Abstract:

We present an explicit pseudorandom generator with polylog(n) seed length for read-once constant-width branching programs that can read their $n$ input bits in any order. This improves upon the work of Impagliazzo, Meka, and Zuckerman (FOCS, 2012), where they required seed length $n^{1/2+o(1)}$.

A central ingredient in our work is a bound on the Fourier spectrum of constant-width branching programs, settling a conjecture posed by Reingold, Steinke, and Vadhan (RANDOM, 2013).

Our analysis crucially uses a notion of local monotonicity on the edge labeling of the branching program. We carry critical parts of our proof under the assumption of local monotonicity and show how to deduce our results for unrestricted branching programs.

(Joint work with Eshan Chattopadhyay, Pooya Hatami, and Omer Reingold)