Problem Set 5
Safe and Secure Software (WS 11/12)

Bauhaus-University Weimar, Chair of Media Security
Prof. Dr. Stefan Lucks, Christian Forler
Url: `http://www.uni-weimar.de/cms/medien/mediensicherheit.html`

Problem 1: Hoare Logic (3 Points)
Show the partical correctness for the following code.

```
{X=0, Y=1}
while X /= N loop
   X := X+1;
   Y := Y*X;
end loop;
{X >= N, Y=N!}
```

Mini-Project 1: Let's Spark Coffee Machine (4 Points)
Modify the package specification with SPARK annotations to allow a complete

- exception freeness,
- data flow, and
- information flow analysis

using the SPARK `Examiner`.

```
package Coffee_Machine is
   -- Simulation of a coin-driven coffee machine
   -- User: - One slot to insert coins (only, 10 or, 20 cents)
   --       - One button to press (''money back'')
   -- Machine: one slot to drop coins, the coffee output
   -- Given 30 cents or more, the coffee is produced immediately
   -- (Note that Overspending is Possible)

   type State is private;
   type Action is(Ten_Cent, Twenty_Cent, Button);
   type Reaction is(Nothing, Drop_All_Coins, Coffee);

   procedure Initialize( X : out State);
   procedure X(S     : in out State;
               Act   : in Action;
               React : out Reaction);

private
   type State is range 0..2;
end Coffee_Machine;
```

Mini-Project 2: Hoare Logic (4 Points)

Show the correctness for the following code.

```
{I=0, S=0, N>0}
while I /= N loop
   I := I+1;
   S := S+(2I-1);
end loop;
{S = N**2 }
```

Mini-Project 3: Graph Algorithms Tests (4 Points)

Consider reasonable test cases for the graph algorithms package specification. Think about equivalence classes, limits, invariants etc. Then write a `testgen` "test driver" and justify each test. Finally, convince your fellow students and lecturer that your test-driver is a good one.