Midterm

This is due in class on November 8.

1. A directed graph $G = (V, E)$ is *strongly connected* if for any two vertices $u, v \in V$ there is a directed path in G from u to v. Let strong-CONN be the problem of deciding whether a given graph is strongly connected.

   (a) Show that strong-CONN is in **NL**.

   (b) Prove the **NL**-completeness of strong-CONN by giving a log-space reduction from ST-CONN to strong-CONN.

2. Suppose that there is a deterministic polynomial-time algorithm A that on input (the description of) a circuit C produces a number $A(C)$ such that

$$\mathbf{Pr}_x[C(x) = 1] - \frac{2}{5} \leq A(C) \leq \mathbf{Pr}_x[C(x) = 1] + \frac{2}{5} \ .$$

   (a) Prove that it follows $\mathbf{P} = \mathbf{BPP}$.

   (b) Prove that there exists a deterministic algorithm A' that, on input a circuit C and a parameter ϵ, runs in time polynomial in the size of C and in $1/\epsilon$ and produces a value $A'(C, \epsilon)$ such that

$$\mathbf{Pr}_x[C(x) = 1] - \epsilon \leq A'(C, \epsilon) \leq \mathbf{Pr}_x[C(x) = 1] + \epsilon \ .$$

   (c) Prove that there exists a deterministic algorithm A'' that, on input a circuit C computing a function $f : \{0,1\}^n \to \{1, \ldots, k\}$ and a parameter ϵ, runs in time polynomial in the size of C, in $1/\epsilon$ and in k, and produces a value $A''(C, \epsilon)$ such that

$$\mathbf{E}_x[f(x)] - \epsilon \leq A''(C, \epsilon) \leq \mathbf{E}_x[f(x)] + \epsilon \ .$$

   [For this question, you can think of C as being a circuit with $\log k$ outputs, and the outputs of $C(x)$ are the binary representation of $f(x)$.]

3. Prove that, for every constant t, $\Sigma_2 \not\subseteq \mathbf{SIZE}(n^t)$.

   [Hint: first prove $\Sigma_4 \not\subseteq \mathbf{SIZE}(n^t)$, which should be easy. Then argue about what happens depending on whether or not $SAT \in \mathbf{SIZE}(n^t)$.]

4. Let f be a one-way permutation and g be a polynomial time computable permutation. Show that $g(f(\cdot))$ and $f(g(\cdot))$ are one-way permutations.

   [Ideally, do the proof in the finite setting: show that if f is (S, ϵ)-one way and g can be computed by a circuit of size t, then $f(g(\cdot))$ and $g(f(\cdot))$ are $(S - t, \epsilon)$-one way. Then derive the asymptotic result from the finite one. Be as detailed as you can in the analysis.]