CS 511 – Quiz 8A: Model-Checking/Spin

2 December 2022

Names:
Section:

Exercise 1

Model the train exercise below from eb5 in Promela. A stub is provided in the next page.

```
// Directions: 0=North, 1=South
tracks = [new Semaphore(1), new Semaphore(1)]; // List with two semaphores
Semaphore permToLoad = new Semaphore(0);
Semaphore doneLoading = new Semaphore(0);

5.times{
    Thread.start { // Passenger
    int dir = (new Random()).nextInt(1);
    tracks[dir].acquire();
    // passengers board/disembark
    tracks[dir].release();
    }
}

2.times {
    Thread.start { // Freight
       int dir = (new Random()).nextInt(1);

    tracks[0].acquire();
    tracks[1].acquire();
    permToLoad.release();
    // getting loaded....
    doneLoading.acquire();
    tracks[0].release();
    tracks[1].release();
    }
}

Thread.start { // Loading machine
    while(true) {
    permToLoad.acquire();
    // loading...
    doneLoading.release();
    }
}
```

Here is the Promela stub.

```
#define PT 5 /* Number of Passenger Trains */
#define FT 2 /* Number of Freight Trains */
byte permToLoad;   /* machine semaphores, 0 permits by default */
byte doneLoading;
byte track[2];     /* track semaphores */

inline acquire(s) {
   atomic {
    s>0;
    s-- }
}

inline release(s) { s++ }

proctype PassengerTrain(int i) {
  /* complete */
}

proctype FreightTrain() {
  /* complete */
}

proctype LoadingMachine() {
  end1: /*  avoids invalid end-state error */
   /* complete */
}

init {
  byte i;
  track[0]=1;
  track[1]=1;

  atomic {
    for (i:1..(PT)) {     /* spawn passenger trains */
      do  /* randomly choose a direction */
        :: run PassengerTrain(0);break;
        :: run PassengerTrain(1);break;
      od
    }
    for (i:0..(FT)) {     /* spawn freight trains */
      run FreightTrain();
    }
    run LoadingMachine(); /* spawn loading machine */
  }
}
```

Exercise 2

Introduce assertions to show that

1. There can be no freight trains when a passenger train acquires a track.
2. There can be no other freight trains nor passenger trains when a freight train acquires both tracks.
3. When the machine loads, there must be exactly one freight train and no passenger trains.

Submission instructions:

Submit a one file named `tr.pml`.