Institut for Matematik og Datalogi
Syddansk Universitet

February 5, 2008
JFB

DM508 – Algorithms and Complexity – F08
Lecture 4

Lecture, February 4

We covered section 3.5 of the DM508 notes, plus median finding from chapter 9 (sections 9.2 and 9.3) in the textbook. We also began on NP-completeness, from chapter 34 in the textbook and the section by Papadimitriou and Steiglitz from the course notes.

Lecture, February 6

We will continue with NP-Completeness, covering Cook's Theorem and beginning on some reductions.

Lecture, February 11

We will continue with NP-Completeness.

Problems to be discussed on February 15

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.