\ 1,\ t^5,\ 1,\ 0,\ t^3,\ 0,\ 0,\ 1,\ t^6,\ t^6,\ t^4,\ t^3,\ t^6,\ t^6,\ t^5,\ t^5,\ t^4,\ t^5,\ t^6,\ t,\ t^4,\ 1,\ t^4,\ t^2,\ t^5,\ t,\ 0,\ t^5)$

E. [9] Makalesindeki II. Üretim Metodu

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 $v = \frac{r-1}{N}$ olsun. α, $\mathbb{F}_r^*$ ın bir üreteci olsun ve $g = \alpha^N$ olarak tanımlansın. Her $0 \le i \le N-2$ için

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

dizileri tanımlansın. Her bir S_i^q, $\mathbb{F}_q$ üzerinde v uzunluğunda dizilerdir.

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

olarak tanımlandığında, $S^{q,m}$ kümesi, $ebob(v, N) = 1$, $q-1 \equiv \frac{N}{2} \pmod N$, $ebob\left(\frac{r-1}{q-1}\ (mod\ N), N\right) = 2$ ve $N > \frac{q-1}{q}\sqrt{r}$

şartları sağlanırsa Lemma 2 daki Peng-Fan Sınırına göre optimal $\left(\frac{r-1}{N}, N, \frac{(r-q+(q-1)\sqrt{r})}{qN}; q\right)$ FHS ailesi oluşturur.

Örnek 5. $p = 3$, $s = 2$ için $\mathbb{F}_3$ üzerinde 2. dereceden $x^2 + 2x + 2$ ilkel polinomun kökü t ile $\mathbb{F}_9$ cismini oluşturalım. $m = 2$ olsun. $\mathbb{F}_{9^2}$ cismini oluşturmak için $x^2 + t^5x + t^3$ ilkel polinomunun kökünü alalım. $N = 16 \mid (9^2 - 1)$ seçilirse $v = \frac{81-1}{16} = 5$ olur. $ebob(v, N) = ebob(5, 16) = 1$, $9 - 1 = 8 \equiv \frac{18}{2} = 8 \pmod{16}$, $ebob\left((\frac{81-1}{9-1} = 10\ (mod\ 16), 16)\right) = 2$ ve $N = 16 > \frac{8}{9}\sqrt{9} = 8$ sağlandığından parametre seçimimiz doğrudur. MAGMA gerçekleştirimi ile hesaplanarak elde edilen optimal (5,15,1;9) FHS ailesinin dizileri aşağıdaki gibidir:

$$S_0^{9,2} = (2,\ t^7,\ t^5,\ t^5,\ t^7)$$

$$S_1^{9,2} = (t,\ 1,\ 2,\ t^5,\ 0)$$

$$S_2^{9,2} = (2,\ 2,\ t^6,\ t^3,\ t^6)$$

$$S_3^{9,2} = (t^3,\ 2,\ 0,\ 1,\ t^7)$$

$$S_4^{9,2} = (t^5,\ t^2,\ t^5,\ t^3,\ t^3)$$

$$S_5^{9,2} = (0,\ t^7,\ t^6,\ t^2,\ t^3)$$

$$S_6^{9,2} = (2,\ t^2,\ t^2,\ 2,\ t)$$

$$S_7^{9,2} = (t^5,\ t,\ t^2,\ 0,\ t^6)$$

$$S_8^{9,2} = (t,\ t^3,\ 1,\ t^3,\ t)$$

$$S_9^{9,2} = (t,\ 0,\ t^5,\ 2,\ 1)$$

$$S_{10}^{9,2} = (t^7,\ t^2,\ 1,\ 1,\ t^2)$$

$$S_{11}^{9,2} = (2,\ t^3,\ t^7,\ 1,\ 0)$$

$$S_{12}^{9,2} = (t^7,\ t^7,\ t,\ t^6,\ t)$$

$$S_{13}^{9,2} = (t^6,\ t^7,\ 0,\ t^3,\ t^2)$$

$$S_{14}^{9,2} = (1,\ t^5,\ 1,\ t^6,\ t^6)$$

$$S_{15}^{9,2} = (0,\ t^2,\ t,\ t^5,\ t^6)$$

III. Nümerik Hesaplamalar

Bu bölümde yaptığımız nümerik dizi üretme çalışmalarından bahsedilecektir. Sonrasında ise çalıştığımız parametreler tablo şeklinde aktarılacaktır. p bir asal sayı ve r pozitif tamsayı olmak üzere $q = p^r$ olsun. Ayrıca kabul edelim ki, m pozitif tamsayı olmak üzere $\mathbb{F}_{q^m}$ sonlu cismi verilsin 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 her $a \in \mathbb{F}_{q^m}^*$ için

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

dizileri oluşturulup bunların Hamming Korelasyonlarını hesaplar ve sınırlarla karşılaştırarak optimalliğine karar verir.

