UNI
FR
UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

Foundations of Dependable Systems
Department of Informatics
University of Fribourg, Switzerland

Verification of Cyber-physical Systems : Exercise Sheet 1

Deadline : Monday 2nd October 2017, 11 :59 pm

Contact information

Prisca Dotti

Office : B402

Email : prisca.dotti@unifr.ch

Exercise 1 : A first *Promela* model

Write a *Promela* model containing two processes and a global `byte` variable initialised to 0 such that :

1. The first process should increment the byte variable, if it is lower than 255.
2. The second process should decrement the byte variable, if it is greater than 0.
3. The processes repeat themselves indefinitely (using the `goto` statement).

Design your model such that we can use the verifier to find out if the variable can reach value 255.

Exercise 2 : Spin's execution model

Using the properties of the *Spin* execution model, write a *Promela* model that is equivalent to the one below, but contains no `if`, `->`, or `goto` statements.

```
mtype = { P , C };

mtype turn = P;

active proctype producer(){
        wait: if
        :: (turn == P)->
                printf("Produce\n");
                turn = C;
                goto wait
            :: else -> goto wait
        fi;
}

active proctype consumer(){
        wait: if
        :: (turn == C)->
                printf("Consume\n");
                turn = P;
                goto wait
        :: else -> goto wait
        fi;
}
```

Exercise 3 : Fairness

Consider the following model :

```
byte x = 2;

active proctype A(){
        do
                :: x = 3-x; progress: skip;
        od
}

active proctype B(){
        do
                :: x = 3-x; progress: skip;
        od
}
```

When looking for non-progress cycles :

1. Does Spin detect an error when using the *weak fairness* constraint ?
2. Does Spin detect an error when is not using the weak fairness constraint ?

Since both processes are identical, we can check fairness of one process by removing one of the `progress` labels. Do you have any idea how to prove fairness not only for one process but for both processes ?

Submit your commented `.pml` files on *Ilias* and also paste it in your PDF submission.