NSWI101: System Behaviour Models and Verification

Lab 04 – More Spin exercises

Jan Kofroň

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

Department of
Distributed and
Dependable
Systems

EXERCISE

Estimate how many reachable states there are for the following model.
Draw the complete reachability tree.

```
#define N 2
init {
        chan dummy = [N] of { byte };
        do
        :: dummy!85
        :: dummy!170
        od
}
```

Exercise – Evaluation

```
$ spin -m -a ex1b.pml    # use -m to ignore buffer overflow
$ gcc -o pan pan.c
$ ./pan -co              # use -co to avoid stopping on errors
```

Comments on Memory usage I.

The efficiency of the conventional reachability analysis is determined by the state space storage functions. To study this, repeat the last verification run with a smaller and a bigger hash table for storing reachable states:

```
$ pan -w10 # hash table with 210 slots ...
$ pan -w20 # hash table with 220 slots ...
```

Comments on Memory usage II.

Bit-state hashing method

- Probabilistic approach
- Uses all available (specified) memory
- Might miss some states

```
$ spin –m –a ex.1b.pml          # as before
$ gcc –DBITSTATE –o pan pan.c   # different
$ ./pan
```

Exercise: Producer-Consumer Model

Describe producer/consumer problem in Promela using channels and check the model for invalid end states (deadlocks) and channels' buffer overruns

- i.e., suppose channels are not blocked (messages get lost instead) and you must control the number of messages within the channel by hand

Distributed consensus (election algorithm)

- Model algorithm for finding coordinator in distributed environment:
  - processes are subjects of being coordinator
  - one special process acts as network both reliable and unreliable (may cut off some processes)
  - fixed architecture, everything transmitted through network process
- What properties would we require?