Semantics of Programming Languages  
Exercise Sheet 12

Use the template file `Ex12_Template.thy`.

**Exercise 12.1  Warm-up**

Write a program `MAX` which stores the maximum value of the two variables 0 and 1 in variable 2. Verify `MAX`, i.e., prove the verification condition induced by `MAX`.

**Exercise 12.2  Multiplication**

Write a program `MULTIPLY` which computes the product of the two variables 0 and 1, storing the result in variable 2. The program must not modify the two input variables, but you can use any auxiliary variables in the program. Prove the verification condition of `MULTIPLY`.

**Exercise 12.3  Factorial**

Write a program `FACTORIAL` which computes the factorial of the variable 0. The result should be stored in variable 1. Your program must not modify the input variable, but can use additional variables during its computation. You may re-use the program `MULTIPLY` from the previous exercise. Prove that your program is sound.

**Homework 12**

*Submission until Wednesday, February 2, 2011, 12:00 (noon).*

Euclid’s algorithm computes the greatest common divisor of two numbers. Its pseudocode looks as follows:

```
while a ≠ b do  
  if a < b then  
    b := b − a  
  else  
    a := a − b
```
(a) Write a program $SUB$ which computes the difference between variable $0$ and variable $1$, without modifying them. The result should be stored in variable $2$. Prove its verification condition.

(b) Write a program $EUCLID$, which implements Euclid’s algorithm, and prove its soundness. The program should not modify the input variables, but otherwise might use any additional variables.