Proeftentamen, uitwerkingen
(open boek) 8.10.2004

We give the answers in the form they would be counted as sufficient for the exam. In some problems there could be more than one correct answer.

1. *Define the Satisfiability problem* SAT *and formulate Cook's theorem.*

   Satsfiability problem SAT: Given a boolean formula $F(x_1, \ldots, x_n)$ determine whether there is an assignment of bits $0, 1$ to variables $x_1, \ldots, x_n$, such that F evaluates to 1 under this assignment.

   Cook Theorem: SAT is a NP-complete problem.

2. *Prove using the pumping lemma that the language* $L = \{0^n 10^n : n \geq 0\}$ *is not regular.*

   Let p be the pumping length and consider the word $w = 0^p 10^p$. By pumping lemma $w = xyz$ such that $|xy| \leq p$, $|y| > 0$ and $xy^i z \in L$, for each $i \geq 0$. The part xy must consist only of zeros, hence $xy^2 z$ violates the definition of L.

3. *Is* $\overline{\mathsf{HALT}} \leq_p \mathsf{HALT}$*?*

   No, this is not the case. For any sets A and B, if $A \leq_p B$ and B is r.e., then so is A. An acceptor for A can be constructed from that for B: given x compute $y = f(x)$ and apply the acceptor for B to y.

4. *Find* $d = gcd(126, 330)$ *following Euclid algorithm. Find integers* n *and* m *such that* $126n + 330m = d$*. (Using a calculator is not allowed in this problem.)*

   Compute by successive divisions:

$$\begin{aligned} 330 &= 126 \cdot 2 + 78 \\ 126 &= 78 \cdot 1 + 48 \\ 78 &= 48 \cdot 1 + 30 \\ 48 &= 30 \cdot 1 + 18 \\ 30 &= 18 \cdot 1 + 12 \\ 18 &= 12 \cdot 1 + 6 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

Hence, $\gcd(330, 126) = 6$, the last non-zero remainder.

Backwards substitution gives:

$$\begin{aligned}
6 &= 18 - 12 \cdot 1 \\
&= 18 - (30 - 18) \\
&= 18 \cdot 2 - 30 \\
&= (48 - 30) \cdot 2 - 30 \\
&= 48 \cdot 2 - 30 \cdot 3 \\
&= 48 \cdot 2 - (78 - 48) \cdot 3 \\
&= 48 \cdot 5 - 78 \cdot 3 \\
&= (126 - 78) \cdot 5 - 78 \cdot 3 \\
&= 126 \cdot 5 - 78 \cdot 8 \\
&= 126 \cdot 5 - (330 - 126 \cdot 2) \cdot 8 \\
&= 126 \cdot 21 - 330 \cdot 8
\end{aligned}$$

Answer: $6 = 330 \cdot (-8) + 126 \cdot 21$.

5. *Show that the problem of testing whether a number is composite (not prime) is in the class NP.*

   A problem A is in NP, if there exists a polytime computable verifier $V(x, c)$ and a polynomial $p(y)$ such that

   $$x \in A \iff \exists c\, (|c| \leq p(|x|) \& V(x, c) \text{ accepts}).$$

   For the problem of compositeness, let $V(x, c)$ accept if c is a number dividing x. Clearly, V is polytime computable. x is composite, if it has a divisor c which is smaller than x, so we can take $p(y) = y$.

6. *Let* Iso-Clique *be the set of all (codes of) triples $\langle G, m, k\rangle$ such that G is a graph, G has a clique of size k and G has (at least) m isolated points ($k, m \leq |G|$). Show that* Iso-Clique *is NP-complete. Hint: construct a p-reduction from* Clique *to* Iso-Clique.

   We have to check 1) that Iso-Clique is from NP and 2) that for any language $A \in$ NP, $A \leq_p$ Iso-Clique.

   1) As a certificate c we take $c = \langle c_1, c_2\rangle$, where c_1 is a set of k points and c_2 is a set of m points. A polytime verifier for Iso-Clique $V(c, x)$

checks in polynomial time if c_1 is a clique and if each of the points from c_2 is isolated.

2) It is sufficient to construct a p-reduction from CLIQUE to ISO-CLIQUE. Given an input $\langle G, k\rangle$ of the CLIQUE problem, we count the number m of isolated points of G (which we can do in polytime) and let the reduction function be defined as follows:

$$f(\langle G, k\rangle) := \langle G, k, m\rangle.$$

Then, as required,

$$x \in \text{CLIQUE} \iff f(x) \in \text{ISO-CLIQUE}.$$

7. *Is* CLIQUE $\leq_p$ TQBF*? (Motivate your answer.)*
Show: If TQBF $\leq_p$ CLIQUE*, then* PSPACE = NP.

1) Yes, because CLIQUE is in NP, hence in PSPACE. Any PSPACE problem is reducible to TQBF, because it is PSPACE-complete.

2) Suppose TQBF $\leq_p$ CLIQUE. Since TQBF is PSPACE-complete, any problem A from PSPACE is reducible to it, and by transitivity of $\leq_p$, $A \leq_p$ CLIQUE. Hence, $A \in$ NP, because CLIQUE $\in$ NP. Thus, we have proved that any problem from PSPACE belongs to NP, that is, PSPACE $\subseteq$ NP. The opposite inclusion holds by Savitch theorem.