Report

Problem 1:

1. The Promela code can be found in problem1.pml
2. The sequence logs for the specified trace are shown in 1B.txt and msc.ps and can be replicated by opening problem1.pml in ispin and clicking on (Re)Run in the Simulate/Replay tab with the random seed set to 123 (default). The description for this trace is as follows:
3. Steps 0-20: System is initializing. In this step, the conditions given in the problem statements with regards to the 4 shuttles and the 2 orders are input into the system.
4. Steps 21-29: The Shuttle Management System sends order 1 to Shuttle 1.
5. Steps 30-33: Shuttle 1 begins processing the offer for the newly received order 1
6. Steps 34-36: The Shuttle Management System sends order 1 to Shuttle 2.
7. Steps 37-50: The Shuttle Management System sends order 1 to Shuttle 3.
8. Steps 51-56: Shuttle 3 begins processing the offer for the newly received order 1
9. Steps 57-59: Shuttle 2 begins processing the offer for the newly received order 1
10. Steps 60-61: The Shuttle Management System sends order 1 to Shuttle 4.
11. Steps 62-70: Shuttle 1 calculates the start destination of order 1 to be 0 stations away from its current position
12. Steps 71-75: Shuttle 4 begins processing the offer for the newly received order 1
13. Steps 80-100: The Shuttle Management System waits for an offer for order 1 from Shuttle 1
14. Steps 101-107: Shuttle 2 calculates the start destination of order 1 to be 0 stations away from its current position
15. Steps 111-115: Shuttle 3 calculates the start destination of order 1 to be 1 station away from its current position
16. Steps 120-127: Shuttle 1 sends an offer to the management system with an acceptance
17. Steps 128-130: Shuttle 4 calculates the start destination of order 1 to be 2 stations away from its current position
18. Steps 131-132: Shuttle 2 sends an offer to the management system with a rejection
19. Steps 135-144: Shuttle 3 sends an offer to the management system with an acceptance
20. Steps 145-152: Shuttle 4 sends an offer to the management system with a rejection
21. Steps 153-156: The Shuttle Management System waits for an offer for order 1 from Shuttle 2
22. Steps 157-168: The Shuttle Management System waits for an offer for order 1 from Shuttle 3
23. Steps 169-178: The Shuttle Management System waits for an offer for order 1 from Shuttle 4
24. Steps 179-188: The Shuttle Management System accepts Shuttle 3’s offer and assigns order 1 to Shuttle 3
25. Steps 255-265: The Shuttle Management System sends order 2 to Shuttle 1.
26. Steps 266-271: The Shuttle Management System sends order 2 to Shuttle 2.
27. Steps 272-275: Shuttle 1 begins processing the offer for the newly received order 2.
28. Steps 276-284: Shuttle 2 begins processing the offer for the newly received order 2.
29. Steps 285-289: The Shuttle Management System sends order 2 to Shuttle 3.
30. Steps 290-293: Shuttle 2 requests access from the Railway Network to travel from station 2 to station 1
31. Steps 294-310: The Shuttle Management System sends order 2 to Shuttle 4.
32. Steps 311-320: Shuttle 4 begins processing the offer for the newly received order 2.
33. Steps 321-328: Shuttle 1 calculates the start destination of order 2 to be 1 station away from its current position
34. Steps 330-339: The Railway Network grants access for Shuttle 2 to travel from station 2 to station 1
35. Steps 340-349: The Shuttle Management System waits for an offer for order 2 from Shuttle 1
36. Steps 350-354: Shuttle 1 sends an offer to the management system with an acceptance
37. Steps 355-355: Shuttle 2 calculates the start destination of order 2 to be 1 station away from its current position
38. Steps 357-364: Shuttle 3 travels from Station 2 to Station 1
39. Steps 365-381: Shuttle 2 sends an offer to the management system with an acceptance
40. Steps 382-392: Shuttle 2 begins processing the offer for the newly received order 2.
41. Steps 393-393: Shuttle 3 loads 4 people at station 1
42. Steps 396-398: Shuttle 4 calculates the start destination of order 2 to be 1 station away from its current position
43. Steps 399-402: The Shuttle Management System waits for an offer for order 2 from Shuttle 2
44. Steps 403-419: Shuttle 4 sends an offer to the management system with an acceptance
45. Steps 420-423: Shuttle 3 begins processing the offer for the newly received order 2.
46. Steps 424-435: The Shuttle Management System waits for an offer for order 2 from Shuttle 3
47. Steps 436-444: Shuttle 3 calculates the start destination of order 2 to be 0 stations away from its current position
48. Steps 445-454: Shuttle 3 sends an offer to the management system with a rejection
49. Steps 455-460: The Shuttle Management System waits for an offer for order 2 from Shuttle 4
50. Steps 461-470: The Shuttle Management System accepts Shuttle 1’s offer and assigns order 2 to Shuttle 1
51. Steps 471-541: Shuttle 1 requests access from the Railway Network to travel from station 1 to station 2
52. Steps 542-565: Shuttle 3 requests access from the Railway Network to travel from station 1 to station 2
53. Steps 566-574: The Railway Network grants access for Shuttle 1 to travel from station 1 to station 2
54. Steps 575-584: Shuttle 1 travels from station 1 to station 2
55. Steps 585-598: The Railway Network rejects access for Shuttle 3 to travel from station 1 to station 2
56. Steps 599-601: Shuttle 1 loads to people at station 2
57. Steps 602-633: Shuttle 1 requests access from the Railway Network to travel from station 2 to station 3
58. Steps 634-640: The Railway Network grants access for Shuttle 3 to travel from station 1 to station 2
59. Steps 641-653: Shuttle 3 travels from station 1 to station 2
60. Steps 654-657: The Railway Network grants access for Shuttle 1 to travel from station 2 to station 3
61. Steps 658-667: Shuttle 1 travels from station 2 to station 3
62. Steps 668-689: Shuttle 1 unloads 2 people at station 3. Order 2 is completed
63. Steps 690-698: Shuttle 3 requests access from the Railway Network to travel from station 2 to station 3
64. Steps 699-707: The Railway Network grants access for Shuttle 3 to travel from station 2 to station 3
65. Steps 708-715: Shuttle 3 travels from station 2 to station 3
66. Steps 716-726: Shuttle 3 unloads 4 people at station 3. Order 1 is completed
67. Steps 726-730: No more pending orders. System terminates
68. The predicate travelling(S) is true if and only if shuttle S is currently on a track (i.e., the shuttle is currently stationed. The predicate noLoad(S) is true if and only if shuttle S has no load (i.e., not carrying any people).

