Institut for Matematik og Datalogi
Syddansk Universitet

February 10, 2012
JFB

DM508 – Algorithms and Complexity – 2012
Lecture 5

Lecture, February 10

We continued with NP-Completeness, showing that 3-SAT, CLIQUE, and HAMILTONIAN CIRCUIT are NP-Complete. problems.

Lecture, February 13

We will cover Cook's Theorem, proving that SATISFIABILITY from the section by Papadimitriou and Steiglitz from the course notes.

Lecture, February 20

We will finish with NP-Completeness, showing that VERTEX COVER, INDEPENDENT SET, and SUBSET SUM are NP-Complete. We will being on amortized analysis from Chapter 17 of the textbook and Fibonacci heaps from chapter 19.

Problems to be discussed on February 17

Do problems:

1. 34.2-5, 34.2-8, 34.2-10.
2. 34.3-2, 34.3-6.
3. 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 $O(\log n)$ 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.