Software Quality FS 2010

Exercise 1 - Discussion

Cédric Jeanneret

Requirements Engineering Research Group
Department of Informatics
University of Zurich
http://www.ifi.uzh.ch/rerg/people/jeanneret

University of Zurich
Department of Informatics

Grading
What does P, S, L, M, A stand for?

- Exercise 1 had 5 parts:
  - P: Introducing Promela (2.1.1 – 2.1.2)
  - S: Verifying LTL properties with SPIN (2.1.3 – 2.1.4.g)
  - L: Investigating the limitations of SPIN (2.1.4.h – 2.1.5)
  - M: Verifying solutions to an SE problem: mutual exclusion (2.3)
  - A: Preparing your Agile Development Environment (3)
- Ordinal scale: X, --, -, ~, +, ++
- Average: **median**
  - The median of 3 assignments is the second-ranked grade

General Remarks

Good in average (but many groups forgot 2.3)

Do not underestimate the effort

Advise 1: start early

Advise 2: read the assignment carefully

- a « bullet » often contains 2 parts: experiment and explain
- when copying from the Internet, copy the right thing

Promela (2.1.2)
Non determinism and d_steps

```
active proctype mutations() {
    do
    :: d_step { nRed && nBlue;
          nRed--; nBlue--; nGreen = nGreen + 2; }
    :: d_step { nRed && nGreen;
          nRed--; nGreen--; nBlue = nBlue + 2; }
    :: d_step { nBlue && nGreen;
          nBlue--; nGreen--; nRed = nRed + 2; }
    :: else
    od }
```

LTL Properties (2.1.3.c & 2.1.4.e)

Safety? Liveness? Both? None?

Safety

- *Something bad will never happen*
- Violations always have a finite witness
- Checked on finite executions
- □¬ all chameleons are of the same color

Liveness

- *Something good will eventually happen*
- Violations never have a finite witness
- Checked on infinite executions
- □◊ some chameleons transmute

Violations of Liveness Properties

Ex: Starvation of P1 with Semaphores

```
spin -t -p  Semaphore.pml
Starting P1 with pid 0
Starting P2 with pid 1
spin: couldn't find claim (ignored)
  2:    proc  1 (P2) line  33 "Semaphore.pml" (state 1) [t2 = 1]
  3:    proc  1 (P2) line  34 "Semaphore.pml" (state 2) [(semaphore)]
  3:    proc  1 (P2) line  34 "Semaphore.pml" (state 3) [semaphore = (semaphore-1)]
  3:    proc  1 (P2) line  35 "Semaphore.pml" (state 4) [c2 = 1]
  5:    proc  0 (P1) line  14 "Semaphore.pml" (state 1) [t1 = 1]
  7:    proc  1 (P2) line  40 "Semaphore.pml" (state 6) [semaphore = (semaphore+1)]
  7:    proc  1 (P2) line  41 "Semaphore.pml" (state 7) [t2 = 0]
  7:    proc  1 (P2) line  42 "Semaphore.pml" (state 8) [c2 = 0]
 <<<<<START OF CYCLE>>>>>
  9:    proc  1 (P2) line  33 "Semaphore.pml" (state 1) [t2 = 1]
 10:    proc  1 (P2) line  34 "Semaphore.pml" (state 2) [(semaphore)]
 10:    proc  1 (P2) line  34 "Semaphore.pml" (state 3) [semaphore = (semaphore-1)]
 10:    proc  1 (P2) line  35 "Semaphore.pml" (state 4) [c2 = 1]
 12:    proc  1 (P2) line  40 "Semaphore.pml" (state 6) [semaphore = (semaphore+1)]
 12:    proc  1 (P2) line  41 "Semaphore.pml" (state 7) [t2 = 0]
 12:    proc  1 (P2) line  42 "Semaphore.pml" (state 8) [c2 = 0]
```

SPIN (2.1.3.h)
Steps, Transitions and States

pan: claim violated! (**at depth 43**)
pan: wrote Colony.pml.trail

(Spin Version 5.2.4 -- 2 December 2009)
Warning: **Search not completed**
+ Partial Order Reduction

[…]

State-vector 28 byte, **depth reached 43**, errors: 1
22 states, stored
0 states, matched
22 transitions (= stored+matched)
0 atomic steps
hash conflicts: 0 (resolved)

4.653 memory usage (Mbyte)

Statistics about the **trace found**
- *Depth*: # of transitions from the initial system state

Statistics about the (incomplete) **search**
- *Transitions*: # of system states
- *Stored states*: # of unique system states
- *Depth*: longest trace

