ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DOKTORA TEZİ

İYİ AİLE KARMAŞIKLIĞI VE ÇAPRAZ KORELASYON ÖLÇÜSÜNE SAHİP DİZİ AİLELERİ

Kenan DOĞAN

MATEMATIK ANABİLİM DALI

ANKARA
2025

ÖZET

Doktora Tezi

İYİ AİLE KARMAŞIKLIĞI VE ÇAPRAZ KORELASYON ÖLÇÜSÜNE SAHİP DİZİ AİLELERİ

Kenan DOĞAN

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Prof. Dr. Murat ŞAHİN

Bu tezde, bir dizi ailesinin sözde-rastgeleliğini(pseudorandomness) iki temel ölçüt açısından inceliyoruz: aile karmaşıklığı (f-karmaşıklık) ve ℓ mertebesindeki çapraz-korelasyon ölçütü. Çalışmamız, hem ikili (binary) hem de k-sembollü alfabeler üzerindeki dizileri kapsamaktadır. Öncelikle, ikili sözde-rastgele dizi ailelerinin oluşturulmasına yönelik bilinen yöntemleri genişletiyor ve belirli indirgenemez polinomların Legendre sembollerinden üretilen geniş bir ikili dizi ailesinin f-karmaşıklığı için bir sınır belirliyoruz. Bu ailenin ve onun dualinin, hem yüksek aile karmaşıklığına hem de görece yüksek bir mertebeye kadar düşük çapraz-korelasyon ölçüsüne sahip olduğunu gösteriyoruz. Ayrıca, benzer şekilde yüksek f-karmaşıklığa ve düşük çapraz-korelasyon ölçüsüne sahip ikinci bir ikili dizi ailesi sunuyoruz. Son olarak, sonuçlarımızı k-sembollü alfabeler üzerindeki dizi ailelerine genelliyoruz.

Ağustos 2025, 81 sayfa

Anahtar Kelimeler: ikili diziler; çapraz-korelasyon ölçütü; aile karmaşıklığı; k-sembollü diziler; sözde-rastgelelik

ABSTRACT

PhD Thesis

FAMILIES OF SEQUENCES WITH GOOD FAMILY COMPLEXITY AND CROSS-CORRELATION MEASURE

Kenan DOĞAN

Ankara University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Prof. Dr. Murat ŞAHİN

In this thesis, we examine the pseudorandomness of a family of sequences with respect to two key measures: family complexity (f-complexity) and cross-correlation measure of order ℓ. Our study encompasses sequences over both binary and k-symbol (k-ary) alphabets. We first extend known methods for constructing families of binary pseudorandom sequences and establish a bound on the f-complexity of a large family of binary sequences generated from the Legendre symbols of certain irreducible polynomials. We demonstrate that this family, as well as its dual, exhibits both high family complexity and low cross-correlation measure up to a relatively high order. Additionally, we present a second family of binary sequences with similarly high f-complexity and low cross-correlation measure. Finally, we generalize our results to families of sequences over the k-symbol alphabets.

August 2025, 81 pages

Key Words: binary sequences; cross-correlation measure; family complexity; k-symbols sequences; pseudorandomness

TEŞEKKÜR

Doktora ders dönemi ve tez hazırlama süreci boyunca bana her zaman destekte bulunan değerli danışmanım Prof. Dr. Murat ŞAHİN'e teşekkür ederim.

Doktora çalışmalarımın pek çok aşamasında düşünsel gelişimime yön veren, yalnızca bilimsel rehberliğiyle değil, aynı zamanda motive edici ve cesaretlendirici tutumuyla da her zaman yanımda olan Doç. Dr. Oğuz YAYLA'ya; süreç boyunca sunduğu yapıcı yaklaşımlar ve samimi desteği için gönülden teşekkür ederim.

Varlığıyla bana huzur veren biricik kızım Roza DOĞAN'a ve hayatımın her döneminde yanımda olan, bana daima inanan ve desteğini hiçbir zaman eksik etmeyen sevgili aileme derin minnet ve şükranlarımı sunarım.

Kenan DOĞAN

Ankara, Ağustos 2025

İÇİNDEKİLER

SİMGELER DİZİNİ

$\mathbb{F}_q$	q elemanlı sonlu cisim
$\mathbb{F}_q^n$	$\mathbb{F}_q$ cismi üzerinde n boyutlu vektör uzayı
$\mathbb{F}_q[X]$	Katsayıları $\mathbb{F}_q$ cisminden olan polinomlar halkası
$\overline{\mathbb{F}}_q$	$\mathbb{F}_q$ cisminin cebirsel kapanışı
$\mathbb{Z}_m$	mod m kalan sınıflar halkası
$U \ll V$, U=O(V)	Büyük O notasyonu
χ	Toplamsal karakter
ψ	Çarpımsal karakter
Tr	İz (trace) fonksiyonu
$\left(\frac{\cdot}{p}\right)$	Legendre sembolü (mod p'ye göre)
$W(E_N)$	N uzunluklu E_N dizisinin iyi-dağılım ölçütü
$C_\ell(E_N)$	E_N dizisinin ℓ dereceden korelasyon ölçütü
$N_\ell(E_N)$	E_N dizisinin ℓ dereceden normallik ölçütü
$Q_\ell(E_N)$	E_N dizisinin ℓ dereceden birleşik ölçütü
$C_{\mathbf{ab}}$	**a** ve **b** dizilerinin korelasyonu
$C_{\mathbf{a}}$	**a** dizisinin otokorelasyonu
LFSR	Doğrusal Geri Beslemeli Kaydırma Kayıtları
$\mathcal{F}$	Dizi ailesi
$\overline{\mathcal{F}}_f$	$\mathcal{F}$ dizi ailesinin duali
$C(\mathcal{F})$	$\mathcal{F}$ dizi ailesinin f-karmaşıklığı
$\Phi_\ell(\mathcal{F})$	$\mathcal{F}$ dizi ailesinin çapraz-korelasyon ölçütü
$\gamma_\ell(\mathcal{F})$	k-sembollü $\mathcal{F}$ dizi ailesinin çapraz-korelasyon ölçütü
obeb	Ortak Bölenlerin En Büyüğü
der (f)	f polinomunun derecesi

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

Sözde-rastgele (pseudorandom) diziler, deterministik kurallar aracılığıyla üretilmelerine rağmen istatistiksel olarak rastgele davranış sergileyen yapılardır. Bu diziler, sembol kümelerine göre sınıflandırıldıklarında; elemanları $\{0, 1\}$ veya $\{-1, +1\}$ kümelerinde yer alanlar *ikili (binary)*, $\{a_1, a_2, \ldots, a_k\}$ kümesinden gelenler ise *k-sembollü* diziler olarak adlandırılır. Bu yapıların üretimi, sonlu cisimler üzerinde tanımlı indirgenemez polinomlar, doğrusal geribeslemeli kaydırmalı yazıcılar, Mersenne Twister, Blum Blum Shub algoritması, kriptografik hash fonksiyonları, hücresel otomatlar ve kaotik sistemler gibi çeşitli yöntemlerle gerçekleştirilebilir.

Sözde-rastgele diziler; telekomünikasyon, kriptografi, simülasyon ve sayısal entegrasyon gibi çok çeşitli uygulama alanlarında kullanılmaktadır [Dick ve Pillichshammer 2010], [Golomb ve Gong 2005], [Niederreiter ve Winterhof 2015], [Topuzoğlu ve Winterhof 2007]. Örneğin telekomünikasyonda; kanal kodlama, hata tespiti ve düzeltimi, yayılı spektrum sistemleri ve CDMA (Kod Bölmeli Çoklu Erişim) yapılarında senkronizasyon görevlerinde etkin biçimde kullanılırlar. Yayılı spektrum teknikleri sayesinde sinyaller, geniş frekans bantlarına yayılarak parazit ve girişimden korunabilir. Kriptografi uygulamalarında ise güvenli anahtar üretimi, akan şifreleme sistemleri ve protokollerde önemli roller üstlenirler. Bu bağlamda yüksek kalitede rastgelelik özellikleri, veri gizliliği, bütünlüğü ve iletiminin güvenliği açısından kritik öneme sahiptir. Simülasyonlarda—özellikle Monte Carlo yöntemlerinde—bu diziler, karmaşık ve rastlantısal süreçlerin gerçekçi biçimde modellenmesine olanak tanır. Sayısal entegrasyon uygulamalarında ise hızlı ve hassas sonuçlar elde edilmesini sağlar.

Bu dizilerin kalitesi çeşitli istatistiksel ve yapısal ölçütler üzerinden değerlendirilir. Özellikle iyi-dağılım ölçütü (well-distribution measure) ve korelasyon ölçütü (correlation measure), tekil dizilerin rastgelelik niteliklerini niceliksel olarak belirlemede kritik rol oynar. Rastgelelik özelliklerini test etmek amacıyla çeşitli istatistiksel test

paketleri geliştirilmiştir. Bunlar arasında L'Ecuyer's TESTU01 [L'Ecuyer ve Simard 2007], Marsaglia'nın Diehard testi [Marsaglia 1996] ve NIST Statistical Test Suite [Rukhin vd. 2001] yer almaktadır. Bu test paketleri, dizilerin hem düzgün dağılımını hem de korelasyon yapılarını çok boyutlu istatistiksel yöntemlerle analiz eder. Ayrıca doğrusal karmaşıklık, oto-korelasyon değerleri ve çok boyutlu dağılımın düzgünlüğünü ölçen discrepancy gibi metrikler, teorik ve uygulamalı düzeyde değerlendirilen önemli kalite göstergeleridir [Gyarmati 2013], [Topuzoğlu ve Winterhof 2007].

Özellikle kriptografik sistemlerde, eşzamanlı olarak üretilen ve istatistiksel bağımsızlık gösteren çoklu sözde-rastgele ikili dizilerden oluşan dizi ailelerine ihtiyaç duyulabilir. Bu dizilerin yüksek düzeyde rastgelelik sergilemesi ve birbirlerinden bağımsız olması beklenir. Bu nedenle, *aile karmaşıklığı* (family complexity), çapraz-korelasyon (cross-correlation), *çakışma direnci* (collision resistance), *minimum mesafe* (minimum distance) ve *çığ etkisi* (avalanche effect) gibi metrikler dikkate alınır [Sárközy 2017]. Aile karmaşıklığı, bir dizi ailesinin belirli konum kümelerinde tüm olası sembol kombinasyonlarını temsil edebilme kapasitesini, dolayısıyla diziler arası ayırt edilebilirlik düzeyini ifade ederken; çapraz-korelasyon ise diziler arasındaki benzerlik miktarını ölçerek, aralarındaki bağımsızlık derecesini belirler. Çakışma direnci, farklı girdilerin aynı çıktıyı üretmesinin hesaplama açısından zor olmasını ifade ederken; çığ etkisi, girişte yapılan küçük bir değişikliğin, çıktı üzerinde büyük ve yaygın değişimlere yol açmasını gerektirir.

Dizi ailesi, belirli bir üretim mekanizması ile oluşturulan ve yapısal açıdan benzer özellikler sergileyen diziler kümesidir; bu tez kapsamında $\mathcal{F}$ ile gösterilecektir. Bu çalışmada, ikili ve k-sembollü diziler üzerine yapılan güncel araştırmalar doğrultusunda, $\mathbb{F}_p$ üzerinde tanımlı bazı indirgenemez polinomlar ve Legendre sembolü kullanılarak iki ayrı özgün dizi ailesi inşa edilmiştir. Söz konusu ailelerin sözde-rastgelelik özellikleri, özellikle çapraz-korelasyon ölçütü ve aile karmaşıklığı metrikleri üzerinden analiz edilmiştir. Ayrıca, bu alandaki mevcut yaklaşımların geliştirilmesi ve daha verimli yöntemlerin önerilmesi hedeflenmiştir.

1.1 Katkılar ve Ana Hatlar

Bu bölümde tezin temel katkıları sunulmakta ve bölümlerin genel yapısına ilişkin bir özet verilmektedir. Çalışmamız, sözde-rastgele dizilerin yapısal özelliklerini inceleyerek, bu dizilerin rastgelelik ve güvenlik kriterleri bakımından analizini amaçlamaktadır.

Bölüm 2, sözde-rastgele dizilerin incelenmesine yönelik teorik bir çerçeve sunmakta ve sonraki bölümler için metodolojik temel oluşturmaktadır. Bu doğrultuda, dizilerin rastgelelik özelliklerini anlamak ve analiz etmek amacıyla gerekli temel matematiksel kavramlar ele alınmıştır. Öncelikle karakter teorisi aracılığıyla dizilerin yapısal ve spektral özellikleri ele alınmış, sonlu abelyen grupların karakterleri üzerinden bu özelliklerin rastgelelik, doğrusal karmaşıklık ve güvenlik üzerindeki etkileri ortaya konmuştur. Ardından, normallik, korelasyon ve iyi dağılım gibi sözde-rastgelelik ölçütleri tanıtılmış ve bu ölçütler arasındaki yapısal ilişkiler ayrıntılı biçimde analiz edilmiştir. Doğrusal Geri Beslemeli Kaydırma Kayıtları (LFSR) ve Legendre sembollerine dayalı üretim teknikleri gibi yöntemler ele alınmış ve bu tekniklerin rastgelelik kriterleri açısından yeterliliği analiz edilmiştir. Ayrıca, doğrusal karmaşıklık kavramı, bir dizinin en kısa üretim yöntemiyle ilişkisi bakımından ele alınmış ve rastgelelik ölçütü bağlamındaki önemi açıklığa kavuşturulmuştur. Son olarak, çeşitli türde dizilerden oluşan dizi aileleri tanıtılmış ve bu yapıların güvenlik açısından taşıdığı özellikler değerlendirilmiştir.

Bölüm 3'te, **?** çalışmasında sunulan ikili sözde-rastgele dizi ailesi genişletilerek

$$\mathcal{F}_1 \coloneqq \left\{ \left(\frac{f_i(n)}{p} \right)_{n=1}^{p-1} : i = 1, \ldots, p-1 \right\}$$

biçimindeki yapı tanımlanmıştır.

Burada p tek asal sayı olmak üzere, her biri indirgenemez olan $f_i(x)$ polinomları

$$f_i(x) = x^d + a_2 i^2 x^{d-2} + a_3 i^3 x^{d-3} + \cdots + a_{d-2} i^{d-2} x^2 + a_d i^d \in \mathbb{F}_p[x]$$

biçimindedir.

? çalışmasındaki sonuçların aksine, Teorem 3.1 kapsamında, bu dizi ailesinin çapraz-korelasyon ölçütünün polinomun d derecesi arttıkça yükseldiği, buna karşılık f-karmaşıklığına dair alt sınırın azaldığı matematiksel olarak gösterilmiştir.

Bölüm 4'te, $\mathbb{F}_p$ üzerinde derecesi d olan ve indirgenemez bir f polinomu kullanılarak

$$\mathcal{F}_2 := \left\{ \left(\frac{f(n)}{p} \right)_{n=1}^{p-1} \right\}$$

ikili dizi ailesi analiz edilmiştir. Burada $d \leq \sqrt{p}/2$ koşulunu sağlayan pozitif bir tamsayıdır. Bu ailenin de hem yüksek f-karmaşıklığa hem de düşük çapraz-korelasyon ölçütüne sahip olduğu gösterilmiş; ancak d arttıkça bu metriklerde bozulma gözlemlenmiştir. Öte yandan, $\mathcal{F}_2$ ailesinin eleman sayısının yaklaşık p^{d-2} olması, bu yapının $\mathcal{F}_1$ ailesine kıyasla daha geniş olduğunu göstermektedir (Teorem 4.1). Benzer bir yapı, [Liu,H. ve Liu,X. 2024] çalışmasında farklı bir yöntemle oluşturulmuştur.

Bölüm 5'te, ikili diziler için sunulan temel kavramlar k-sembollü alfabe yapısına genellenmiş ve çapraz-korelasyon ile f-karmaşıklık ölçütleri bağlamında teorik sınırlar türetilmiştir. Son olarak, Bölüm 6'da, $\mathcal{F}_2$ ailesinin k-alfabe üzerindeki genellemesinin hem yüksek f-karmaşıklığa hem de düşük çapraz-korelasyon ölçütüne sahip olduğu gösterilmiştir.

Not 1.1. *Burada $U \ll V$ ve $U = \mathcal{O}(V)$ notasyonları, pozitif bir sabit c için $|U| \leq cV$ anlamında kullanışmıştır. Ayrıca, $f(n) = o(1)$ ifadesi, $n \to \infty$ iken $\lim_{n\to\infty} f(n) = 0$ koşulunu ifade etmek üzere kullanılmıştır.*

2. TEMEL KAVRAMLAR

2.1 Karakter Teorisi

Karakter teorisi, dizilerin yapısal ve spektral özelliklerini inceleme imkânı sunar ve bu sayede rastgelelik düzeyi, doğrusal karmaşıklık ve kriptografik güvenlik açısından kapsamlı analizlerin yapılabilmesini mümkün kılar. Bu nedenle karakter teorisi, özellikle kriptografide dizilerin tasarımı, analizi ve güvenli biçimde kullanılmasına yönelik temel bir matematiksel araç niteliğindedir.

Bu bölümde, sonlu cisimlerin toplamsal ve çarpımsal gruplarına ait karakterler incelenmiştir. Sunulan bilgiler için temel kaynak olarak [Lidl ve Niederreiter 1986] kullanılmaktadır.

G, sonlu bir abelyen grup (çarpımsal biçimde yazılmış) olsun. Bu durumda, $|G|$, G grubunun mertebesini; 1_G, birim elemanı gösterir. G'nin bir karakteri χ, G'den karmaşık düzlemde birim çember üzerindeki sayıların oluşturduğu U çarpımsal grubuna bir homomorfizmadır. Yani, her $g_1, g_2 \in G$ için

$$\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$$

özelliği sağlanmaktadır.

Bir χ karakteri için

1. $\chi(1_G) = 1$,
2. $\chi(g^{-1}) = \overline{\chi(g)}$

özellikleri geçerlidir; burada $\overline{\chi(g)}$ ifadesi, $\chi(g)$ karakter değerinin kompleks eşleniğini belirtmektedir.

Sonlu bir abelyen grup olan G üzerindeki tüm karakterlerin oluşturduğu küme, yine bir grup yapısı taşır. Bu grup, *karakter grubu* olarak adlandırılır ve $\widehat{G}$ ile gösterilir. Karakter grubunun mertebesi, G grubunun mertebesine eşittir; yani $|\widehat{G}| = |G|$'dir.

Her $\chi \in \widehat{G}$ için

$$\sum_{g \in G} \chi(g) = \begin{cases} |G|, & \text{eğer } \chi = \chi_0, \\ 0, & \text{eğer } \chi \neq \chi_0 \end{cases}$$

karakteristik toplam eşitliği sağlanır. Burada χ_0, G grubunun *aşikar karakteri* olup, her $g \in G$ için $\chi_0(g) = 1$ biçiminde tanımlanır.

Örnek 2.1. *[Lidl ve Niederreiter 1986] Mertebesi n olan sonlu ve devirli bir grup G ve bu grubun bir üreteci g olsun. Bu durumda, her $0 \leq j \leq n-1$ için*

$$\chi_j(g^k) \coloneqq e^{2\pi ijk/n}, \quad k = 0, 1, \ldots, n-1$$

şeklinde tanımlanan fonksiyon, grup G üzerinde tanımlı bir karakterdir. Burada χ_j karakterlerinin tamamı, G üzerindeki tüm karakterleri oluşturarak $\widehat{G}$ olarak adlandırılan dual grubu meydana getirir.

Sonlu $\mathbb{F}_q$ cisminin toplamsal grup olarak $(\mathbb{F}_q, +)$ ve çarpımsal grup olarak $(\mathbb{F}_q^*, \cdot)$ şeklinde iki önemli abelyen grup yapısı mevcuttur.

Öncelikle $(\mathbb{F}_q, +)$ toplamsal grubunu ele alalım. Bu grubun karakterlerine toplamsal karakterler denir. Karakteristiği p olan $\mathbb{F}_q$, bir sonlu cisim olup, asal cismi $\mathbb{F}_p$'dir. Bu asal cisim $\mathbb{F}_p$, $\mathbb{Z}/\langle p \rangle$ yapısıyla izomorftur.

$\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ biçiminde tanımlanan *iz fonksiyonu* (trace function), $\mathbb{F}_q$ üzerinde doğ-

rusal bir fonksiyondur.

$\mathbb{F}_q$ sonlu cismi, $q = p^d$ olmak üzere, $\mathbb{F}_p$ üzerinde tanımlı d boyutlu bir vektör uzayıdır. Bu bağlamda, iz fonksiyonu

$$\mathrm{Tr}(c) \coloneqq c + c^p + c^{p^2} + \cdots + c^{p^{d-1}}, \quad \forall c \in \mathbb{F}_q$$

şeklinde tanımlanır ve bu tanım her $c \in \mathbb{F}_q$ için bir $\mathbb{F}_p$ elemanı üretir.

İz fonksiyonu yardımıyla tanımlanan

$$\chi_1(c) \coloneqq e^{2\pi i \cdot \mathrm{Tr}(c)/p}, \quad \forall c \in \mathbb{F}_q \tag{2.1}$$

fonksiyonu, $(\mathbb{F}_q, +)$ grubu üzerinde bir karakterdir.

Gerçekten de, her $c_1, c_2 \in \mathbb{F}_q$ için iz fonksiyonunun doğrusallığı sayesinde

$$\chi_1(c_1 + c_2) = e^{2\pi i \cdot \mathrm{Tr}(c_1+c_2)/p} = e^{2\pi i \cdot (\mathrm{Tr}(c_1)+\mathrm{Tr}(c_2))/p} = \chi_1(c_1)\chi_1(c_2)$$

eşitliği sağlanır. Bu nedenle χ_1, $\mathbb{F}_q$ toplamsal grubunun *kanonik toplamsal karakteri* olarak adlandırılır.

Teorem 2.1. *$\mathbb{F}_q$ cismi üzerinde, her $b \in \mathbb{F}_q$ için*

$$\chi_b(c) \coloneqq \chi_1(bc), \quad \forall c \in \mathbb{F}_q,$$

şeklinde tanımlanan fonksiyon, $(\mathbb{F}_q, +)$ grubunun bir karakteridir. Ayrıca, bu gruptaki her toplamsal karakter bu yolla elde edilebilir.

$(\mathbb{F}_q^*, \cdot)$ grubunun karakterlerine, bu grubun çarpımsal karakterleri denir.

Teorem 2.2. *$\mathbb{F}_q$ sonlu cisminde g bir ilkel eleman olsun. Her $j = 0, 1, \ldots, q-2$ için tanımlanan*

$$\psi_j \colon \mathbb{F}_q^* \to \mathbb{C}^*, \quad \psi_j(g^k) \coloneqq e^{2\pi ijk/(q-1)}$$

fonksiyonu, $\mathbb{F}_q$ üzerinde bir çarpımsal karakterdir. Dahası:

1. *ψ_j karakterleri, $\widehat{\mathbb{F}_q^*}$ karakter grubunun tüm elemanlarını oluşturur.*
2. *$\mathbb{F}_q^*$'ın her karakteri, yalnızca bir $j \in \{0, 1, \ldots, q-2\}$ indisi için ψ_j şeklindedir.*

Tanımda kullanılan herhangi bir $g \in \mathbb{F}_q^*$ üretecinden bağımsız olarak, ψ_0 fonksiyonu *aşikâr* (trivial) çarpımsal karakteri temsil eder ve her $c \in \mathbb{F}_q^*$ için $\psi_0(c) = 1$ olacak şekilde tanımlanır.

