Contribution ID: **68** Type: **not specified**

New PRGs for Unbounded-width/Adaptive-order Read-once Branching Programs

Wednesday, July 12, 2023 10:55 AM (20 minutes)

Lijie Chen, Xin Lyu, Avishay Tal and Hongxun Wu

Abstract: We give the first pseudorandom generators with sub-linear seed length for the following variants of read-once branching programs (roBPs):

1. First, we show there is an explicit PRG of seed length O(log^2(n/eps) log(n)) that fools unbounded-width unordered permutation branching programs with a single accept state, where n is the length of the program. Previously, [Lee-Pyne-Vadhan RANDOM 2022] gave a PRG with seed length Omega(n) for this class. For the ordered case, [Hoza-Pyne-Vadhan ITCS 2021] gave a PRG with seed length O~(log(n)log(1/eps)).
2. Second, we show there is an explicit PRG fooling unbounded-width unordered regular branching programs with a single accept state with seed length O~(sqrt(n log(n/eps))). Previously, no non-trivial PRG (with seed length less than n) was known for this class (even in the ordered setting). For the ordered case, [Bogdanov-Hoza-Prakriya-Pyne CCC 2022] gave an HSG with seed length O~(log(n)log(1/eps)).
3. Third, we show there is an explicit PRG fooling width w adaptive branching programs with seed length O(log(n)log^2(nw/eps)). Here, the branching program can choose an input bit to read depending on its current state, while it is guaranteed that on any input x \in {0,1}^n, the branching program reads each input bit exactly once. Previously, no PRG with a non-trivial seed length is known for this class. We remark that there are some functions computable by constant-width adaptive branching programs but not by sub-exponential-width unordered branching programs.

In terms of techniques, we indeed show that the Forbes-Kelly PRG (with the right parameters) from [Forbes-Kelly FOCS 2018] already fools all variants of roBPs above. Our proof adds several new ideas to the original analysis of Forbes-Kelly, and we believe it further demonstrates the versatility of the Forbes-Kelly PRG.

Presenter: WU, Hongxun

Session Classification: Track A-4