CS 424 Midterm 1.

INSTRUCTIONS: Please work on this midterm independently. The midterm is open book. Use of books, notes, calculators, laptops, and Internet resources is allowed. Collaboration is ***not allowed*** (which includes use of electronic communication such as chat, Skype, etc). Please read each question carefully and answer what the question asks for. Do not assume that the answer necessarily needs you to use all the data in the question. Please return only the answer sheet in the back. You can optionally attach an extra sheet to show your work (intermediate steps).

Due 10/15 in class.

Questions (Do not return this part):

Q1 (Reliability): In year 2030, SpaceZ Corporation launches a probe to Mars to record a new set of experimental scientific observations on the Martian surface. All observations are to be recorded in five independent copies, each on a different physical storage device. These devices are extremely reliable and will not alter, miss, or incorrectly record the data. The *only* failure mode to worry about is if the protective shield of a device is punctured by a physical collision with falling space debris showers on the planet's surface, in which case all data on the device is lost. (Mars atmosphere is thin, allowing such space debris to reach the surface.) The probability that a single device is punctured with falling debris is 1/40 in a week on the surface of Mars. At least one device must survive for the data to be recovered.

a) Compute the mean time to failure (in **hours**) of an individual storage device. Round to the nearest hour. **(2 points)**

e-$^{t/T}$= 39/40 → -(7x24)/T = ln (39/40) → T = 6636 hours

b) If the probe remains on Mars for 10 weeks, what is the probability that scientists are unable to retrieve data from the probe upon return to Earth *(assuming device failures are independent)*? **(1 point)**

P(device failure) = 1 – P(success for 10 weeks) = 1 - (39/40)^{10}.

P(all failure) = P(device failure)^{5} = 0.0005598

c) In reality, failures are not independent. Further analysis reveals that the probability of experiencing a shower of falling debris around the probe within a week is 5%. Moreover, the probability that any one storage device is punctured given that such a shower occurs that week, is 50%. If there was no other way for the storage device to fail, what is the *mean time to failure* of the storage system as a whole (in **hours**)? Note that, the system fails if data cannot be retrieved from any of the five devices. **(2 points)**

Cancelled due to difficulty level (accounting for cumulative partial failures)

d) What is the probability that scientists are unable to retrieve any data from the probe upon return from the 10-week stay on Mars? **(1 point)**

Cancelled due to difficulty level (accounting for cumulative partial failures)

Q2 (Well-formed dependencies): The software used for flight control in the above Martian mission includes three components:

(1) Deep-learning-based flight trajectory optimization: The reliability of this component (in the sense of producing correct and "bug-free" answers) is unknown due to its complexity and our inability to comprehensively test all possible corner-cases. Simulation-based tests, however, show that this component is generally able to save up to 10% on fuel when used.

(2) Coarse trajectory planning: This component uses geometry and physics to compute safe corridors and flight trajectories. A flight trajectory is considered safe as long as it remains within the computed safe corridors. Safety is defined as satisfying two conditions: The fuel must remain sufficient for the journey if the trajectory is followed, and the trajectory must avoid collisions with other space objects while in flight. This component is proven to be 100% reliable, but simulations show that trajectories within the computed corridors may differ in fuel consumption from each other by as much as 10%. This component cannot predict the exact fuel consumption of a trajectory because it overestimates fuel consumption to remain on the safe side. Simulations do confirm that when the rocket departs from the computed safe corridors, its fuel supply may get depleted before the journey is over.

(3) Corridor departure watchdog: This simple and 100% reliable component sends an alert if the trajectory of the rocket is about to depart from the safe corridors computed by component *(2)* above.

a) Which components can be part of the safety core (that guarantees system safety)? **(1 point)**

2 and 3

b) Which additional components can be used for performance optimization? **(1 point)**

1

c) Which of the dependencies below are allowed (i.e., are well formed)? **(2 points**

(i) Component #3 depends on component #2. Allowed

(ii) Component #2 depends on component #1. Not allowed

(iii) Component #3 uses but does not depend on component #1. Allowed

(iv) Component #1 depends on component #2. Allowed

d) Complete this sentence: "An architecture that satisfies safety while optimizing fuel can use component #__1__ in the common case in order to compute trajectories, as long as component #__3__ does not object. If component #__3__ raises a safety warning, component #__2__ should take over in computing trajectories." **(2 points)**

Q3 (Rate monotonic scheduling): For each of the following three task sets, please indicate whether the task set is schedulable or not using *rate monotonic* scheduling. In the task sets below, Pi refers to the period of task i, Ci refers to the execution time of task i, and Di refers to the relative deadline of task i. All times are in seconds. If relative deadline Di is not mentioned, assume that it is equal to Pi. **(3 points)**

1. Task set #1:

P1=10, C1=5
P2=20, C2=7
P3=100, C3=13
P4=200, C4=7

2. Task set #2:

P1=10, C1=6
P2=41, C2=17

3. Task set #3:

P1=11, C1=3.1
P2=67, C2=1, D2=4

None are schedulable

Q4 (Exact schedulability analysis). In task set #1 of Q3, use the exact schedulability test to compute the worst-case response time for tasks 1, 2, and 3, assuming rate monotonic scheduling. **(3 points)**

5, 17, 98

Q5 (EDF): Repeat Q3 in the case where the scheduling policy is *earliest deadline first*. **(3 points)**

Only task set 3 is schedulable

Q6 (Blocking): Consider the table below, where rows indicate tasks (smaller task numbers imply higher priority) and columns indicate resources. A cell at row X and column Y is set to 1 if task X uses resource Y. Each resource is protected by its own semaphore. When a task needs resource Y, it executes a Lock(Y) operation. When it is done, it executes Unlock(Y). The priority *ceiling* algorithm is used together with *rate monotonic* scheduling. Indicate which of the lock/unlock sequences below are possible and which are impossible. Assume that each sequence represents all lock/unlock operations that (presumably) occurred. Assume that no other blocking occurs except on the semaphores below. **(4 points)**

	Resource R1	Resource R2	Resource R3	Resource R4	Resource R5
Task T1	1			1	
Task T2	1	1			1
Task T3		1	1		
Task T4				1	1

a) T3 locks R2, T2 locks R1, T2 unlocks R1, T3 unlocks R2. Not possible

b) T3 locks R2, T1 locks R1, T1 unlocks R1, T3 unlocks R2. Possible

c) T4 locks R4, T4 unlocks R4, T2 locks R5, T2 unlocks R5. Possible

d) T4 locks R5, T1 locks R1, T4 unlocks R5, T1 unlocks R1. **Cancelled.**