Computational Analogues of Entropy

Boaz Barak[1], Ronen Shaltiel[1], and Avi Wigderson[2]

[1] Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel. Emails: {boaz,ronens}@wisdom.weizmann.ac.il
[2] School of Mathematics, Institute for Advanced Study, Princeton, NJ and Hebrew University, Jerusalem, Israel. Email: avi@ias.edu

Abstract. Min-entropy is a statistical measure of the amount of randomness that a particular distribution contains. In this paper we investigate the notion of *computational min-entropy* which is the computational analog of statistical min-entropy. We consider three possible definitions for this notion, and show equivalence and separation results for these definitions in various computational models.
We also study whether or not certain properties of statistical min-entropy have a computational analog. In particular, we consider the following questions:

1. Let X be a distribution with high computational min-entropy. Does one get a pseudo-random distribution when applying a "randomness extractor" on X?
2. Let X and Y be (possibly dependent) random variables. Is the computational min-entropy of (X, Y) at least as large as the computational min-entropy of X?
3. Let X be a distribution over $\{0,1\}^n$ that is "weakly unpredictable" in the sense that it is hard to predict a constant fraction of the coordinates of X with a constant bias. Does X have computational min-entropy $\Omega(n)$?

We show that the answers to these questions depend on the computational model considered. In some natural models the answer is false and in others the answer is true. Our positive results for the third question exhibit models in which the "hybrid argument bottleneck" in "moving from a distinguisher to a predictor" can be avoided.

1 Introduction

One of the most fundamental notions in theoretical computer science is that of *computaional indistinuishability* [1, 2]. Two probability distributions are deemed close if no *efficient*[3] test can tell them apart - this comes in stark contrast to the information theoretic view which allows *any* test whatsoever. The discovery [3, 2, 4] that simple computational assumptions (namely the existance of one-way functions) make the computational and information theoretic notions completely

[3] What is meant by "efficient" can naturally vary by specifying machine models and resource bounds on them