Hitting Sets with Near-Optimal Error for Read-Once Branching Programs

Sumegha Garg
Princeton University

3/28/2018 at 11:00 am
CoRE 301

Abstract

Nisan [Nis92] constructed a pseudorandom generator for length n, width n read-once branching programs (ROBPs) with error and seed length O(logˆ2(n) + log(n) log(1/)). A major goal in complexity theory is to reduce the seed length, hopefully, to the optimal O(log(n) + log(1/)), or to construct improved hitting sets, as these would yield stronger derandomization of BPL and RL, respectively. In this talk, we make the first improvement by constructing a hitting set with seed length ˜O(logˆ2(n) + log(1/)). That is, we decouple and n, and obtain near-optimal dependence on the former. The regime of parameters in which our construction strictly improves upon prior works, namely, log(1/) log n, is well- motivated by the work of Saks and Zhou [SZ99] who use pseudorandom generators with error = 2ˆ{logˆ2(n)} in their proof for BPL Lˆ{3/2}.

Joint work with Mark Braverman and Gil Cohen.

Bio

I am a third year PhD student in the Department of Computer Science at Princeton University. I am extremely fortunate to be advised by Mark Braverman. Before coming here, I finished my undergraduate studies in the Department of Computer Science and Engineering at Indian Institute of Technology, Delhi.

I am interested in Theoretical Computer Science, particularly in information theory, complexity theory and quantum computing. CV

Organizer(s): Pranjal Awasthi and Shubhangi Saraf