PSEUDORANDOMNESS IN COMPUTER SCIENCE
AND IN ADDITIVE COMBINATORICS

LUCA TREVISAN*

Dedicated to Endre Szemerédi on the occasion of his 70th birthday

Notions of pseudorandomness and (implicitly) of indistinguishability arise in several key results in additive combinatorics. In this expository paper, we show how several results can be translated from the analytic language of norms, decompositions, and transference to the computer science language of indistinguishability, simulability and pseudoentropy. Some of these results, once so reformulated, can be given "computer science proofs" which are quantitatively better in some respects, and which have some applications.

We discuss variants of the Szemerédi regularity lemma for graphs; the inverse theorems for the Gowers uniformity norms; a key step in the "transference" results of Green, Tao and Ziegler; and various "decomposition" results.

1. INTRODUCTION

We outline how the computer science notions of “pseudorandomness”, “indistinguishability” and “simulability”, which arise in computational complexity theory and in the foundations of cryptography, can be used to reformulate several results in additive combinatorics, which are usually stated in the analytic language of norms and decompositions.

We discuss the following points.

• The notion of “quasirandomness” of a graph, introduced by Chung, Graham and Wilson [6] and Thomason [41], can be defined in terms

*This material is based upon work supported by the National Science Foundation under grant No. CCF-0729137 and by the BSF under grant 2006060.
of the computer science notion of pseudorandomness of distributions: a graph is quasirandom if and only if the uniform distribution over its edge set is indistinguishable from the uniform distribution over all vertex pairs by the family of adversaries defined by characteristic functions of partial cuts.

Similarly, the notion in which a regular partition of a graph (as given by the Szemerédi regularity lemma [35, 36]) gives an "approximation" of the graph can be formulated in terms of indistinguishability of the given graph from a graph derived from the regular partition.

- Although the notion of "quasirandomness" of functions defined by the Gowers uniformity norm [15, 16] is incomparable with the computer science notions of pseudorandomness and indistinguishability, the recently proved Gowers inverse conjectures can be seen as asserting that two functions are close in Gowers norm if and only if they are indistinguishable by a certain set of adversaries.

- Several "decomposition" results in additive combinatorics [20, 46, 24, 23], as well as various versions of the Szemerédi regularity lemma [35, 36, 8, 2, 39] can be generalized to "regularity lemmas for functions", which, stated in computer science language, assert that every high entropy distribution is indistinguishable from a high-entropy efficiently computable (and samplable) distribution. A "weak regularity lemma for functions" in which all complexity parameters are polynomial can be proven using computer science techniques [43].

- The Green–Tao theorem [20] that the primes contain arbitrarily long arithmetic progressions is proved by constructing a "dense model" of the prime numbers, showing that the primes and the dense model are "indistinguishable" in a sense that has implications for the counting of arithmetic progressions, and using the fact that the dense model must have many long arithmetic progressions from Szemerédi’s theorem. A more abstract "dense-model theorem" can be proven with computer science techniques and fully polynomial parameters and has applications to cryptography [32, 7, 27, 30].

Overview of the paper. In Sections 2 and 3 we define the computer science notions of indistinguishability, pseudorandomness and simulability of distributions, and in Section 4 we define the combinatorial notion of quasirandom graph and state three versions of the Szemerédi regularity lemma.