Coin Tossing, Randomness Extraction, and Algorithmic Randomness

Dr. Christopher Porter

March 23, 2015

Abstract

Suppose you are given a biased coin and asked to use it to generate an unbiased random sequence. Can this be done? Von Neumann answered this question in the affirmative in 1951, providing a simple algorithm for producing unbiased bits from biased ones. Suppose instead of a biased coin, you are given access to some device for producing random bits that induces a computable probability distribution P on the space of infinite binary sequences. Is there an effective procedure for converting P-random bits into unbiased random bits?

To answer this question, I will introduce some basic definitions of algorithmic randomness,a sub-branch of computability theory that draws upon areas such as classical probability theory and information theory. As I will discuss, from a computability-theoretic point of view, we only interested in whether such an effective procedure exists in principle (completely ignoring concerns of time- and space-complexity). After providing an affirmative answer to the above question, I will consider some circumstances in which the initial biased random sequences are so distorted that the conversion procedure for producing unbiased random bits from these biased sequences is maximally inefficient in a sense that I will make precise.