Tanım 2.1. *$\mathbb{F}_q$ cismi üzerinde tanımlı çarpımsal karakterlerin kümesi, aşağıdaki özelliklere sahip, $q-1$ elemanlı, sonlu ve devirli bir Abel grubudur:*

- *Grup işlemi, karakterlerin noktasal çarpımıyla tanımlanır. Yani her $x \in \mathbb{F}_q^*$ için*

  $$(\psi_1 \cdot \psi_2)(x) = \psi_1(x)\psi_2(x)$$

  eşitliği sağlanır.

- *Bu grubun birim elemanı, trivial karakter olan ψ_0'dır ve her $x \in \mathbb{F}_q^*$ için $\psi_0(x) = 1$ eşitliği geçerlidir.*

- *Her karakterin tersi, karmaşık eşlenik alınarak elde edilir. Yani her ψ karakteri için ters eleman*

  $$\psi^{-1}(x) = \overline{\psi(x)}$$

  biçimindedir.

- *Karakterler kümesi devirli bir gruptur. Dolayısıyla her çarpımsal karakter, bir üreteç karakterin uygun bir kuvveti şeklinde yazılabilir.*

Örnek 2.2. *q bir tek asal kuvveti olmak üzere ($q = p^n$), η fonksiyonu, her $c \in \mathbb{F}_q^*$ için*

$$\eta(c) \coloneqq \begin{cases} 1, & \text{eğer } c \in \mathbb{F}_q^* \text{ kare eleman,} \\ -1, & \text{eğer } c \in \mathbb{F}_q^* \text{ kare olmayan eleman} \end{cases}$$

olarak tanımlanır. Bu fonksiyon çarpımsaldır ve yalnızca elemanın karesel olma durumuna göre değer aldığından, ***kuadratik karakter*** *olarak adlandırılır.*

Teorem 2.2'e göre, η karakteri, $\mathbb{F}_q^*$'nın çarpımsal karakter grubunun bir üretecinin $\frac{q-1}{2}$-inci kuvveti olarak ifade edilebilir.

Özellikle $q = p$ (tek asal) durumunda, kuadratik karakter η her $c \in \mathbb{F}_p$ için

$$\eta(c) = \left(\frac{c}{p}\right)$$

şeklinde yazılır. Burada kullanılan

$$\left(\frac{c}{p}\right) \coloneqq \begin{cases} 0, & \text{eğer } c \equiv 0 \pmod{p}, \\ 1, & \text{eğer } c \text{ bir kuadratik kalan ise,} \\ -1, & \text{eğer } c \text{ bir kuadratik kalan değilse} \end{cases}$$

tanımı **Legendre sembolü** olarak bilinir.

Not 2.1. *Bir kuadratik karakter, $(\mathbb{F}_q^*, \cdot)$ grubunun elemanlarını 1 ve -1 değerleriyle eşleyerek iki alt kümeye ayıran bir fonksiyondur. Ancak karakteristiği 2 olan bir cisimde $-1 \equiv 1 \pmod 2$ olduğundan bu ayrım anlamsızlaşır. Dolayısıyla kuadratik karakterler, karakteristiği 2 olan cisimlerde iyi tanımlı değildir.*

Çarpımsal karakterlerin önemli bir uygulaması, sonlu cisimler üzerindeki polinom-

lara ait karakter toplamlarının mutlak değeri için üst sınır elde edilmesinde kullanılan *Weil Teoremi*'dir. Bu çalışmada sunulan dizi ailelerinin üretiminde bu sınır kritik rol oynamaktadır.

Teorem 2.3. *[Weil 1948][**Weil Sınırı**]* $\mathbb{F}_q$ *sonlu cismi üzerinde tanımlı, aşikâr olmayan çarpımsal bir karakter* χ *ve* $f(x) \in \mathbb{F}_q[x]$ *polinomu verilsin. Eğer* $f(x)$ *kare-çarpansız bir polinomsa (yani* $\overline{\mathbb{F}}_q$ *üzerinde tüm kökleri ayrık ise), aşağıdaki eşitsizlik sağlanır:*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq (\deg(f) - 1) \cdot q^{1/2}$$

ve bu eşitsizlik, karakter toplamlarının büyüklüğü için üst sınır oluşturmaktadır.

1990'lı yılların ikinci yarısında Mauduit ve Sárközy, sonlu ikili dizilerin sözde-rastgelelik özelliklerini analiz edebilmek amacıyla *iyi-dağılım*, *korelasyon* ve *normallik* ölçütlerini ortaya koymuşlardır [Mauduit ve Sárközy 1997].

2.2 Sözde-Rastgele Ölçütlerinin Tanımı

Sonlu ikili dizilerin rastgelelik özelliklerini değerlendirmek amacıyla çeşitli ölçütler geliştirilmiştir. Bu bağlamda, bir dizinin elemanlarının dağılım düzenliliğini ve ardışık terimler arasındaki istatistiksel bağımlılığı nicel olarak değerlendirmeye yarayan iki temel ölçüt öne çıkmaktadır: *iyi-dağılım ölçütü* (well-distribution measure) ve *korelasyon ölçütü* (correlation measure). İyi-dağılım ölçütü, dizinin belirli aritmetik alt diziler üzerindeki toplamlarının büyüklüğünü temel alarak, dizideki elemanların ne derece dengeli dağıldığını ölçmektedir. Korelasyon ölçütü ise belirli aralıklardaki ardışık terimlerin çarpımına dayalı toplamları inceleyerek, farklı konumlardaki terimler arasında istatistiksel bir ilişkinin varlığını araştırmaktadır. Bu ölçütler, dizilerin ne ölçüde deterministik veya rastgele yapı sergilediğinin belirlenmesinde temel kriterler arasında yer almaktadır. Aşağıda her iki ölçütün tanımı ayrıntılı biçimde

sunulmaktadır.

Söz konusu ölçütler, çoğunlukla $\{-1,+1\}$ kümesinden elemanlar içeren sonlu ikili dizilere uygulanır. Bu bağlamda, uzunluğu N olan bir E_N ikili dizisi

$$E_N = (e_1, e_2, \ldots, e_N) \in \{-1,+1\}^N$$

şeklinde ifade edilmektedir.

Tanım 2.2. *[Mauduit ve Sárközy 1997] Bir E_N dizisi için, $a, b, t \in \mathbb{N}$ olmak üzere*

$$U(E_N, t, a, b) \coloneqq \sum_{j=1}^{t} e_{a+jb}$$

şeklinde tanımlanan fonksiyon, dizinin belirli bir aritmetik alt dizisindeki terimlerin toplamını ölçmektedir.

Öte yandan, $D = (d_1, d_2, \ldots, d_\ell)$ olmak üzere $0 \leq d_1 < d_2 < \cdots < d_\ell$ koşulunu sağlayan artan bir dizi verildiğinde ve $M \in \mathbb{N}$ için

$$V(E_N, M, D) \coloneqq \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_\ell}$$

fonksiyonu tanımlanır. Burada ℓ için en fazla $\ell = \mathcal{O}(\log N)$ kabul edilir. Bu fonksiyon, dizide belirli konumlardaki terimlerin çarpımına dayalı yapıların toplamını dikkate alarak korelasyon ilişkisini değerlendirmektedir.

*Bu tanımlar doğrultusunda, E_N dizisinin **iyi-dağılım ölçütü***

$$W(E_N) \coloneqq \max_{a,b,t} |U(E_N, t, a, b)| = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right| \tag{2.2}$$

biçiminde ifade edilir. Burada maksimum, $a, b, t \in \mathbb{N}$ olmak üzere $1 \leq a \leq a + (t-1)b \leq N$ koşulunu sağlayan tüm (a, b, t) üçlüleri üzerinden alınmaktadır.

Benzer şekilde, E_N dizisinin ℓ mertebeden ***korelasyon ölçütü***

$$C_\ell(E_N) \coloneqq \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_\ell} \right| \tag{2.3}$$

şeklinde tanımlanır. Burada maksimum, M ve $D = (d_1, \ldots, d_\ell)$ değerleri üzerinde alınmakta olup, $M + d_\ell \leq N$ koşulunun sağlanması gerekmektedir.

Bir ikili dizinin sözde-rastgelelik özelliğini değerlendirmede, ardışık alt dizilerin çeşitliliği temel bir ölçüt olarak öne çıkar. Uzunluğu ℓ olan bir alt dizinin alabileceği tüm olası desen sayısı 2^ℓ'dir. Öte yandan, uzunluğu N olan bir dizide örtüşmeli biçimde elde edilebilecek ardışık ℓ-uzunluklu alt dizilerin sayısı en fazla

$$N - \ell + 1$$

olabilir. Tüm olası desenlerin dizide tekrar etmeksizin yer alabilmesi için $2^\ell \leq N - \ell + 1$ koşulu ve buna denk olarak $N \geq 2^\ell + \ell - 1$ koşulunun sağlanması gerekir.

Bu durum, korelasyon analizinde istatistiksel anlamlılık taşıyan ℓ uzunluklarının belirlenmesinde kritik bir rol oynar. Uygulamada, bu eşitsizlikten yaklaşık bir sınır elde edilir:

$$\ell \leq \lfloor \log_2 N \rfloor$$

ve bu sınır, korelasyon ölçütlerinin hesaplanmasında dikkate alınabilecek en büyük ℓ değerini belirler. Zira uzunluğu $\log_2 N$'den büyük olan alt dizilerin dizide tekrarsız biçimde yer alabilme olasılığı oldukça düşüktür.

Bu bağlamda ardışık alt dizilerin incelenmesi özellikle önemlidir; çünkü dizinin her pozisyonunda başlatılan ve kayan pencere yaklaşımıyla elde edilen bu alt diziler, dizinin yerel yapısını ortaya koyar. Her bir ardışık alt dizinin özgünlüğü, dizideki örüntülerin tekrarlanma eğilimiyle doğrudan ilişkilidir ve rastgeleliğe dair önemli

bir gösterge sunar.

Örnek 2.3. *$N = 5$ ve $\ell = 2$ için, $E_5 = (e_1, e_2, \ldots, e_5)$ dizisinin ardışık 2 uzunluklu alt dizileri*

$$(e_1, e_2),\ (e_2, e_3),\ (e_3, e_4),\ (e_4, e_5)$$

şeklindedir ve toplam $5 - 2 + 1 = 4$ adet alt dizi elde edilir. Bu durumda $2^2 = 4$ olduğundan, her olası desen dizide bir kez yer alabilir. Ancak $\ell = 3$ için $2^3 = 8 > 5 - 3 + 1 = 3$ olduğundan, yalnızca 3 adet ardışık alt dizi bulunabilir ve bu sayı, tüm olası desenleri kapsamak için yetersizdir. Bu nedenle, uzunluğu 3 olan tüm desenlerin dizide yer alması teorik olarak imkânsızdır.

Bu örnek, yukarıdaki eşitsizliğin korelasyon ölçütlerinin güvenilir biçimde değerlendirilebilmesi açısından neden temel bir sınır sunduğunu açık biçimde göstermektedir.

Örnek 2.4. *Uzunluğu $N = 6$ olan $E_N = (e_1, e_2, \ldots, e_6) \in \{-1, +1\}^6$ şeklinde tanımlı bir dizi ele alalım. Bu dizinin iyi dağılmış olup olmadığını değerlendirmek amacıyla, $a, b, t \in \mathbb{N}$ olmak üzere $1 \leq a \leq a + (t-1)b \leq 6$ koşulunu sağlayan tüm (a, b, t) üçlülerinde yapılan hesaplamalar Çizelge 2.1'de gösterilmiştir.*

Örnek 2.5. *Uzunluğu $N = 10$ olan bir $E_N = (e_1, e_2, \ldots, e_{10}) \in \{-1, +1\}^{10}$ ikili dizisi ele alalım. Korelasyon ölçütü hesaplanırken, kullanılabilecek en büyük ℓ değeri*

$$\ell \leq \frac{\log N}{\log 2} = \frac{\log 10}{\log 2} \approx 3.3$$

olduğundan, $\ell = 3$ seçimi uygundur. Bu durumda, artan bir kayma dizisi olarak $D = (1, 3, 6)$ alınabilir.

Çizelge 2.1 $W(E_N)$ değerlerinin farklı (a, b, t) kombinasyonları için hesaplanması

$W(E_N) = \max_{a,b,t} \left\lvert \sum_{j=0}^{t-1} e_{a+jb} \right\rvert$			
t	a	b	$\left\lvert \sum_{j=0}^{t-1} e_{a+jb} \right\rvert$
t=2	1	1	$\lvert e_1 + e_2 \rvert$
	1	2	$\lvert e_1 + e_3 \rvert$
	2	1	$\lvert e_2 + e_3 \rvert$
	2	2	$\lvert e_2 + e_4 \rvert$
	2	3	$\lvert e_2 + e_5 \rvert$
	2	4	$\lvert e_2 + e_6 \rvert$
	3	1	$\lvert e_3 + e_4 \rvert$
	3	2	$\lvert e_3 + e_5 \rvert$
	3	3	$\lvert e_3 + e_6 \rvert$
t=3	1	1	$\lvert e_1 + e_2 + e_3 \rvert$
	1	2	$\lvert e_1 + e_3 + e_5 \rvert$
	2	1	$\lvert e_2 + e_3 + e_4 \rvert$
	2	2	$\lvert e_2 + e_4 + e_6 \rvert$
t=4	1	1	$\lvert e_1 + e_2 + e_3 + e_4 \rvert$
	2	1	$\lvert e_2 + e_3 + e_4 + e_5 \rvert$
t=5	1	1	$\lvert e_1 + e_2 + e_3 + e_4 + e_5 \rvert$
	2	1	$\lvert e_2 + e_3 + e_4 + e_5 + e_6 \rvert$
t=6	1	1	$\lvert e_1 + e_2 + e_3 + e_4 + e_5 + e_6 \rvert$

Üçüncü mertebeden korelasyon ölçütü

$$C_3(E_N) \coloneqq \max_{M,D} \left| \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} e_{n+d_3} \right|$$

şeklinde tanımlanır. Burada $D = (d_1, d_2, d_3)$ *olmak üzere, toplamın sınırları içinde kalması için* $M + d_3 \leq N$ *koşulu sağlanmalıdır. Seçilen* $D = (1, 3, 6)$ *için bu koşuldan* $M \leq 4$ *elde edilir; dolayısıyla* $M \in \{2, 3, 4\}$ *değerleri dikkate alınır.*

Çizelge 2.2'de, her M *için hesaplanan korelasyon toplamları gösterilmiştir:*

Çizelge 2.2 $D = (1, 3, 6)$ kayma dizisi için $C_3(E_N)$ korelasyon değerleri

M	$C_3(E_N) = \left\lvert \sum_{n=1}^{M} e_{n+1} e_{n+3} e_{n+6} \right\rvert$
1	$= \lvert e_2\, e_4\, e_7 \rvert$
2	$= \lvert e_2\, e_4\, e_7 + e_3\, e_5\, e_8 \rvert$
3	$= \lvert e_2\, e_4\, e_7 + e_3\, e_5\, e_8 + e_4\, e_5\, e_9 \rvert$
4	$= \lvert e_2\, e_4\, e_7 + e_3\, e_5\, e_8 + e_4\, e_5\, e_9 + e_5\, e_6\, e_{10} \rvert$

Sonuç olarak, bu mutlak değerli toplamların en büyüğü, dizinin üçüncü mertebeden korelasyon ölçütü olan $C_3(E_N)$ değerini verir.

Bir E_N dizisinin sözde-rastgelelik özellikleri ℓ. mertebeden çapraz-korelasyon ölçütü $C_\ell(E_N)$ ve iyi-dağılım ölçütü $W(E_N)$ olarak başlıca iki matematiksel ölçütle nicelendirilir. Bu ölçütlerin küçük değerlere sahip olması durumunda, ilgili dizi **iyi sözde-rastgele dizi** (good pseudorandom sequence) olarak kabul edilir.

Sözde-rastgeleliği daha hassas biçimde değerlendirebilmek amacıyla, normallik ölçütü literatüre kazandırılmıştır [Mauduit ve Sárközy 1997]. $N_\ell(E_N)$ ölçütü, uzunluğu N olan ikili bir dizide belirli bir ℓ-uzunluklu desenin beklenen frekansından ne ölçüde saptığını ölçer. Bu ölçüt, dizinin istatistiksel rastgeleliğini analiz etmede önemli bir araçtır. $N_\ell(E_N)$ değerinin küçük olması, dizinin tüm ℓ-uzunluklu desenleri yaklaşık olarak eşit sıklıkta içerdiğini ve dolayısıyla yüksek düzeyde sözde-rastgelelik özelliği taşıdığını gösterir.

Tanım 2.3. *[Mauduit ve Sárközy 1997] $E_N = (e_1, e_2, \ldots, e_N) \in \{-1, +1\}^N$ bir ikili dizi ve $X = (x_1, x_2, \ldots, x_\ell)$ herhangi bir ℓ-uzunluklu desen olsun. E_N dizisinin X deseniyle eşleşme sayısı*

$$T(E_N, M, X) \coloneqq |\{n : 0 \leq n < M, \quad (e_{n+1}, e_{n+2}, \ldots, e_{n+\ell}) = X\}|$$

*ile verilir. E_N dizisinin ℓ dereceden **normallik ölçütü** (**normality measure**)*

$$N_\ell(E_N) \coloneqq \max_{M,X} \left| T(E_N, M, X) - \frac{M}{2^\ell} \right|$$

olarak tanımlanır. Maksimum değer, tüm $X \in \{-1, +1\}^\ell$ desenleri ve $M \leq N - \ell + 1$

koşulunu sağlayan M değerleri üzerinden alınır.

Birleşik sözde-rastgelelik ölçütü, iyi-dağılım ve korelasyon ölçütlerinin ortak bir genellemesi olarak tanımlanır [Mauduit ve Sárközy 1997].

Tanım 2.4. *$E_N = (e_1, \ldots, e_N) \in \{-1, +1\}^N$ bir ikili dizi olsun. Her $\ell \in \mathbb{N}$ için, $D = (d_1, \ldots, d_\ell)$ $(0 \leq d_1 < \cdots < d_\ell)$ kaydırma dizisi ve $a, b, t \in \mathbb{N}$ parametreleriyle,*

$$Z(E_N, a, b, t, D) \coloneqq \sum_{j=0}^{t} e_{a+jb+d_1} \cdots e_{a+jb+d_\ell}$$

şeklinde tanımlanan toplam yardımıyla, ℓ dereceden ***birleşik ölçüt***

$$Q_\ell(E_N) = \max_{\substack{a,b,t \\ D}} |Z(E_N, a, b, t, D)|$$

olarak verilir. Dizinin ***genel birleşik ölçütü*** *ise*

$$Q(E_N) = \max_{1 \leq \ell \leq \lfloor \frac{\log N}{\log 2} \rfloor} Q_\ell(E_N)$$

şeklinde tanımlanır. Burada maksimumlar, $a + jb + d_i \in \{1, 2, \ldots, N\}$ koşulunu sağlayan tüm parametreler üzerinden alınır.

Özetle, $Q_\ell(E_N)$ bir E_N dizisinin ℓ dereceden korelasyonunun, aritmetik ilerlemeler üzerindeki davranışını ölçer.

Her ne kadar W, C_ℓ, N_ℓ ve Q_ℓ gibi ölçütler dizilerin birçok sözde-rastgele özelliğini incelemeye olanak verse de, bu ölçütlerle tüm rastgelelik özelliklerinin eksiksiz biçimde karakterize edilmesi mümkün değildir. Nitekim Topuzoğlu ve Winterhof (2007) tarafından sunulan *Discrepancy*, *Uniform Distribution*, *Nonlinearity*, *Lattice Test*, *Linear Complexity*, *Linear Complexity Profile* ve *Simetri* gibi ölçütler, dizilerin sözde-rastgeleliğini tanımlamada başlıca araçlar olarak kullanılmaktadır.

Bu alanda yürütülen çalışmaların son yıllarda hızla gelişmesi nedeniyle tüm testlerin uygulanmasından çok, uygulamalarda yeterli güvenliği sağlayabilecek sınırlı ancak etkili bir temel ölçüt kümesinin belirlenmesi daha uygun bir yaklaşımdır. Güncel araştırmalar, W ve C_ℓ ölçütlerinin bu temel kriterleri sağladığını ortaya koymaktadır.

2.3 Sözde-Rastgele Dizi İnşa Yöntemleri

Legendre sembolü kullanılarak iyi-sözde-rastgele diziler üretmeye yönelik ilk yöntem, [Mauduit ve Sárközy 1997]'de incelenmiştir.

İnşa 2.1. *p asal sayı ve $N = p - 1$ olmak üzere, bir $E_N = (e_1, e_2, \ldots, e_N)$ Legendre dizisi*

$$e_n \coloneqq \left(\frac{n}{p}\right)$$

kuralına göre oluşturulur. Burada $\left(\frac{\cdot}{p}\right)$ Legendre sembolünü temsil eder.

Bu durumda, İnşa 2.1 ile tanımlanan E_N dizisi için [Mauduit ve Sárközy 1997] [Teorem-1]'e göre

$$W(E_N) \ll N^{1/2} \log N,$$
$$C_\ell(E_N) \ll \ell N^{1/2} \log N$$

üst sınırları elde edilir.

Bu sınırlar, literatürde bilinen en iyi sonuçlar arasındadır. Ayrıca, söz konusu üretim yöntemi uygulamada oldukça hızlı ve pratiktir. Burada kullanılan $\ll$ notasyonu Vinogradov simgesidir; $f(x) \ll g(x)$ ifadesi $f(x) = \mathcal{O}(g(x))$ anlamına gelir.

Örnek 2.6. *$p = 59$ asal sayısı için İnşa 2.1 (Legendre yöntemi) ile oluşturulan $N = 58$ olan dizi*

E_N =[1, -1, 1, 1, 1, -1, 1, -1, 1, -1, -1, 1, -1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, 1, 1, 1, -1, -1, -1, -1, -1, 1, 1, -1, -1, -1, -1, 1, -1, -1, -1, 1, 1, -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, 1, -1]

şeklindedir. Bu dizinin iyi-dağılım ölçütü $W(E_N) = 9$'dur. Bazı asal sayılar için hesaplanan iyi-dağılım ölçütü değerleri Çizelge 2.3'te verilmiştir.

Çizelge 2.3 $W(E_N)$ değerleri

p	$W(E_N)$	$\approx N^{1/2} \log N$
59	9	10.1
79	10	12.1
97	12	19.5
257	20	38.4
577	32	66.2
983	43	94

Bu bağlamda, dizinin kontrol edilmesi gereken maksimum korelasyon derecesi

$$\ell \leq \frac{\log N}{\log 2} = \frac{\log 59}{\log 2} \approx 5.8$$

şeklinde hesaplanır. Bazı asallar için korelasyon ölçütleri Çizelge 2.4'te sunulmuştur.

Çizelge 2.4 $C_\ell(E_N)$ değerleri

p	N	ℓ	$\max_{\ell \leq \frac{\log N}{\log 2}} C_\ell(E_N)$	$\ell N^{1/2} \log N$
61	60	5	26	68.8
59	58	5	23	67.1
53	52	5	21	61.8
37	36	5	19	46.7
29	28	4	12	30.6

[Mauduit ve Sarkozy 1998] çalışmasında, Legendre sembolü temelli İnşa 2.1 yöntemi, belirli koşullar altında $g(x) \in \mathbb{F}_p[x]$ biçimindeki permütasyon polinomları kullanılarak genelleştirilmiştir. Bu genellemede, klasik $\left(\frac{n}{p}\right)$ ifadesi yerine $\left(\frac{g(n)}{p}\right)$ kullanılarak yeni bir iyi-sözde-rastgele dizi üretim yöntemi elde edilmiştir.

