GAS STATION PROBLEM

(Robert Meolic, 2006, 2013)

The system consists of an operator, a pump, and customers. A queue is added to the system for holding customers requests. The operator initially accepts money prepaid by customers and then activates the pump if it is available. On receiving the charge information from the pump, the operator gives the change to the customer.

The problem is taken from: S.C. Cheung and J. Kramer. Checking Subsystem Safety Properties in Compositional Reachability Analysis. In The Proceedings of ICSE, pages 144-154, 1996.
http://repository.ust.hk/dspace/bitstream/1783.1/2095/1/1_5checksub.pdf

File **gas2.ccs** contains description of the system and safety properties:

```
OPERATOR = (?prepay1+?prepay2).OP_PREPAID + (?charge1.!payment1+?charge2.!
payment2).OP_CHARGED
OP_PREPAID = (?available.!activate+!occupied).OPERATOR
OP_CHARGED = (!change1.!return1+!change2.!return2).(?wait.!activate+!
none).OPERATOR
QUEUE = !available.QUEUE_ACTIVE
QUEUE_ACTIVE = ?none.QUEUE + ?occupied.!wait.QUEUE_ACTIVE
PUMP = ?activate.(?start1+?start2).(?stop1+?stop2).(!charge1+!charge2).PUMP
CUST = !prepay.!start.!stop.?change.CUST
net COUNTER = OPERATOR |[available,occupied,none,wait]| QUEUE
net STATION = COUNTER |[activate,charge1,charge2]| PUMP
net CUSTOMERS = (CUST [prepay1/prepay][start1/start][stop1/stop][change1/change]
                 ||| CUST [prepay2/prepay][start2/start][stop2/stop]
[change2/change])
net SYSTEM = STATION |
[prepay1,prepay2,start1,start2,stop1,stop2,change1,change2]| CUSTOMERS

property F1 == NOT EF <!payment1> E[true {NOT !return1} U {!return2} true];
property F2 == NOT EF <!payment2> E[true {NOT !return2} U {!return1} true];
property F3 == AG [!payment1] A[true {NOT !payment2} U {!return1} true];
property F4 == AG [!payment2] A[true {NOT !payment1} U {!return2} true];
```

Here is the log from EST:

```
Efficient Symbolic Tools, 2nd Edition, Copyright (C) 2003-2013 UM-FERI
This is free software, and comes with ABSOLUTELY NO WARRANTY.
You are welcome to redistribute EST; type "license" for details.

Running on i686 (Linux, 3.2.0-40-generic-pae) with tcl 8.5.11 and tk 8.5.11.

Initialization of GUI package... OK
Initialization of BDD package... OK
Initialization of Process_Algebra package... OK
Initialization of Versis package... OK
Initialization of Model checking package... OK
Initialization of Strucval package... OK
Initialization of CCS package... OK
Ready.

>cd "/home/meolic/est/est-2ed/data/gas"; source "gas2.tcl"; cd "/home/meolic/est/est-2ed/data"
Reading file: gas2.ccs
  Process OPERATOR ... OK
  Process OP_PREPAID ... OK
  Process OP_CHARGED ... OK
  Process QUEUE ... OK
```

```
  Process QUEUE_ACTIVE ... OK
  Process PUMP ... OK
  Process CUST ... OK
  Net COUNTER
    Composition ... OK
    Creating process COUNTER ... OK
  Net STATION
    Composition ... OK
    Creating process STATION ... OK
  Net CUSTOMERS
    Composition ... OK
    Creating process CUSTOMERS ... OK
  Net SYSTEM
    Composition ... OK
    Creating process SYSTEM ... OK
  Property F1
    F1 = NOT EF <!payment1> E[true {NOT !return1}U{!return2} true];
  Property F2
    F2 = NOT EF <!payment2> E[true {NOT !return2}U{!return1} true];
  Property F3
    F3 = AG [!payment1] A[true {NOT !payment2}U{!return1} true];
  Property F4
    F4 = AG [!payment2] A[true {NOT !payment1}U{!return2} true];

ACTL/ACTLW model checking on process SYSTEM
NOT EF <!payment1> E[true {NOT !return1}U{!return2} true] ==> FALSE
Counterexample: (TAU)(TAU)(TAU)(TAU)(TAU)(TAU)(payment1!)(TAU)(return2!)

ACTL/ACTLW model checking on process SYSTEM
NOT EF <!payment2> E[true {NOT !return2}U{!return1} true] ==> FALSE
Counterexample: (TAU)(TAU)(TAU)(TAU)(TAU)(TAU)(payment2!)(TAU)(return1!)

ACTL/ACTLW model checking on process SYSTEM
AG [!payment1] A[true {NOT !payment2}U{!return1} true] ==> FALSE
Counterexample: (TAU)(TAU)(TAU)(TAU)(TAU)(TAU)(payment1!)(TAU)(return2!)(TAU)(TAU)(TAU)(TAU)(TAU)
(TAU)(TAU)(payment2!)

ACTL/ACTLW model checking on process SYSTEM
AG [!payment2] A[true {NOT !payment1}U{!return2} true] ==> FALSE
Counterexample: (TAU)(TAU)(TAU)(TAU)(TAU)(TAU)(payment2!)(TAU)(return1!)(TAU)(TAU)(TAU)(TAU)(TAU)
(TAU)(TAU)(payment1!)
```