Typically-Correct Derandomization for Small Time and Space

Abstract:

Suppose a language L can be decided by a bounded-error randomized algorithm that runs in space S and time n * poly(S). We give a randomized algorithm for L that still runs in space O(S) and time n * poly(S) that uses only O(S) random bits; our algorithm has a low failure probability on all but a negligible fraction of inputs of each length. An immediate corollary is a deterministic algorithm for L that runs in space O(S) and succeeds on all but a negligible fraction of inputs of each length. We also discuss additional complexity-theoretic applications of our technique.