Bir $f(x) \in \mathbb{F}_q[x]$ polinomu, $\mathbb{F}_q$ cismi üzerinde birebir ve örten bir fonksiyon tanımlıyorsa, f'ye **permütasyon polinomu** adı verilir.

Bazı önemli permütasyon polinomları aşağıda sıralanmıştır:

1. **Doğrusal polinomlar:** $a \in \mathbb{F}_q^*$ ve $b \in \mathbb{F}_q$ olmak üzere, $f(x) = ax + b$ biçimindeki polinomlar permütasyon polinomudur.

2. **Monomiyaller:** $f(x) = x^k$ biçimindeki monomiyaller, $obeb\ (k, q-1) = 1$ koşulu sağlandığında permütasyon polinomu olur.

3. **Özyinelemeli polinomlar:** $n \in \mathbb{N}$ ve $a \in \mathbb{F}_q^*$ parametreleriyle tanımlanan $\{D_n(x,a)\}$ polinom dizisi

$$\begin{aligned} D_0(x,a) &= 2 \\ D_1(x,a) &= x \\ D_{n+2}(x,a) &= xD_{n+1}(x,a) - aD_n(x,a) \end{aligned}$$

özyineleme bağıntısını sağlar. $obeb(n, q^2-1) = 1$ koşulu altında $D_n(x,a)$ polinomları $\mathbb{F}_q$ üzerinde permütasyon polinomu özelliği gösterir.

İnşa 2.2. *[Mauduit ve Sarkozy 1998] p asal sayı ve $g(x)$, $\mathbb{F}_p$ üzerinde derecesi m olan bir permütasyon polinomu olsun ve*

$$g(x) \text{ polinomunun kökünün katlılığı tek sayıda olmalıdır.} \tag{2.4}$$

koşulu sağlansın. $E_p = (e_1, \ldots, e_p)$ dizisi

$$e_n := \begin{cases} \left(\dfrac{g(n)}{p}\right), & \text{eğer } g(n) \not\equiv 0 \pmod p, \\ 1, & \text{eğer } g(n) \equiv 0 \pmod p \end{cases}$$

kuralına göre oluşturulur. Bu durumda, her $k \in \mathbb{N}$ *ve* $k < p$ *için*

$$Q_k(E_N) < 11kmp^{1/2} \log p$$

sağlanır.

Örnek 2.7. *Örnek 2.6'da verilen Legendre yöntemiyle elde edilen 58 uzunluklu dizi,* $g(n) = n^3$ *permütasyon polinomu kullanılarak, İnşa 2.2'deki yöntemle elde edilebilir.*

Not 2.2.

1. *Doğrusal polinomlar;* $q > 2$ *ve* $(k, q-1) = 1$ *koşulu altında, her* $a \in \mathbb{F}_q$ *için tanımlanan* $x^k + a$ *biçimindeki polinomlar; ayrıca* $a \in \mathbb{F}_q^*$ *ve* $(5, q^2-1) = 1$ *koşulları altında tanımlanan* $D_5(x, a)$ *Dickson polinomları, Koşul (2.4)'ü sağlar.*

2. *Koşul (2.4)'ün sağlanması ve kullanılan polinomun derecesinin düşük olması durumunda,* $Q_k(E_N)$ *ölçütü için daha elverişli bir üst sınır elde edilebilir.*

Legendre (İnşa 2.1) yönteminde, sabit bir N sayısı için yalnızca uzunluğu N olan tek bir dizi üretilebilir. Ancak birçok uygulama, birden fazla sözde-rastgele ikili dizi gerektirir. Goubin ve diğerleri, Legendre sembolüne dayalı geniş sözde-rastgele ikili dizi aileleri oluşturmayı başarmıştır [Goubin vd. 2004].

İnşa 2.3. *Kolay* $K \in \mathbb{N}$ *ve* p *asal sayı olsun.* $\mathcal{P}$, $\mathbb{F}_p[x]$*'te derecesi* $0 < k \leq K$ *olan ve* $\overline{\mathbb{F}}_p$ *(*$\mathbb{F}_p$*'nin cebirsel kapanışı) üzerinde katlı kök içermeyen polinomların kümesini göstersin. Her* $f \in \mathcal{P}$ *için* $E_p(f) \coloneqq (e_1, \ldots, e_p)$ *dizisi*

$$e_n \coloneqq \begin{cases} \left(\frac{f(n)}{p}\right), & \text{eğer } obeb(f(n), p) = 1, \\ +1, & \text{eğer } p \mid f(n) \end{cases} \tag{2.5}$$

kuralına göre tanımlanır. Bu dizilerden oluşan aile $\mathcal{F} \coloneqq \{E_p(f) : f \in \mathcal{P}\}$ *ile gösterilir.*

Bu durumda, $\mathcal{F}$ açıkça geniş bir sözde-rastgele ikili dizi ailesini ifade eder. Goubin ve diğerleri, belirli koşullar altında f polinomları için $E_p(f)$ dizisinin güçlü sözde-rastgele özelliklere sahip olduğunu ispatlamışlardır [Goubin vd. 2004].

Teorem 2.4. *İnşa 2.3'teki p, $\mathcal{P}$ ve $\mathcal{F}$ tanımlarıyla, $f \in \mathcal{P}$ ve $E_p = E_p(f) \in \mathcal{F}$ için (f'nin derecesi k olmak üzere)*

$$W(E_p) \ll kp^{1/2} \log p$$

eşitsizliği geçerlidir. Ayrıca, $\ell \in \mathbb{N}$ için

1. $\ell = 2$,
2. $\ell < p$ *ve* 2, p*'ye göre ilkel bir kök,*
3. $(4k)^\ell < p$,

koşullarından herhangi biri geçerliyse

$$C_\ell(E_p) \ll k\ell p^{1/2} \log p$$

sağlanır.

[Rivat vd. Sárközy 2006] çalışmasında, İnşa 2.3 ile elde edilen dizilerin NIST-STS test paketindeki tüm testleri geçtiği gösterilmiştir.

Bilinen permütasyon polinomlarının hem sayıca az hem de çeşitlilik bakımından sınırlı olması nedeniyle, İnşa 2.2 yöntemi kullanılarak yeterli büyüklükte dizi aileleri üretmek mümkün olmamaktadır. Ancak Gaubin ve diğerleri tarafından geliştirilen bir yaklaşımla, belirli yapısal özellikleri sağlayan polinomlar seçilerek yeni ve daha

geniş dizi aileleri elde edilmiştir [Goubin vd. 2004].

Tanım 2.5. *$m \in \mathbb{N}$ ve $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_m$ için*

$$r(c) \coloneqq \#\{(a,b) \in \mathcal{A} \times \mathcal{B} : a + b = c\}$$

olmak üzere, her $c \in \mathbb{Z}_m$ için $r(c) \equiv 0 \pmod 2$ ise $\mathcal{A} + \mathcal{B}$ toplamı $\mathcal{P}$ ***özelliğine (property) sahiptir****.*

Tanım 2.6. *$k, \ell, m \in \mathbb{N}$ ve $k, \ell \leq m$ olmak üzere, eğer $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_m$ kümeleri için $|\mathcal{A}| = k$, $|\mathcal{B}| = \ell$ ve $\mathcal{A} + \mathcal{B}$ toplamı $\mathcal{P}$ özelliğine sahip olacak hiçbir küme çifti yoksa, bu durumda (k, ℓ, m) üçlüsüne* ***uygun üçlü*** *(admissible triple) denir.*

Not 2.3. *İnşa 2.3'te tanımlanan, derecesi k olan bir f polinomu kullanılarak elde edilen $E_p(f)$ dizisinin ℓ-mertebeden çapraz-korelasyon ölçütü $C_\ell(E_p)$, her $r \leq k$ için (r, ℓ, p) üçlüsünün uygun olması durumunda, Teorem 2.4'te verilen üst sınırları sağlamaktadır.*

İnşa 2.3'ün uygulanabilmesi için, *uygun* (k, ℓ, p) üçlülerinin bulunması gerekmektedir. Bu üçlülerin uygunluğu için gerekli koşullar [Goubin vd. 2004] çalışmasında aşağıdaki şekilde verilmiştir.

Teorem 2.5. *[Goubin vd. 2004]*

1. *$k \in \mathbb{N}$, $k < p$ ve her asal p için $(k, 2, p)$ üçlüsü uygundur.*
2. *Eğer p asal sayı, $k, \ell \in \mathbb{N}$ ve $(4k)^\ell < p$ koşulu sağlanıyorsa, (k, ℓ, p) üçlüsü uygundur.*
3. *p asal sayı ve mod p'de 2 bir primitif kök ise, $k < p$ ve $\ell < p$ olacak şekilde*

her $k, \ell \in \mathbb{N}$ için (k, ℓ, p) üçlüsü uygundur.

Tanım 2.7. *$k < m$ ve $\ell < m$ olacak şekilde her $k, \ell \in \mathbb{N}$ çifti için (k, ℓ, p) üçlüsü uygun ise, m sayısı **iyi** olarak adlandırılır.*

Teorem 2.6. *[Goubin vd. 2004] Bir tek asal sayı p için, p'nin iyi olması için gerek ve yeter koşul, 2'nin mod p'de bir primitif kök olmasıdır.*

Not 2.4. *p tek asal sayı ve 2 sayısı mod p'de primitif kök olmak üzere, $k \geq 0$ için bir m sayısının iyi olması, ancak ve ancak $m = 4$, p^k veya $2p^k$ biçimindeyse mümkündür.*

Örnek 2.8. *$p = 7$ asal sayısı için $1 + x^7$ polinomunun $\mathbb{F}_2[x]$ halkasında çarpanlara ayrılışı*

$$1 + x^7 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$$

şeklindedir. Bu çarpanlar, aşağıda verilen iki farklı $\mathcal{A}$ ve $\mathcal{B}$ küme çiftine karşılık gelir. Her bir küme, ilgili polinomda yer alan terimlerin derecelerinden (yani x'in üslerinden) oluşur:

- *$\mathcal{A} = \{0, 1, 3\}$ ve $\mathcal{B} = \{0, 1, 2, 4\}$,*
  sırasıyla $(1 + x + x^3)$ ve $(1 + x)(1 + x^2 + x^3) = 1 + x + x^2 + x^4$ polinomlarından elde edilir.
- *$\mathcal{A} = \{0, 2, 3\}$ ve $\mathcal{B} = \{0, 2, 3, 4\}$,*
  sırasıyla $(1 + x^2 + x^3)$ ve $(1 + x)(1 + x + x^3) = 1 + x^2 + x^3 + x^4$ polinomlarından elde edilir.

Bu küme çiftlerinden oluşturulan çoklu küme toplamı $\mathcal{A} + \mathcal{B}$, her $c \in \mathbb{Z}_7$ için $r(c)$

değerinin çift olmasını sağladığı için, $\mathcal{P}$ özelliğine sahiptir. Bu nedenle $(3,4,7)$ ve $(4,3,7)$ üçlüleri uygun değildir.

Genel olarak, $p=7$ için $\mathcal{A},\mathcal{B}\subset\mathbb{Z}_7$ olacak şekilde $\mathcal{P}$ özelliğine sahip bir $\mathcal{A}+\mathcal{B}$ çoklu kümesi bulmak mümkündür. Bu problem, derecesi 7'den küçük olan iki polinom $P_{\mathcal{A}}$ ve $P_{\mathcal{B}}$'nin

$$P_{\mathcal{A}}(x)\cdot P_{\mathcal{B}}(x)$$

çarpımının $(1+x)(1+x+x^3)(1+x^2+x^3)$ polinomunun bir katı olması koşulunu sağlayacak şekilde seçilmesi problemine denktir.

Örneğin,

$$(1+x+x^2+x^3)(1+x^7)=(1+x^3+x^5+x^6)(1+x+x^2+x^4)$$

çarpımı dikkate alındığında, buradan

$$\mathcal{A}=\{0,3,5,6\},\quad \mathcal{B}=\{0,1,2,4\}$$

kümeleri elde edilir ve bu çiftin oluşturduğu $\mathcal{A}+\mathcal{B}$ çoklu kümesi yine $\mathcal{P}$ özelliğine sahiptir.

Sonuç olarak, $p=7$ için $(3,4,7)$, $(4,3,7)$ ve $(4,4,7)$ üçlüleri uygun değildir.

Örnek 2.9. *$p=19$ olsun. $1+x^{19}$ polinomunun $\mathbb{F}_2[x]$ üzerindeki çarpanlarına ayrılışı:*

$$1+x^{19}=(1+x)\big(x^{18}+x^{17}+x^{16}+\cdots+x+1\big)$$

şeklindedir. Bu yapının üzerinden $\mathcal{A}$ ve $\mathcal{B}$ küme çiftinin elde edilmesi mümkün değildir.

Bununla birlikte, Teorem 2.6 uyarınca 2 sayısı mod 19'da primitif kök olduğundan, 19 sayısı iyi bir sayıdır. Tanım 2.7'ye göre, $k < 19$ ve $\ell < 19$ koşullarını sağlayan her (k, ℓ) çifti için $(k, \ell, 19)$ üçlüsü uygundur.

$\mathbb{F}_{19}[x]$ üzerinde derecesi $k = 15$ olan, indirgenemez

$$f(x) = x^{15} + 5x^{14} + 16x^{13} + 11x^{12} + 7x^{11} + 16x^{10} + x^9 + 6x^8 + 5x^7 + 16x^6 + 7x^5 + 18x^4 + 15x^3 + 18x^2 + 13x + 3$$

polinomunu ele alalım. Bu polinomun $\overline{\mathbb{F}}_{19}$ içinde katlı kökü yoktur.

İnşa 2.3'teki dizi üretim yöntemiyle aşağıdaki dizi elde edilmiştir:

$$E_{19} := (1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, -1, 1, 1, -1).$$

Bu dizinin maksimum korelasyon ölçütü değeri $C_3(E_{19}) = 9$ ve iyi-dağılım değeri 6'dır.

Legendre sembolü kullanılarak sözde-rastgele dizi üretimi amacıyla tanımlanan İnşa 2.1, *indis* kavramı yardımıyla alternatif bir biçimde de ifade edilebilir.

p bir asal sayı ve g, mod$p$ altında bir primitif kök olmak üzere, her $a \in \mathbb{F}_p^*$ elemanı için $g^{\operatorname{ind} a} \equiv a \pmod{p}$ koşulunu sağlayan $\operatorname{ind} a$ sayısı, a'nın g tabanındaki **indisi** olarak tanımlanır. Bu değer, her $a \in \mathbb{F}_p^*$ için tektir ve genellikle $1 \leq \operatorname{ind} a \leq p - 1$ aralığında alınır.

Bu tanıma göre, $n = 1, 2, \ldots, p - 1$ için dizinin n'inci terimi, $\operatorname{ind} n$ çift olduğunda $+1$, tek olduğunda ise -1 olarak atanır. Yani,

$$e_n = \begin{cases} +1, & \text{eğer } \operatorname{ind} n \text{ çift ise,} \\ -1, & \text{eğer } \operatorname{ind} n \text{ tek ise} \end{cases}$$

şeklinde tanımlanır.

Bu yaklaşım, Legendre sembolünün indis cinsinden ifadesine karşılık gelir. Gerçekten de, $\operatorname{ind} n$ çift olduğunda n bir ikinci dereceden kalandır ve bu durumda $\left(\frac{n}{p}\right) = +1$ olurken; $\operatorname{ind} n$ tek olduğunda n bir ikinci dereceden kalmayan olur ve bu durumda $\left(\frac{n}{p}\right) = -1$ eşitliği sağlanır.

Böylece, $\mathbb{F}_p^*$ kümesinin $p-1$ elemanı Legendre sembolü kullanılarak iki gruba ayrılır; bir yarısı $+1$, diğer yarısı ise -1 değeriyle eşlenerek ikili bir dizi oluşturulur. Benzer bir eşleme yaklaşımı, İnşa 2.4'te farklı bir dizi üretim yöntemi çerçevesinde sunulmuştur.

İnşa 2.4. *[Sárközy 2001] p tek asal sayı ve $N = p-1$ olmak üzere, $E_N = (e_1, \ldots, e_N)$ dizisi*

$$e_n = \begin{cases} +1, & \text{eğer } 1 \le \operatorname{ind} n \le \frac{p-1}{2}, \\ -1, & \text{eğer } \frac{p+1}{2} \le \operatorname{ind} n \le p-1 \end{cases}$$

kuralına göre oluşturulur. Bu dizi için iyi dağılım ölçütü $W(E_N)$

$$W(E_N) < 4p^{1/2}(\log p)^2 < 20N^{1/2}(\log N)^2$$

eşitsizliğini sağlar. Ayrıca, her $k \in \mathbb{N}$ ve $k < p$ için korelasyon ölçütü $C_k(E_N)$

$$C_k(E_N) < 9k \cdot 4^k \cdot p^{1/2} \cdot (\log p)^{k+1} < 27k \cdot 8^k \cdot 20N^{1/2} \cdot (\log N)^{k+1}$$

üst sınırını sağlar.

Uyarı 2.1. *E_N dizisi, p asal sayısı için seçilen primitif köke bağlı olarak oluşturulur. Farklı bir primitif kök seçildiğinde, her elemanın $\operatorname{ind} n$ değeri orijinal indislerin bir permütasyonu hâline gelir. Dolayısıyla dizinin bit değerleri değişmez; yalnızca sıraları farklı olur. Bu nedenle, iyi dağılım ölçütü $W(E_N)$ ve tüm ℓ-mertebeden korelasyon ölçütleri $C_\ell(E_N)$ aynı kalır.*

Örnek 2.10. *$p = 59$ asal sayısını ele alalım. Bu durumda, $\mathbb{F}_{59}^*$ çarpımsal grubunun mertebesi 58'dir. Mod 59'da 6 sayısı bir primitif kök olduğundan, bu kökün kuvvetleri tüm $\mathbb{F}_{59}^*$ elemanlarını üretir. Aşağıdaki çizelgede $6^n \bmod 59$ değerleri, karşılık gelen indisler ve e_n bit değerleri verilmiştir:*

Çizelge 2.5 $p = 59$ için $6^n \bmod 59$ değerleri, indisler ve E_{58} dizisinin bitleri

Sayı	**Kuvvet** ($6^n \bmod 59$)	**İndis** (n)	**Bit Değeri** (e_n)
1	6^{58}	58	-1
2	6^{33}	33	-1
3	6^{26}	26	$+1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
57	6^{10}	10	$+1$
58	6^{55}	55	-1

Bu çizelgeye göre, $E_{58} = (e_1, e_2, \ldots, e_{58})$ dizisi

$$e_n := \begin{cases} +1 & \text{eğer } 1 \leq ind\, n \leq 29, \\ -1 & \text{eğer } 30 \leq ind\, n \leq 58 \end{cases}$$

kuralına göre oluşturulur. Elde edilen tam dizi E_{58} şu şekildedir:

$$[-1,-1,+1,+1,+1,+1,+1,-1,-1,-1,+1,-1,-1,-1,-1,+1,-1,+1,-1,-1,-1,-1,$$
$$-1,+1,-1,+1,+1,+1,-1,+1,-1,-1,-1,+1,-1,+1,+1,+1,+1,+1,-1,+1,-1,+1,$$
$$+1,+1,+1,-1,+1,+1,+1,-1,-1,-1,-1,-1,+1,+1]$$

Bu dizinin rastgelelik ölçütleri:

- *İyi dağılım değeri:* 12,
- *Maksimum korelasyon ölçütü (ilk 5 mertebe için):* 30

değerlerini almakta olup, her iki değer de teorik üst sınırların altında kalarak dizinin sözde-rastgelelik açısından uygun olduğunu göstermektedir.

İnşa 2.4'te doğrudan n üzerinde tanımlanan üretim yöntemi, İnşa 2.5'te n yerine $f(n)$ uygulanarak genelleştirilmiştir.

İnşa 2.5. *[Gyarmati 2004] p bir tek asal sayı ve g, $\mathbb{F}_p^*$ çarpımsal grubunun bir primitif kökü olsun. Derecesi k olan bir $f(x) \in \mathbb{F}_p[x]$ polinomu için, uzunluğu $p-1$ olan $E_{p-1} = (e_1, \ldots, e_{p-1})$ ikili dizisi*

$$e_n = \begin{cases} +1 & \text{eğer } 1 \leq ind\ f(n) \leq \frac{p-1}{2}, \\ -1 & \text{eğer } \frac{p+1}{2} \leq ind\ f(n) \leq p-1 \text{ veya } p \mid f(n) \end{cases} \tag{2.6}$$

şeklinde tanımlanır.

Uyarı 2.2. *Bu dizi üretim yöntemi, İnşa 2.3 ile benzer istatistiksel özellikler sunsa da, pratikte önemli bir hesaplama zorluğu içerir. Özellikle, e_n değerlerinin belirlenmesi, ayrık logaritma problemine (DLP) indirgenebilecek bir işlem gerektirir. Bu problem için bilinen en hızlı klasik algoritmalar $\mathcal{O}(\sqrt{p})$ zaman karmaşıklığına sahiptir. Dolayısıyla, p büyük asal sayılar için seçildiğinde, bu yöntem hesaplama açısından verimsiz hale gelir.*

2.4 Doğrusal Karmaşıklık ve LFSR

Tanım 2.8. *Bir periyodik dizinin **doğrusal karmaşıklığı** (linear complexity), bu diziyi üreten en kısa LFSR'nin derecesidir. Başka bir deyişle, diziyi üreten karakteristik polinomun derecesi doğrusal karmaşıklığı belirler.*

Doğrusal karmaşıklık, bir dizinin tahmin edilebilirlik düzeyini ve yapısal karmaşıklığını nicel olarak ölçen temel bir ölçüttür; bu değerin yüksek olması, dizinin kriptografik açıdan güçlü olduğunu, düşük olması ise kolay tahmin edilebilir bir yapıya sahip olduğunu gösterir.

Bu bölümde, yüksek rastgelelik özellikleri taşıyan periyodik dizilerin üretiminde sıkça kullanılan LFSR sisteminin yapısı, bu sistemle üretilen dizilerin korelasyon özellikleri ve doğrusal karmaşıklık ölçütü incelenecektir. Ayrıca doğrusal karmaşıklığın rastgelelik ölçütleriyle ilişkisi de ele alınacaktır.

$\mathbb{F}_q$ sonlu cismi üzerinde tanımlı diziler, haberleşme, kriptografi ve hata düzeltme kodları gibi birçok alanda önemli bir rol oynar. Bu dizilerin otokorelasyon değeri, dizinin kendisiyle farklı kaydırmalardaki benzerliğini; çapraz korelasyon değeri ise iki farklı dizi arasındaki benzerliği ölçer. Düşük otokorelasyon, dizinin rastgeleliğe yakın bir yapı sergilediğini gösterirken; düşük çapraz korelasyon, sinyallerin birbirinden ayırt edilebilirliğini artırır.

