Modern Cryptography

Entropy: Notes on September 3, 2021

Jeffrey Goldberg
jeffrey@goldmark.org

August 27, 2021
Revised May 8, 2024

“Entropy”: Borrowed from Physics

The term “entropy” was introduced into Information Theory because of the analogous concept in Statistical Mechanics.

> *Ludwig Boltzmann, who spent much of his life studying statistical mechanics, died in 1906, by his own hand. Paul Ehrenfest, carrying on the work, died similarly in 1933. Now it is our turn to study statistical mechanics.* [*States of matter* [Goo75]]

Now it is our turn to study entropy.

The simple case: Uniform and Independent

When a probability distribution is uniform and independent of other information we may care about entropy of a signal of the number of ways that signal could be different. It is the logarithm of the number of possible signals.

Updating entropy: Relative to prior information

Entropy of a signal is a measure of its capacity to update the information state of the recipient.

Updating information state is the same as reducing uncertainty.

Non-unform distributions

There are multiple ways to compute the entropy of non-uniform distributions.

Shannon entropy	H	Most commonly used.
Rényi entropy	H_α	Allows more bias toward the higher probability items depending on α
Min-entropy	H_∞	Looks only at the probability of the most likely element

Table 1: Different definitions of H: For non-uniform distributions, there are different notions of entropy. Shannon entropy is the original and default. Min-H is right for passwords. All produce identical results when the distribution is uniform.

Resources

References I

[Aum17] Jean-Philippe Aumasson. ***Serious cryptography: a practical introduction to modern encryption.*** No Starch Press, 2017.

[Goo75] David L. Goodstein. ***States of matter.*** Prentice-Hall physics series. Englewood Cliffs, N.J.: Prentice-Hall, 1975.