We define the following LTL property: ∀S GFG(!travelling(S) ∧ noLoad(S)). !travelling(S) is represented in spin as predicate p (!travelling). noLoad(S) is represented in spin as predicate q (currentLoad == 0).

We run verification (with non-progress cycles) on the system in problem1-ltl.pml using the LTL property p1 {always eventually always (p && q)}, which results in an acceptance cycle found (at depth 718)). The output (with acceptance cycles) is shown below and can be found in pan1.out and problem1-ltl.pml.trail:

Pid: 13228

Depth= 410 States= 1e+006 Transitions= 1.39e+006 Memory= 928.699 t= 3.93 R= 3e+005

Hence, it is shown that the system always returns into a state that all shuttles are

at stations without load.

<<<<<START OF CYCLE>>>>>

MSC: ~G line 13

719: proc - (p1:1) \_spin\_nvr.tmp:13 (state 15) [(!(((((!(travelling[0])&&!(travelling[1]))&&!(travelling[2]))&&!(travelling[3]))&&((((currentLoad[0]==0)&&(currentLoad[1]==0))&&(currentLoad[2]==0))&&(currentLoad[3]==0)))))]

Never claim moves to line 13 [(!(((((!(travelling[0])&&!(travelling[1]))&&!(travelling[2]))&&!(travelling[3]))&&((((currentLoad[0]==0)&&(currentLoad[1]==0))&&(currentLoad[2]==0))&&(currentLoad[3]==0)))))]

720: proc 1 (Shuttle:1) problem1-ltl.pml:149 (state 88) [else]