Tanım 2.9. *$\mathbb{F}_q$ sonlu cismi üzerinde periyodu N olan iki dizi $\mathbf{a} = (a_0, \ldots, a_{N-1})$ ve $\mathbf{b} = (b_0, \ldots, b_{N-1})$ verildiğinde, bu dizilere ait* ***çapraz korelasyon***

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{N-1} \omega^{a_{i+\tau} - b_i}$$

şeklinde tanımlanır ve $0 \leq \tau < N$ için geçerlidir. Burada $\omega = e^{2\pi i/q}$ ifadesiyle tanımlanan q dereceden birim köktür. Ayrıca, $a_{i+\tau}$ ifadesindeki tüm indisler $\bmod N$ *altında değerlendirilir.*

Özellikle, $\mathbf{a} = \mathbf{b}$ durumunda bu ifade

$$C_{\mathbf{a}}(\tau) = \sum_{i=0}^{N-1} \omega^{a_{i+\tau} - a_i}$$

biçimini alır ve bu durumda **a** *dizisinin* ***otokorelasyonu*** *elde edilir.*

Periyodu N olan bir ikili **a** dizisinde, ardışık k adet 0 (ya da 1) içeren bir bloğun başlangıcında ve sonunda 1 (ya da 0) bulunan k uzunluğundaki alt dizilere **run** adı verilir. Golomb, ikili periyodik dizilerin rastgeleliğini değerlendirmek üzere üç temel varsayım ortaya koymuştur:

1. **Denge Varsayımı (Balance Postulate)**: Dizideki 0 ve 1'lerin sayıları birbirine mümkün olduğunca yakın olmalıdır.
2. **Run Varsayımı (Run Postulate)**: Dizinin her periyodunda, run sayılarının yarısı uzunluğu 1 olan, dörtte biri uzunluğu 2 olan, sekizde biri uzunluğu 3 olan biçimde olmalıdır.
3. **Otokorelasyon Varsayımı (Autocorrelation Postulate)**: Dizinin kaydırılmış hallerine göre otokorelasyon değerleri mümkün olduğunca düşük olmalıdır. Bu durum, diziyle onun kaydırılmış halleri arasında düşük benzerliğin olduğunu gösterir ve rastgelelik algısını destekler.

LFSR'ler, kriptografi, hata tespiti, rastgele sayı üretimi ve dijital haberleşme gibi pek çok alanda etkin biçimde kullanılır; özellikle maksimum periyotlu diziler (m-dizileri) üretebilmeleri, onları güvenli iletişim sistemlerinin temel bileşenlerinden biri haline getirir.

LFSR dizileri, rastgelelik özellikleri ve donanımsal olarak kolay uygulanabilirlikleri sayesinde, mesafe ölçüm, navigasyon, yayılmış spektrumlu iletişim ve CDMA tabanlı mobil ağlar gibi pek çok sistemde yaygın olarak kullanılmaktadır. Ayrıca, akan şifreleyicilere (stream cipher) dayalı kriptografik yapılarda da önemli bir rol üstlenirler.

Klasik kriptografide temel ilke, sistem güvenliğinin algoritmanın gizliliğine değil, yalnızca anahtar bilgisinin gizli tutulmasına bağlı olmasıdır. Bu açıdan, LFSR tabanlı

sistemler söz konusu ilkeyi karşılar; çünkü sistemin yapısı açıkça bilinse bile, başlangıç durumunun gizli kalması dizinin fazını belirlemeyi zorlaştırır. Bu özellik, mobil iletişim altyapılarında güvenli veri iletimi sağlamak bakımından önemli bir avantaj sunar.

İkili cisim $\mathbb{F}_2 = \{0, 1\}$ bu çalışmada temel cebirsel yapı olarak kullanılacaktır. Bu durumda

$$\mathbb{F}_2^n = \{(a_0, a_1, \ldots, a_{n-1}) \mid a_i \in \mathbb{F}_2\}$$

kümesi, $\mathbb{F}_2$ cismi üzerinde tanımlı n boyutlu bir vektör uzayıdır.

İkili çıktı üreten ve n adet ikili girdiyi işleyen fonksiyonlara n-değişkenli Boole fonksiyonları adı verilir. Bu fonksiyonlar,

$$f : \mathbb{F}_2^n \to \mathbb{F}_2$$

şeklinde tanımlanır. Doğrusal bir Boole fonksiyonu, tüm katsayıları $\mathbb{F}_2$ cismine ait olmak üzere

$$f(x) = f(x_0, x_1, \ldots, x_{n-1}) = c_0x_0 + c_1x_1 + \cdots + c_{n-1}x_{n-1}$$

şeklinde ifade edilir.

Bir LFSR, sıfır olmayan bir $(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_2^n$ başlangıç değeriyle başlatılır. Her adımda, kaydırma kaydındaki bitler sağa kaydırılır; en sağdaki bit çıkış olarak alınırken, en soldaki bit geri besleme fonksiyonuyla elde edilir. Bu yapı, dizinin elemanları arasında aşağıdaki özyinelemeli ilişkiyi oluşturur:

$$a_{k+n} = f(a_k, a_{k+1}, \ldots, a_{k+n-1}), \quad k = 0, 1, 2, \ldots.$$

Elemanları $\mathbb{F}$ cismine ait sonsuz diziler kümesi

$$V(\mathbb{F}) \coloneqq \{\mathbf{a} = (a_0, a_1, \ldots) \mid a_i \in \mathbb{F}\}$$

şeklinde tanımlanır. Bu kümede toplama ve skaler çarpma işlemleri

$$\mathbf{a} + \mathbf{b} = (a_0 + b_0, a_1 + b_1, \ldots), \quad c\mathbf{a} = (ca_0, ca_1, \ldots)$$

şeklinde tanımlanır ve bu işlemlerle $V(\mathbb{F})$, $\mathbb{F}$ üzerinde sonsuz boyutlu bir vektör uzayı oluşturur. Bu uzayın sıfır vektörü

$$\mathbf{0} \coloneqq (0, 0, 0, \ldots)$$

şeklindedir.

Bir $\mathbf{a} = (a_0, a_1, a_2, \ldots) \in V(\mathbb{F})$ dizisi bir LFSR dizisidir. LFSR yapısında, her yeni terim sabit katsayılarla önceki n terimin doğrusal birleşimi olarak belirlendiğinden, üretilen dizi

$$a_{n+k} = \sum_{i=0}^{n-1} c_i a_{k+i}, \quad k = 0, 1, \ldots, \tag{2.7}$$

doğrusal özyineleme bağıntısını sağlar. Burada $c_0, c_1, \ldots, c_{n-1} \in \mathbb{F}$ sabit katsayılardır.

LFSR dizileri üzerinde tanımlı sola kaydırma işlemi, $L : V(\mathbb{F}) \to V(\mathbb{F})$ doğrusal operatörü

$$L\mathbf{a} \coloneqq (a_1, a_2, a_3, \ldots)$$

ile tanımlanır ve bu işlem için $L^i\mathbf{a} = (a_i, a_{i+1}, a_{i+2}, \ldots)$, $L^0\mathbf{a} = \mathbf{a}$ eşitlikleri geçerlidir.

Bu operatör yardımıyla (2.7) bağıntısı

$$L^n\mathbf{a} = \sum_{i=0}^{n-1} c_i L^i\mathbf{a} \quad \text{ya da} \quad \left(L^n - \sum_{i=0}^{n-1} c_i L^i\right)\mathbf{a} = 0$$

şeklinde yazılabilir.

Bu çerçevede, LFSR tarafından üretilen diziyi tanımlayan karakteristik polinom $f(x)$

$$f(x) = x^n - (c_{n-1}x^{n-1} + \cdots + c_0)$$

olarak ifade edilir. Bu polinomun sola kaydırma operatörü L cinsinden karşılığı ise

$$f(L) = L^n - (c_{n-1}L^{n-1} + \cdots + c_0 I)$$

şeklindedir ve dolayısıyla $f(L)\mathbf{a} = 0$ eşitliği sağlanır. Bu eşitlik, dizinin $f(x)$ karakteristik polinomu tarafından belirlenen doğrusal bağıntıya uygun olduğunu gösterir.

Tanım 2.10. *Sonsuz bir dizi* $\mathbf{a} \in V(\mathbb{F})$ *için,* $f(L)\mathbf{a} = 0$ *eşitliğini sağlayan bir monik bir polinom* $f(x) \in \mathbb{F}[x]$ *varsa,* $\mathbf{a}$ *dizisine bir* ***doğrusal özyinelemeli dizi*** *(linear recurring sequence) ya da bir* ***LFSR dizisi*** *denir. Bu durumda,* $f(x)$ *polinomu,* $\mathbf{a}$ *dizisinin* $\mathbb{F}$ *cismi üzerindeki* ***karakteristik polinomu*** *olarak adlandırılır. Polinomun terslenmiş (reciprocal) hali ise dizinin* ***geri besleme (feedback) polinomu*** *olarak tanımlanır.*

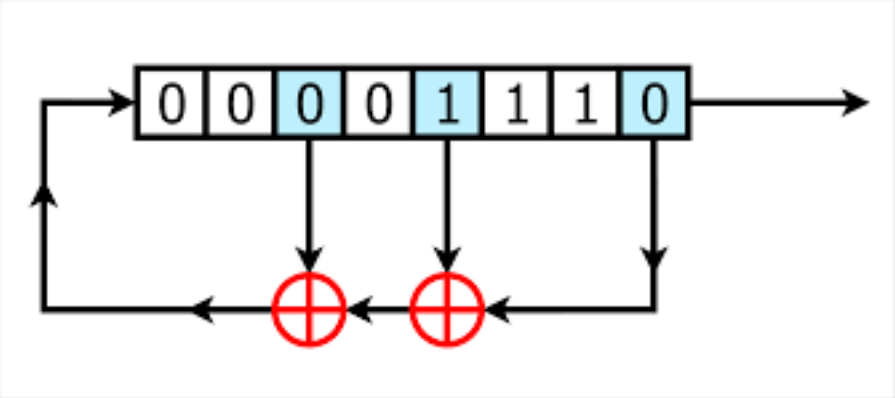
LFSR yapısında geri besleme işlemi, belirli bir karakteristik polinom aracılığıyla tanımlanır. Örneğin, $P(x) = x^8 + x^5 + x^3 + 1$ polinomu için, kaydırma kaydının 8., 5. ve 3. konumlarındaki bitler XOR işlemiyle birleştirilerek en sol bite geri beslenir. Bu yapıya ait LFSR devresi Şekil 2.1'de gösterilmiştir. Bu durumda $k = 0, 1, 2, \ldots$ için

$$a_{8+k} = a_k \oplus a_{3+k} \oplus a_{5+k}$$

özyineleme bağıntısı elde edilir.

Bu LFSR'nin periyodu 23'tür. Başlangıç durumu $[0, 0, 0, 0, 0, 0, 0, 1]$ olan dizi için ilk birkaç terim aşağıda verilmiştir:

[0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, ...]



Şekil 2.1 Geri besleme polinomu $P(x) = x^8 + x^5 + x^3 + 1$ olan bir LFSR devresi

Bu mekanizma, LFSR'nin döngüsel olarak sözde-rastgele bit dizileri üretmesini sağlar. Elde edilen dizinin periyodu, kullanılan geri besleme polinomunun yapısı ve başlangıç durumu tarafından belirlenir. Eğer derecesi n olan primitif bir polinom kullanılırsa, elde edilen dizinin maksimal periyodun uzunluğu $2^n - 1$ olur.

Örnek 2.11. *Örnek 2.6'da, $p = 59$ asal sayısı ile Legendre yöntemi kullanılarak elde edilen dizinin doğrusal karmaşıklığı $L(s) = p = 59$ olarak bulunur. Bu diziyi üreten geri besleme polinomu ise $m(x) = x^p - 1 = x^{59} - 1$ biçimindedir.*

Berlekamp–Massey algoritması, verilen sonlu bir dizinin doğrusal karmaşıklık değerini hesaplamak için yaygın olarak kullanılan bir yöntemdir. Bu algoritma, genellikle $\{0, 1\}$ elemanlı diziler üzerinde çalışmak üzere geliştirilmiştir. Ancak bu tez kapsamında, $\{-1, +1\}$ değerlerinden oluşan diziler ele alınmıştır. Bu iki gösterim arasındaki dönüşüm, $\phi\colon \{-1, +1\}^N \to \{0, 1\}^N$ biçiminde tanımlanan doğal bir eşleştirme yoluyla sağlanabilir.

Bir $E_N \in \{-1, +1\}^N$ dizisinin ϕ dönüşümü

$$\phi(E_N) \coloneqq \phi((e_1, e_2, \ldots, e_N)) = \mathbf{a}_N = (a_0, a_1, \ldots, a_{N-1}),$$

$$a_i := \frac{1 - e_{i+1}}{2}$$

şeklinde tanımlanır. Buradan da görülebileceği gibi, $a_i = 0$ olduğunda $e_{i+1} = +1$, $a_i = 1$ olduğunda ise $e_{i+1} = -1$ olur.

Bu durumda, $E_N \in \{-1, +1\}^N$ dizisinin doğrusal karmaşıklığı

$$L(E_N) := L(\phi(E_N))$$

şeklinde tanımlanır. Winterhof ve Brandstätter, bir E_N dizisinin doğrusal karmaşıklığının dizinin korelasyon ölçütleriyle ilişkilendirilebileceğini kanıtlamışlardır **?**.

Teorem 2.7. *$N \geq 2$ ve E_N bir ikili dizi olmak üzere, dizinin doğrusal karmaşıklığı ile korelasyon ölçütleri arasında*

$$L(E_N) \geq N - \max_{1 \leq k \leq L(E_N)+1} C_k(E_N)$$

ilişkisi vardır.

Bu eşitsizlik, belirli yapılardan elde edilen diziler için doğrusal karmaşıklıkta güçlü alt sınırlar sağlar. Ancak teoremin bir dezavantajı, yüksek mertebeden korelasyon ölçütlerinin kullanılmasını gerektirmesidir. Böyle korelasyonların tahmini genellikle zordur. Andics, yalnızca ikinci mertebeden korelasyon ölçütünü kullanan bir eşitsizlik ortaya koymuştur [Andics 2005].

Teorem 2.8. *Eğer $N \in \mathbb{N}$ ve E_N bir ikili dizi ise, bu durumda dizinin doğrusal karmaşıklığı ile ikinci mertebeden korelasyon ölçütü arasında*

$$2^{L(E_N)} \geq N - C_2(E_N)$$

eşitsizliği geçerli olur.

2.5 Dizi Aileleri

Pek çok uygulamada yalnızca bir dizi ailesinin, yani $\mathcal{F}$ kümesinin, büyük sayıda dizi içermesi yeterli değildir. Örneğin, $\mathcal{F}$ çok sayıda dizi içermesine rağmen, diziler yalnızca birkaç bite göre farklılık gösteriyorsa, bu tür bir yapı kriptografik uygulamalarda zayıf kalır. Bu nedenle, $\mathcal{F}$ ailesinin hem çeşitlilik hem de karmaşıklık açısından zengin bir yapıya sahip olması gerekir. Özellikle, aile içinde birbirine yapısal olarak benzemeyen ve istatistiksel açıdan bağımsız dizilerin bulunması önem arz eder. Bu tür özelliklerin değerlendirilmesi amacıyla f-karmaşıklık ve çapraz-korelasyon gibi ölçütler tanımlanmıştır. Bu doğrultuda, ilk aile ölçütü Ahlswede ve diğerleri tarafından 2003 yılında tanıtılmıştır [Ahlswede vd. 2003].

Tanım 2.11. *[Ahlswede vd. 2003] Uzunluğu N olan ve $E_N \in \{-1,+1\}^N$ biçimindeki ikili dizilerden oluşan bir $\mathcal{F}$ ailesinin f-**karmaşıklığı** $C(\mathcal{F})$, her $1 \le i_1 < i_2 < \cdots < i_j \le N$ konum seçimi ve her $\epsilon_1, \epsilon_2, \ldots, \epsilon_j \in \{-1,+1\}$ desenine karşılık*

$$e_{i_1} = \epsilon_1, \quad e_{i_2} = \epsilon_2, \quad \ldots, \quad e_{i_j} = \epsilon_j$$

eşitliklerini sağlayan bir $E_N = (e_1, e_2, \ldots, e_N) \in \mathcal{F}$ dizisinin bulunabildiği en büyük $j \ge 0$ tam sayısıdır.

Bu tanım, aile içerisindeki dizilerin ne ölçüde farklı sembol kombinasyonları kapsayabildiğini belirler. $C(\mathcal{F}) = j$ olması, ailedeki dizilerin her j pozisyonda tüm olası sembol dizilimlerini içerebildiğini, ancak $j+1$ pozisyon için bu kapsamanın sağlanamayabileceğini belirtir. Bu nedenle, $C(\mathcal{F})$ değeri ne kadar büyükse, ilgili dizi ailesi o ölçüde zengin ve karmaşık bir yapıya sahiptir. Bu tür bir yapı, özellikle kriptografik sistemlerin güvenliğinde kritik bir rol oynar.

Örneğin, anahtar dizisi olarak $E_N = (e_1, \ldots, e_N) \in \mathcal{F}$ alınsın. Bu anahtar dizisi kullanılarak bir metnin şifrelenmesi şu şekilde gerçekleştirilir: Öncelikle, gönderilecek

metin uygun bir kodlama yöntemiyle $U_N \in \{-1,+1\}^N$ olacak şekilde bir işaret dizisine dönüştürülür. Ardından bu dizi,

$$U_N = (u_1, \ldots, u_N) \xrightarrow{E_N} V_N \coloneqq (v_1, \ldots, v_N) = (e_1 u_1, \ldots, e_N u_N)$$

biçiminde şifrelenir ve V_N dizisi elde edilir. Şifreli metni orijinaline dönüştürmek için

$$U_N = E_N(V_N) \coloneqq (e_1 v_1, \ldots, e_N v_N) = (u_1, \ldots, u_N)$$

şeklindeki ters işlem uygulanır.

Şimdi, bu şifreleme sistemini kırmak isteyen bir saldırganın izleyebileceği olası stratejileri ele alalım. Böyle bir saldırgan, şifre çözme sürecinde aşağıdaki iki senaryoyu dikkate alabilir:

Durum 1. Saldırgan, $U_N \xrightarrow{E_N} V_N$ şifreleme işlemi sırasında, orijinal metnin belirli düzenliliklerini ve tekrar eden yapılarını koruduğunu varsayar. Bu yapısal özelliklerden yararlanarak, anahtar dizisi $E_N = (e_1, \ldots, e_N)$'nin bazı bitlerine ilişkin

$$e_{i_1} = \varepsilon_1, \ldots, e_{i_j} = \varepsilon_j \quad (i_1 < \cdots < i_j) \tag{2.8}$$

şeklinde kısmi bilgi edinmeye çalışır.

Durum 2. Saldırgan, (2.8) ifadesiyle elde ettiği bu kısmi bilgiye dayanarak, anahtar dizisi E_N'nin geri kalan bitlerini de tahmin etmeyi hedefler.

Şifreleme sisteminin kırılmaya karşı dayanıklı olabilmesi için, yukarıda tanımlanan her iki durumun da dikkate alınması ve bu doğrultuda güvenlik önlemlerinin güçlendirilmesi gerekir. *Durum 1* için, iyi sözde-rastgele dizilerden seçilen bir E_N anahtarı yeterli güvenlik sağlayabilir. Öte yandan, *Durum 2*'ye karşı güvenliği sağlamak için, dizi ailesinin yapısal karmaşıklık özelliklerinin yüksek olması gerekir.

Bu amaçla, f-karmaşıklık $C(\mathcal{F})$ için bir üst sınır elde etmek üzere,

$$e_{i_1} = \varepsilon_1, \quad e_{i_2} = \varepsilon_2, \quad \ldots, \quad e_{C(\mathcal{F})} = \varepsilon_{C(\mathcal{F})} \tag{2.9}$$

koşulunu sağlayan tüm olasılıklar göz önünde bulundurulur.

f-karmaşıklık tanımına göre, $\mathcal{F}$ ailesine ait en az bir E_N dizisi bu koşulu sağlamalıdır. Her bir konum kombinasyonu için iki farklı bit seçilebildiğinden, toplamda $2^{C(\mathcal{F})}$ farklı olasılık söz konusudur. Bu durum,

$$2^{C(\mathcal{F})} \leq |\mathcal{F}| \tag{2.10}$$

şeklindeki temel eşitsizlikle ifade edilir.

Bu bağıntıdan hareketle, f-karmaşıklık için

$$C(\mathcal{F}) \leq \frac{\log |\mathcal{F}|}{\log 2} \tag{2.11}$$

şeklinde bir üst sınır elde edilir.

$\mathbb{F}_p$ üzerinde tanımlı ve derecesi K'dan küçük polinomlar kullanılarak (2.5) bağıntısıyla oluşturulan ikili diziler, Legendre sembolü yardımıyla üretilmekte olup, bu dizilerden oluşan aile $\mathcal{F}(K, p)$ ile gösterilsin.

[Ahlswede vd. 2003] (Teorem 1.A) ile bu dizi ailesinin f-karmaşıklığının en az K olduğu gösterilmiştir. $\mathbb{F}_p$ üzerinde derecesi K'dan küçük olan tüm polinomlardan elde edilen $\mathcal{F}(K, p)$ ailesi, yeterli çeşitliliğe sahiptir. Özellikle, her K'lı konum seçimi $(i_1, \ldots, i_K)$ ve her $(\varepsilon_1, \ldots, \varepsilon_K) \in \{-1, +1\}^K$ kombinasyonu için

$$\left(\frac{f(i_k)}{p}\right) = \varepsilon_k \quad (1 \leq \mathrm{k} \leq \mathrm{K})$$

koşulunu sağlayan bir $f(x) \in \mathbb{F}_p[x]$ polinomu bulunabilir. Bu durum iki temel göz-

leme dayanmaktadır:

- Derecesi en fazla $K-1$ olan bir polinom, K farklı noktada verilen herhangi bir ± 1 değer kombinasyonunu gerçekleştirebilecek biçimde seçilebilir.
- Her $\varepsilon_k \in \{-1,+1\}$ değeri için, Legendre sembolü $\left(\frac{a}{p}\right) = \varepsilon_k$ eşitliğini sağlayan yeterli sayıda $a \in \mathbb{F}_p$ elemanı mevcuttur.

Dolayısıyla, tanım gereği $C(\mathcal{F}(K,p)) \geq K$ eşitsizliği sağlanır.

Öte yandan, (2.11) ifadesi dikkate alındığında, $\mathbb{F}_p$ üzerinde derecesi K'dan küçük olan polinomlardan oluşan kümenin büyüklüğü $|\mathcal{F}(K,p)| = p^K$ olarak alınabilir. Bu değer, aşağıdaki üst sınır bağıntısına yerleştirildiğinde

$$C(\mathcal{F}(K,p)) \leq \frac{\log|\mathcal{F}(K,p)|}{\log 2} \leq \frac{\log p^K}{\log 2}$$

eşitsizliği elde edilir. Sonuç olarak, $\mathcal{F}(K,p)$ ailesinin f-karmaşıklığı için

$$K \leq C(\mathcal{F}(K,p)) \leq \frac{K}{\log 2}\log p$$

şeklinde çift yönlü bir sınır geçerlidir. Bu sınırlar, dizilerin karmaşıklığının hem kullanılan polinomların derecesi K hem de tanımlı oldukları cismin büyüklüğü p ile doğrudan ilişkili olduğunu göstermektedir.

Gyarmati ve diğerleri, ℓ mertebesindeki çapraz-korelasyon ölçütünü tanımlamışlardır [Gyarmati vd. 2014].

