Complexity Theory 2004 – Paper 6 Question 12 (AD)

(*a*) Define a one-way function. [4 marks]

A one-way function is a function f meeting the following conditions:

1. f is one-to-one.
2. for each x, $|x|^{1/k} \leq |f(x)| \leq |x|^k$ for some k.
3. $f \in \text{FP}$.
4. $f^{-1} \notin \text{FP}$.

(*b*) Explain why the existence of one-way functions would imply that P≠NP. [7 marks]

Suppose f is a one-way function. Define the language $L_f = \{(x, y) \mid \exists z(z \leq x \text{ and } f(z) = y\}$. It is easy to see that this language is in NP. Given an input (x, y), we can nondeterministically guess a value $z \leq x$, compute $f(z)$ and verify the result is y. Since f is computable in polynomial time, this verification is in polynomial time.

Now, suppose L_f was in P. Then, using a binary search algorithm we could compute f^{-1} in polynomial time. This contradicts part (4) of the definition. Thus, if f is a one-way function then L_f is a language that is in NP but not in P.

(*c*) Recall that `Reach` is the problem of deciding, given a graph G a source vertex s and a target vertex t whether G contains a path from s to t; and `Sat` is the problem of deciding whether a given Boolean formula is satisfiable.

For each of the following statements, state whether it is true or false and justify your answer.

(*i*) If `Reach` is NP-complete then P=NP. [3 marks]

True. `Reach` is known to be in P. If it was NP-complete, then every problem in NP would be in P.

(*ii*) If `Reach` is NP-complete then NP≠PSPACE. [3 marks]

True. `Reach` is in the class NL. If it were NP-complete, then every problem in NP would be in NL. But, since PSPACE is known to be different to NL.

(*iii*) If `Sat` is PSPACE-complete then NP=PSPACE. [3 marks]

True. `Sat` is known to be in NP. If it were PSPACE-complete, then every problem in PSPACE would be in NP.

One-way functions are defined in Lecture 9. The first two parts of the question cover cryptographic complexity, relating to the fourth of the objectives of the course.

Part (c) relates to space complexity and the reachability method, covered in Lectures 10 and 11. It requires knowledge of the interrelationships between complexity classes (objective 3).