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 0 to Shuttle 0.
5. Steps 30-33: Shuttle 0 begins processing the offer for the newly received order 0
6. Steps 34-36: The Shuttle Management System sends order 0 to Shuttle 1.
7. Steps 37-50: The Shuttle Management System sends order 0 to Shuttle 2.
8. Steps 51-56: Shuttle 2 begins processing the offer for the newly received order 0
9. Steps 57-59: Shuttle 1 begins processing the offer for the newly received order 0
10. Steps 60-61: The Shuttle Management System sends order 0 to Shuttle 3.
11. Steps 62-70: Shuttle 0 calculates the start destination of order 0 to be 0 stations away from its current position
12. Steps 71-75: Shuttle 3 begins processing the offer for the newly received order 0
13. Steps 80-100: The Shuttle Management System waits for an offer for order 0 from Shuttle 0
14. Steps 101-107: Shuttle 1 calculates the start destination of order 0 to be 0 stations away from its current position
15. Steps 111-115: Shuttle 2 calculates the start destination of order 0 to be 1 stations away from its current position
16. Steps 120-127: Shuttle 0 sends an offer to the management system with an acceptance
17. Steps 128-130: Shuttle 3 calculates the start destination of order 0 to be 2 stations away from its current position
18. Steps 131-132: Shuttle 1 sends an offer to the management system with a rejection
19. Steps 135-144: Shuttle 2 sends an offer to the management system with an acceptance
20. Steps 145-152: Shuttle 3 sends an offer to the management system with a rejection
21. Steps 153-156: The Shuttle Management System waits for an offer for order 0 from Shuttle 1
22. Steps 157-168: The Shuttle Management System waits for an offer for order 0 from Shuttle 2
23. Steps 169-178: The Shuttle Management System waits for an offer for order 0 from Shuttle 3
24. Steps 179-188: The Shuttle Management System accepts Shuttle 2’s offer and assigns order 0 to Shuttle 2
25. Steps 255-265: The Shuttle Management System sends order 1 to Shuttle 0.
26. Steps 266-271: The Shuttle Management System sends order 1 to Shuttle 1.
27. Steps 272-275: Shuttle 0 begins processing the offer for the newly received order 1.
28. Steps 276-284: Shuttle 1 begins processing the offer for the newly received order 1.
29. Steps 285-289: The Shuttle Management System sends order 1 to Shuttle 2.
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 1 to Shuttle 3.
32. Steps 311-320: Shuttle 3 begins processing the offer for the newly received order 1.
33. Steps 321-328: Shuttle 0 calculates the start destination of order 1 to be 1 stations 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 1 from Shuttle 0
36. Steps 350-354: Shuttle 0 sends an offer to the management system with an acceptance
37. Steps 355-355: Shuttle 1 calculates the start destination of order 1 to be 1 stations away from its current position
38. Steps 357-364: Shuttle 2 travels from Station 2 to Station 1
39. Steps 365-381: Shuttle 1 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 1.
41. Steps 393-393: Shuttle 3 calculates the start destination of order 1 to be 1 stations away from its current position
42. Steps 396-403: The Shuttle Management System waits for an offer for order 1 from Shuttle 1
43. Steps 404-408: Shuttle 3 sends an offer to the management system with an acceptance
44. Steps 409-428: The Shuttle Management System waits for an offer for order 1 from Shuttle 2
45. Steps 429-430: Shuttle 2 calculates the start destination of order 1 to be 1 stations away from its current position
46. Steps 432-438: Shuttle 2 sends an offer to the management system with an acceptance
47. Steps 439-448: The Shuttle Management System waits for an offer for order 1 from Shuttle 3
48. Steps 449-458: The Shuttle Management System accepts Shuttle 2’s offer and assigns order 1 to Shuttle 2
49. Steps 498-510: Shuttle 2 loads 4 people at station 1
50. Steps 526-541: Shuttle 2 requests access from the Railway Network to travel from station 1 to station 2
51. Steps 542-550: The Railway Network grants access for Shuttle 2 to travel from station 1 to station 2
52. Steps 551-558: Shuttle 2 travels from station 1 to station 2
53. Steps 559-578: Shuttle 2 requests access from the Railway Network to travel from station 2 to station 3
54. Steps 579-587: The Railway Network grants access for Shuttle 2 to travel from station 2 to station 3
55. Steps 588-595: Shuttle 2 travels from station 2 to station 3
56. Steps 596-606: Shuttle 2 unloads 4 people at station 2. Order 0 is complete
57. Steps 620-633: Shuttle 2 requests access from the Railway Network to travel from station 3 to station 2
58. Steps 634-642: The Railway Network grants access for Shuttle 2 to travel from station 3 to station 2
59. Steps 643-650: Shuttle 2 travels from station 3 to station 2
60. Steps 651-661: Shuttle 2 loads 2 people at station 2
61. Steps 668-682: Shuttle 2 requests access from the Railway Network to travel from station 2 to station 3
62. Steps 683-691: The Railway Network grants access to travel from station 2 to station 3
63. Steps 692-699: Shuttle 2 travels from station 2 to station 3
64. Steps 700-710: Shuttle 2 unloads 2 people at station 3. Order 1 is complete
65. The predicate moving(S) is true if and only if shuttle S is not 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 GF(!moving(S) ∧ noLoad(S))

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.

Problem 2:

1. The Promela code can be found in problem2.pml
2. Show that there exists a deadlock and provide a clear interpretation of the counter-example obtained from SPIN.
3. Can you find any additional problems in the protocol? Please state what property you verified and clear explanation of any errors you found.