Tanım 2.12. *Uzunluğu N olan ikili dizilerden oluşan bir $\mathcal{F}$ ailesi*

$$E_{i,N} = (e_{i,1}, e_{i,2}, \ldots, e_{i,N}) \in \{-1,+1\}^N, \quad i = 1,2,\ldots,F$$

şeklinde tanımlansın. Bu ailenin ℓ mertebedeki ***çapraz-korelasyon ölçütü***

$$\Phi_\ell(\mathcal{F}) := \max_{M,D,I} \left| \sum_{n=1}^{M} e_{i_1,n+d_1} \cdots e_{i_\ell,n+d_\ell} \right|$$

olarak tanımlanır. Burada,

- $D = (d_1, d_2, \ldots, d_\ell)$, $0 \leq d_1 \leq d_2 \leq \cdots \leq d_\ell$ *koşulunu sağlayan bir tam sayı dizisidir,*
- $M + d_\ell \leq N$ *olmalıdır,*
- $I = (i_1, i_2, \ldots, i_\ell)$, $\{1, 2, \ldots, F\}^\ell$ *kümesinden seçilen bir ℓ-uzunluklu sıralıdır.*

Ayrıca, $i \neq j$ ve $E_{i,N} = E_{j,N}$ durumlarında $d_i \neq d_j$ koşulu sağlanmalıdır. Bu koşul, aynı diziye karşılık gelen farklı indekslerin aynı kaydırma değeriyle birlikte çarpımda yer almasını önlemek amacıyla getirilmiştir.

Bu ölçüt, ℓ adet dizide belirli kaymalarla seçilen elemanların çarpımlarının toplamını alarak bu diziler arasındaki yapısal benzerlikleri ölçer. Eğer bu toplam büyükse, bu diziler belirli alt diziler üzerinde senkronize davranıyor demektir; bu da rastgelelik açısından olumsuz bir durumdur.

Örnek 2.12. *Uzunluğu $N = 10$ olan ikili dizilerden oluşan bir $\mathcal{F}$ ailesi için, $I = [1, 2, 3, 7, 8]$ ve $D = [0, 0, 2, 3, 5]$ seçimleri yapıldığında, çapraz-korelasyon ölçütü $\ell = |I| = |D| = 5$ için hesaplanacaktır.*

Verilen kaydırma vektörü D dikkate alındığında, $0 \leq d_1 \leq d_2 \leq \cdots \leq d_\ell$ koşulu sağlanmakta ve $M + d_\ell \leq N$ şartı altında M en çok 5 olabilir. Örneğin, $M = 4$ için çapraz-korelasyon toplamı

$$\Phi_5(\mathcal{F}) := \max_{4,D,I} \left| \sum_{n=1}^{4} e_{i_1,n+d_1} \cdots e_{i_5,n+d_5} \right|$$

$$= |e_{1,1}e_{2,1}e_{3,3}e_{7,4}e_{8,6} + e_{1,2}e_{2,2}e_{3,4}e_{7,5}e_{8,7} + e_{1,3}e_{2,3}e_{3,5}e_{7,6}e_{8,8} + e_{1,4}e_{2,4}e_{3,6}e_{7,7}e_{8,9}|$$

şeklinde hesaplanır.

Çapraz-korelasyon toplamında yer alan çarpım terimlerindeki dizi elemanlarının konumları, Çizelge 2.6'da renk kodlarıyla görselleştirilmiştir.

Çizelge 2.6 M=4 için $\Phi(\mathcal{F})$ çapraz-korelasyon terimlerinin gösterimi

	1	2	3	4	5	6	7	8	9	10
1	$e_{1,1}$	$e_{1,2}$	$e_{1,3}$	$e_{1,4}$	$e_{1,5}$	$e_{1,6}$	$e_{1,7}$	$e_{1,8}$	$e_{1,9}$	$e_{1,10}$
2	$e_{2,1}$	$e_{2,2}$	$e_{2,3}$	$e_{2,4}$	$e_{2,5}$	$e_{2,6}$	$e_{2,7}$	$e_{2,8}$	$e_{2,9}$	$e_{2,10}$
3	$e_{3,1}$	$e_{3,2}$	$e_{3,3}$	$e_{3,4}$	$e_{3,5}$	$e_{3,6}$	$e_{3,7}$	$e_{3,8}$	$e_{3,9}$	$e_{3,10}$
4	$e_{4,1}$	$e_{4,2}$	$e_{4,3}$	$e_{4,4}$	$e_{4,5}$	$e_{4,6}$	$e_{4,7}$	$e_{4,8}$	$e_{4,9}$	$e_{4,10}$
5	$e_{5,1}$	$e_{5,2}$	$e_{5,3}$	$e_{5,4}$	$e_{5,5}$	$e_{5,6}$	$e_{5,7}$	$e_{5,8}$	$e_{5,9}$	$e_{5,10}$
6	$e_{6,1}$	$e_{6,2}$	$e_{6,3}$	$e_{6,4}$	$e_{6,5}$	$e_{6,6}$	$e_{6,7}$	$e_{6,8}$	$e_{6,9}$	$e_{6,10}$
7	$e_{7,1}$	$e_{7,2}$	$e_{7,3}$	$e_{7,4}$	$e_{7,5}$	$e_{7,6}$	$e_{7,7}$	$e_{7,8}$	$e_{7,9}$	$e_{7,10}$
8	$e_{8,1}$	$e_{8,2}$	$e_{8,3}$	$e_{8,4}$	$e_{8,5}$	$e_{8,6}$	$e_{8,7}$	$e_{8,8}$	$e_{8,9}$	$e_{8,10}$
9	$e_{9,1}$	$e_{9,2}$	$e_{9,3}$	$e_{9,4}$	$e_{9,5}$	$e_{9,6}$	$e_{9,7}$	$e_{9,8}$	$e_{9,9}$	$e_{9,10}$
10	$e_{10,1}$	$e_{10,2}$	$e_{10,3}$	$e_{10,4}$	$e_{10,5}$	$e_{10,6}$	$e_{10,7}$	$e_{10,8}$	$e_{10,9}$	$e_{10,10}$

Uzunluğu N olan ve $|\mathcal{F}| < 2^{N/12}$ koşulunu sağlayan bir ikili dizi ailesi $\mathcal{F}$ için, $\ell \leq \frac{N}{6\log_2|\mathcal{F}|}$ koşulu altında çapraz-korelasyon ölçütünün beklenen değeri yaklaşık olarak

$$\Phi_\ell(\mathcal{F}) \approx \left(N \log \binom{N}{\ell} + \ell \log |\mathcal{F}| \right)^{1/2}$$

şeklindedir [Mérai 2016]. Sabit $M = F$ ve tüm $i \in \{1, 2, \ldots, \ell\}$ için $d_i = 0$ alındığında hesaplanan çapraz-korelasyon için Φ_ℓ° notasyonu kullanılır.

Tanım 2.13. *Uzunluğu N olan F adet ikili diziden oluşan bir $\mathcal{F}$ ailesi verilsin. Bu ailenin **dual ailesi** $\overline{\mathcal{F}}$, orijinal dizilerin sütunlarından oluşturulan yeni diziler kümesidir.*

Matematiksel olarak, $\mathcal{F} = \{(e_{i,1}, \ldots, e_{i,N}) \in \{-1, +1\}^N \mid 1 \leq i \leq F\}$ şeklinde

tanımlanan aile için, her $n \in \{1, \ldots, N\}$ *sütun indeksine karşılık gelen*

$$C_n = (e_{1,n}, e_{2,n}, \ldots, e_{F,n}) \in \{-1, +1\}^F$$

sütun vektörlerinin tümü $\overline{\mathcal{F}}$ *dual ailesini oluşturur. Bu yapı, orijinal* $F \times N$ *boyutlu dizi matrisinin transpozu alınarak elde edilen* $N \times F$ *boyutlu matrise karşılık gelir.*

? çalışmasında ikili dizi ailelerinin karmaşıklık ölçütleri ile dual ailelerin çapraz-korelasyon özellikleri arasında temel bir bağıntı kurulmuştur.

F adet ikili diziden oluşan bir $\mathcal{F}$ ailesinin her bir elemanı

$$E_{i,N} = (e_{i,1}, e_{i,2}, \ldots, e_{i,N}) \in \{-1, +1\}^N$$

şeklinde tanımlansın. Burada $i = 1, \ldots, F$ olmak üzere, ailenin f-karmaşıklığı $C(\mathcal{F})$ ile dual aile $\overline{\mathcal{F}}$'nin çapraz-korelasyon ölçütü $\Phi_\ell(\overline{\mathcal{F}})$ arasında, her $\ell \in \{1, 2, \ldots, \log_2 F\}$ için

$$C(\mathcal{F}) \geq \left\lceil \log_2 F - \log_2 \left(\max_{1 \leq \ell \leq \log_2 F} \Phi_\ell(\overline{\mathcal{F}}) \right) \right\rceil - 1 \tag{2.12}$$

eşitsizliği elde edilmiştir. Bu sonuç, bir dizi ailesinin yapısal karmaşıklığı ile ona karşılık gelen dual ailenin korelasyon özellikleri arasında doğrudan bir ilişki olduğunu göstermektedir.

Bu tezin temel katkılarından biri, Bölüm 3 ve Bölüm 4'te tanımlanan iki yeni dizi ailesinin inşasıdır. Bu aileler için f-karmaşıklık alt sınırlarının hesaplanmasında, yukarıda verilen (2.12) numaralı eşitsizlik doğrudan kullanılmıştır. Elde edilen uygulama sonuçları ve bu sınırların etkinliği, ilgili bölümlerde ayrıntılı olarak ele alınacaktır.

3. SINIRLI ÇAPRAZ-KORELASYON VE AİLE KARMAŞIKLIĞI ÖLÇÜTLERİNE SAHİP BİR AİLE VE DUALİ

Legendre sembolü ve indirgenemez polinomlar kullanılarak tanımlanan ikili dizi ailelerine ilişkin çeşitli yapılar literatürde yer almaktadır **?**, [Gyarmati vd. 2014], [Gyarmati 2009]. Bu bölümde, **?** çalışmasında tanıtılan dizi ailelerinin bazı yapısal özelliklerini taşıyan yeni bir yapı ele alınmaktadır.

İlgili çalışmada, $p > 2$ asal bir sayı ve b, mod p'ye göre bir kare olmayan (quadratic nonresidue) bir sayı olmak üzere,

$$\mathcal{F} = \left\{ \left(\frac{n^2 - bi^2}{p} \right)_{i=1}^{(p-1)/2} : n = 1, \ldots, \frac{p-1}{2} \right\}$$

biçiminde tanımlanan dizi ailesi $\mathcal{F}$ ile bu ailenin duali $\overline{\mathcal{F}}$ incelenmiştir.

Her $k \in \mathbb{N}^+$ için, bu dizi ailelerinin çapraz-korelasyon ölçütlerinin

$$\Phi_k(\mathcal{F}) \ll kp^{1/2} \log p \quad \text{ve} \quad \Phi_k(\overline{\mathcal{F}}) \ll kp^{1/2} \log p$$

şeklinde üstten sınırlandığı gösterilmiştir. Burada, dizi ailesinin duali Tanım 2.12'de belirtildiği şekilde tanımlanmaktadır. Elde edilen bu üst sınırlar, (2.12) bağıntısıyla birlikte değerlendirildiğinde, $\mathcal{F}$ ve $\overline{\mathcal{F}}$ ailelerine ait f-karmaşıklık için

$$C(\mathcal{F}) \geq \left(\frac{1}{2} - o(1) \right) \frac{\log p}{\log 2} \quad \text{ve} \quad C(\overline{\mathcal{F}}) \geq \left(\frac{1}{2} - o(1) \right) \frac{\log p}{\log 2}$$

şeklinde alt sınırlar elde edilmektedir.

Bu bölümde elde edilen yapı, **?** çalışmasında tanımlanan dizi ailesinin bir genellemesidir. Söz konusu çalışmada, $p > 2$ asal sayısı için uzunluğu $(p-1)/2$ olan diziler tanımlanmıştır. Bu bölümde ise, $\mathbb{F}_p$ üzerindeki indirgenemez polinomlar kullanılarak

uzunluğu $p-1$ olan yeni bir dizi ailesi oluşturulmakta ve bu ailenin hem kendisi hem de dualeri için çapraz-korelasyon ve f-karmaşıklık ölçütlerine dair benzer sınırların sağlandığı gösterilmektedir.

Bu amaçla, $p > 2$ asal bir sayı ve $d \geq 5$ olmak üzere, $\mathbb{F}_p$ üzerindeki d dereceli indirgenemez polinomlardan oluşan

$$\Omega_{p,d} = \left\{ x^d + a_2 x^{d-2} + \cdots + a_{d-2}x^2 + a_d \in \mathbb{F}_p[x] \,\middle|\, a_2, a_3 \neq 0 \right\}$$

kümesi tanımlanır. Bu yapı üzerine kurulu yeni dizi ailesi ve onun dualeri, hem yüksek f-karmaşıklık hem de düşük çapraz-korelasyon ölçütleri bakımından analiz edilmiştir.

Teorem 3.1. *$p > 2$ asal sayı ve $d < p^{1/2}/2$ olmak üzere, $f \in \Omega_{p,d}$ seçilsin. Her $i \in \{1, 2, \ldots, p-1\}$ için, $f_i(X) \coloneqq i^d f(X/i)$ biçiminde tanımlanan polinomlar yardımıyla*

$$\mathcal{F}_f = \left\{ \left(\frac{f_i(n)}{p} \right)_{n=1}^{p-1} : i = 1, \ldots, p-1 \right\}$$

şeklinde tanımlanan $\mathcal{F}_f$ ikili dizi ailesi ve onun duali $\overline{\mathcal{F}}_f$ ele alındığında, her $k \in \{1, 2, \ldots, p-1\}$ için

$$\Phi_k(\mathcal{F}_f) \ll dkp^{1/2} \log p \quad ve \quad \Phi_k(\overline{\mathcal{F}}_f) \ll dkp^{1/2} \log p \tag{3.1}$$

şeklinde çapraz-korelasyon üst sınırları elde edilir.

Ayrıca, bu dizi ailesi ile dualine ilişkin f-karmaşıklık açısından

$$C(\mathcal{F}_f) \geq \left(\frac{1}{2} - o(1) \right) \frac{\log(p/d^2)}{\log 2}, \tag{3.2}$$

$$C(\overline{\mathcal{F}}_f) \geq \left(\frac{1}{2} - o(1) \right) \frac{\log(p/d^2)}{\log 2} \tag{3.3}$$

biçiminde alt sınırlar sağlanmaktadır. Özellikle, $d = p^{\varepsilon}$ biçiminde bir seçim yapıldı-

ğında karmaşıklık için

$$\left(\frac{1}{2} - \varepsilon - o(1)\right) \frac{\log p}{\log 2}$$

alt sınırı elde edilir. Bu sınır, $\varepsilon \geq 1/2$ *durumunda anlamsız hale gelir.*

İspat. Çapraz-korelasyon ölçütüne ilişkin üst sınırların elde edilmesi için karakter toplamlarının analiz edilmesi gerekir. $\mathbb{F}_p$ üzerinde tanımlı çarpımsal karakter toplamları

$$\sum_{x \in \mathbb{F}_p} \chi(f(x))$$

şeklinde ifade edilir. Burada χ sonlu cisim $\mathbb{F}_p$ üzerindeki Legendre karakterini, $f(x)$ ise sabit olmayan ve kare çarpansız bir polinomu temsil eder.

Weil teoremi (Teorem 2.3) kullanılarak karakter toplamlarının mutlak değeri

$$\left| \sum_{x \in \mathbb{F}_p} \chi(f(x)) \right| \leq (\mathrm{der} f - 1) \cdot p^{1/2}$$

şeklinde sınırlandırılır.

$\mathcal{F}_f$ ailesindeki her bir ikili dizi

$$E_{i,p-1} = (e_{i,1}, e_{i,2}, \ldots, e_{i,p-1}) \in \{-1, +1\}^{p-1}$$

olarak tanımlanır. Bu diziler üzerinde k-mertebeden çapraz-korelasyon ölçütü

$$\Phi_k(\mathcal{F}_f) = \max_{M,D,I} \left| \sum_{n=1}^{M} e_{i_1,n+d_1} \cdots e_{i_k,n+d_k} \right|$$

şeklinde ifade edilir.

Bu ölçüt $\mathcal{F}_f$ ailesine uygulandığında çapraz-korelasyon toplamı

$$\Phi_k(\mathcal{F}_f) = \max_{M,D,I} \left| \sum_{n=1}^{M} \left(\frac{f_{i_1}(n+d_1)}{p} \right) \cdots \left(\frac{f_{i_k}(n+d_k)}{p} \right) \right|$$

şeklinde yazılır. Legendre sembolünün çarpımsallığı kullanılarak bu ifade

$$\Phi_k(\mathcal{F}_f) = \max_{M,D,I} \left| \sum_{n=1}^{M} \left(\frac{f_{i_1}(n+d_1) \cdots f_{i_k}(n+d_k)}{p} \right) \right|$$

olarak sadeleştirilir.

Teorem 3.1'de belirtildiği gibi her $f_i(X)$ polinomu

$$f_i(X) \coloneqq i^d f(X/i)$$

şeklinde elde edilir. $f(X)$ polinomunun indirgenemez olması nedeniyle türetilen her $f_i(X)$ polinomu da indirgenemez kalır.

$h(X)$ polinomunun kare çarpansız olduğunu göstermek için farklı (i_j, d_j) çiftleri için $f_{i_j}(X+d_j)$ polinomlarının birbirinden farklı olduğu ispatlanır. Bazı $i_j \neq i_\ell$ için

$$f_{i_j}(X+d_j) = f_{i_\ell}(X+d_\ell)$$

eşitliği sağlanmış olsun. Bu durumda, her iki polinomun X^{d-1} teriminin katsayıları da eşit olmalıdır. Binom açılımı dikkate alındığında bu katsayılar sırasıyla

$$\binom{d}{1} X^{d-1} d_j \quad \text{ve} \quad \binom{d}{1} X^{d-1} d_\ell$$

biçimindedir. Dolayısıyla

$$d \cdot d_j = d \cdot d_\ell \pmod{p}$$

eşitliği sağlanır. $\text{obeb}(p, d) = 1$ varsayımı altında

$$d_j = d_\ell$$

eşitliği elde edilir.

Bu durumda X^{d-2} ve X^{d-3} terimlerinin katsayılarının incelenmesi

$$a_2 i_j^2 = a_2 i_\ell^2 \quad \text{ve} \quad a_3 i_j^3 = a_3 i_\ell^3$$

eşitliklerini gerektirir. Buradan

$$i_j = i_\ell$$

çelişkisi elde edilir. Dolayısıyla, tüm $f_{i_j}(X + d_j)$ polinomları birbirinden farklıdır. Bu da $h(X)$ polinomunun ayırt edilebilir çarpanlardan oluştuğunu ve bu nedenle kare çarpansız olduğunu gösterir.

Derecesi dk olan kare çarpansız $h(X)$ polinomu için Weil sınırı uygulanarak,

$$\Phi_k(\mathcal{F}_f) \ll dk\, p^{1/2} \log p \quad \text{ve} \quad \Phi_k(\overline{\mathcal{F}}_f) \ll dk\, p^{1/2} \log p$$

üst sınırları elde edilir.

Son olarak, (2.12) eşitsizliği kullanılarak dizi ailesinin f-karmaşıklığı için

$$\begin{aligned}
C(\mathcal{F}_f) &\geq \log_2 \left(\frac{F}{\max\limits_{1 \leq \ell \leq \log_2 F} \Phi_\ell^\circ(\overline{\mathcal{F}}_f)} \right) \\
&\geq \log_2 \left(\frac{p-1}{d\, k\, p^{1/2}\, \log p} \right) \\
&= \log_2 \left(\frac{p-1}{d\, (\log_2 p)\, p^{1/2}\, \log p} \right) \\
&\geq \log_2 \left(\frac{p^{1/2}}{d\, (\log_2 p)\, \log p} \right) \\
&= \frac{1}{2} \log_2 \left(\frac{p}{d^2} \right) - \log_2 \log^2 p \\
&\geq \left(\frac{1}{2} - o(1) \right) \frac{\log(p/d^2)}{\log 2}
\end{aligned}$$

alt sınırı elde edilir. Burada, (2.11) ifadesinde belirtildiği gibi, f-karmaşıklık ta-

nımı gereği en fazla $k \leq \log_2 |\mathcal{F}_f|$ mertebesine kadar olan değerlerin dikkate alınması gerektiğinden, üst sınırın tahmininde $k \approx \log_2 p$ kabul edilmiştir. Öte yandan, $\log_2 \log^2 p$ terimi, p büyüdükçe $\log(p/d^2)$ ifadesine kıyasla ihmal edilebilir hâle geldiğinden, bu fark $o(1)$ terimiyle ifade edilerek karmaşıklık için elde edilen alt sınırın asimptotik geçerliliği korunmuştur.