MSC: ~G line 9

721: proc - (p1:1) \_spin\_nvr.tmp:9 (state 10) [(1)]

Never claim moves to line 9 [(1)]

722: proc 1 (Shuttle:1) problem1-ltl.pml:149 (state 89) [(1)]

MSC: ~G line 13

723: proc - (p1:1) \_spin\_nvr.tmp:13 (state 15) [(!(((((!(travelling[0])&&!(travelling[1]))&&!(travelling[2]))&&!(travelling[3]))&&((((currentLoad[0]==0)&&(currentLoad[1]==0))&&(currentLoad[2]==0))&&(currentLoad[3]==0)))))]

Never claim moves to line 13 [(!(((((!(travelling[0])&&!(travelling[1]))&&!(travelling[2]))&&!(travelling[3]))&&((((currentLoad[0]==0)&&(currentLoad[1]==0))&&(currentLoad[2]==0))&&(currentLoad[3]==0)))))]

724: proc 1 (Shuttle:1) problem1-ltl.pml:145 (state 84) [shuttleRequests!request.track,request.direction,request.id]

MSC: ~G line 9

725: proc - (p1:1) \_spin\_nvr.tmp:9 (state 10) [(1)]

Never claim moves to line 9 [(1)]

726: proc 6 (RailwayNetwork:1) problem1-ltl.pml:188 (state 1) [shuttleRequests?request.track,request.direction,request.id]

MSC: ~G line 13

727: proc - (p1:1) \_spin\_nvr.tmp:13 (state 15) [(!(((((!(travelling[0])&&!(travelling[1]))&&!(travelling[2]))&&!(travelling[3]))&&((((currentLoad[0]==0)&&(currentLoad[1]==0))&&(currentLoad[2]==0))&&(currentLoad[3]==0)))))]

Never claim moves to line 13 [(!(((((!(travelling[0])&&!(travelling[1]))&&!(travelling[2]))&&!(travelling[3]))&&((((currentLoad[0]==0)&&(currentLoad[1]==0))&&(currentLoad[2]==0))&&(currentLoad[3]==0)))))]

728: proc 6 (RailwayNetwork:1) problem1-ltl.pml:190 (state 2) []

MSC: ~G line 9

729: proc - (p1:1) \_spin\_nvr.tmp:9 (state 10) [(1)]

Never claim moves to line 9 [(1)]

730: proc 6 (RailwayNetwork:1) problem1-ltl.pml:191 (state 3) [((request.direction==1))]

MSC: ~G line 13

731: proc - (p1:1) \_spin\_nvr.tmp:13 (state 15) [(!(((((!(travelling[0])&&!(travelling[1]))&&!(travelling[2]))&&!(travelling[3]))&&((((currentLoad[0]==0)&&(currentLoad[1]==0))&&(currentLoad[2]==0))&&(currentLoad[3]==0)))))]

Never claim moves to line 13 [(!(((((!(travelling[0])&&!(travelling[1]))&&!(travelling[2]))&&!(travelling[3]))&&((((currentLoad[0]==0)&&(currentLoad[1]==0))&&(currentLoad[2]==0))&&(currentLoad[3]==0)))))]

732: proc 6 (RailwayNetwork:1) problem1-ltl.pml:195 (state 8) [else]

MSC: ~G line 9

733: proc - (p1:1) \_spin\_nvr.tmp:9 (state 10) [(1)]

Never claim moves to line 9 [(1)]

734: proc 6 (RailwayNetwork:1) problem1-ltl.pml:195 (state 9) [reply.granted = 0]

Railway Network: rejecting access to track from station 2 to station 3

734: proc 6 (RailwayNetwork:1) problem1-ltl.pml:196 (state 10) [printf('Railway Network: rejecting access to track from station %d to station %d\\n',request.track,((request.track+1)%4))]

MSC: ~G line 13

735: proc - (p1:1) \_spin\_nvr.tmp:13 (state 15) [(!(((((!(travelling[0])&&!(travelling[1]))&&!(travelling[2]))&&!(travelling[3]))&&((((currentLoad[0]==0)&&(currentLoad[1]==0))&&(currentLoad[2]==0))&&(currentLoad[3]==0)))))]

