Notes on Coding Theory, and Cryptography.

Alec Zabel-Mena

September 13, 2020

Chapter 1

Entropy, Uncertainty, and Information.

1.1 Uncertainty.

Suppose that X and Y are distinct random variables such that:

$$P(X = 0) = p \qquad P(X = 1) = 1 - p$$
$$P(Y = 100) = p \qquad P(200) = 1 - p$$

where $0 < p < 1$. We would like to define "uncertainty" for X and Y.

Definition. The **uncertainty** of a random variable Z, which takes values a_i with probabilities p_i for $1 \leq i \leq n$, is a function H if the probabilities p_i such that:

(A1) $H(p_1, \ldots, p_n)$ attains a maximum at $p_1 = \cdots = p_n = \frac{1}{n}$.

(A2) For anny permutation π of $(1, 2, \ldots, n)$ we have that: $H(p_1, \ldots, p_n) = H(p_{\pi(1)}, \ldots, p_{\pi(n)})$. I.e, H is symmetric.

(A3) $H(p_1, \ldots, p_n) \geq 0$ and equals 0 only when $p_i = 1$ for some $1 \leq i \leq n$.

(A4) $H(\frac{1}{n}, \ldots, \frac{1}{n}) \leq H(\frac{1}{n+1}, \ldots, \frac{1}{n+1})$.

(A5) H is a continuous function.

(A6) If $m, n \in \mathbb{Z}^+$, then $H(\frac{1}{mn}, \ldots, \frac{1}{mn}) = H(\frac{1}{m}, \ldots, \frac{1}{m}) + H(\frac{1}{n}, \ldots, \frac{1}{n})$

(A7) Let $p = p_1 + \cdots + p_m$ and $q = q_1 + \cdots + q_n$ with both $p_i, q_i \geq 0$ (for $1 \leq i \leq n$) and $p + q = 1$. Then:

$$H(p_1, \ldots, p_m, q_1, \ldots, q_n) = H(p, q) + pH(\frac{p_1}{p}, \ldots, \frac{p_m}{p}) + qH(\frac{q_1}{q}, \ldots, \frac{q_n}{q})$$

We call H an **entropy function**.

Theorem 1.1.1. *Let H be a function defined over any integer n and all probabilities $p_i \geq 0$ with $1 \leq i \leq n$, and:*

$$\sum_{i=0}^{n} p_i = 1 \tag{1.1}$$

If H is to be an entropy function, then:

$$H(p_1, \ldots, p_n) = -\lambda \sum_k p_k \log p_k \tag{1.2}$$

With λ a positive constant and where the sum is over those k for which $p_k > 0$.

We defer the proof.

Definition. Let X be a random variable taking a finite set of values with probabilities $p_1, \ldots, p_n$. We define the **entropy** (or **uncertainty**) of X to be the function:

$$H(X) = -\sum_k p_k \log_2 p_k \tag{1.3}$$

Where the sum is over all k for which $p_k > 0$.

Theorem 1.1.2. *The function $H(X) = -\sum_k p_k \log_2 p_k$ is an entropy function.*

Proof. ∎

1.2 Uncertainty.

As we have defined the entropy of a random variable X to be:

$$H(X) = -\sum_k p_k \log p_k \tag{1.4}$$

we can define entropy similarly for a random vector $\mathbf{X}$