Bu bağıntı, özellikle $d = p^{\varepsilon}$ biçiminde bir seçim yapıldığında daha sade bir biçime indirgenebilir. Bu durumda

$$\log(p/d^2) = \log(p/p^{2\varepsilon}) = \log(p^{1-2\varepsilon}) = (1-2\varepsilon)\log p$$

eşitliği sağlanır ve böylece f-karmaşıklık için

$$C(\mathcal{F}_f) \geq \left(\frac{1}{2} - \varepsilon - o(1)\right) \frac{\log p}{\log 2}$$

şeklinde bir alt sınır elde edilir. Ancak $\varepsilon \geq 1/2$ olması durumunda, bu sınır negatif değerlere karşılık geleceğinden, asimptotik anlamda anlamlı bir bilgi sunmaz. □

Uyarı 3.1. *Teorem 3.1'de kullanılan $\Omega_{p,d}$ kümesi tanımlanırken, a_1 ve a_{d-1} katsayılarının sıfır olarak seçilmesi tesadüfi değildir. Bu tercih, $f_i(X) = i^d f(X/i)$ dönüşümü ve ardından uygulanan kaydırma işlemi $f_i(X+d)$ sonucunda elde edilen polinomların katsayı yapılarının birbirinden farklı kalmasını sağlamak amacıyla yapılmıştır. Özellikle $a_1 \neq 0$ veya $a_{d-1} \neq 0$ durumlarında, farklı (i,d) çiftlerinden elde edilen bazı polinomların eşit olabilme riski doğar. Böyle bir durumda, çapraz-korelasyon analizinde incelenen toplamda yer alan çarpım polinomu $h(X)$ aynı çarpanı birden fazla kez içerebilir. Bu ise $h(X)$'in kare çarpanlı olmasına, dolayısıyla Weil teoreminin uygulanamaz hale gelmesine neden olur. Weil teoreminin geçerli olabilmesi için $h(X)$ polinomunun kare çarpansız olması zorunlu olduğundan, $a_1 = a_{d-1} = 0$ koşulu teknik açıdan gereklidir.*

Uyarı 3.2. *Teorem 3.1 kapsamında elde edilen çapraz-korelasyon üst sınırları, belirli*

çarpımsal karakter toplamlarının analizi ile ilişkilidir. Bu toplamlar

$$\sum_{n=1}^{M} \left(\frac{h(n)}{p} \right)$$

şeklinde ifade edilir ve burada $h(X) \coloneqq f_{i_1}(X + d_1) \cdots f_{i_k}(X + d_k)$ *biçiminde tanımlanan, derecesi* dk *olan* h *polinomu yer alır. Her bir* $f_{i_j}(X + d_j)$ *ifadesi, başlangıçta sabit olarak seçilen bir* $f(X)$ *polinomunun önce* $f_i(X) = i^d f(X/i)$ *biçiminde ölçeklenmesi ve ardından değişken kaydırması* $X \mapsto X + d_j$ *uygulanmasıyla elde edilen bir türevidir. İspatta gösterildiği üzere,* $h(X)$ *polinomu kare çarpansız bir yapıya sahiptir.*

Eğer toplam tüm $\mathbb{F}_p$ *üzerinde alınsaydı, Weil teoremi (bkz. Teorem 2.3) doğrudan uygulanabilir ve*

$$\left| \sum_{x \in \mathbb{F}_p} \left(\frac{h(x)}{p} \right) \right| \leq (derh - 1) \cdot p^{1/2} = (dk - 1) \cdot p^{1/2}$$

biçiminde bir üst sınır elde edilebilirdi. Ancak Teorem 3.1'de olduğu gibi toplam yalnızca $n = 1$ *ile* $M \leq p - 1$ *arasındaki sınırlı bir aralıkta alındığında, Weil sınırı doğrudan uygulanamaz. Bu durumda karakter toplamları üzerindeki kontrol, Pólya–Vinogradov eşitsizliği yardımıyla sağlanır ve bu yaklaşım bir* $\log p$ *çarpanı doğurur. Söz konusu eşitsizlik aşağıdaki analiz adımlarına dayanır.*

1. ***Fourier açılımı*** *kullanılarak, karakter toplamı* $w(n)$ *gösterimi yardımıyla*

$$\sum_{n=1}^{M} \chi(n) = \sum_{n \in \mathbb{F}_p} \chi(n)\, w(n)$$

biçiminde ifade edilir. Burada $w(n)$*, yalnızca* $[1, M]$ *aralığında* 1*, diğer yerlerde* 0 *olan bir ağırlık fonksiyonudur. Bu fonksiyonun Fourier açılımı*

$$w(n) = \sum_{r=0}^{p-1} \widehat{w}(r)\, e_p(nr)$$

şeklindedir. Burada $e_p(x) \coloneqq e^{2\pi i x/p}$ *ifadesi,* $\mathbb{F}_p$ *üzerinde tanımlı toplamsal karakterdir.*

2. ***Gauss toplamı*** *kullanılarak karakter toplamı, Fourier açılımı*

$$\sum_{n\in\mathbb{Z}/p\mathbb{Z}} \chi(n)\, w(n) = \sum_{r=0}^{p-1} \widehat{w}(r) \underbrace{\sum_{n=1}^{p} \chi(n)\, e_p(nr)}_{G(\chi,\psi_r)}.$$

şeklinde yeniden yazılır. Burada χ *çarpımsal,* $\psi_r(n) = e_p(nr)$ *ise toplamsal karakterdir ve iç toplam klasik Gauss toplamını verir. Eğer* χ *birim olmayan bir karakterse, her* r *için*

$$|G(\chi, \psi_r)| \leq \sqrt{p}$$

bağıntısı geçerlidir.

3. ***Fourier katsayılarının büyüklüğü*** *açısından, ağırlık fonksiyonu yalnızca* $[1, M]$ *aralığında tanımlı olduğundan, Fourier katsayıları*

$$\widehat{w}(r) = \frac{1}{p} \sum_{n=1}^{M} e_p(-nr)$$

genellikle $\sim 1/r$ *mertebesinde azalan bir yapı gösterir. Katsayıların büyüklüğünü analiz etmek için geometrik seri özelliğini kullanarak*

$$\widehat{w}(r) = \frac{1}{p} \cdot \frac{e_p(-r) - e_p(-(M+1)r)}{1 - e_p(-r)}$$

ifadesini elde ederiz. Paydayı Taylor serisiyle açtığımızda ($r \neq 0$ *için)*

$$|1 - e_p(-r)| \approx \left|\frac{2\pi r}{p}\right|$$

olduğunu görürüz, bu da bize katsayıların büyüklüğünün

$$|\widehat{w}(r)| \sim \frac{1}{\pi r}$$

şeklinde davrandığını gösterir. Bu katsayıların toplam büyüklüğü yaklaşık ola-

rak harmonik seri davranışı sergileyerek

$$\sum_{r=1}^{p-1} |\widehat{w}(r)| \sim \sum_{r=1}^{p-1} \frac{1}{r} \approx \log p + \gamma + \mathcal{O}(1/p)$$

değerini alır, burada $\gamma \approx 0.5772$ *Euler sabitidir.*

4. ***Sonuç*** *olarak*

$$\left| \sum_{n=1}^{M} \chi(n) \right| \leq \sum_{r=0}^{p-1} |\widehat{w}(r)| \cdot |G(\chi, \psi_r)| \ll \sqrt{p} \log p$$

bağıntısı elde edilir.

Dolayısıyla, Teorem 3.1'deki çapraz-korelasyon üst sınırlarında görülen $\log p$ *çarpanı, karakter toplamlarının yalnızca sınırlı bir aralıkta değerlendirilmesi nedeniyle ortaya çıkar. Weil teoremi yalnızca tam toplamlar için geçerliyken, kısmi toplamlar durumunda Fourier analizi ve Gauss toplamlarına dayanan Pólya–Vinogradov yöntemi kullanılmakta ve bu yöntem doğal olarak* $\log p$ *büyüklüğünde bir çarpan üretmektedir.*

Uyarı 3.3. *Diziler arasındaki çapraz-korelasyon ölçütü, her bir dizinin farklı kaymalarla çarpılıp toplanmasıyla elde edilen karakter toplamlarına dayanmaktadır. Bu toplamlar, diziler arasında oluşan yapısal benzerlikleri ölçmekte ve Legendre sembolü gibi karakterler aracılığıyla değerlendirilmektedir. Böylece, korelasyon yapısı Weil sınırı kullanılarak üstten sınırlanabilir.*

Karakter toplamlarının büyüklüğü ile f*-karmaşıklık arasında ters yönlü bir ilişki bulunmaktadır. Yüksek korelasyon, yani toplamların büyük olması, diziler arasında güçlü yapısal benzerliklerin varlığına işaret eder; bu durum, dizilerin daha öngörülebilir hâle gelmesine ve dolayısıyla* f*-karmaşıklığın azalmasına neden olur. Öte yandan, karakter toplamlarının küçük olması diziler arası ayrışmayı artırır ve daha yüksek bir* f*-karmaşıklık düzeyine karşılık gelir.*

Bu sezgisel ilişki, **?** *çalışmasında verilen*

$$C(\mathcal{F}_f) \geq \log_2 \left(\frac{F}{\max\limits_{1 \leq \ell \leq \log_2 F} \Phi_\ell^\circ(\overline{\mathcal{F}}_f)} \right)$$

şeklindeki eşitsizlik ile matematiksel olarak ifade edilmiştir. Bu eşitsizlik, çapraz-korelasyon küçüldükçe f-karmaşıklığın artmasına katkı sağladığını açık biçimde ortaya koymaktadır.

Uyarı 3.4. *Teorem 3.1'de tanımlanan $\mathcal{F}_f$ ailesine ait sonuçların, polinom derecesi d arttıkça zayıfladığı; buna karşın aile büyüklüğünün sabit kaldığı, yani $|\mathcal{F}_f| = p - 1$ olduğu gözlemlenmektedir.*

İyi yapılandırılmış bir dizi ailesi için f-karmaşıklığın, $\log F$ mertebesinde olması beklenir. Bu bağlamda, Teorem 3.1'de elde edilen

$$C(\mathcal{F}_f) \geq \left(\frac{1}{2} - o(1) \right) \frac{\log(p/d^2)}{\log 2}$$

alt sınırı, aile büyüklüğü cinsinden yeniden yazıldığında

$$C(\mathcal{F}_f) \geq \left(\frac{1}{2} - o(1) \right) \left(\frac{\log |\mathcal{F}_f|}{\log 2} - \frac{2 \log d}{\log 2} \right)$$

şeklini alır. Özellikle d küçük seçildiğinde, $\log d \ll \log |\mathcal{F}_f|$ olacağından ikinci terim ihmal edilebilir düzeydedir. Bu durumda karmaşıklık için yaklaşık alt sınır olarak

$$C(\mathcal{F}_f) \geq \frac{\log |\mathcal{F}_f|}{2 \log 2}$$

ifadesi geçerli olur. Bununla birlikte, $C(\mathcal{F}_f)$ için benzer mertebede bir üst sınır da sağlanabilir ve mevcut alt sınır daha da iyileştirilebilirse, $\mathcal{F}_f$ ailesi iyi bir dizi ailesi olarak değerlendirilebilir.

Örnek 3.1. *$d = 5$ ve $p = 11$ için $f(x) = x^5 + x^3 + 2x^2 + 3$ polinomu $\Omega_{11,5}$ kümesine*

aittir. Her $i \in \{1, 2, \ldots, 10\}$ *için tanımlanan* $f_i(x) = i^5 f(x/i)$ *polinomları sırasıyla*

$$\begin{aligned} f_1(x) &= x^5 + x^3 + 2x^2 + 3, & f_2(x) &= x^5 + 4x^3 + 5x^2 + 8, \\ f_3(x) &= x^5 + 9x^3 + 10x^2 + 3, & f_4(x) &= x^5 + 5x^3 + 7x^2 + 3, \\ f_5(x) &= x^5 + 3x^3 + 8x^2 + 3, & f_6(x) &= x^5 + 3x^3 + 3x^2 + 8, \\ f_7(x) &= x^5 + 5x^3 + 4x^2 + 8, & f_8(x) &= x^5 + 9x^3 + x^2 + 8, \\ f_9(x) &= x^5 + 4x^3 + 6x^2 + 3, & f_{10}(x) &= x^5 + x^3 + 9x^2 + 8 \end{aligned}$$

şeklinde elde edilir.

Bu polinomlardan elde edilen ve her biri 10 uzunluğunda olan $p - 1 = 10$ *adet dizi Tablo 3.1'de verilmiştir. Bu dizi ailesi 3-karmaşıklığa sahip değildir, çünkü* $\mathbb{F}_2^3$

Çizelge 3.1 $d = 5$, $p = 11$ için elde edilen diziler

Dizi No	**Dizi**
E_1	$(-1, -1, \ 1, \ 1, \ 1, \ 1, \ 1, \ 1, \ 1, \ 1)$
E_2	$(-1, \ 1, -1, \ 1, -1, -1, -1, -1, -1, -1)$
E_3	$(\ 1, \ 1, -1, \ 1, \ 1, -1, \ 1, \ 1, \ 1, \ 1)$
E_4	$(\ 1, \ 1, \ 1, -1, \ 1, \ 1, \ 1, -1, \ 1, \ 1)$
E_5	$(\ 1, \ 1, \ 1, \ 1, -1, \ 1, \ 1, \ 1, \ 1, -1)$
E_6	$(\ 1, -1, -1, -1, -1, \ 1, -1, -1, -1, -1)$
E_7	$(-1, -1, \ 1, -1, -1, -1, \ 1, -1, -1, -1)$
E_8	$(-1, -1, -1, -1, \ 1, -1, -1, \ 1, -1, -1)$
E_9	$(\ 1, \ 1, \ 1, \ 1, \ 1, \ 1, -1, \ 1, -1, \ 1)$
E_{10}	$(-1, -1, -1, -1, -1, -1, -1, -1, \ 1, \ 1)$

uzayındaki tüm vektörleri kapsayan üçlü alt diziler arasında

$$\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} -1 \\ -1 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ -1 \\ -1 \end{bmatrix} \right\},$$

vektörlerinin tamamı bulunmamaktadır. Örneğin dizilerin ilk üç bitinden oluşan alt

diziler

$$\left[\begin{bmatrix}-1\\-1\\1\end{bmatrix},\begin{bmatrix}-1\\1\\-1\end{bmatrix},\begin{bmatrix}1\\1\\-1\end{bmatrix},\begin{bmatrix}1\\1\\1\end{bmatrix},\begin{bmatrix}1\\1\\1\end{bmatrix},\begin{bmatrix}1\\-1\\-1\end{bmatrix},\begin{bmatrix}-1\\-1\\1\end{bmatrix},\begin{bmatrix}-1\\-1\\-1\end{bmatrix},\begin{bmatrix}1\\1\\1\end{bmatrix},\begin{bmatrix}-1\\-1\\-1\end{bmatrix}\right]$$

şeklindedir ve tüm olasılıkları kapsamamaktadır. Bu nedenle dizi ailesi 3 f-karmaşıklığa sahip değildir. Öte yandan, tüm ikili kombinasyonları içerdiğinden $\mathcal{F}$ ailesi 2 f-karmaşıklığa sahiptir.

Bu dizi ailesinin 5. mertebeden çapraz-korelasyon ölçütü, $M = 10$, $I = [2, 6, 7, 8, 10]$ ve $D = [0, 0, 0, 0, 0]$ için maksimum değer olan 10'dur. Dual aile $\overline{\mathcal{F}_f}$, $I = [3, 4, 6, 9, 10]$ ve $D = [0, 0, 0, 1, 1]$ seçimleriyle bu ölçütte 9 değerini alır. Dual ailenin karmaşıklığı ise 1'dir.

Bu örnekte $p = 11$ gibi görece küçük bir asal sayı kullanıldığından, (3.1) ifadesinde verilen asimptotik çapraz-korelasyon üst sınırı, gözlemlenen değerle karşılaştırıldığında oldukça yüksek kalmaktadır. Gerçekte $\Phi_5(\mathcal{F}_f) = 10$ iken, teorik üst sınır yaklaşık olarak 75'tir. Bu fark, ilgili sınırın yalnızca p yeterince büyük olduğunda geçerli bir öngörü sunduğunu göstermektedir.

Benzer şekilde, (3.2) ve (3.3) ifadeleriyle elde edilen f-karmaşıklık alt sınırı da $p = 11$ ve $d = 5$ için yaklaşık -0.43 olmakta ve negatif bir değere karşılık geldiğinden, bu tür sınırların yalnızca büyük asal sayılar için anlamlı sonuçlar verdiği anlaşılmaktadır.

Teorem 3.1'de tanımlanan $\mathcal{F}_f$ (veya $\overline{\mathcal{F}}_f$) ailesinde yer alan dizilerin birbirinden farklı olduğu, çapraz-korelasyon ölçütü için verilen üst sınırdan anlaşılabilir. Aynı aile içerisinde iki dizinin özdeş olması durumunda, bu diziler arasındaki çapraz-korelasyon toplamı en büyük değere, yani $p - 1$'e ulaşırdı. Ancak Teorem 3.1'de verilen Φ_2 üst sınırı, $d < p^{1/2}/2$ koşulu sağlandığında bu değerin altında kalmaktadır. Dolayısıyla, bu koşul altında dizilerin birbirinden ayırt edilebilir olduğu ve aile büyüklüğünün

$|\mathcal{F}_f| = p - 1$ olduğu garanti edilir. Örnek olarak verilen $d = 5$ ve $p = 11$ için bu koşul sağlanmasa da, teoremin asimptotik geçerliliği bağlamında dizilerin farklılığı korunmaktadır.

Öte yandan, $\#\{\mathcal{F}_f \mid f \in \Omega_{p,n}\}$ ile gösterilen farklı dizi ailelerinin sayısı tam olarak bilinmemektedir. Aşağıdaki sonuçta, bu sayıya ilişkin bir üst sınır verilmektedir. Söz konusu sonuç doğrudan [Çakıroglu vd. 2022] çalışmasından alınmıştır.

Bu sonuca geçmeden önce bazı gösterimleri tanımlayalım. Her $\alpha \in \mathbb{F}_p^*$ için, $C_\alpha : x(y^p + y) = \alpha(x^2 + 1)$ denklemi ile verilen bir $\mathbb{F}_p$-üzerinde tanımlı cebirsel eğri tanımlanır. C_α eğrisi üzerindeki $\mathbb{F}_{p^n}$-noktalarının sayısını

$$\#C_\alpha(\mathbb{F}_{p^n})$$

ile gösterelir. Bu duurumda, sapma fonksiyonu

$$S_\alpha(\mathbb{F}_{p^n}) := \#C_\alpha(\mathbb{F}_{p^n}) - (p^n + 1)$$

şeklinde tanımlanır.

Burada μ Möbius fonksiyonunu; $[p \mid n]$ ise bir doğruluk göstergesini ifade eder. Bu gösterim

$$[p \mid n] := \begin{cases} 1, & \text{eğer } p \text{ sayısı } n\text{'yi bölüyorsa,} \\ 0, & \text{eğer } p \text{ sayısı } n\text{'yi bölmüyorsa} \end{cases}$$

şeklinde tanımlanır.

Bu tanımlar altında, aşağıdaki üst sınır elde edilmiştir.

Sonuç 3.1. *$\Omega_{p,n}$ kümesindeki indirgenemez polinomlarla tanımlanabilen $\mathcal{F}_f$ dizi aile-*

lerinin sayısı için

$$\#\{\mathcal{F}_f \mid f \in \Omega_{p,n}\} < \frac{1}{n}\sum_{\substack{d|n \\ p\nmid d}} \mu(d)\left(F_p(n/d) - [p \mid n]\cdot p^{n/pd}\right)$$

eşitsizliği geçerlidir. Burada $F_p(n)$ *fonksiyonu*

$$F_p(n) = p^{n-2} + \frac{(p-1)^2}{p^2} + \frac{1}{p^2}\sum_{\alpha\in\mathbb{F}_p^*} S_\alpha(\mathbb{F}_{p^n})$$

şeklinde tanımlanır.

İspat. $\mathcal{F}$ ailesi, $\Omega_{p,n}$ kümesinde yer alan her bir indirgenemez polinom f kullanılarak inşa edilmiştir. [Çakıroglu vd. 2022][Theorem-1] sonucuna göre, indirgenemez polinomların sayısı $F_p(n)$ cinsinden ifade edilebilmektedir. Ardından, [Çakıroglu vd. 2022][Teorem-5] bu sonucu sunar. □

4. DÜŞÜK ÇAPRAZ KORELASYON VE YÜKSEK AİLE KARMAŞIKLIĞINA SAHİP BÜYÜK BİR DİZİ AİLESİ

Bu bölümde, hem düşük çapraz-korelasyon ölçütüne hem de yüksek f-karmaşıklığa sahip büyük bir ikili dizi ailesi tanımlanmaktadır. Ancak, bu dizi ailelerinin dualleri için geçerli genel bir sonuç elde edilememiştir.

Teorem 4.1. *$p > 2$ asal sayı, $d \in \mathbb{Z}^+$ ve $p \nmid d$ olmak üzere, $\mathbb{F}_p[X]$ üzerindeki indirgenemez polinomlardan oluşan*

$$\Omega_d \coloneqq \left\{ f(X) = X^d + a_2 X^{d-2} + \cdots + a_d \in \mathbb{F}_p[X] : f \text{ indirgenemezdir} \right\}$$

kümesi tanımlansın. Bu kümedeki her bir f polinomuna karşılık gelen ikili dizi ailesi

$$\mathcal{F}_d \coloneqq \left\{ \left(\frac{f(n)}{p} \right)_{n=1}^{p-1} : f \in \Omega_d \right\}$$

şeklinde tanımlanır. Bu durumda, f-karmaşıklık için

$$C(\mathcal{F}_d) \geq \left(\frac{1}{2} - o(1) \right) \frac{\log(p^{d-2}/d^2)}{\log 2} \tag{4.1}$$

alt sınırı sağlanır. Ayrıca, $3 \leq d < p^{1/2}/2$ koşulu altında, dizi ailesinin büyüklüğü

$$|\mathcal{F}_d| = \frac{p^{d-1}}{d} - O\left(p^{\lfloor d/2 \rfloor}\right)$$

şeklindedir.

İspat. Weil sınırı, karakter toplamları üzerinde sağladığı güçlü analitik sınırlar sayesinde, farklı indirgenemez polinomlardan türetilen dizilerin birbirinden ayırt edilebilmesini sağlayan temel bir araçtır. Bu sınır, genel durumda farklı polinomlara

karşılık gelen dizilerin karakter değerlerinin çakışma olasılığını önemli ölçüde azalttığını gösterir. Böylece, her bir polinomdan elde edilen dizinin diğerlerinden farklı olduğu varsayılabilir ve dizi ailesinin büyüklüğü, kullanılan indirgenemez polinomların sayısına eşit alınır.

?'da $p \nmid d$ koşulunu sağlayan ve iz fonksiyonunun değeri sıfırdan farklı olan d dereceden indirgenemez polinomların sayısı

$$\frac{1}{dp}\sum_{t|d}\mu(t)p^{d/t}$$

olarak hesaplanmıştır.

Doğrudan hesaplama yapıldığında,

$$\sum_{i=1}^{d/2}p^i = \frac{p^{d/2+1}-p}{p-1} = \frac{p}{p-1}\left(p^{d/2}-1\right)$$

sonucuna ulaşılır. $p>2$ asalları içinde en küçük değer olan $p=3$ için,

$$\frac{1}{dp}\sum_{t|d}\mu(t)p^{d/t} \geq \frac{p^d}{dp} - \sum_{i=1}^{\lfloor d/2\rfloor}p^i \geq \frac{p^{d-1}}{d} - \frac{3}{2}p^{\lfloor d/2\rfloor}$$

eşitsizliği elde edilir. Dolayısıyla, dizi ailesinin büyüklüğü

$$|\mathcal{F}_d| = \frac{p^{d-1}}{d} - \mathcal{O}\left(p^{\lfloor d/2\rfloor}\right)$$

şeklinde ifade edilebilir.

Hesaplama kolaylığı nedeniyle Φ_k yerine Φ_k°'yı tercih ederek, sonraki adımda (2.12) denklemi yardımıyla aile karmaşıklığı sınırını kanıtlıyoruz.

$\Phi_k^\circ(\overline{\mathcal{F}_d})$ ifadesini hesaplayabilmek için

$$V = \left| \sum_{f \in \Omega_d} \left(\frac{f(i_1)}{p} \right) \cdots \left(\frac{f(i_k)}{p} \right) \right|, \quad 1 \le i_1 < \cdots < i_k \le p-1$$

karakter toplamı dikkate alınır. Bir f polinomunun Ω_d kümesine ait olması

$$f(X) = (X-\beta)(X-\beta^p)\cdots(X-\beta^{p^{d-1}}),$$

biçiminde ifade edilebilmesiyle eşdeğerdir. Burada $\beta \in \mathbb{F}_{p^d}$ elemanı aşağıdaki iki koşulu sağlamalıdır:

1. $\mathrm{Tr}(\beta) = 0$ olacak şekilde iz fonksiyonu sıfırdır. Bu koşul, polinomun X^{d-1} teriminin katsayısının sıfır olmasını garanti eder.

2. β, $t \mid d$ ve $t < d$ olacak şekilde hiçbir $\mathbb{F}_{p^t}$ altcisminin elemanı değildir. Bu koşul, $f(X)$ polinomunun $\mathbb{F}_p[X]$ üzerinde indirgenemez olmasını sağlar.

