Assignment 3 of Automated Software Validation Course

Tool to be used: PVS theorem prover http://pvs.csl.sri.com/

Due Date: June 19, 2007

Attach a tar file in a single e-mail to abhik@csa.iisc.ernet.in

The assignment should be done individually. No late submissions please.

In this assignment, your task is to define insertion sort and prove its correctness using the PVS theorem prover. For this question, we only consider sorting of **lists of natural numbers**.

You will need the functions ***insert***, ***sort*** and a predicate ***sorted***

In particular, ***insert x xs*** should insert a natural number ***x*** into an already sorted list of natural numbers ***xs*** and return the resultant list.

Further, ***sort xs*** should build on insert to return the sorted version of the list ***xs***.

Finally, the predicate ***sorted xs*** is true if and only if the list ***xs*** is sorted.

You should try to formalize and prove a theorem of the form

For all lists of natural numbers ***xs***, ***sorted(sort xs)*** is true

Is the above theorem enough to prove the correctness of insertion sort? In particular, does it guarantee that given a list of natural numbers ***xs***, the function ***sort*** will always return the sorted version of ***xs***? If you think the above theorem is enough to prove correctness, give justifications for your answer. If you think that the above theorem is not enough, propose additional theorems and prove them using PVS.

Submit the relevant PVS files, as well as a separate report (pdf file) describing your proof attempt as well as the relevant proof trees. All of these should be submitted as a single tar file and attached with your e-mail.