Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и технологий
Кафедра компьютерных систем и программных технологий

Верификация анализ программ

Отчет по лабораторной работе №2
Проверка модели семафора

Работу выполнил:
Тарасов С.И.
Группа:
3540901/91502
Преподаватель:
Ицыксон В.М.

Санкт-Петербург
2020

Содержание

1. Цель работы

Составить при помощи NuSMV модель программы с 5-ю пользователями и ресурсом, который защищён семафором. Проверить свойства при помощи LTL формул:

1) При инициализации семафора значением 1 убедиться, что в критической секции не может быть больше одного процесса

2) Убедиться, что каждый процесс в конце концов получит доступ к критической секции

3) При инициализации семафора значением 3 убедиться, что в критической секции может быть 1, 2 или 3 процесса

4) При инициализации семафора значением 3 убедиться, что в критической секции не может быть 4 процесса

2. Теоретическая информация

Семафор - инструмент синхронизации доступа к ресурсу при помощи специальных токенов, максимальное количество которых задаётся при инициализации. От количества токенов зависит максимальное число потоков, которые могут использовать ресурс одновременно. При отсутствии токенов, семафор блокирует все процессы до высвобождения токенов.

3. Ход выполнения работы

Для моделирования программы использовался NuSMV - расширение SMV, которое производит проверку моделей на соответствие LTL или CTL формулам, которые выражают некоторые свойства программы. Программа представляется в виде конечного автомата.

Программа моделирования представлена на листинге.

Листинг 1: Программа моделирования

```
1  MODULE main
2   VAR
3      semaphore    : {0,1,2,3,4,5,6,7,8,9,10};
4      apr          :0 .. 4                    ;
5      proc0        : process user(semaphore,0,apr);
6      proc1        : process user(semaphore,1,apr);
7      proc2        : process user(semaphore,2,apr);
8      proc3        : process user(semaphore,3,apr);
9      proc4        : process user(semaphore,4,apr);
10   ASSIGN
11     init(semaphore) := 1;
12     init(apr) :=0;
13
14
15 LTLSPEC (F (proc0.state = critical2) & F (proc1.state = critical2) & F (proc2.
       ↪ state = critical2) & F (proc3.state = critical2) & F (proc4.state =
       ↪ critical2))
16 LTLSPEC (! F (proc0.state = critical2 & proc1.state = idle & proc2.state = idle
       ↪ & proc3.state = idle & proc4.state = idle))
17 LTLSPEC (! F (proc0.state = critical2 & proc1.state = critical2 & proc2.state =
       ↪ idle & proc3.state = idle & proc4.state = idle))
18 LTLSPEC (! F (proc0.state = critical2 & proc1.state = critical2 & proc2.state =
       ↪ critical2 & proc3.state = idle & proc4.state = idle))
```

```
19 LTLSPEC (! F (proc0.state = critical2 & proc1.state = critical2 & proc2.state =
     ↪ critical2 & proc3.state = critical2 & proc4.state = idle))
20 LTLSPEC (! F (proc0.state = critical2 & proc1.state = critical2 & proc2.state =
     ↪ critical2 & proc3.state = critical2 & proc4.state = critical2))
21
22
23 MODULE user(semaphore, pNum, apr)
24  VAR
25    state : {idle, enqueue, critical1, critical2, exiting};
26  ASSIGN
27    init(state) := idle;
28    next(state) :=
29      case
30        state = idle                                                    :
     ↪ enqueue;
31        state = enqueue & semaphore >0 & apr = pNum                    :
     ↪ critical1;
32        state = critical1                                               :
     ↪ critical2;
33        state = critical2                                               :
     ↪ exiting;
34        state = exiting                                                 :
     ↪ idle;
35        TRUE                                                            :
     ↪ state;
36      esac;
37
38    next(semaphore) :=
39      case
40        state = enqueue & semaphore >0 & apr = pNum  : semaphore -1;
41        state = exiting & semaphore < 1               : semaphore +1;
42        TRUE                                          : semaphore;
43      esac;
44
45    next(apr) :=
46        case
47          state = enqueue & semaphore >0 & apr = pNum & apr < 4      : apr +1;
48          state = enqueue & semaphore >0 & apr = pNum & apr = 4      :0;
49          TRUE                                                        : apr;
50        esac;
51  FAIRNESS
52    running
```

Запуск программы проверки.

