GCMPSC 266 - Formal Specification and Verification

Homework #3 - Winter 2009

Program Proofs Using UNISEX

Due: Tuesday 27 Jan 09

Consider the following program which divides x by y and returns the quotient in quot and the remainder in rem.

```
 1  program divide;
 2  var
 3    x,y,quot,rem: integer;
 4  begin
 5    {: assume ((x>=0),(y>=0)) :};
 6    quot := 0;
 7    rem := x;
 8    {: assert ((x=quot*y+rem),(rem>=0),(x=x'),(y=y')) :}
 9    while rem>=y do
10       begin
11          quot := quot+1;
12          rem := rem-y
13       end;
14     {: prove ((x'=quot*y'+rem),(rem>=0),(rem<y')) :}
15  end.
```

1. Use the UNISEX system to generate the necessary verification conditions to verify that this program is consistent with its specifications.

2. Use the UNISEX system to generate the necessary verification conditions to verify the program that you symbolically executed by hand for the second part of homework #2.

I want you to hand in a transcript of both sessions. You can use the script command to do this.

3. Use the UNISEX system to test/and verify a program using arrays. You need not turn in this problem, but you will be expected to know how to deal with arrays on the final exam.

The UNISEX symbolic executer for Red Hat Linux is at

/usr/local/bin/unisex

Therefore, you should not need to change your PATH.

Unfortunately, the only Red Hat Linux 7.3 machine is pepe. Therefore, you will have to ssh to pepe to run unisex.