Q&A Session

CS4211 - Formal Methods for Software Engineering

Prepared by: Zhiyu Fan

Command Questions

Question 1:

I have installed iSpin, Dot from Graphviz and MinGW C compiler in Windows.
When I try to run the Automata View, I get this error: Format: "tk" not recognized. Use one of:

Answer:

Please try the command “dot -v” in windows shell. If there is an output saying “Perhaps "dot -c" needs to be run (with installer's privileges) to register the plugins?”, then try the command “dot -c” with admin privilege in windows shell.

Command Questions

Question 2:

I have installed SPIN, and it works in terminal, but the jspin still doesn't work in Mac.

Answer:

Please modify the config.cfg file under jspin folder accordingly.

Command Questions

Question 3:

I have installed SPIN and modified the config.cfg file, but the jspin still doesn't work in Mac.
The error says "Running /Users/xxx/Desktop -a -o3 /Users/xxx/Desktop/example-7.pml"

Answer:

You may have wrongly config the config.cfg file.
Please try to modify this line "SPIN=/Users/xxx/Desktop" to "SPIN=/Users/xxx/Desktop/spin" in your config.cfg

Command Questions

Question 4:

I have installed SPIN, but the command line SPIN doesn't work in Linux.
My path environment is "spin=../../../spin"

Answer:

You do not need to add the "/spin" suffix. Just specify the path to spin folder

Command Questions

Question 5:

For Q1, “augment the provided model to make the above property true”. Does this mean that we have to build up on the original code given, and cannot delete any line of code from the given code?

Answer:

You should minimally change the given template code.
You can delete, if you really think necessary.

Command Questions

Question 6:

For question 2, how should I be implementing the node process? More specifically, am I supposed to only implement 1 process (the node) which receives data and sends the data when the three colours are all present?

Answer:

You should implement three processes for each type of message, and each process only send specific type of message.
You should have a buffer process to receive and reassemble those incoming messages and send the reassembled outgoing message.
You should have another process to receive the outgoing message.

Command Questions

Question 7:

I want to clarify if the way and the number of processes that I implement for question 2 and 3 is fixed or whether I can have any number of processes, so long as I can prove the properties in the other parts of the question using the SPIN checker.

Answer:

You can have any number of processes, so long as I can prove the properties.

Questions During Q&A

Question 1:

Regarding to question 1.1, assuming my LTL is correct. And I run the claim on the template code, I should see an error trail???

Answer:

Yes, there should be an error trail.

Questions During Q&A

Question 2:

Do I just use the default settings in the Verifications tab?

Answer:

Yes, but you need select the use claim option and fill name of your LTL property

Questions During Q&A

Question 3:

For question 1 and 2, the system deadlocks even without a claim. When I run it with a claim, it reaches the deadlock before finding a cycle. Does that mean my claim is wrong?

Answer:

You can use any SPIN features to find the deadlock. It doesn't mean your claim is wrong.

Questions During Q&A

Question 4:

In question 2.3, it asks "use SPIN to prove that it can be violated, and show the counter-example.". For the violation, do I show a screenshot of the verification output or the message sequence chart?

Answer:

You can submit the screenshot of the verification output and the message sequence chart. The generated trail file and msc.ps file are also fine.

Questions During Q&A

Question 5:

so a deadlock from regular simulation is considered an error trail?

Answer:

As long as the deadlock is what we asked, it can be considered an error trail.
If the error trail of deadlock is because of your implementation, we will not accept it

Questions During Q&A

Question 6:

For q1, can I augment the code to remove the deadlock

Answer:

Yes, if your augmentation is reasonable, you'll be awarded with more credits.

Questions During Q&A

Question 7:

In the problem description of Q1, it says operator 1a handles data communication from station 1 to station 2, but in the given code, operator 1a in station 1 can also send data to the operator in station 2.

Answer:

Please try to think in this way. We have 2 stations, and each station has two processes. You do not need to think about which station is 1 or 2, and which process is operator 1a and 1b.

They all can send and receive data and their role can keep changing.
Assume "run station(0,up[1],down[1]);" is operator in station 1 in above description and "run station(1,down[1],up[1]);" is operator in station 2 in above description
When "run station(0,up[1],down[1]);" sends data, it can be operator 1a.When "run station(0,up[1],down[1]);" receives data, it can be operator 1b.
They do not have a fixed role.