Strong Average-Case Circuit Lower Bounds from Non-trivial Derandomization

Abstract:

We prove that for all constants a, NQP = NTIME[n^polylog(n)] cannot be (1/2 + 2^(−log^a n))-(1/2 + 2^(−log^a n))-approximated by 2^(log^a n)-size ACC^0 of THR circuits (ACC^0 circuits with a bottom layer of threshold gates). Previously, it was even open whether E^NP can be (1/2+1/sqrt(n))-approximated by AC^0[2] circuits.

More generally, we establish a connection showing that, for a typical circuit class C, non-trivial nondeterministic CAPP algorithms imply strong (1/2 + 1/n^{omega(1)}) average-case lower bounds for nondeterministic time classes against C circuits. The existence of such (deterministic) algorithms is much weaker than the widely believed conjecture PromiseBPP = PromiseP.

Our new results build on a line of recent works, including [Murray and Williams, STOC 2018], [Chen and Williams, CCC 2019], and [Chen, FOCS 2019]. In particular, it strengthens the corresponding (1/2 + 1/polylog(n))-inapproximability average-case lower bounds in [Chen, FOCS 2019]. The two important technical ingredients are techniques from Cryptography in NC^0 [Applebaum et al., SICOMP 2006], and Probabilistic Checkable Proofs of Proximity with NC^1-computable proofs.