MPRI C.2.3, Concurrency
Final exam
Part 3, Probabilistic models and applications

Question 1 (25%) Consider the following modification of Lehmann and Rabin's randomized algorithm for the dining philosophers.

```
1. think
2. randomly choose fork in {left,right}
3. if taken(fork) then goto 2
4.                else take(fork)
5. if taken(other(fork)) then release(fork); goto 2
6.                       else take(other(fork))
7. eat
8. release(other(fork))
9. release(fork)
10. goto 1
```

The only difference is line 3, in which `goto 3` has been replaced with `goto 2`. In other words, instead of doing busy waiting on the selected fork, the philosopher performs the random choice again.

Is this algorithm still correct assuming a *fair scheduler*? I.e. does it ensure that, for every fair scheduler, eventually a philosopher will eath with probability 1? Explain in detail your answer.

Question 2 (40%) The purpose of this question is to investigate whether probabilistic choice distributes over non-deterministic choice, i.e. whether their order can be exchanged.

Consider two processes P, Q which both toss i) a (fair) probabilistic coin and ii) a non-deterministic coin, and check whether the outcome is the same.

- In the case of P, the non-deterministic coin is tossed first
- In the case of Q, the probabilistic coin is tossed first

If the outcome of both coins is the same, both P, Q perform a success action $\bar{a}$.

2.1 Model P, Q in CCS with internal probabilistic choice and draw the generated probabilistic automata.

2.2 How many schedulers exist for each process (describe them). What is the maximum probability for each process to perform $\bar{a}$?

2.3 Which of the following hold?

$$P \sqsubseteq_{\textbf{may}} Q \qquad\qquad Q \sqsubseteq_{\textbf{may}} P$$
$$P \sqsubseteq_{\textbf{must}} Q \qquad\qquad Q \sqsubseteq_{\textbf{must}} P$$

Give proof or counter-example and explain.

2.4 According to the definition of $\sqsubseteq_{\textbf{may}}$ from lecture 3, $P \sqsubseteq_{\textbf{may}} Q$ requires that whenever P passes O with non-zero probability, Q can also pass it with non-zero probability. However, Q's probability of passing the test could actually be smaller (and similarly for $\sqsubseteq_{\textbf{must}}$). Give an alternative definition of $\sqsubseteq_{\textbf{may}}, \sqsubseteq_{\textbf{must}}$ that considers the exact probability of success, and repeat question 2.3 for the alternative definition.

Question 3 (35%) Consider an instance of the Dining Cryptographers protocol with 3 cryptographers on a ring (i.e. 3 coins, each visible to 2 cryptographers). The difference with respect to the standard protocol is that two of the coins are fair, while the third gives heads with probability $p \in [0, 1]$.

3.1 Model this protocol using a Markov Decision Process. You can either describe the states and transitions explicitely, or use PRISM's language (easier).

3.2 State strong anonymity (with respect to an external observer) in this model using PCTL formulas.

3.3 Does this instance satisfy strong anonymity for $p = 0.2$?

3.4 Find sufficient and necessary conditions on p for satisfying strong anonymity.