[5], [6], [7] ve [9] makalelerindeki üretim metodlarında 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. 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). Tabloların son sütunlarında parametreler [5], [6], [7] ve [9] makalelerinde işlenmiş ise referansı verilmektedir. Ayrıca, dizilerde dizi uzunluğunu $\frac{q^m-1}{l} \leq q$, dizi çiftlerinde dizi uzunluğunu $\frac{q^m-1}{l} \leq \frac{q}{2}$ olacak şekilde veren parametreleri *aşikar* olarak nitelendirdik. Bunların dışındaki optimal dizi veya çift oluşturan parametreleri de *yeni* olarak nitelendirdik.

TABLO I
P=2 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
4	2	3	var	var	[6], [7]
		5	var	yok	aşikar
4	3	3	yok	yok	
		7	yok	yok	
		9	var	yok	yeni
		21	var	yok	aşikar
4	4	3	var	var	[6], [7]
		5	yok	yok	
		15	yok	yok	
		17	var	yok	yeni
		51	var	var	yeni
		85	var	yok	aşikar
8	2	3	yok	yok	
		7	var	var	[6], [7]
		9	var	yok	aşikar
		21	var	var	aşikar
8	3	7	var	var	[6], [7]
		73	var	yok	aşikar
16	2	3	var	var	[6], [7]
		5	var	var	[6], [7]
		15	var	var	[6], [7]
		17	var	yok	aşikar
		51	var	var	aşikar
		85	var	var	aşikar

TABLO II
P=3 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
3	2	2	yok	yok	
		4	var	yok	aşikar
3	3	2	var	var	[5], [7]
		13	var	yok	aşikar
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
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

TABLO III
P=5 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
5	2	2	yok	yok	
		3	yok	yok	
		4	yok	yok	
		6	var	yok	aşikar
		8	var	var	yeni
		12	var	var	aşikar
5	3	2	var	var	[5], [7]
		4	var	var	[6], [7]
		31	var	yok	yeni
		62	var	yok	aşikar

TABLO IV
P=7 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
7	2	2	yok	yok	
		3	var	var	[7]
		4	yok	yok	
		6	yok	yok	
		8	var	yok	aşikar
		12	var	yok	
		16	var	var	aşikar
		24	var	var	aşikar
7	3	2	var	var	[5], [7]
		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

TABLO V
P=11 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
11	2	2	yok	yok	
		3	yok	yok	
		4	yok	yok	
		5	var	var	[7]
		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

TABLO VI
P=13 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
13	2	2	yok	yok	
		3	var	var	[7]
		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	[9]
		28	var	var	aşikar
		42	var	var	aşikar
		56	var	var	aşikar
		84	var	var	aşikar

TABLO VII
P=17 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
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

TABLO VIII
P=19 İÇİN ELDE EDİLEN NÜMERİK SONUÇLAR

q	m	l	Optimal Dizi	Optimal Çift	Açıklama
19	2	2	yok	yok	
		3	var	var	[7]
		4	yok	yok	
		5	yok	yok	
		6	yok	yok	
		8	yok	yok	
		9	var	var	[7]
		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

IV. SONUÇ

Bu çalışmada, FH-CDMA, Bluetooth ve ultra geniş bant gibi popüler sistemlerde kullanılan Optimal Frekans Atlamalı Diziler ve bu dizilerin iz fonksiyonu ile oluşturulmasıyla ilgili literatür incelenmiş ve metodların MAGMA ile gerçekleştirimleri yapılarak örnekler verilmiştir. Ayrıca parametrelerde yapılan yeniliklerle yeni optimal dizilerin varlığı araştırılmıştır. Bazı parametreler için, incelenen dört makalede bulunmayan optimal dizi veya çiftlere rastlanılmıştır. Bunların genelleştirilmesiyle ilgili çalışmalarımız devam etmektedir.

TEŞEKKÜRLER

Bu çalışma TÜBİTAK 109T344 referans numaralı proje tarafından desteklenmiştir. Projedeki desteklerinden dolayı TÜBİTAK'a teşekkür ederiz.

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] 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.
[3] 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.
[4] Chu W., Colbourn C.J. *Optimal frequency-hopping sequences via cyclotomy*, IEEE Trans.Inf. Theory, vol. 51, no. 3, pp 1139-1141, March 2005.
[5] 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.
[6] Ding C., Yin J. *Sets of Optimal Frequency Hopping Sequences*, IEEE Trans. Inf. Theory, vol. IT-54, no. 8, pp 3741-3745, August 2008.
[7] 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.
[8] 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.
[9] 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 .
[10] Chung J., Yang K. *Optimal Frequency-Hopping Sequences With New Parameters*, IEEE Trans.Inf. Theory, vol. 56, No. 4, pp 1685-1693, April 2010.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] 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.
[16] Computational Algebra Group, MAGMA Computational Algebra System(V2.10-22). 'http://magma.maths.usyd.edu.au/magma/'.
[17] S. Kahraman, Optimal Frekans Atlamalı Diziler, M.S. Tezi, Mat. Böl., TOBB ETÜ, Ank., 2011.
[18] K. Bayraktar, Frekans Atlamalı Diziler, M.S. Tezi, Mat. Böl., TOBB ETÜ, Ank., 2010.
[19] F. Halsall, *Data Communications, Computer Networks and Open Systems*. USA: Addison-Wesley, 1995.