Institut for Matematik og Datalogi
Syddansk Universitet

April 19, 2013
JFB

DM508 – Algorithms and Complexity – 2013
Lecture 5

Lecture, April 17

We continued with NP-Completeness, defining reductions (section 34.3 in the textbook) and showing that Circuit Satisfiability, 3-SAT and CLIQUE are NP-Complete. The latter two reductions are in sections 34.4 and 34.5 in the textbook.

Lecture, April 22

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

Lecture, April 29

We will show that HAMILTONIAN CIRCUIT, SUBSET SUM, VERTEX COVER and INDEPENDENT SET are NP-Compete. This is in section 34.5 in the textbook.

Problems to be discussed on April 30

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.

Assignment due Monday, May 6, 10:15

Note that this is part of your exam project, so it must be approved in order for you to take the exam in June, and you may not work with or get help from others not in your group (though you may talk with Marie Christ or myself). No part of your work may be taken from another source. You may work in groups of two or three. You may write your solutions in English or Danish, but write very neatly if you do it by hand. Submit the assignment via Blackboard's "SDU Assignment" as one PDF file. Turn in one assignment per group.

1. In the *Partition* problem, a finite set A is given, along with a positive integer size $s(a)$, for each $a \in A$. The problem is to determine if there exists a subset $A' \subset A$ such that $\sum_{a \in A'} s(a) = \sum_{a \in A \setminus A'} s(a)$ (i.e. can you partition the set into two subsets so the sizes of the items add together to exactly the same amount?).

   In the *Bin Packing* problem, a positive integer bin capacity B, a positive integer K, and a finite set A is given, along with a positive integer size $s(a)$, for each $a \in A$. The problem is to determine if there exists a partition of A into disjoint sets $A_1, A_2, ..., A_K$ such that the sum of the sizes of the items in each A_i is B or less. (This partition into disjoint sets gives a packing into K bins.)

   - Partition is known to be NP-complete. Using this fact, prove that Bin Packing is also NP-complete.
   - Show that if there is an algorithm for Bin Packing which runs in time $f(n)$ for some function f, then there is an algorithm for the cost version (evaluation version) of Bin Packing (find the cost of the packing which uses fewest bins, where the cost is the number of bins used) which runs in time $O(p(f(n))$ for some polynomial p.
   - Suppose that you know that in the optimal packing there are at most 8 items per bin and that there is an algorithm for Bin Packing which runs in time $f(n)$ for some function f. Show that then there is an algorithm for finding an optimal packing (one that uses the smallest possible number of bins) which runs in time $O(p(f(n))$ for some polynomial p.

2. In the *half true 4-CNF satisfiability* problem, a 4-CNF formula (CNF form, with exactly 4 literals per clause) F is given. One knows that at least half of the clauses

are satisfiable by any truth assignment. The problem is to determine if there exists a truth assignment to the variables of F which satisfies the entire formula. Prove that the half true 4-CNF satisfiability problem is NP-complete.