Homework 2
Due 2006/5/17

Amnon Ta-Shma
Dept. of Computer Science
Tel Aviv University

Topic today: Non-uniformity, branching programs, space-bounded computations.

1. (non-uniformity). A language L is in $\mathsf{DTIME}(t(n))|a(n)$ if there exists a machine $M \in \mathsf{DTIME}(t(n))$ and a set $\left\{a_n \in \{0,1\}^{a(n)}\right\}$ of advice strings (that depend on the input length but not on the specific input) such that $\forall x$, $x \in L$ iff $M(x, a_{|X|})$ accepts.

   (a) Prove that there exists an undecidable language L in $\mathsf{P}|1$.

   (b) Prove that L has polynomial size circuits iff $L \in \mathsf{P}|poly$.

   (c) Prove that $\mathsf{BPP} \subseteq \mathsf{P}|poly$.

   (d) Prove that if $\mathsf{NP} \subseteq \mathsf{P}|log$ then $\mathsf{NP} = \mathsf{P}$

   (e) Prove that for every $c > 0$ there exists $L \in \mathsf{PH}$ that requires circuits of size n^c.

   (f) Prove that if $\mathsf{PSPACE} \subseteq \mathsf{P}|poly$ then $\mathsf{PSPACE} = \mathsf{MA} = \Sigma_2$
   hint: use $\mathsf{IP} = \mathsf{PSPACE}$.

2. (NC^k,AC^k) We say a language L is in non-uniform AC^k if there exists a sequence of circuits $\{C_n\}$ solving L, with $\{\wedge, \vee, \neg\}$ gates, unbounded fan-in, $O(\log^k n)$ depth and polynomial size. We say L is in non-uniform NC^k if in addition the fan-in of the circuits is at most two. The uniform classes are the ones where there exists a uniform machine outputting the n'th circuit using only $O(\log(n))$ space.

   (a) Prove that $\mathsf{NC}^k \subseteq Space(O(\log^k n)$ and in particular $\mathsf{NC}^1 \subseteq L$.

   (b) Prove that $\mathsf{NL} \subseteq \mathsf{AC}^1$.

   (c) Let $f : \{0,1\}^n \to \{0,1\}^n$. Prove that f has non-uniform polynomial size formulas iff f is in non-uniform-NC^1.

   (d) Prove that every problem solvable in non-uniform bounded width polynomial size branching program, is solvable in NC^1.

3. In the following exercises pay attention to the crucial difference between read-once and multiple-access branching programs.

   (a) Let $Exactly_{n/2}$ be the function that gets n boolean values and returns one iff their sum is exactly $n/2$. Find a branching program for the problem with $O(n\log(n))$ length and $O(\log(n))$ width.

   (b) Let $Exact - Clique_{n/2}$ be the function that gets an undirected graph $G = (V, E)$ on n vertices and returns one iff it is a clique on $n/2$ vertices (and no other edges). Prove that any read-one branching program (of arbitrary width) for the problem requires $2^n/poly(n)$ size.

Homework 2
Due 2006/5/17

Amnon Ta-Shma
Dept. of Computer Science
Tel Aviv University

4. In this exercise we consider multiple-access, space bounded machines. Let BPL denote the probabilistic, logarithmic-space bounded class with two sided errors (for $x \in L$ the acceptance probability is at least $2/3$, for $x \notin L$ at most $1/3$). Let RL denote the one-sided error (for $x \in L$ the acceptance probability is at least $1/2$, for $x \notin L$ it is zero) and ZPL be the zero-sided class (for every input with probability at least half the answer is the correct one, and otherwise it is don't-know). Let $\mathsf{BPL}^*, \mathsf{RL}^*, \mathsf{ZPL}^*$ be the corresponding classes where the machine has multiple access to the random tape, i.e., the random tape is polynomially long, initialized uniformly at random, read-only, and the tape head can go left or right over it. Similarly NL^* denotes NL with multiple access to the witness tape.

   (a) Prove that $\mathsf{NL}^* = \mathsf{NP}$.

   (b) Prove that $\mathsf{BPL} \subseteq \mathsf{ZPL}^*$
   hint: using Nisan's generator.

   (c) Prove that a pseudo-random generator against small space, multiple access branching program with only a polynomial stretch, suffices to derandomize BPL.