Institut for Matematik og Datalogi
Syddansk Universitet

November 9, 2004
JFB

DM19 – Algorithms and Complexity – E04 – Lecture 10

Lecture, November 8

We continued with NP-completeness from chapter 34 in the textbook and the section by Papadimitriou and Steiglitz from the first set of notes. We finished Cook's Theorem, and began on reductions, proving that CIRCUIT-SATISFIABILITY, 3-SAT, and CLIQUE were NP-Complete.

Lecture, November 15

We will continue with NP-completeness and begin on approximation algorithms from chapter 35 in the textbook.

Problems to be discussed November 25 and 19

1. 34.5-2, 34.5-4 (you may check on pages 1044–1045 for a hint), 34.5-5 (warning: it is tempting to think that this one is completely trivial; it is not), 34.5-6.

2. 34-2, 34-3.

3. The following argument is incorrect. Find the most important error.

   Consider the following algorithm:

   Input: $n \in I\!N$

   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 $O(\log n)$ via binary search for an integer k such that $n = i \cdot k$.

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