Never claim moves to line 13 [(!(((((!(travelling[0])&&!(travelling[1]))&&!(travelling[2]))&&!(travelling[3]))&&((((currentLoad[0]==0)&&(currentLoad[1]==0))&&(currentLoad[2]==0))&&(currentLoad[3]==0)))))]

736: proc 6 (RailwayNetwork:1) problem1-ltl.pml:206 (state 25) [railwayReplies[request.id]!reply.granted]

MSC: ~G line 9

737: proc - (p1:1) \_spin\_nvr.tmp:9 (state 10) [(1)]

Never claim moves to line 9 [(1)]

738: proc 1 (Shuttle:1) problem1-ltl.pml:146 (state 85) [railwayReplies[id]?reply.granted]

spin: trail ends after 738 steps

1. Can you find any additional problems in the system, by verifying other properties? Please state what property you verified and give a clear explanation of any errors you found.

The system only checks the current load of the shuttle and not future load. Consider the case where an empty shuttle has a pending order (o1) that hasn’t yet been loaded, and another order (o2) to which the shuttle is required to reply with an offer to the shuttle management system. When the shuttle is processing the offer for o2, it will only consider the current empty load and not the future load with o1 included.

Consider the when the combined size of o1 and o2 were to exceed the shuttle’s capacity. If o2’s starting station is located before o1’s ending station, the shuttle would end up loading o1 first and then o2 before it unloads o1. The capacity of the shuttle would be exceeded and there would be an error in the system when o2 is being loaded.

We represent the above property in spin as predicate r (currentLoad <= capacity).

We can run verification on the system (with acceptance cycles) in problem1-additional.pml using the LTL property p2 { always r}, which results in a acceptance cycle found (at depth 718)). The output for this (with acceptance cycles) is unable to be shown in pan1-additional.out and problem1-additional.pml.trail.

Hence, it is shown that the capacity of the shuttle can be exceeded by the current load.

<<<<<START OF CYCLE>>>>>

720: proc 1 (Shuttle:1) problem1-additional.pml:149 (state 88) [else]

722: proc 1 (Shuttle:1) problem1-additional.pml:149 (state 89) [(1)]

724: proc 1 (Shuttle:1) problem1-additional.pml:145 (state 84) [shuttleRequests!request.track,request.direction,request.id]

726: proc 6 (RailwayNetwork:1) problem1-additional.pml:188 (state 1) [shuttleRequests?request.track,request.direction,request.id]

728: proc 6 (RailwayNetwork:1) problem1-additional.pml:190 (state 2) []

730: proc 6 (RailwayNetwork:1) problem1-additional.pml:191 (state 3) [((request.direction==1))]

732: proc 6 (RailwayNetwork:1) problem1-additional.pml:195 (state 8) [else]

734: proc 6 (RailwayNetwork:1) problem1-additional.pml:195 (state 9) [reply.granted = 0]

Railway Network: rejecting access to track from station 2 to station 3

734: proc 6 (RailwayNetwork:1) problem1-additional.pml:196 (state 10) [printf('Railway Network: rejecting access to track from station %d to station %d\\n',request.track,((request.track+1)%4))]

736: proc 6 (RailwayNetwork:1) problem1-additional.pml:206 (state 25) [railwayReplies[request.id]!reply.granted]

738: proc 1 (Shuttle:1) problem1-additional.pml:146 (state 85) [railwayReplies[id]?reply.granted]

spin: trail ends after 738 steps

Problem 2:

1. The Promela code can be found in problem2.pml
2. We run verification (with safety) on the system in problem2.pml, which results in an invalid end state (deadlock) at depth 734. The output for the deadlock can be found in pan2.out and problem2.pml.trail.

