Evaluating Min-Entropy of Random Bits by Markov Chains

Maciej Skórski[*]

April 17, 2018

Abstract

Reliable entropy estimation is crucial for determining and ensuring quality of random number generators. Technically, this boils down to building a stochastic model and fitting it to empirical data; entropy in long run can be then determined by theoretical formulas or simulations. In practice however, neither developing stochastic models nor evaluating their entropy (cryptography uses min-entropy instead of standard Shannon entropy) is easy.

Finite order Markov chains appear to be particularly handy for randomness evaluation. First, they can model sources with dependencies. Second, their stochastic properties in long run are quite well understood.

In the talk I will discuss how to *fit a Markov model and estimate the min-entropy rate*, focusing on algorithmic aspects (time and memory optimization). Entropy calculations are based on the recent formula (Kamath and Verdu, ISIT 2016), optimized by dynamic programming. The demonstrated solution extends the more heuristic framework proposed in the NIST standard 800-90B. Finally, I will show results of experiments on hardware; this is based on the joint work with Allini, Petura, Bernard, Laban and Fischer.

[*]Currently Data Science Project Consultant at Dell