Листинг 2: Программа запуска

```
1 ./NuSMV-2.6.0-Linux/bin/NuSMV ./code/smv/test.smv
```

На строках 15 - 20 выписаны LTL формулы. Первая формула проверяет, что в все потоки в конечном счёте побывают в критической секции. Вторая формула, что невозможно наличие 1 потока в критической секции. Третья - 2 потока. Четвертая - 3 потока. Пятая - 4 потока. Шестая - 5 потоков. В рамках семафора так же организована очередь с приоритетом (переменная apr) для того, чтобы ни один из потоков был заблокирован вечно.

При инициализации семафора значениями от 0 до 5 выходят результаты, представленные в примечании. При отрицательном результате проверки формулы выписывается контрпример. В приложении из логов контрпример есть только для первой формулы. Из других логов контрпример убран для сокращения размеров отчёта.

4. Выводы

В рамках работы была создана программа по построению ACT для Java кода. На данный момент программа поддерживает только базовые конструкции. Полное корректное парсирование возможно с использованием специальных инструментов.

5. Приложения

5.1. Приложение A

Ссылка на проект: https://github.com/StasyanOi/DijkstraSemaphoreNuSMV

5.2. Приложение B

Результаты моделирования при инициализации семафора нулём.

Листинг 3: Инициализация семаформа - 0

```
1  *** This is NuSMV 2.6.0 (compiled on Wed Oct 14 15:36:56 2015)
2  *** Enabled addons are: compass
3  *** For more information on NuSMV see <http://nusmv.fbk.eu>
4  *** or email to <nusmv-users@list.fbk.eu>.
5  *** Please report bugs to <Please report bugs to <nusmv-users@fbk.eu>>
6
7  *** Copyright (c) 2010-2014, Fondazione Bruno Kessler
8
9  *** This version of NuSMV is linked to the CUDD library version 2.4.1
10 *** Copyright (c) 1995-2004, Regents of the University of Colorado
11
12 *** This version of NuSMV is linked to the MiniSat SAT solver.
13 *** See http://minisat.se/MiniSat.html
14 *** Copyright (c) 2003-2006, Niklas Een, Niklas Sorensson
15 *** Copyright (c) 2007-2010, Niklas Sorensson
16
17 WARNING *** Processes are still supported, but deprecated.      ***
18 WARNING *** In the future processes may be no longer supported. ***
19
20 WARNING *** The model contains PROCESSes or ISAs. ***
21 WARNING *** The HRC hierarchy will not be usable. ***
22 -- specification ((((( F proc0.state = critical2 &  F proc1.state = critical2) &
     ↪  F proc2.state = critical2) &  F proc3.state = critical2) &  F proc4.state
     ↪  = critical2)  is false
23 -- as demonstrated by the following execution sequence
24 Trace Description: LTL Counterexample
25 Trace Type: Counterexample
26   -> State: 1.1 <-
27     semaphore = 0
28     apr = 0
29     proc0.state = idle
30     proc1.state = idle
31     proc2.state = idle
32     proc3.state = idle
33     proc4.state = idle
34   -> Input: 1.2 <-
35     _process_selector_ = proc0
36     running = FALSE
37     proc4.running = FALSE
38     proc3.running = FALSE
```

```
39      proc2.running = FALSE
40      proc1.running = FALSE
41      proc0.running = TRUE
42    -> State: 1.2 <-
43      proc0.state = enqueue
44    -> Input: 1.3 <-
45      _process_selector_ = proc1
46      proc1.running = TRUE
47      proc0.running = FALSE
48    -> State: 1.3 <-
49      proc1.state = enqueue
50    -> Input: 1.4 <-
51      _process_selector_ = proc2
52      proc2.running = TRUE
53      proc1.running = FALSE
54    -> State: 1.4 <-
55      proc2.state = enqueue
56    -> Input: 1.5 <-
57      _process_selector_ = proc3
58      proc3.running = TRUE
59      proc2.running = FALSE
60    -> State: 1.5 <-
61      proc3.state = enqueue
62    -> Input: 1.6 <-
63      _process_selector_ = proc4
64      proc4.running = TRUE
65      proc3.running = FALSE
66    -- Loop starts here
67    -> State: 1.6 <-
68      proc4.state = enqueue
69    -> Input: 1.7 <-
70      _process_selector_ = main
71      running = TRUE
72      proc4.running = FALSE
73    -- Loop starts here
74    -> State: 1.7 <-
75    -> Input: 1.8 <-
76      _process_selector_ = proc0
77      running = FALSE
78      proc0.running = TRUE
79    -- Loop starts here
80    -> State: 1.8 <-
81    -> Input: 1.9 <-
82      _process_selector_ = proc1
83      proc1.running = TRUE
84      proc0.running = FALSE
85    -- Loop starts here
86    -> State: 1.9 <-
87    -> Input: 1.10 <-
88      _process_selector_ = proc2
89      proc2.running = TRUE
90      proc1.running = FALSE
91    -- Loop starts here
92    -> State: 1.10 <-
93    -> Input: 1.11 <-
94      _process_selector_ = proc3
95      proc3.running = TRUE
96      proc2.running = FALSE
97    -- Loop starts here
98    -> State: 1.11 <-
```

```
  -> Input: 1.12 <-
    _process_selector_ = proc4
    proc4.running = TRUE
    proc3.running = FALSE
  -- Loop starts here
  -> State: 1.12 <-
  -> Input: 1.13 <-
    _process_selector_ = main
    running = TRUE
    proc4.running = FALSE
  -> State: 1.13 <-
-- specification !( F ((((proc0.state = critical2 & proc1.state = idle) & proc2.
   ↪ state = idle) & proc3.state = idle) & proc4.state = idle))  is true
-- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
   ↪ proc2.state = idle) & proc3.state = idle) & proc4.state = idle))  is true
-- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
   ↪ proc2.state = critical2) & proc3.state = idle) & proc4.state = idle))  is
   ↪ true
-- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
   ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state = idle))
   ↪   is true
-- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
   ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state =
   ↪ critical2))  is true
```

5.3. Приложение C

Результаты моделирования при инициализации семафора 1-й.

Листинг 4: Инициализация семаформа - 1

```
*** This is NuSMV 2.6.0 (compiled on Wed Oct 14 15:36:56 2015)
*** Enabled addons are: compass
*** For more information on NuSMV see <http://nusmv.fbk.eu>
*** or email to <nusmv-users@list.fbk.eu>.
*** Please report bugs to <Please report bugs to <nusmv-users@fbk.eu>>

*** Copyright (c) 2010-2014, Fondazione Bruno Kessler

*** This version of NuSMV is linked to the CUDD library version 2.4.1
*** Copyright (c) 1995-2004, Regents of the University of Colorado

*** This version of NuSMV is linked to the MiniSat SAT solver.
*** See http://minisat.se/MiniSat.html
*** Copyright (c) 2003-2006, Niklas Een, Niklas Sorensson
*** Copyright (c) 2007-2010, Niklas Sorensson

WARNING *** The model contains PROCESSes or ISAs. ***
WARNING *** The HRC hierarchy will not be usable. ***
-- specification ((( F proc0.state = critical2 &  F proc1.state = critical2) &
   ↪  F proc2.state = critical2) &  F proc3.state = critical2) &  F proc4.state
   ↪  = critical2)  is true
-- specification !( F ((((proc0.state = critical2 & proc1.state = idle) & proc2.
   ↪ state = idle) & proc3.state = idle) & proc4.state = idle))  is false
-- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
   ↪ proc2.state = idle) & proc3.state = idle) & proc4.state = idle))  is true
-- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
   ↪ proc2.state = critical2) & proc3.state = idle) & proc4.state = idle))  is
   ↪ true
```

```
23 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state = idle))
     ↪   is true
24 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state =
     ↪ critical2))  is true
```

5.4. Приложение D

Результаты моделирования при инициализации семафора 2-й.

