Institut for Matematik og Datalogi
Syddansk Universitet

November 3, 2005
JFB

DM19 – Algorithms and Complexity – E05 – Lecture 9

Lecture, November 2

We continued with NP-completeness, covering Cook's Theorem and covering the reductions from SATISFIABILITY to CIRCUIT SATISFIABILITY and 3-SAT.

Lectures, November 10 and 11

Since there is no lecture on Wednesday in this week, the second half of the discussion section times will be used for lecture, with the same material covered both days. We will finish NP-completeness.

Lecture, November 16

We will begin on approximation algorithms from chapter 35 in the textbook.

Problems to be discussed in week 46

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: $n \in \mathbb{N}$
   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.

Announcement

Igen i år afholder fakultetet KarriereKick, hvor de studerende kan få inspiration til fremtidens job og karriere. Arrangementet, som er gratis, finder sted torsdag d. 17. november kl. 15 i U45. Man skal tilmelde sig på nettet: www.karrierekick.sdu.dk