**Homework 8: Theory/Research**

**1. Shannon Entropy and Other Diversity Measures**

**Shannon Entropy**

* **Definition**: Shannon entropy measures the **uncertainty** or **information content** of a random variable. It is commonly used in information theory to quantify the diversity, randomness, or unpredictability of a distribution.
* **Formula**:

H(X)=−∑i=1nP(xi)log⁡bP(xi)H(X) = -\sum\_{i=1}^{n} P(x\_i) \log\_b P(x\_i)

where:

* + H(X)H(X): Shannon entropy of random variable XX
  + P(xi)P(x\_i): Probability of occurrence of outcome xix\_i
  + bb: Base of the logarithm (usually 2 for bits, or natural logarithm for nats)
* **Applications**:
  + In machine learning: Understanding feature importance and model uncertainty.
  + In biology: Measuring genetic diversity or species richness.
  + In cryptography: Evaluating randomness in keys.

**Other Diversity Measures**

* **Simpson's Index**: A measure of dominance, giving more weight to common elements in the distribution.

D=∑i=1nP(xi)2D = \sum\_{i=1}^{n} P(x\_i)^2

DD approaches 0 when the diversity is high and 1 when one outcome dominates.

* **Gini-Simpson Index**: Complementary to Simpson's Index, used to measure diversity.

1−D=1−∑i=1nP(xi)21 - D = 1 - \sum\_{i=1}^{n} P(x\_i)^2

* **Renyi Entropy**: A generalization of Shannon entropy.

Hα(X)=11−αlog⁡∑i=1nP(xi)αH\_{\alpha}(X) = \frac{1}{1 - \alpha} \log \sum\_{i=1}^{n} P(x\_i)^{\alpha}

Here, α\alpha determines the weight given to less probable events.

* **Applications of Diversity Measures**:
  + In ecology: Understanding species diversity in ecosystems.
  + In network theory: Analyzing the diversity of connectivity patterns.

**2. Primitive Root Modulo pp**

* **Definition**: A **primitive root modulo pp** (where pp is a prime number) is an integer gg such that every integer aa coprime to pp can be expressed as gkmod  pg^k \mod p for some integer kk.
* **Key Concepts**:
  + **Primitive Root Properties**:
    - g1mod  p,g2mod  p,…,gp−1mod  pg^1 \mod p, g^2 \mod p, \dots, g^{p-1} \mod p generates all integers from 1 to p−1p-1 (mod pp).
    - gg is called a **generator** of the group (Zp∗,⋅)(\mathbb{Z}\_p^\*, \cdot), the set of integers coprime to pp under multiplication modulo pp.
  + **Primitive Roots Count**:
    - The number of primitive roots modulo pp is ϕ(p−1)\phi(p-1), where ϕ\phi is the Euler totient function.
  + **Finding Primitive Roots**:
    - Compute ϕ(p−1)\phi(p-1).
    - Check all integers g∈[2,p−1]g \in [2, p-1].
    - Verify that gkmod  pg^k \mod p generates all values coprime to pp.
* **Examples**:
  + For p=7p = 7:
    - Possible values: 1,2,3,4,5,61, 2, 3, 4, 5, 6.
    - g=3g = 3 is a primitive root because 31mod  7=33^1 \mod 7 = 3, 32mod  7=23^2 \mod 7 = 2, 33mod  7=63^3 \mod 7 = 6, 34mod  7=43^4 \mod 7 = 4, 35mod  7=53^5 \mod 7 = 5, 36mod  7=13^6 \mod 7 = 1.
* **Applications**:
  + **Cryptography**:
    - Used in Diffie-Hellman key exchange and RSA encryption.
  + **Number Theory**:
    - Studying cyclic groups in modular arithmetic.

A screenshot of a computer

Description automatically generated