6.045J/18.400J: Automata, Computability and Complexity Prof. Nancy Lynch, Nati Srebro

Recitation 10: NP-Completeness

April 16, 2003 *Susan Hohenberger*

Readings: Sections 7.4, 7.5

Outline for Today:

1. History of NP-completeness
   (a) Who are Stephen Cook and Leonid Levin?
   (b) $SAT = \{\langle\phi\rangle | \ \phi$ is a satisfiable Boolean formula$\}$
   (c) Cook-Levin Theorem: $SAT \in$ P iff P=NP. That is, SAT is NP-complete.
   (d) Review proof of Cook-Levin Theorem
   (e) What about coNP-completeness?
2. Practice polynomial time reductions.
3. Languages vs Functions: a fun example related to cryptography.

Problem 1: Show that DOUBLE-SAT=$\{\langle\phi\rangle | \ \phi$ has at least two satisfying assignments$\}$ is NP-complete.

Problem 2: Show that PRIMES=$\{n \mid n$ is a prime number in binary$\}$ is in NP and coNP. (And actually Agarwal, Saxena, and Kayal recently showed that it is also in P!)

Problem 3: (Sipser 7.28) Show that, if P=NP, we can factor integers in polynomial time.

(Note: NP is a class of *languages* and the factoring problem is a *function*. Thus simply saying that, "because factoring is in NP, you are done" isn't enough!)