CSG399: Gems of Theoretical Computer Science. Spring 2009
Instructor: Emanuele Viola

Problems

Problem 1 [generator for $\mathrm{P} = \mathrm{BPP}$**]:** Suppose that for every n there is a generator $G : \{0,1\}^{c \log n} \to \{0,1\}^n$ that fools circuits of size n with error $1/n$, where c is an absolute constant. Suppose that there is an algorithm that, given $x \in \{0,1\}^{c \log n}$, computes $G(x) \in \{0,1\}^n$ in time polynomial in $n = |G(x)|$. (This time requirement to compute the generator is more relaxed than the one seen in class, and is sufficient for this problem.)

Prove that $\mathrm{P} = \mathrm{BPP}$.

Where is your proof using that the generator fools *circuits*, as opposed to polynomial-time algorithms?

Problem 2 [parameters of the generator for constant-depth circuits]: Assuming (1) the Nisan-Wigderson theorem (together with the remark that the reduction in the proof of correctness increases the depth by a constant at most), (2) the design construction via polynomials, and (3) the correlation bound for parity, prove (i.e., work out the parameters establishing) that for every d there is an explicit generator $G : \{0,1\}^{\log^{c \cdot d} n} \to \{0,1\}^n$ that fools circuits of size n and depth d with error $1/n$, where c is an absolute constant.

Problem 3 [application of the generator for constant-depth circuits]: Somebody hands you an algorithm $M : (\{0,1\}^a)^b \to \{0,1\}$ that on input $(x_1, \ldots, x_b) \in (\{0,1\}^a)^b$ evaluates to 1 if and only if for every i, $x_i \in A_i$, where $A_1, \ldots, A_b$ are subsets of $\{0,1\}^a$.

Exhibit a trivial algorithm that makes $2^{a \cdot b}$ queries to M and computes an approximation ϵ to the volume $\prod_{i=1}^{b} |A_i|/2^a$ such that $|\epsilon - \prod_{i=1}^{b} |A_i|/2^a| \leq 1/100$.

Now derive an algorithm that gives the same approximation but makes $2^{\mathrm{poly}(a, \log b)}$ queries to M (which for $b \gg a$ is much less). Hint: Use Problem 2.

Problem 4 [constant-depth vs. majority]:

(1) Prove that the majority function on n bits requires (unbounded fan-in) circuits of depth d and size $w \geq \exp(n^{\Omega(1/d)})$ (i.e., qualitatively the same bound we obtained in class for the parity function). Hint: If you could compute majority with these resources, then you could compute parity as well.

(2) Exhibit a circuit of depth $O(1)$ and size $O(1)$ that has correlation at least $1/n^{O(1)}$ with the majority function. Hint: The circuit is *simple.*

(3) Construct a circuit C of depth $d = O(1)$ and size $n^{O(1)}$ that computes *approximate majority*, i.e., for any input $x \in \{0,1\}^n$ whose hamming weight is at least $2n/3$, $C(x) = 1$, while for any input $x \in \{0,1\}^n$ whose hamming weight is at most $n/3$, $C(x) = 0$. The value of the circuit can be arbitrary on inputs whose hamming weight is between $n/3$ and $2n/3$. Hint: Build C incrementally and using the probabilistic method. As a first step, consider

the AND of $c \cdot \log n$ randomly selected input variables. Analyze the probability that this AND evaluates to 1 in the two cases. Flip the answer and repeat.

Problem 5 [branching programs vs. circuits]:

(1) Prove that any function $f : \{0,1\}^n \to \{0,1\}$ computable by branching programs of length n and width n can be computed by fan-in 2 circuits of depth $O(\log^2 n)$.

(2) Strengthen (1) to obtain unbounded fan-in circuits of depth $O(\log n)$.

Problem 6 [universal traversal sequences]: Let d be a fixed constant. Prove that for every n there is a sequence $U = (u_1, \ldots, u_\ell) \in [d]^\ell$ such that for any d-regular undirected graph G on n nodes and any starting node s, walking from s in G according to U will touch every node connected to s in G. Explain why this implies that undirected reachability can be computed by branching programs of polynomial width and polynomial length.