SPIN (2.1.3.h)
Steps, Transitions and States

./pan –d

Automaton for the mutation process

```
proctype mutations
      state  23 -(tr   7)-> state  23  [id   6 tp   2] [D---G] line 13 => D_STEP
      state  23 -(tr   8)-> state  23  [id  13 tp   2] [D---G] line 13 => D_STEP
      state  23 -(tr   9)-> state  23  [id  20 tp   2] [D---G] line 13 => D_STEP
      state  23 -(tr   2)-> state  23  [id  21 tp   2] [----G] line 13 => else
state 23 line 13 is a loopstate
proctype :never:
      state   5 -(tr   3)-> state   7  [id  31 tp   2] [----G] line 48 =>
               (!((((nRed&&nBlue)||(nRed&&nGreen))||(nGreen&&nBlue))))
      state   5 -(tr   1)-> state   5  [id  33 tp   2] [----G] line 48 => (1)
      state   7 -(tr   1)-> state   8  [id  37 tp   2] [-a--L] line 52 => (1)
      state   8 -(tr   4)-> state   0  [id  38 tp 3500] [--e-L] line 53 => -end-      [(257,9)]
state 5 line 48 is a loopstate
```

Automaton for the verification of the property

SPIN (2.1.3.h)
Steps, Transitions and States

```
./spin –t Colony.pml
spin: couldn't find claim (ignored)
        (1) 19 R, 16 B, 18 G chameleons
        (2) 18 R, 15 B, 20 G chameleons
        […]
        (19) 1 R, 1 B, 51 G chameleons
        (20) 0 R, 0 B, 53 G chameleons
spin: trail ends after 43 steps
#processes: 1
                nMut = 20
                nRed = 0
                nBlue = 0
                nGreen = 53
 43:proc  0 (mutations) line  12 "Colony.pml" (state 23)
1 process created
```

SPIN (2.1.4.g – 2.1.5)
Limitations

Number of states explodes rapidly.

- for N=250 (400 Mb, 7.6 sec)
  - ~ 2 million reachable states
  - ~1 million steps deep

If the search is not exhaustive, no guarantee to find a violation, even within the search range.

- extinction possible with N=25, but not with N=300

The order of process declarations changes the shape of the search tree.

Agile Development Environment

Everybody is ready for assignment #2

Observe discipline within a development team!

Have a look at…

- Tickets: http://daiquiri.ifi.uzh.ch/trac/swq10/report/6
- Commits: http://daiquiri.ifi.uzh.ch/trac/swq10/browser

Agile Development Environment
Tickets

Ex 1 Complete (8 matches)

Ticket	Summary	Component	Status	Resolution	Version	Type	Priority	Owner	Modified
#13	access to svn	SVN Registration	accepted	None		task	blocker	m1049749	03/15/10
#20	Access to version control repository	SVN Registration	accepted	None		task	major	m1049749	03/21/10
#2	Registration of s0280007	SVN Registration	closed	fixed		task	major	m1049749	03/22/10
#6	Request for access to SVN	ImageJ	closed	fixed	1.0-SNAPSHOT	task	major	m1049749	03/20/10
#12	Access to svn	SVN Registration	closed	fixed		task	blocker	m1049749	03/17/10
#10	Access to SVN	SVN Registration	closed	fixed	1.0-SNAPSHOT	task	major	m1049749	03/15/10
#8	SVN access	SVN Registration	closed	fixed		task	blocker	m1049749	03/15/10
#1	Registration of m1049749	SVN Registration	closed	fixed		task	major	m1049749	03/11/10

Ticket	Summary	Component	Status	Resolution	Version	Type	Priority	Owner	Modified
#9	Bug Tracking Trac	ImageJ	accepted	None		defect	major	m1049749	03/13/10
#19	3.1.b)	ImageJ	accepted	None		defect	major	m1049749	03/19/10
#11	swq10 / access for svn repository	SVN Registration	accepted	None		task	major	m1049749	03/18/10
#17	access to the version control repository	SVN Registration	accepted	None		task	major	m1049749	03/21/10
#18	Can you give me access to the SVN please?	SVN Registration	closed	fixed		task	major	m1049749	03/22/10
#14	Access to the version control repository	SVN Registration	closed	fixed		task	major	m1049749	03/21/10
#3	Registration of s0405498	SVN Registration	closed	fixed		defect	major	m1049749	03/19/10
#16	access to the version control repository	ImageJ	closed	fixed		task	major	m1049749	03/18/10
#4	Can I have access to the SVN repository?	SVN Registration	closed	fixed		task	major	m1049749	03/15/10
#5	access to SVN repository	SVN Registration	closed	fixed		task	major	m1049749	03/15/10
#7	Request for access to SVN	ImageJ	closed	fixed		task	major	m1049749	03/15/10
#15	access for svn repository	SVN Registration	closed	fixed		task	major	m1049749	03/15/10

Agile Development Environment
Commits

Name	Size	Rev	Age	Last Change
ImageJ		15	6 days	s057081: Initial import.
Maven 2		15	6 days	s057081: Initial import.
ImageJ		20	4 days	s057081: Initial import.
Maven		20	4 days	s057081: Initial import.
Maven 2 Trunk		16	6 days	s057081: Initial import.
Maven2		21	4 days	s057081: Initial import.
Maven 2		22	4 days	s057081: Initial import.
src		2	3 weeks	m1049749:
main		2	3 weeks	m1049749:
test		2	3 weeks	m1049749:
Participants.txt	300 bytes	24	3 days	s0280007: Exercise Registration ~~ticket:2~~
pom.xml	476 bytes	2	3 weeks	m1049749:

Property **svn:ignore** set to target