Institut for Matematik og Datalogi
Syddansk Universitet

April 3, 2018
JFB

DM553 – Complexity and Computability – 2018
Lecture 11

Lecture, March 20

We finished showing that PCP is undecidable by doing the reduction from A_{TM} to MPCP from section 5.2. Then, we began on NP-Completeness, introducing definitions, covering the following in Sipser's book: Definitions 7.7, 7.9, 7.12, and most of section 7.3.

Lectures, April 10 and 12

We will first show that 3-SAT is NP-Complete. To do this, we assume that CNF-SAT is NP-Complete. The proof that 3-SAT is NP-Complete combines the proofs in both the Sipser and the CLRS books. and the definition of P is on page 286.

Then, we will show that CLIQUE is NP-Complete. We will cover the proof that SATISFIABILITY (actually CNF-SAT) is NP-Complete, from section 7.4 in Sipser's textbook. We will also do more reductions from chapter 34 in CLRS.

Problems to be discussed on April 11

1. Problem 5.29 in Sipser's book.
2. 34.2-4 (skip Kleene star), 34.2-8.
3. 34.3-7 (34.3-6 has the definition of complete you need).
4. The following argument is incorrect. Find the most important error.

   Consider the following algorithm:

   Input: $n \in \mathbb{N}$
   for $i = 2$ to $n-1$ **do**
   check if i divides n
   if it does **then** output i
   endfor
   output -1 if no output yet

Checking if i divides n can be done in time $O(\log^3 n)$ via binary search for an integer k such that $n = i \cdot k$ (the multiplication can clearly be done in time $O(\log^2 n)$).

Thus, the total running time is $O(n \cdot \log^3 n)$ in the worst case. Since $O(n \cdot \log^3 n) \subset O(n^2)$, and n^2 is a polynomial, this algorithm runs in polynomial time. Thus, we have an efficient algorithm for factoring, so we can break RSA, a famous cryptosystem which is believed to be secure.

5. Suppose you have a Boolean formula form, with exactly three literals per clause. Show how to add some constant number of clauses (also with exactly three literals per clause) to F to create a formula F' which is guaranteed to be false.

6. In the CLRS textbook, do the following:

   - 34.2-5, 34.2-10.
   - 34.3-6.
   - 34.4-4, 34.4-5, 34.4-6, 34.4-7. (Probably for next time.)