Preface

Indistinguishable things are identical.[1]

G.W. Leibniz (1646–1714)

This primer to the theory of pseudorandomness presents a fresh look at the *question of randomness*, which arises from a complexity theoretic approach to randomness. The crux of this (complexity theoretic) approach is the postulate that a distribution is random (or rather pseudorandom) if it cannot be distinguished from the uniform distribution by *any efficient procedure*. Thus, (pseudo)randomness is not an inherent property of an object, but is rather subjective to the observer.

At the extreme, this approach says that the question of whether the world is actually deterministic or allows for some free choice (which may be viewed as a source of randomness) is irrelevant. *What matters is how the world looks to us and to various computationally bounded devices*. That is, if some phenomenon looks random, then we may treat it as if it is random. Likewise, if we can generate sequences that cannot be distinguished from the uniform distribution by any efficient procedure, then we can use these sequences in any efficient randomized application instead of the ideal coin tosses that are postulated in the design of this application.

The pivot of the foregoing approach is the notion of *computational indistinguishability*, which refers to pairs of distributions that cannot be distinguished by efficient procedures. The most fundamental incarnation of this notion associates efficient procedures with polynomial-time algorithms, but other incarnations that restrict attention to different classes of distinguishing procedures also lead to important insights. Likewise, the *effective generation* of pseudorandom objects, which is of major concern, is actually a general paradigm with numerous useful incarnations (which differ in the computational complexity limitations imposed on the generation process).

Following the foregoing principles, we briefly outline some of the key elements of the theory of pseudorandomness. Indeed, the key concept is that of a pseudorandom generator, which is an efficient deterministic procedure that stretches short random seeds into longer pseudorandom sequences. Thus, a generic formulation of pseudorandom generators consists of specifying three fundamental aspects – the *stretch measure* of the generators; the class of distinguishers that the generators are

[1] This is Leibniz's *Principle of Identity of Indiscernibles*. Leibniz admits that counterexamples to this principle are conceivable but will not occur in real life because God is much too benevolent. We thus believe that he would have agreed to the theme of this text, which asserts that *indistinguishable things should be considered as if they were identical*.

supposed to fool (i.e., the algorithms with respect to which the *computational indistinguishability* requirement should hold); and the resources that the generators are allowed to use (i.e., their own *computational complexity*).

The archetypical case of pseudorandom generators refers to efficient generators that fool any feasible procedure; that is, the potential distinguisher is any probabilistic polynomial-time algorithm, which may be more complex than the generator itself (which, in turn, has time-complexity bounded by a fixed polynomial). These generators are called general-purpose, because their output can be safely used in any efficient application. Such (general-purpose) pseudorandom generators exist if and only if there exist functions (called one-way functions) that are easy to evaluate but hard to invert.

In contrast to such (general-purpose) pseudorandom generators, for the purpose of derandomization (i.e., converting randomized algorithms into corresponding deterministic ones), a relaxed definition of pseudorandom generators suffices. In particular, for such a purpose, one may use pseudorandom generators that are somewhat more complex than the potential distinguisher (which represents a randomized algorithm to be derandomized). Following this approach, adequate pseudorandom generators yield a full derandomization of probabilistic polynomial-time algorithms (e.g., $\mathcal{BPP} = \mathcal{P}$), and such generators can be constructed based on the assumption that some exponential-time solvable problems (i.e., problems in $\mathcal{E}$) have no sub-exponential size circuits.

Indeed, both the general-purpose pseudorandom generators and the aforementioned "derandomizers" demonstrate that randomness and computational difficulty are related. This trade-off is not surprising in light of the fact that the very definition of pseudorandomness refers to computational difficulty (i.e., the difficulty of distinguishing the pseudorandom distribution from a truly random one).

Finally, we mention that it is also beneficial to consider pseudorandom generators that fool space-bounded distinguishers and generators that exhibit some limited random behavior (e.g., outputting a pairwise independent or a small-bias sequence). Such (special-purpose) pseudorandom generators can be constructed without relying on any computational complexity assumptions, because the behavior of the corresponding (limited) distinguishers can be analyzed even at the current historical time. Nevertheless, such (special-purpose) pseudorandom generators offer numerous applications.

Note: The study of pseudorandom generators is part of complexity theory (cf. e.g., [24]), and some basic familiarity with complexity theory will be assumed in the current text. In fact, the current primer is an abbreviated (and somewhat revised) version of [24, Chap. 8]. Nevertheless, we believe that there are merits to providing a separate treatment of the theory of pseudorandomness, since this theory is of natural interest to various branches of mathematics and science. In particular, we hope to reach readers that may not have a general interest in complexity theory at large and/or do not wish to purchase a book on the latter topic.

Acknowledgments. We are grateful to Alina Arbitman and Ron Rothblum for their comments and suggestions regarding this primer.

Oded Goldreich
Weizmann Institute of Science