Листинг 5: Инициализация семаформа - 2

```
1  *** This is NuSMV 2.6.0 (compiled on Wed Oct 14 15:36:56 2015)
2  *** Enabled addons are: compass
3  *** For more information on NuSMV see <http://nusmv.fbk.eu>
4  *** or email to <nusmv-users@list.fbk.eu>.
5  *** Please report bugs to <Please report bugs to <nusmv-users@fbk.eu>>
6
7  *** Copyright (c) 2010-2014, Fondazione Bruno Kessler
8
9  *** This version of NuSMV is linked to the CUDD library version 2.4.1
10 *** Copyright (c) 1995-2004, Regents of the University of Colorado
11
12 *** This version of NuSMV is linked to the MiniSat SAT solver.
13 *** See http://minisat.se/MiniSat.html
14 *** Copyright (c) 2003-2006, Niklas Een, Niklas Sorensson
15 *** Copyright (c) 2007-2010, Niklas Sorensson
16
17 WARNING *** The model contains PROCESSes or ISAs. ***
18 WARNING *** The HRC hierarchy will not be usable. ***
19 -- specification (((( F proc0.state = critical2 &  F proc1.state = critical2) &
     ↪  F proc2.state = critical2) &  F proc3.state = critical2) &  F proc4.state
     ↪  = critical2)  is true
20 -- specification !( F ((((proc0.state = critical2 & proc1.state = idle) & proc2.
     ↪ state = idle) & proc3.state = idle) & proc4.state = idle))  is false
21 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = idle) & proc3.state = idle) & proc4.state = idle))  is false
22 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = critical2) & proc3.state = idle) & proc4.state = idle))  is
     ↪ true
23 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state = idle))
     ↪   is true
24 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state =
     ↪ critical2))  is true
```

5.5. Приложение E

Результаты моделирования при инициализации семафора 3-й.

Листинг 6: 3Инициализация семаформа - 3

```
1  *** This is NuSMV 2.6.0 (compiled on Wed Oct 14 15:36:56 2015)
2  *** Enabled addons are: compass
3  *** For more information on NuSMV see <http://nusmv.fbk.eu>
4  *** or email to <nusmv-users@list.fbk.eu>.
5  *** Please report bugs to <Please report bugs to <nusmv-users@fbk.eu>>
```

```
6
7  *** Copyright (c) 2010-2014, Fondazione Bruno Kessler
8
9  *** This version of NuSMV is linked to the CUDD library version 2.4.1
10 *** Copyright (c) 1995-2004, Regents of the University of Colorado
11
12 *** This version of NuSMV is linked to the MiniSat SAT solver.
13 *** See http://minisat.se/MiniSat.html
14 *** Copyright (c) 2003-2006, Niklas Een, Niklas Sorensson
15 *** Copyright (c) 2007-2010, Niklas Sorensson
16
17 WARNING *** The model contains PROCESSes or ISAs. ***
18 WARNING *** The HRC hierarchy will not be usable. ***
19 -- specification ((((( F proc0.state = critical2 &  F proc1.state = critical2) &
       ↪  F proc2.state = critical2) &  F proc3.state = critical2) &  F proc4.state
       ↪  = critical2)  is true
20 -- specification !( F ((((proc0.state = critical2 & proc1.state = idle) & proc2.
       ↪ state = idle) & proc3.state = idle) & proc4.state = idle))  is false
21 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
       ↪ proc2.state = idle) & proc3.state = idle) & proc4.state = idle))  is false
22 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
       ↪ proc2.state = critical2) & proc3.state = idle) & proc4.state = idle))  is
       ↪ false
23 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
       ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state = idle))
       ↪   is true
24 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
       ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state =
       ↪ critical2))  is true
```

