DENEY FÖYÜ

# Deneyin Adı:

NIST Test Paketlerinin Teorik Olarak İncelenmesi

# Deneyin Amacı:

Bu deneyin amacı, rastgele sayı üreticilerinin kalitesini değerlendirmek amacıyla geliştirilen NIST test paketlerini teorik olarak incelemektir. Testlerin altında yatan matematiksel temeller analiz edilerek, bu testlerin rastgelelik ölçümünde nasıl kullanıldıkları kavranacaktır.

# Teorik Bilgi:

1. NIST Test Paketi Nedir?

* NIST (National Institute of Standards and Technology) tarafından geliştirilen bu test paketi, kriptografik amaçlarla kullanılan rastgele sayıların istatistiksel olarak rastgeleliğini ölçmek için kullanılır. Toplamda 15 farklı test içerir.

2. Neden Kullanılır?

* Kriptografi, güvenlik ve simülasyon gibi alanlarda kullanılan rastgele sayıların gerçekten rastgele olup olmadığını anlamak için.

3. Temel NIST Testleri ve Amaçları:

|  |  |
| --- | --- |
| Test Adı | Açıklama |
| Frequency (Monobit) Test | 0 ve 1 sayılarının dengeli olup olmadığını test eder. |
| Runs Test | Bit dizisinde art arda gelen 0 ve 1’lerin uzunluklarını değerlendirir. |
| Longest Run of Ones | 1’lerin en uzun ardışık dizisini analiz eder. |
| Discrete Fourier Transform | Frekans bileşenleri yardımıyla rastgelelik dışı desenleri inceler. |
| Approximate Entropy | Bit dizisindeki örüntü tekrarlarını ölçerek entropiyi değerlendirir. |
| Cumulative Sums Test (Cusum) | Toplamların yönünü analiz ederek dengesizlik arar. |

4. Matematiksel Temeller:

- Testler genellikle hipotez testi temeline dayanır.  
 - H0 (Null Hypothesis): Bit dizisi rastgeledir.  
 - H1 (Alternative Hypothesis): Bit dizisi rastgele değildir.  
- Test sonuçları genellikle bir p-değeri (p-value) üretir.  
 - Eğer p-değeri > 0.01 ise dizi rastgele kabul edilir.

# Uygulama (Teorik İnceleme):

Her testin algoritmik ve istatistiksel olarak ne yaptığı incelenir. Gerçek bir uygulama yapılmadan, testlerin nasıl çalıştığı, hangi durumlarda başarılı/başarısız oldukları analiz edilir.

# Sonuç ve Yorum:

NIST test paketi, bir rastgele sayı üreticisinin güvenilirliğini ve kalitesini anlamak için çok katmanlı ve güçlü bir yaklaşımdır. Her test farklı bir istatistiksel özelliği ölçtüğünden, üreticinin genel başarımını değerlendirmek için tüm testlerin birlikte yorumlanması gerekir.