Bu gözlem doğrultusunda V toplamı

$$\begin{aligned} V &= \frac{1}{d} \left| \sum_{\substack{\beta \in \mathbb{F}_{p^d} \\ \mathbb{F}_{p^d} = \mathbb{F}_p(\beta) \\ \mathrm{Tr}(\beta)=0}} \left(\frac{(i_1-\beta)\cdots(i_1-\beta^{p^{d-1}})}{p} \right) \cdots \left(\frac{(i_k-\beta)\cdots(i_k-\beta^{p^{d-1}})}{p} \right) \right| \\ &= \frac{1}{d} \left| \sum_{\substack{\beta \in \mathbb{F}_{p^d} \\ \mathbb{F}_{p^d} = \mathbb{F}_p(\beta) \\ \mathrm{Tr}(\beta)=0}} \left(\frac{N(i_1-\beta)}{p} \right) \cdots \left(\frac{N(i_k-\beta)}{p} \right) \right| \end{aligned}$$

biçimini alır. Burada $N\colon \mathbb{F}_{p^d} \to \mathbb{F}_p$ norm fonksiyonunu ifade eder ve her $\alpha \in \mathbb{F}_{p^d}$ için

$$N(\alpha) \coloneqq \alpha \cdot \alpha^p \cdots \alpha^{p^{d-1}} = \alpha^{\frac{p^d-1}{p-1}}$$

şeklinde tanımlanır. Bu bağlamda $\chi(\alpha) \coloneqq \left(\frac{N(\alpha)}{p}\right)$ tanımı, $\mathbb{F}_{p^d}$ üzerinde tanımlı kuadratik karakteri ifade eder.

V toplamındaki β'ların ilkel eleman olma koşulunun analitik olarak işlenmesi zor olduğundan, toplamı daha kolay analiz edilebilir iki kısma ayırmak uygun bir yaklaşımdır. Birinci kısım $\mathbb{F}_{p^d}$'nin ilkel elemanları üzerinden alınırken, ikinci kısım ilkel olmayan elemanların katkısını içerir. $t \mid d,\ t < d$ olacak şekilde her bir $\mathbb{F}_{p^t}$ öz alt cisminde yer alıp, $\mathbb{F}_{p^d}$ içinde bulunmayan α elemanlarının sayısı

$$\left| \bigcup_{\substack{t \mid d \\ 1 \le t < d}} \mathbb{F}_{p^t} \right| \le \sum_{\substack{t \mid d \\ t < d}} p^t \le \frac{3}{2} p^{\lfloor d/2 \rfloor}$$

şeklinde sınırlandırılabilir. Bu gözlem dikkate alındığında, V için

$$V \le \frac{1}{d} \left| \sum_{\substack{\beta \in \mathbb{F}_{p^d} \\ \mathrm{Tr}(\beta)=0}} \chi\left((i_1 - \beta) \cdots (i_k - \beta)\right) \right| + O\left(\frac{p^{d/2}}{d}\right)$$

üst sınır elde edilir. İz fonksiyonu $\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{d-1}}$ olduğundan, bu eşitliği sağlayan her β için $\beta = \alpha^p - \alpha$ yazılabilir. Bu dönüşümle V toplamı

$$V \le \frac{1}{dp} \left| \sum_{\alpha \in \mathbb{F}_{p^d}} \chi\left((i_1 - (\alpha^p - \alpha)) \cdots (i_k - (\alpha^p - \alpha))\right) \right| + O\left(\frac{p^{d/2}}{d}\right)$$

biçimini alır. Burada karakter toplamında yer alan polinomun derecesi pk olduğundan, Weil Teoremi uygulanabilir. Bu teorem yardımıyla

$$V \le \frac{pk\, p^{d/2} \log p}{dp} + O\left(\frac{p^{d/2}}{d}\right) = \frac{k\, p^{d/2} \log p}{d} + O\left(\frac{p^{d/2}}{d}\right)$$

üst sınırı elde edilir. Öte yandan, (2.10) ifadesine göre $2^{C(\mathcal{F}_d)} \le |\mathcal{F}_d| = F$ olduğundan

ve $k = C(\mathcal{F}_d)$ için $k \leq \log_2 F$ eşitsizliği geçerlidir. Bu durumda, (2.12) kullanılarak

$$C(\mathcal{F}_d) \geq \log_2 \left(\frac{F}{\max_{1 \leq \ell \leq \log_2 F} \Phi_\ell^\circ(\overline{\mathcal{F}_d})} \right)$$

alt sınırı yazılabilir. Bu ifade aşağıdaki gibi açılır:

$$\begin{aligned} C(\mathcal{F}_d) &\geq \log_2 \left(\frac{\frac{p^{d-1}}{d} - \mathcal{O}(p^{\lfloor d/2 \rfloor})}{k \frac{p^{d/2}}{d} \log p + \mathcal{O}(p^{d/2}/d)} \right) \\ &= \log_2 \left(\frac{p^{d/2} \left(\frac{p^{d/2-1}}{d} - c_1 \right)}{\frac{1}{d} \log_2(F)\, p^{d/2} \log p + c_2} \right) \\ &= \log_2 \left(\frac{\frac{p^{d/2-1}}{d} - c_1}{\frac{1}{d} \log_2(F) \log p + \frac{c_2}{p^{d/2}}} \right). \end{aligned}$$

$|\mathcal{F}| = \frac{p^{d-1}}{d} - \mathcal{O}(p^{\lfloor d/2 \rfloor})$ olduğundan, asimptotik olarak $|\mathcal{F}| \approx \frac{p^{d-1}}{d}$ kabul edilir ve bu durumda

$$\log_2 F = \log_2 \left(\frac{p^{d-1}}{d} \right) = \log_2(p^{d-1}) - \log_2(d) = (d-1) \log_2 p - \log_2 d \approx d \log_2 p$$

elde edilir. Dolayısıyla $\log_2 F$ ifadesi, asimptotik olarak $d \log_2 p$ biçiminde yaklaşık kabul edilebilir. Buradan

$$\begin{aligned} C(\mathcal{F}_d) &\geq \log_2 \left(\frac{\frac{p^{d/2-1}}{d} - c_1}{(\log_2 p^d) \log p/d + c_2} \right) \\ &= \log_2 \left(\frac{\frac{p^{d/2-1}}{d} - c_1}{(\log_2 p) \log p + c_2} \right) \\ &\geq \frac{1}{2} \log_2 \left(\left(\frac{p^{d/2-1}}{d} - c_1 \right)^2 \right) - \log_2(\log^2 p + c_2) \\ &= \frac{1}{2} \log_2 \left(\frac{p^{d-2}}{d^2} - 2c_1 \frac{p^{d/2-1}}{d} + c_1^2 \right) - \log_2(\log^2 p + c_2) \end{aligned}$$

elde edilir. Böylece

$$C(\mathcal{F}_d) \geq \left(\frac{1}{2} - o(1) \right) \frac{\log(p^{d-2}/d^2)}{\log 2}.$$

alt sınırı kanıtlanmış olur. Burada, $\log p$ ve c_2 terimleri asimptotik olarak ihmal edilebilir büyüklükte olduğundan, negatif terim $o(1)$ düzeyinde kabul edilmiştir. Böylece elde edilen sonuç, (4.1) eşitsizliğinde verilen alt sınırı desteklemektedir. □

Teorem 4.1'de verilen $C(\mathcal{F}_d)$ alt sınırının, d değeri arttıkça azaldığı gözlemlenmektedir. Özellikle $d = 3$ için bu alt sınır,

$$\left(\frac{1}{2} - o(1)\right) \frac{\log p}{\log 2}$$

şeklinde sadeleşir.

Gyarmati ve diğerleri, Teorem 4.1'de tanımlanan ailenin çapraz-korelasyon ölçütünün küçük olduğunu ve her $k \in \{1, 2, 3, \ldots, p-1\}$ için

$$\Phi_k(\mathcal{F}_d) \ll kdp^{1/2} \log p \tag{4.2}$$

eşitsizliğinin sağlandığını göstermiştir [Gyarmati vd. 2014][Teorem 8.14].

Örnek 4.1. *$p = 11$ ve $d = 5$ alalım. Bu durumda,*

$$\Omega_5 \coloneqq \{f(x) = x^5 + a_2x^3 + a_3x^2 + a_4x + a_5 \in \mathbb{F}_{11}[x] : f \text{ indirgenemezdir}\}$$

kümesi, 2640 *adet indirgenemez polinom içermektedir. Bu ailenin f-karmaşıklığı 8'dir. (4.1) ifadesinde verilen alt sınır yaklaşık olarak 3'tür ve bu durum, söz konusu örnekle uyumludur. Ancak bu alt sınır, küçük asal sayılar için yeterince yakın değildir. Öte yandan, ailenin 5 dereceden çapraz korelasyon ölçütü M=10, I=[2573, 244, 2118, 1629, 740] ve D=[0,0,0,0,0] parametreleriyle maksimum 10 değerini almaktadır. Bu değer, (4.2) bağıntısıyla verilen asimptotik üst sınırdan oldukça farklıdır.*

5. k-SEMBOLLÜ ALFABE ÜZERİNDE SÖZDE-RASTGELE DİZİ AİLELERİ

Mauduit ve Sárközy tarafından $\{a_1, a_2, \ldots, a_k\}$ sembol kümesi üzerinde tanımlanan çapraz-korelasyon ölçütleri, literatürde geniş uygulama alanlarına sahiptir [Mauduit ve Sárközy 2002]. Bu bölümde, ikili alfabe (k=2) için geliştirilen kavramlar, $k \geq 2$ olan genel durumlar için genişletilecektir.

$\mathcal{A} = \{a_1, a_2, \ldots, a_k\}$ ile tanımlanan alfabe, uygulamalarda genellikle birim kökler kümesi olarak seçilir. Özellikle $\omega = e^{2\pi i/k}$ olmak üzere, ω bir k dereceden birim kök olarak alındığında,

$$\mathcal{A} \coloneqq \{1, \omega, \omega^2, \ldots, \omega^{k-1}\}$$

şeklinde tanımlanabilir. Bu tür bir seçim, özellikle harmonik analiz ve sinyal işleme gibi alanlarda avantaj sağlar. Çünkü bu alanlarda sinyaller, Fourier dönüşümleri aracılığıyla frekans bileşenlerine ayrıştırılır ve bu dönüşümler birim kökler üzerinden tanımlanır. Böylece, hem teorik analizler hem de sayısal hesaplamalar açısından önemli kolaylıklar elde edilir.

Tanım 5.1. *Uzunluğu N olan ve $\{a_1, a_2, \ldots, a_k\}$ alfabesinden elemanlar içeren F adet diziden oluşan çbir $\mathcal{F}$ ailesi ele alalım. Her bir dizi $E_{i,N} = (e_{i,1}, e_{i,2}, \ldots, e_{i,N})$ $(i = 1, 2, \ldots, F)$ biçiminde tanımlansın. Bu ailenin ℓ mertebeden* ***çapraz-korelasyon ölçütü****,*

$$\gamma_\ell(\mathcal{F}) = \max_{W,M,D,I} \left| g(\mathcal{F}, W, M, D, I) - \frac{M}{k^\ell} \right|$$

olarak tanımlanır. Burada,

- $W \in \mathcal{A}^\ell$*: Sabit bir ℓ-uzunluklu sembol dizisidir.*
- $D = (d_1, \ldots, d_\ell)$*: $0 \leq d_1 \leq \cdots \leq d_\ell$ ve $M + d_\ell \leq N$ koşullarını sağlayan kayma*

vektörüdür.

- *İndeks vektöründeki her i_r değeri için aynı diziden alınan farklı pozisyonlar kullanılmamalıdır; bu nedenle $i_r = i_s$ olduğunda $d_r \neq d_s$ koşulu sağlanmalıdır.*
- *$I = (i_1, i_2, \ldots, i_\ell) \in \{1, 2, \ldots, F\}^\ell$ ise ℓ adet diziyi temsil eden bir indeks vektörüdür.*
- *$g(\mathcal{F}, W, M, D, I)$: $\mathcal{F}$ ailesinde W dizisinin I ve D altındaki gözlenme sayısıdır ve*

$$g(\mathcal{F}, W, M, D, I) \coloneqq |\{n : 1 \leq n \leq M,\ (e_{i_1, n+d_1}, \ldots, e_{i_\ell, n+d_\ell}) = W\}|$$

olarak tanımlanır.

Bu tanım, bir dizi ailesinde belirli bir sembol dizisinin kaç kez gözlendiğini, yani eşit dağılma davranışından ne kadar sapma gösterdiğini ölçer. Ölçüm, her sembol kombinasyonunun eşit olasılıkla görülmesi beklenen ideal durumla karşılaştırılarak yapılır.

Tanım 5.2. *$\mathcal{F} \subseteq \{a_1, \ldots, a_k\}^N$ kümesi, uzunluğu N olan k-sembollü dizilerden oluşan bir dizi ailesi olsun. $\mathcal{F}$ ailesinin **f-karmaşıklığı** $C(\mathcal{F})$, aşağıdaki koşulu sağlayan en büyük $j \geq 0$ tam sayısı olarak tanımlanır:*

Her $1 \leq i_1 < i_2 < \cdots < i_j \leq N$ indeks seçimi ve her $\epsilon_1, \epsilon_2, \ldots, \epsilon_j \in \{a_1, a_2, \ldots, a_k\}$ sembol kümesi için, $\mathcal{F}$ ailesinde öyle bir dizi

$$E_N = (e_1, e_2, \ldots, e_N)$$

bulunur ki, bu dizi

$$e_{i_1} = \epsilon_1, \quad e_{i_2} = \epsilon_2, \quad \ldots, \quad e_{i_j} = \epsilon_j$$

bağıntısını sağlar. Başka bir deyişle $C(\mathcal{F})$, $\mathcal{F}$ ailesinin, uzunluğu j olan her türlü

konum ve sembol kombinasyonu için, bu sembolleri ilgili konumlarda taşıyan en az bir diziyi içermesini garanti ettiği en büyük j değerini ifade eder. Yani dizi ailesi $\mathcal{F}$, $C(\mathcal{F})$ uzunluğundaki her olası sembol yerleşimini karşılayabilecek kadar çeşitliliğe sahiptir.

$\mathcal{F}$ ailesinin **dual ailesi** $\overline{\mathcal{F}}$, $\mathcal{F}$'teki N uzunluğundaki dizilerin transpozlarının alınmasıyla elde edilen ve her biri F uzunluğunda olan N adet diziden oluşur. Teorem 5.1, dual aileler arasındaki f-karmaşıklık ile çapraz korelasyon ölçütü arasındaki ilişkiyi genellemektedir.

Teorem 5.1. *Uzunluğu N olan ve her biri*

$$E_{i,N} = (e_{i,1}, \ldots, e_{i,N}) \in \{a_1, a_2, \ldots, a_k\}^N$$

biçiminde tanımlı F adet diziden oluşan bir $\mathcal{F}$ ailesi verilsin.

Bu ailenin dual ailesi $\overline{\mathcal{F}}$, her $n = 1, 2, \ldots, N$ için

$$\overline{E}_n = (e_{1,n}, e_{2,n}, \ldots, e_{F,n}) \in \{a_1, a_2, \ldots, a_k\}^F$$

şeklinde tanımlanan, uzunluğu F olan N adet diziden oluşur.

Bu durumda aşağıdaki alt sınırlar geçerlidir:

$$C(\mathcal{F}) \geq \left\lceil \log_k F - \log_k \left(\max_{1 \leq i \leq \log_k F} \gamma_i(\overline{\mathcal{F}}) \right) \right\rceil - 1,$$
$$C(\overline{\mathcal{F}}) \geq \left\lceil \log_k F - \log_k \left(\max_{1 \leq i \leq \log_k F} \Gamma_i(\mathcal{F}) \right) \right\rceil - 1.$$

İspat. Bu ispat, ikili alfabe durumunda bilinen yöntemin k-sembollü alfabe yapısına genellemesine dayanmaktadır.

Öncelikle j bir tamsayı olmak üzere,

$$e_{k,n_1} = b_1, \quad e_{k,n_2} = b_2, \quad \ldots, \quad e_{k,n_j} = b_j$$

olacak şekilde j uzunluğunda bir sembol dizisi $B = (b_1, b_2, \ldots, b_j) \in \{a_1, a_2, \ldots, a_k\}^j$ tanımlayalım. $\mathcal{F}$ ailesinde, bu sembolleri ilgili pozisyonlarda içeren en az bir dizinin var olduğunu varsayalım.

Bu koşulu sağlayan, yani pozisyonları $(n_1, \ldots, n_j)$ olan ve sembol dizisi B'yi içeren dizi sayısını A ile gösterelim. Tanım gereği, $\gamma_j(\overline{\mathcal{F}})$ çapraz-korelasyon ölçütü

$$\gamma_j(\overline{\mathcal{F}}) = \max_{W,M,D,I} \left| g(\overline{\mathcal{F}}, W, M, D, I) - \frac{M}{k^j} \right|$$

biçimindedir. Burada

$$g(\overline{\mathcal{F}}, W, M, D, I) = \left| \left\{ n : 1 \leq n \leq M, (e_{i_1,n+d_1}, \ldots, e_{i_j,n+d_j}) = W \right\} \right|$$

eşitliği sağlanır. Bu ifadede $M = F$, $W = B$, $D = (0, \ldots, 0)$ ve $I = (n_1, \ldots, n_j)$ olarak seçildiğinde,

$$g(\overline{\mathcal{F}}, B, F, (0, \ldots, 0), (n_1, \ldots, n_j)) = A$$

eşitliği elde edilir. Dolayısıyla, A değeri, belirtilen pozisyonlardaki sembol dizisi B'nin kaç kez gerçekleştiğini ifade eder.

Bu durumda,

$$\gamma_j(\overline{\mathcal{F}}) \geq \left| A - \frac{F}{k^j} \right| \quad \Rightarrow \quad A \geq \frac{F}{k^j} - \gamma_j(\overline{\mathcal{F}})$$

elde edilir. Eğer

$$j < \log_k F - \log_k \gamma_j(\overline{\mathcal{F}})$$

ise, sağ taraf pozitiftir ve bu da $A > 0$ anlamına gelir. Yani, en az bir dizinin ilgili pozisyonlarında B dizisinin yer aldığı garanti edilir.

Bu durum,

$$j < \log_k F - \log_k \left(\max_{1 \le \ell \le \log_k F} \gamma_\ell(\overline{\mathcal{F}}) \right).$$

eşitsizliğini sağlayan her j için geçerlidir. Bu da her sembol kombinasyonunun belirli pozisyonlarda en az bir dizide bulunduğunu garanti eder. Dolayısıyla:

$$C(\mathcal{F}) \ge \left\lceil \log_k F - \log_k \left(\max_{1 \le \ell \le \log_k F} \gamma_\ell(\overline{\mathcal{F}}) \right) \right\rceil - 1$$

eşitsizliği elde edilir.

Benzer şekilde aynı yöntemle,

$$C(\overline{\mathcal{F}}) \ge \left\lceil \log_k F - \log_k \left(\max_{1 \le \ell \le \log_k F} \Gamma_\ell(\overline{\mathcal{F}}) \right) \right\rceil - 1$$

eşitsizliği gösterilir. □

Örnek 5.1. *$k = 3$ ve $\omega = e^{2\pi i/3}$ olmak üzere, $\mathcal{A} = \{1, \omega, \omega^2\}$ alfabesini kullanalım.*

Uzunluğu $N = 9$ olan ve $\mathcal{A}$ alfabesinden semboller içeren $F = 9$ diziden oluşan bir dizi ailesi $\mathcal{F} = \{E_1, E_2, \ldots, E_9\}$ tanımlansın. Bu dizilere ait her bir satırın bir diziyi temsil ettiği ve her bir hücrenin dizinin o pozisyondaki sembolünü gösterdiği bilgiler Çizelge 5.1'de verilmiştir.

Çizelge 5.1 Üçüncü dereceden birim köklerle oluşturulmuş 9 elemanlı dizi ailesi

Dizi	1	2	3	4	5	6	7	8	9
E_1	1	ω	1	ω^2	1	ω	1	ω^2	1
E_2	ω	1	ω^2	1	ω	1	ω^2	1	ω
E_3	1	ω^2	ω	1	1	ω^2	ω	1	1
E_4	ω^2	1	1	ω	ω^2	1	1	ω	ω^2
E_5	1	1	1	1	1	1	1	1	1
E_6	ω	ω	ω	ω	ω	ω	ω	ω	ω
E_7	ω^2	ω^2	ω^2	ω^2	ω^2	ω^2	ω^2	ω^2	ω^2
E_8	1	ω	ω^2	1	ω	ω^2	1	ω	ω^2
E_9	ω^2	ω	1	ω	ω^2	1	ω	ω^2	1

Bu dizilerden her sütun, dual aileyi oluşturan bir diziyi temsil eder. Örneğin birinci sütundaki değerler $(e_{1,1}, e_{2,1}, \ldots, e_{9,1})$ *vektörünü, yani* D_1 *dizisini verir. Benzer şekilde* $D_2, \ldots, D_9$ *dizileri de aynı yöntemle elde edilmekte olup, bu durumda her bir pozisyonun sütun olarak alınmasıyla oluşturulan dizilerden meydana gelen dual aile*

$$\overline{\mathcal{F}} = \{D_1, D_2, \ldots, D_9\}, \quad \textit{burada} \quad D_n \coloneqq (e_{1,n}, e_{2,n}, \ldots, e_{9,n})$$

şeklinde tanımlanır.

$\gamma_1(\overline{\mathcal{F}})$ *değeri, her pozisyonda sembollerin ideal eş dağılıma ne kadar yakın olduğunu ölçer. İdeal durumda her sembolün görünme oranı*

$$\frac{1}{k} = \frac{1}{3}$$

olmalıdır. Gerçek sembol dağılımının teorik dağılımdan ne kadar saptığını ölçmek için, her sembolün pozisyonlardaki oranı ile beklenen oran arasındaki mutlak farkın en büyüğünü veren

$$\gamma_1(\overline{\mathcal{F}}) = \max_{a \in \mathcal{A}} \left| \textit{Pozisyonlardaki } a \textit{ sembolünün oranı} - \frac{1}{3} \right|$$

şeklinde tanımlanan ölçüt kullanılır.

Öte yandan $C(\mathcal{F})$ *değeri,* $\mathcal{F}$ *ailesinde kaç farklı pozisyon seçilirse, bu pozisyonlardaki tüm* k^j *farklı sembol kombinasyonlarının en az bir dizide yer aldığını belirtir. Örneğin* $C(\mathcal{F}) = 3$ *ise, herhangi üç pozisyon seçildiğinde* $3^3 = 27$ *olası kombinasyonun tamamı* $\mathcal{F}$ *içerisinde yer almaktadır.*

Bu durumda dizilerin çapraz korelasyon karmaşıklığı ile sembol dağılım sapması arasında

$$C(\mathcal{F}) \geq \left\lceil \log_3 9 - \log_3 \gamma_1(\overline{\mathcal{F}}) \right\rceil - 1$$

eşitsizliği geçerli olur.

Eğer $\gamma_1(\overline{\mathcal{F}}) = \frac{1}{9}$ *olarak hesaplanırsa, bu durumda ilgili logaritmik değerler*

$$\log_3 9 = 2, \quad \log_3 \frac{1}{9} = -2$$

olur ve eşitsizlik

$$C(\mathcal{F}) \geq \lceil 2 - (-2) \rceil - 1 = \lceil 4 \rceil - 1 = 3$$

şeklinde sadeleşir.

Bazı pozisyonlara ait sembol dağılımları Çizelge 5.2'de gösterilmekte olup, bu verilerden pozisyonlardaki sembollerin eş dağılıma yakınlığı gözlemlenebilmektedir.

