Main question of this research: Is BPP = P?

Definition of PRG  Note: this is not the same as the definition of secure PRG we use in crypto.

Unconditional existence of inefficient PRG’s

PRG’s imply derandomization

NW Generator  Statement of theorem, corollaries.

Proof of NW Generator

Some facts about the permanent PH reduces to perm. perm is downward self reducible.

Uniform derandomization  If EXP \( \not\subseteq \) BPP then BPP has a “pretty good” subexponential simulation.

Lower bounds from derandomization

Derandomization of AM

---

Homework Assignments

§1 (20 points) Exercise 16.1

§2 (30 points) Suppose that there exists a polynomial-time algorithm \( G \) and a constant \( c > 0 \) such that for any \( s \), and any circuit \( C \) of size \( \leq s \), if \( x \) is chosen at random from \( \{0,1\}^{c\log s} \) then

\[
|\Pr[C(G(1^s,x)) = 1] - \Pr[C(U_s) = 1]| < \frac{1}{10}
\]

(where if \( C \) is takes \( n \leq s \) bits as input, then by \( C(y) \) we mean apply \( C \) to the first \( n \) bits of \( y \).)

Prove that there exists a function \( f \in E = \text{DTIME}(2^{O(n)}) \) (with one bit of output) such that \( f \) is not computable by \( 2^n/\log^n \text{size circuits} \).

§3 (30 points) Exercise 16.4.  (Recall that MA is the class of languages proven by a two-round interactive proof between an all powerful prover Merlin and a probabilistic polynomial-time verifier Arthur where Merlin sends the first message. Thus, all that Arthur can do is use a probabilistic algorithm to decide whether or not to accept the proof.)

§4 (30 points) Show the following limitation on designs: prove that if \( S_1, \ldots, S_k \) are subsets of a universe \( U \) such that for some \( \rho > 0 \), \( |S_i| = \rho |U| \) and \( |S_i \cap S_j| \leq \rho^2 |U| / 2 \) for every distinct \( i,j \in [k] \) then \( k \leq 2/\rho \).