5.6. Приложение F

Результаты моделирования при инициализации семафора 4-й

Листинг 7: Инициализация семаформа - 4

```
1  *** This is NuSMV 2.6.0 (compiled on Wed Oct 14 15:36:56 2015)
2  *** Enabled addons are: compass
3  *** For more information on NuSMV see <http://nusmv.fbk.eu>
4  *** or email to <nusmv-users@list.fbk.eu>.
5  *** Please report bugs to <Please report bugs to <nusmv-users@fbk.eu>>
6
7  *** Copyright (c) 2010-2014, Fondazione Bruno Kessler
8
9  *** This version of NuSMV is linked to the CUDD library version 2.4.1
10 *** Copyright (c) 1995-2004, Regents of the University of Colorado
11
12 *** This version of NuSMV is linked to the MiniSat SAT solver.
13 *** See http://minisat.se/MiniSat.html
14 *** Copyright (c) 2003-2006, Niklas Een, Niklas Sorensson
15 *** Copyright (c) 2007-2010, Niklas Sorensson
16
17 WARNING *** The model contains PROCESSes or ISAs. ***
18 WARNING *** The HRC hierarchy will not be usable. ***
19 -- specification ((((( F proc0.state = critical2 &  F proc1.state = critical2) &
       ↪  F proc2.state = critical2) &  F proc3.state = critical2) &  F proc4.state
       ↪  = critical2)  is true
20 -- specification !( F ((((proc0.state = critical2 & proc1.state = idle) & proc2.
       ↪ state = idle) & proc3.state = idle) & proc4.state = idle))  is false
```

```
21 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = idle) & proc3.state = idle) & proc4.state = idle))  is false
22 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = critical2) & proc3.state = idle) & proc4.state = idle))  is
     ↪ false
23 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state = idle))
     ↪   is false
24 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state =
     ↪ critical2))  is true
```

5.7. Приложение G

Результаты моделирования при инициализации семафора 5-й

Листинг 8: Инициализация семаформа - 5

```
1  *** This is NuSMV 2.6.0 (compiled on Wed Oct 14 15:36:56 2015)
2  *** Enabled addons are: compass
3  *** For more information on NuSMV see <http://nusmv.fbk.eu>
4  *** or email to <nusmv-users@list.fbk.eu>.
5  *** Please report bugs to <Please report bugs to <nusmv-users@fbk.eu>>
6
7  *** Copyright (c) 2010-2014, Fondazione Bruno Kessler
8
9  *** This version of NuSMV is linked to the CUDD library version 2.4.1
10 *** Copyright (c) 1995-2004, Regents of the University of Colorado
11
12 *** This version of NuSMV is linked to the MiniSat SAT solver.
13 *** See http://minisat.se/MiniSat.html
14 *** Copyright (c) 2003-2006, Niklas Een, Niklas Sorensson
15 *** Copyright (c) 2007-2010, Niklas Sorensson
16
17 WARNING *** The model contains PROCESSes or ISAs. ***
18 WARNING *** The HRC hierarchy will not be usable. ***
19 -- specification (((( F proc0.state = critical2 &  F proc1.state = critical2) &
     ↪  F proc2.state = critical2) &  F proc3.state = critical2) &  F proc4.state
     ↪  = critical2)  is true
20 -- specification !( F ((((proc0.state = critical2 & proc1.state = idle) & proc2.
     ↪ state = idle) & proc3.state = idle) & proc4.state = idle))  is false
21 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = idle) & proc3.state = idle) & proc4.state = idle))  is false
22 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = critical2) & proc3.state = idle) & proc4.state = idle))  is
     ↪ false
23 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state = idle))
     ↪   is false
24 -- specification !( F ((((proc0.state = critical2 & proc1.state = critical2) &
     ↪ proc2.state = critical2) & proc3.state = critical2) & proc4.state =
     ↪ critical2))  is false
```