In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

CSE - ITCSC Joint Seminar

New questions in pseudo-randomness for answering old problems

By
Prof. Periklis Papakonstantinou, Assistant Professor
Institute for Theoretical Computer Science, Tsinghua University

September 8, 2011, Thursday

2:30pm – 4:30pm

Room 121, 1/F., Ho Sin Hang Engineering Building, CUHK

Abstract: Derandomizing probabilistic polynomial time (e.g. BPP) and proving circuit lower bounds for NEXP are two well-related and long standing open questions in computational complexity. We show that a certain refinement of these questions becomes possible through a new "streaming model" for accessing the randomness during the computation of a probabilistic algorithm. From this follows that derandomizing "interesting parts" of BPP is related to the question of existence of pseudorandom generators that extend the classical PRG by Nisan. Furthermore, the existence of such types of PRGs also relates to other long-standing questions in computational complexity; e.g. separating L from NP.

This work blends old (and long forgotten) works and models in computational complexity, streaming, concrete complexity related to pseudo-randomness, and communication complexity.

In this talk I'll briefly outline research that appears in recent papers, and I will explain how all these seemingly different works relate to each other. I also plan to give a list of open questions pertaining to new models for pseudo-randomness and Communication Complexity. These questions are also of independent interest. This appears in joint works with: Andrej Bogdanov, Matei David, Phuong Nguyen, Anastasios Sidiropoulos, and Andrew Wan

Biography: I am an Assistant Professor at the Institute for Theoretical Computer Science of the Institute for Interdisciplinary Information Sciences, Tsinghua University. Right before that I did a PhD in Computer Science, an MSc in Mathematics (simultaneously to the PhD), and before that an MSc in Computer Science, all from the University of Toronto. My undegraduate studies were in Computer Engineering and Science, University of Patras, and I'm a licensed Electronics Engineer with the Technical Chamber of Greece.

My research biases are towards Computational Complexity, Foundations of Cryptography, computational problems with engineering motivation -- in particular their intersection with Algebra, Combinatorics, and Randomness.

******* ALL ARE WELCOME *******

Hosted By: Prof. Andrej Bogdanov
Enquiries : Institute of Theoretical Computer Science and Communications Tel: 2696 1257