unreached in proctype Client

problem2.pml:36, state 2, "cmConnectRequest!id"

problem2.pml:37, state 3, "printf('Client %d: requesting connection\n',(id+1))"

problem2.pml:38, state 4, "cmConnectReply[id]?reply"

problem2.pml:40, state 6, "cmStatus[id]?currStatus"

problem2.pml:40, state 7, "connected = 1"

problem2.pml:42, state 10, "(1)"

problem2.pml:40, state 12, "((reply==2))"

problem2.pml:40, state 12, "else"

problem2.pml:47, state 16, "cmCommand[id]?currCommand"

problem2.pml:49, state 18, "cmStatus[id]?currStatus"

problem2.pml:50, state 19, "printf('Client %d: getting new info\n',(id+1))"

problem2.pml:56, state 27, "clientReport!2,id"

problem2.pml:57, state 28, "cmCommand[id]?currCommand"

problem2.pml:59, state 30, "cmStatus[id]?currStatus"

problem2.pml:60, state 31, "printf('Client %d: using new info\n',(id+1))"

problem2.pml:63, state 37, "clientReport!1,id"

problem2.pml:64, state 38, "cmStatus[id]?currStatus"

problem2.pml:64, state 39, "connected = 0"

problem2.pml:56, state 41, "(getInfoSuccess)"

problem2.pml:56, state 41, "else"

problem2.pml:70, state 46, "clientReport!2,id"

problem2.pml:71, state 47, "cmStatus[id]?currStatus"

problem2.pml:72, state 49, "clientReport!1,id"

problem2.pml:73, state 50, "connected = 0"

problem2.pml:73, state 51, "cmStatus[id]?currStatus"

problem2.pml:74, state 52, "printf('Client %d: post-initialization failed. disconnected\n',(id+1))"

problem2.pml:70, state 53, "(useNewInfoSuccess)"

problem2.pml:70, state 53, "else"

problem2.pml:99, state 82, "clientReport!1,id"

problem2.pml:100, state 83, "cmCommand[id]?currCommand"

problem2.pml:102, state 85, "cmStatus[id]?currStatus"

problem2.pml:103, state 86, "printf('Client %d: using old info\n',(id+1))"

problem2.pml:112, state 99, "clientReport!1,id"

problem2.pml:113, state 100, "connected = 0"

problem2.pml:113, state 101, "cmStatus[id]?currStatus"

problem2.pml:118, state 107, "printf('Client %d: update failed. disconnected\n',(id+1))"

problem2.pml:124, state 115, "clientReport!2,id"

problem2.pml:125, state 116, "cmStatus[id]?currStatus"

problem2.pml:126, state 118, "clientReport!1,id"

problem2.pml:127, state 119, "connected = 0"

problem2.pml:127, state 120, "cmStatus[id]?currStatus"

problem2.pml:124, state 121, "(useOldInfoSuccess)"

problem2.pml:124, state 121, "else"

problem2.pml:129, state 123, "cmCommand[id]?currCommand"

problem2.pml:132, state 126, "printf('Client %d: revert failed. disconnected\n',(id+1))"

problem2.pml:136, state 134, "-end-"

(42 of 134 states)

unreached in proctype CommsManager

problem2.pml:152, state 14, "cmConnectRequest?id"

problem2.pml:153, state 15, "printf('CommsManager: connection request received from client %d\n',(id+1))"

problem2.pml:157, state 19, "currStatus = 7"

problem2.pml:157, state 20, "cmStatus[id]!7"

problem2.pml:158, state 21, "connectedClients[id] = 1"

problem2.pml:158, state 22, "cmAbleWcp!1"

problem2.pml:159, state 24, "reply = 1"

problem2.pml:156, state 25, "((currStatus==8))"

problem2.pml:156, state 25, "else"

problem2.pml:161, state 27, "cmConnectReply[id]!reply"

problem2.pml:164, state 30, "cmCommand[id]!5"

problem2.pml:165, state 31, "currStatus = 6"

problem2.pml:165, state 32, "cmStatus[id]!6"

problem2.pml:168, state 35, "clientReport?reportStatus,id"

problem2.pml:170, state 37, "cmCommand[id]!4"

problem2.pml:171, state 38, "currStatus = 5"

problem2.pml:171, state 39, "cmStatus[id]!5"

problem2.pml:173, state 42, "currStatus = 8"

problem2.pml:173, state 43, "cmStatus[id]!8"

problem2.pml:170, state 44, "((reportStatus==2))"

problem2.pml:170, state 44, "((reportStatus==1))"

problem2.pml:177, state 48, "clientReport?reportStatus,id"

problem2.pml:179, state 51, "cmStatus[id]!8"

problem2.pml:180, state 52, "cmAbleWcp!2"

problem2.pml:182, state 55, "currStatus = 8"

problem2.pml:182, state 56, "cmStatus[id]!8"

problem2.pml:183, state 57, "cmAbleWcp!2"

problem2.pml:179, state 58, "((reportStatus==2))"

problem2.pml:179, state 58, "((reportStatus==1))"

problem2.pml:192, state 69, "(1)"

problem2.pml:202, state 88, "(1)"

problem2.pml:214, state 107, "printf('CommsManager: update failed by Client %d\n',(i+1))"

problem2.pml:217, state 113, "(1)"

problem2.pml:224, state 126, "cmCommand[i]!3"

problem2.pml:224, state 127, "cmStatus[i]!1"

problem2.pml:225, state 129, "(1)"

problem2.pml:224, state 130, "(connectedClients[i])"

problem2.pml:224, state 130, "else"

problem2.pml:233, state 146, "(1)"

problem2.pml:246, state 167, "printf('CommsManager: post-update failed by Client %d\n',(i+1))"

problem2.pml:249, state 173, "(1)"

problem2.pml:254, state 184, "i = 0"

problem2.pml:256, state 187, "cmStatus[i]!8"

problem2.pml:256, state 188, "cmCommand[i]!2"

problem2.pml:257, state 190, "(1)"

problem2.pml:256, state 191, "(connectedClients[i])"

problem2.pml:256, state 191, "else"

problem2.pml:254, state 196, "((i<=(4-1)))"

problem2.pml:254, state 196, "else"

problem2.pml:260, state 199, "cmAbleWcp!2"

problem2.pml:265, state 208, "(1)"

problem2.pml:272, state 222, "hasFail = 0"

problem2.pml:273, state 223, "i = 0"

problem2.pml:275, state 226, "clientReport?reportStatus,id"

problem2.pml:278, state 229, "printf('CommsManager: post-revert failed by Client %d\n',(i+1))"

problem2.pml:279, state 231, "(1)"

problem2.pml:277, state 232, "((reportStatus==1))"

problem2.pml:277, state 232, "else"

problem2.pml:281, state 235, "(1)"

problem2.pml:275, state 236, "(connectedClients[i])"

problem2.pml:275, state 236, "else"

problem2.pml:273, state 241, "((i<=(4-1)))"

problem2.pml:273, state 241, "else"

problem2.pml:286, state 246, "i = 0"

problem2.pml:288, state 249, "cmStatus[i]!8"

problem2.pml:288, state 250, "cmCommand[i]!2"

problem2.pml:289, state 252, "(1)"

problem2.pml:288, state 253, "(connectedClients[i])"

problem2.pml:288, state 253, "else"

problem2.pml:286, state 258, "((i<=(4-1)))"

problem2.pml:286, state 258, "else"

problem2.pml:292, state 261, "cmAbleWcp!2"

problem2.pml:293, state 263, "currStatus = 8"

problem2.pml:296, state 267, "cmStatus[i]!8"

problem2.pml:296, state 268, "cmCommand[i]!1"

problem2.pml:297, state 270, "(1)"

problem2.pml:296, state 271, "(connectedClients[i])"

problem2.pml:296, state 271, "else"

problem2.pml:294, state 276, "((i<=(4-1)))"

problem2.pml:294, state 276, "else"

problem2.pml:300, state 279, "cmAbleWcp!2"

problem2.pml:285, state 280, "(hasFail)"

problem2.pml:285, state 280, "else"

problem2.pml:303, state 285, "-end-"

(70 of 285 states)

unreached in proctype ControlPanel

problem2.pml:324, state 19, "-end-"

(1 of 19 states)

unreached in init

(0 of 8 states)

1. Can you find any additional problems in the protocol? Please state what property you verified and clear explanation of any errors you found.