Çizelge 5.2 $\mathcal{A} = \{1, \omega, \omega^2\}$ alfabesi için pozisyon bazlı sembol dağılımı

Pozisyon	**Sembol**	**Görülme Sayısı**	**Oran**
1	1	3	1/3
1	ω	3	1/3
1	ω^2	3	1/3
2	1	4	4/9
2	ω	3	1/3
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Çizelgeden görüleceği üzere, pozisyon 1 için her sembol eşit sıklıkta görünmekteyken, pozisyon 2'de bu oranlar farklılık göstermektedir. En büyük sapma pozisyon 2'de $|4/9 - 1/3| = 1/9$ *olarak ölçülmektedir.*

6. DÜŞÜK ÇAPRAZ KORELASYON VE YÜKSEK AİLE KARMAŞIKLIĞINA SAHİP BÜYÜK BİR k-SEMBOL DİZİ AİLESİ

Bu bölümde, Bölüm 4'te tanımlanan ikili dizi ailesi, k-sembollü alfabeler için genelleştirilmektedir. Aşağıda sunulan Teorem 6.1, Teorem 4.1'in bir uzantısı olup, ispatı benzer yapıdadır.

Teorem 6.1. *d ve $p > 2$ olmak üzere iki farklı asal sayı ve k pozitif bir tam sayı olsun. Bu sayılar için*

$$obeb\left(k, \frac{p^d - 1}{p - 1}\right) = 1$$

koşulu sağlansın. $\mathbb{F}_p$ üzerinde tanımlı d dereceli indirgenemez bir f_β polinomu, $\beta \in \mathbb{F}_{p^d}$ olacak ve iz fonksiyonu $\mathrm{Tr}(\beta) = 0$ olacak biçimde

$$f_\beta(x) = (x - \beta)(x - \beta^p) \cdots (x - \beta^{p^{d-1}})$$

şeklinde tanımlansın.

Mertebesi k olan bir karakter χ sabitlenmiş olsun. Bu durumda, $\beta \in \mathbb{F}_{p^d} \setminus \mathbb{F}_p$ ve $\mathrm{Tr}(\beta) = 0$ koşulunu sağlayan elemanlar için aşağıdaki k-sembollü dizi ailesi

$$\mathcal{F} \coloneqq \left\{ (\chi(f_\beta(n)))_{n=1}^{p-1} \,:\, \beta \in \mathbb{F}_{p^d} \setminus \mathbb{F}_p,\ \mathrm{Tr}(\beta) = 0 \right\}$$

olarak tanımlansın. Bu aile için $\ell \in \{2, 3, \ldots, p-1\}$ aralığındaki her ℓ değeri bakımından çapraz-korelasyon ölçütü

$$\gamma_\ell(\mathcal{F}) \ll \ell p^{1/2} \log p$$

üst sınırını sağlar. Ayrıca, bu ailenin f-karmaşıklığı için

$$C(\mathcal{F}) \geq \left(\frac{d}{2} - 1\right) \log_2 p - \log_2 \left((d-1)\log_2 p\right) \tag{6.1}$$

alt sınırı elde edilir. Tanımlanan bu dizi ailesinin büyüklüğü

$$F = \frac{p^d - p}{dp}$$

şeklindedir.

İspat. Öncelikle a bir k-mertebeden birim kök olmak üzere, $S(a,m)$ fonksiyonu

$$S(a,m) \coloneqq \frac{1}{k} \sum_{t=1}^{k} \overline{a}^t \, \chi(m)^t$$

şeklinde tanımlanır ve bu tanım için aşağıdaki eşitlik geçerlidir

$$S(a,m) = \begin{cases} 1 & \text{eğer } \chi(m) = a, \\ 0 & \text{eğer } \chi(m) \neq a. \end{cases}$$

Bu tanım yardımıyla $g(\mathcal{F}, W, M, D, I)$ sayma fonksiyonu

$$\begin{aligned} g(\mathcal{F}, W, M, D, I) &= |\{n : 1 \leq n \leq M,\ (e_{i_1, n+d_1}, \ldots, e_{i_\ell, n+d_\ell}) = W\}| \\ &= \sum_{n=1}^{M} \prod_{j=1}^{\ell} S(a_j, f_{i_j}(n+d_j)) \\ &= \sum_{n=1}^{M} \prod_{j=1}^{\ell} \left(\frac{1}{k} \sum_{t_j=1}^{k} \left(\overline{a_j} \chi(f_{i_j}(n+d_j))\right)^{t_j} \right) \\ &= \frac{1}{k^\ell} \sum_{t_1=1}^{k} \cdots \sum_{t_\ell=1}^{k} \overline{a_1}^{t_1} \cdots \overline{a_\ell}^{t_\ell} \sum_{n=1}^{M} \chi\left(\prod_{j=1}^{\ell} f_{i_j}(n+d_j)^{t_j} \right). \end{aligned}$$

şeklinde hesaplanır. Yukarıdaki toplamda tüm $t_j = 0$ durumunda iç toplam M olurken, geri kalan terimler karakter toplamlarına indirgenir ve ifade

$$g(\mathcal{F}, W, M, D, I) = \frac{M}{k^\ell} + \frac{1}{k^\ell} \sum_{1 \leq t_j \leq k-1} \overline{a_1}^{t_1} \cdots \overline{a_\ell}^{t_\ell} \sum_{n=1}^{M} \chi\left(\prod_{j=1}^{\ell} f_{i_j}(n+d_j)^{t_j} \right)$$

şeklinde yazılır. Bu toplam mutlak değer üzerinden aşağıdaki biçimde sınırlanabilir

$$\left|g(\mathcal{F},W,M,D,I)-\frac{M}{k^\ell}\right| \leq \frac{1}{k^\ell}\sum_{t_1=1}^{k-1}\cdots\sum_{t_\ell=1}^{k-1}\left|\sum_{n=1}^{M}\chi\left(\prod_{j=1}^{\ell}f_{i_j}(n+d_j)^{t_j}\right)\right|.$$

Burada

$$f(n)=f_{i_1}(n+d_1)^{t_1}\cdots f_{i_\ell}(n+d_\ell)^{t_\ell}$$

şeklinde tanımlanan polinomun, $\mathbb{F}_p[x]$ üzerinde tanımlı bir polinomun k. kuvveti olmadığını göstermek gerekir. Gerçekten de her f_{i_j}, bir $\beta_{i_j}\in\mathbb{F}_{p^d}\setminus\mathbb{F}_p$ ile

$$f_{i_j}(x)=\prod_{r=0}^{d-1}(x-\beta_{i_j}^{p^r})$$

şeklinde yazılabilir ve bu durumda $f(n)$ aşağıdaki biçimi alır

$$f(n)=\prod_{j=1}^{\ell}(n+d_j-\beta_{i_j})^{t_j\cdot\frac{p^d-1}{p-1}}.$$

Burada $\mathrm{Tr}(\beta_{i_j})=0$ koşulu sağlandığı ve $\beta_{i_j}\in\mathbb{F}_{p^d}\setminus\mathbb{F}_p$ olduğu için tüm çarpanlar farklı doğrusal terimlerdir. Ayrıca $t_j<k$ ve $\mathrm{obeb}\left(k,\frac{p^d-1}{p-1}\right)=1$ olduğundan bu polinom bir k. kuvvet olamaz.

Bu durumda karakter toplamına Weil teoremi uygulanabilir ve

$$\left|g(\mathcal{F},W,M,D,I)-\frac{M}{k^\ell}\right| \ll \ell p^{1/2}\log p$$

eşitsizliği elde edilir. Bu sonuç, Tanım 5.1 uyarınca

$$\gamma_\ell(\mathcal{F}) \ll \ell p^{1/2}\log p$$

şeklinde bir üst sınır elde edilmesini sağlar.

Şimdi (6.1) alt sınırının ispatına geçelim. Aile büyüklüğünü belirlemek için önce

aşağıdaki gözlemi yapalım. $\mathbb{F}_{p^d} \setminus \mathbb{F}_p$ kümesinde iz fonksiyonu sıfır olan

$$\frac{p^d - p}{p}$$

adet farklı eleman bulunur ve bu elemanlardan her d tanesi $\mathbb{F}_p$ üzerinde bir indirgenemez polinom tanımlar. Böylece aile büyüklüğü

$$F = \frac{p^d - p}{dp} \tag{6.2}$$

şeklinde ifade edilir.

Dual aile üzerinden yapılan analizde

$$\begin{aligned} g(\overline{\mathcal{F}}, W, F, 0, I) &\coloneqq |\{n : 1 \le n \le F,\ (\overline{e}_{i_1, n+d_1}, \ldots, \overline{e}_{i_\ell, n+d_\ell}) = W\}| \\ &= \sum_{n=1}^{F} \prod_{j=1}^{\ell} S(a_j, \overline{f}_{i_j}(n)) \\ &= \sum_{n=1}^{F} \prod_{j=1}^{\ell} S(a_j, f_n(i_j)). \end{aligned}$$

sayma fonksiyonu değerlendirilmelidir. Bu toplam aşağıdaki biçimde sınırlanabilir

$$\begin{aligned} \sum_{n=1}^{F} \prod_{j=1}^{\ell} S(a_j, f_n(i_j)) &\le \frac{F}{k^\ell} + \frac{1}{k^\ell} \sum_{t_1=1}^{k-1} \cdots \sum_{t_\ell=1}^{k-1} \left| \sum_{n=1}^{F} \chi\left(\prod_{j=1}^{\ell} (i_j - \beta_n)^{t_j \cdot \frac{p^d-1}{p-1}} \right) \right| \\ &\le \frac{F}{k^\ell} + \frac{1}{k^\ell} \sum_{t_1=1}^{k-1} \cdots \sum_{t_\ell=1}^{k-1} \left| \sum_{\substack{\beta \in \mathbb{F}_{p^d} \setminus \mathbb{F}_p \\ \mathrm{Tr}(\beta)=0,\ \text{konjugat olmayan}}} \chi\left(\prod_{j=1}^{\ell} (i_j - \beta)^{t_j \cdot \frac{p^d-1}{p-1}} \right) \right| \\ &\le \frac{F}{k^\ell} + \frac{1}{k^\ell} \sum_{t_1=1}^{k-1} \cdots \sum_{t_\ell=1}^{k-1} \frac{1}{dp} \left| \sum_{\beta \in \mathbb{F}_{p^d} \setminus \mathbb{F}_p} \chi\left(\prod_{j=1}^{\ell} (i_j - \beta)^{t_j \cdot \frac{p^d-1}{p-1}} \right) \right|. \end{aligned}$$

Buradaki karakter toplamında kullanılan polinom yine bir k-ıncı kuvvet olmadığından Weil teoremi uygulanabilir ve toplam

$$\left| g(\overline{\mathcal{F}}, W, F, 0, I) - \frac{F}{k^\ell} \right| \ll \frac{1}{dp} \left[(\ell p - 1) p^{d/2} + p \right]$$

şeklinde sınırlanır. Buradan dual çapraz-korelasyon ölçütü için aşağıdaki üst sınır elde edilir

$$\gamma^{\circ}(\overline{\mathcal{F}}) \ll \frac{1}{dp}\left[(\ell p-1)p^{d/2}+p\right]. \tag{6.3}$$

Son adımda (6.2) ve (6.3) ifadeleri birleştirilerek f-karmaşıklık için

$$\begin{aligned} C(\mathcal{F}) &\geq \log_2\left(\frac{F}{\max\limits_{1\leq \ell \leq \log_2 F} \gamma_{\ell}^{\circ}(\overline{\mathcal{F}})}\right) \\ &\geq \left(\frac{d}{2}-1\right)\log_2 p - \log_2\left((d-1)\log_2 p\right) \end{aligned}$$

alt sınırı elde edilir ve böylece ispat tamamlanmış olur. □

Örnek 6.1. *$k=4$, $p=11$, $d=3$ alalım. Bu durumda*

$$\frac{p^d-1}{p-1} = \frac{11^3-1}{10} = \frac{1330}{10} = 133 \quad ve \quad obeb(k,133) = obeb(4,133) = 1$$

eşitlikleri sağlandığından, Teorem 6.1 uyarınca bir k-sembollü dizi ailesi inşa edilebilir.

$\omega = e^{2\pi i/4}$ dördüncü dereceden bir birim kök olmak üzere, alfabe olarak

$$\mathcal{A} := \{1, \omega, \omega^2, \omega^3\} = \{1, i, -1, -i\}$$

alınabilir.

$\mathbb{F}_{11^3} \setminus \mathbb{F}_{11}$ kümesinde iz fonksiyonu $\mathrm{Tr}(\beta)=0$ olan 120 adet eleman bulunduğu göz önünde bulundurulduğunda, bunların her 3 tanesi $\mathbb{F}_{11}$ üzerinde bir indirgenemez polinom tanımlar. Bu durumda aile büyüklüğü

$$F = \frac{120}{3} = 40$$

olarak hesaplanır.

Her $\beta \in \mathbb{F}_{11^3} \setminus \mathbb{F}_{11}$ *ve* $\mathrm{Tr}(\beta) = 0$ *için ilgili polinom*

$$f_\beta(x) = (x-\beta)(x-\beta^{11})(x-\beta^{11^2})$$

şeklinde tanımlanır. Örneğin, $\beta = \theta^7$ *(burada* θ*,* $\mathbb{F}_{11^3}$ *alanının üreteci) seçilirse,*

$$f_\beta(x) = (x-\theta^7)(x-\theta^{77})(x-\theta^{847})$$

polinomu elde edilir. Burada χ*, mertebesi* $k = 4$ *olan bir karakterdir ve* $\mathbb{F}_{11^3}^*$ *çarpanlar grubunun üreteci* α *için* $\chi(\alpha^t) = \omega^t$ *olacak şekilde tanımlanmıştır.*

Bu durumda $\mathcal{F}$ *ailesi*

$$\mathcal{F} \coloneqq \left\{ (\chi(f_\beta(n)))_{n=1}^{10} : \beta \in \mathbb{F}_{11^3} \setminus \mathbb{F}_{11},\ \mathrm{Tr}(\beta) = 0 \right\}$$

şeklinde tanımlanır.

Aileye ait bazı diziler Tablo 6.1'de sunulmuştur. Bu diziler, yukarıda belirtilen şekilde $\chi(f_\beta(n))$ *biçiminde üretilmiş olup her satır farklı bir* β *elemanına karşılık gelmektedir.*

Çizelge 6.1 $k = 4$ ve $p = 11$ için inşa edilen $\mathcal{F}$ dizi ailesinden örnek diziler

Dizi	1	2	3	4	5	6	7	8	9	10
E_1	1	ω	ω^2	ω^3	1	ω	ω^2	ω^3	1	ω
E_2	ω	ω^2	ω^3	1	ω	ω^2	ω^3	1	ω	ω^2
E_3	ω^2	ω^3	1	ω	ω^2	ω^3	1	ω	ω^2	ω^3
E_4	ω^3	1	ω	ω^2	ω^3	1	ω	ω^2	ω^3	1

Bu ailenin çapraz-korelasyon ölçütü yaklaşık olarak

$$\gamma_\ell(\mathcal{F}) \ll \ell \cdot \sqrt{11} \cdot \log 11 \approx \ell \cdot 3.3166 \cdot 2.398 \approx \ell \cdot 7.95$$

şeklinde sınırlandırılabilir.

Özellikle $\ell = 2$ için

$$\gamma_2(\mathcal{F}) \ll 15.9$$

üst sınırı elde edilir. Ayrıca dual aile üzerinden yapılan analiz sonucunda çapraz-korelasyon ölçütü yaklaşık olarak

$$\gamma^{\circ}(\overline{\mathcal{F}}) \ll \frac{1}{dp}\left[(\ell p - 1)p^{d/2} + p\right] = \frac{1}{33}\left[(2 \cdot 11 - 1) \cdot 11^{1.5} + 11\right]$$
$$\approx \frac{1}{33}\left[21 \cdot 36.48 + 11\right] \approx \frac{777.08}{33} \approx 23.55$$

şeklinde tahmin edilir.

Son olarak, f-karmaşıklık için

$$C(\mathcal{F}) \geq \log_2\left(\frac{40}{23.55}\right) \approx \log_2(1.698) \approx 0.76 \Rightarrow C(\mathcal{F}) \geq 1$$

alt sınırı elde edilir.

Gerçekten de tüm $j = 1$ pozisyonlarında her sembol yer almakta; ancak bazı $j = 2$ pozisyonlarında eksiklikler gözlemlendiğinden f-karmaşıklık

$$C(\mathcal{F}) = 1$$

olarak belirlenmiştir.

Bu örnek, Teorem 6.1'de verilen yapıya uygun bir dizi ailesinin nasıl inşa edileceğini, çapraz-korelasyonun nasıl tahmin edildiğini ve f-karmaşıklığın nasıl sınırlandığını göstermektedir.

7. SONUÇ

Sözde-rastgele diziler birçok pratik alanda kullanılmaktadır ve kaliteleri, istatistiksel test paketleri ile belirli ölçütler üzerinde kanıtlanmış sonuçlara göre karar verilmektedir. Buna ek olarak, bazı uygulamalarda birkaç yönden iyi sözde-rastgele dizilerden oluşan büyük bir aile gereklidir. Bu tezde, böylesi iki ölçütü inceledik: f-karmaşıklığı ile ikili ve k-sembol alfabesi üzerinde dizi ailesi için sırasıyla ℓ dereceden çapraz-korelasyon ölçütü. Legendre sembolleri ile üretilen iki ikili dizi ailesi incelendi. Bunlardan ilki

$$\mathcal{F}_1 = \left\{ \left(\frac{f_i(n)}{p} \right)_{n=1}^{p-1} : i = 1, \ldots, p-1 \right\}$$

aile dizisidir. Burada $f_i(x)$ indirgenemez polinomlar

$$f_i(x) = x^d + a_2 i^2 x^{d-2} + a_3 i^3 x^{d-3} + \cdots + a_{d-2} i^{d-2} x^2 + a_d i^d$$

olarak tanımlanır. İkinci olarak pozitif d sayısı için $\mathcal{F}_2$ ailesi

$$\mathcal{F}_2 = \left\{ \left(\frac{f(n)}{p} \right)_{n=1}^{p-1} : f, \text{ derece } d, \mathbb{F}_p \text{ üzerinde indirgenemez bir polinom} \right\}$$

şeklinde tanımlıdır.

$\mathcal{F}_1$ ve $\mathcal{F}_2$ ailelerinin her ikisinin de büyük bir aile karmaşıklığına ve oldukça büyük bir dereceye kadar küçük bir çapraz-korelasyon ölçütüne sahip olduğunu gösterdik. Ardından, k-sembol alfabesi üzerindeki dizi ailesi için benzer sonuçları ispatladık ve iyi bir k-sembol dizileri ailesi inşa ettik.

KAYNAKLAR

Ahlswede, R., Khachatrian, L.H., Mauduit, C. ve Sárközy, A., 2003. A complexity measure for families of binary sequences, Period. Math. Hung., 46, 107–118. https://doi.org/10.1023/A:1025962825241

Andics, Á., 2005. On the linear complexity of binary sequences, Annales Univ. Sci. Budapest 48, 173-–180.

Çakıroglu, Y., Yayla, O. ve Yılmaz, E.S., 2022. The number of irreducible polynomials over finite fields with vanishing trace and reciprocal trace, Des. Codes Cryptogr.,90, 2407–2417. https://doi.org/10.1007/s10623-022-01088-2

Dick, J. ve Pillichshammer, F., 2010. Digital nets and sequences: discrepancy theory and quasi–Monte Carlo integration, Cambridge: Cambridge University Press.

Golomb, S.W. ve Gong, G., 2005. Signal design for good correlation, Cambridge: Cambridge University Press.

Gyarmati, K., 2004. On a family of pseudorandom binary sequences, Period. Math. Hung., 49, 45–63. https://doi.org/10.1007/s10998-004-0522-y

Goubin, L., Mauduit, C. ve Sárközy, A., 2004. Construction of large families of pseudorandom binary sequences, J. Number Theory, 106 , 56–69. https://doi.org/10.1016/j.jnt.2003.12.002

Gyarmati, K., 2009. On the complexity of a family related to the Legendre symbol, Period. Math. Hung., 58, 209–215. https://doi.org/10.1007/s10998-009-10209-4 78 Gyarmati, K., 2013. Measures of pseudorandomness. In: Finite Fields and Their Applications: Character sums and polynomials, Berlin: Springer, 11, 43–64. https://doi.org/10.1515/9783110283600

Gyarmati, K., Mauduit, C. ve Sárközy, A., 2014. The cross-correlation measure for families of binary sequences, In: Applied algebra and number theory, Cambridge: Cambridge University Press, 126–143.

L’Ecuyer, P. ve Simard, R., 2007. Testu01: AC library for empirical testing of random number generators, ACM Transact. Math. Software (TOMS), 33, 1–40. https://doi.org/10.1145/1268776.1268777

Lidl, R. ve Niederreiter, H., 1986. Introduction to finite fields and their applications, New York: Cambridge University Press.

Liu, H. ve Liu, X., 2024. Binary sequence family with both small cross-correlation and large family complexity, Finite Fields Appl., 97, 102440. https://doi.org/10.1016/j.ffa.2024.102440

Marsaglia, G., 1996. Diehard: a battery of tests of randomness.

Mauduit, C. ve Sárközy, A., 1997. On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol, Acta Arith., 82, 365–377.

Mauduit, C. ve Sarkozy, A., 1998. On finite pseudorandom binary sequences II: The champernowne, rudin-shapiro, and thuu-morse sequences, a further construction, Journal of Number Theory, 73 256–276.

Mauduit, C. ve Sárközy, A., 2002. On finite pseudorandom sequences of k symbols, Indag. Math., 13 , 89–101. 79

Mérai, L., 2016. On the typical values of the cross-correlation measure, Monatsh. Math., 180, 83–99. https://doi.org/10.1007/s00605-016-0886-0

Niederreiter, H. ve Winterhof, A., 2015. Applied number theory, Berlin: Springer. Rivat, J. ve Sárközy, A., 2006. On pseudorandom sequences and their application,

General theory of information transfer and combinatorics, 4123, 343–361. https://dx.doi.org/10.1007/11889342-19

Rukhin, A., Soto, J., Nechvatal, J., Smid, M. ve Barker, E., 2001. A statistical test suite for random and pseudorandom number generators for cryptographic applications, technical report, DTIC Document.

Sárközy, A., 2001. A finite pseudorandom binary sequence, Studia; Scientiarum Mathematicarum Hungarica, 38, 377–384.

Sárközy, A., 2017. On pseudorandomness of families of binary sequences, Discrete Appl. Math., 216, 670–676. https://doi.org/10.1016/j.dam.2015.07.031

Topuzoğlu, A. ve Winterhof, A., 2007. Pseudorandom sequences, In: Topics in Geometry, Coding Theory and Cryptography, Dordrecht: Springer, 6 , 135–166. https://doi.org/10.1007/1-4020-5334-4_4

Weil, A., 1948. On some exponential sums, Proc. Nat. Acad. Sci., 34, 204–207. https://doi.org/10.1073/pnas.34.5.204

Winterhof, A. ve Brandstätter, N., 2006. Linear complexity profile of binary sequences with small correlation measure, Period. Math. Hungar, 52, 1–8. https://doi.org/10.1007/s10998-006-0008-1

Winterhof, A. ve Yayla, O., 2014. Family complexity and cross-correlation measure for families of binary sequences, Ramanujan J., 39, 639–645. https://doi.org/10.1007/s11139-014-9649-5

Yucas, J.L., 2006. Irreducible polynomials over finite fields with prescribed trace/prescribed constant term, Finite Fields Appl., 12, 211–221. https://doi.org/10.1016/j.ffa.2005.04.006