Polynomial-Time Pseudodeterministic Constructions

Igor C. Oliveira
University of Warwick, UK

Abstract

A randomised algorithm for a search problem is pseudodeterministic if it produces a fixed canonical solution to the search problem with high probability. In their seminal work on the topic, Gat and Goldwasser (2011) posed as their main open problem whether prime numbers can be pseudodeterministically constructed in polynomial time.

We provide a positive solution to this question in the infinitely-often regime. In more detail, we give an unconditional polynomial-time randomised algorithm B such that, for infinitely many values of n, $B(1^n)$ outputs a canonical n-bit prime p_n with high probability. More generally, we prove that for every dense property Q of strings that can be decided in polynomial time, there is an infinitely-often pseudodeterministic polynomial-time construction of strings satisfying Q. This improves upon a subexponential-time pseudodeterministic construction of Oliveira and Santhanam (2017).

This talk will cover the main ideas behind these constructions and discuss their implications, such as the existence of infinitely many primes with succinct and efficient representations.

2012 ACM Subject Classification Theory of computation → Computational complexity and cryptography; Theory of computation → Pseudorandomness and derandomization

Keywords and phrases Pseudorandomness, Explicit Constructions, Pseudodeterministic Algorithms

Digital Object Identifier 10.4230/LIPIcs.STACS.2024.1

Category Invited Talk

41st International Symposium on Theoretical Aspects of Computer Science (STACS 2024).
Editors: Olaf Beyersdorff, Mamadou Moustapha Kanté, Orna Kupferman, and Daniel Lokshtanov;
Article No. 1; pp. 1:1–1:1
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany