CSIE 5452, Fall 2022: Quiz 2

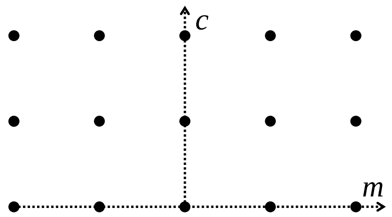
Due at 3:30pm; Marked as Last Submission after 3:30pm; Gradescope Closed at 3:40pm

There are totally 50 points. You are expected to use X minutes for a question with X points. When you submit your solutions on Gradescope, please select the corresponding page(s) of each question.

1 Hough Transform (6pts)

Perform the Hough Transform between the (x, y)-space and the (m, c)-space, where $y = mx + c$. No explanation is required.

1. (4pts) Given $(0, 0), (0, 1), (1, 2), (-1, 0)$ in the (x, y)-space, draw their corresponding lines in the (m, c)-space.



2. (1pt) Write down the coordinates of the point which receives the most "votes" in the (m, c)-space.

3. (1pt) Given the coordinates above in the (m, c)-space, write down the corresponding equation in the (x, y)-space.

2 Short Answers: Non-Security (12pts)

1. (2pts) Regarding the sensing range, answer the *longest* and *shortest* ones among the following items: (1) automotive-use camera, (2) automotive-use radar, (3) automotive-use ultrasonic sensor. No explanation is required. No partial credit will be given.

2. (2pts) Regarding the robustness against snow, fog, or rain, answer the *most* and *least* robust ones among the following items: (1) automotive-use camera (2) automotive-use radar, (3) automotive-use lidar. No explanation is required. No partial credit will be given.

3. (4pts) For safety applications, does Dedicated Short Range Communications (DSRC) use the Internet Protocol (IP)? Answer "Yes" or "No" and explain the reason.

4. (4pts) If a vehicle has the feature of object detection, explain (1) why the feature plus mapping can assist localization and (2) why the feature plus localization can assist mapping.

3 Short Answers: Security (12pts)

1. (4pts) Regarding security key management, compared with the pair-wise key distribution, list one *advantage* and one *disadvantage* of the one-key-for-all key distribution.

2. (4pts) Regarding security key management, compared with the pair-wise key distribution, list one *advantage* and one *disadvantage* of the timed efficient stream loss tolerant authentication (TESLA).

3. (4pts) The timing analysis in the early lectures computes the worst-case response time (R) of a message. With the timed efficient stream loss tolerant authentication (TESLA), is there any security concern if a sender releases a key right after an overestimated R? Answer "Yes" or "No" and explain the reason.

4 Computation Tree Logic (8pts)

Algorithm 1: Pseudocode

```
Input: $x$
$y \leftarrow 2022 +$ (the last digit of your student ID number; 0 if it is an alphabet);
if $x > 0$ then
    for $i \leftarrow 0$ to $x$ do
        if $y$ is even then
            $y \leftarrow y/2$;
        else
            $y \leftarrow y + 1$;
        end
    end
end
```

Given the pseudocode where x, y, z are integers, determine whether the following properties are true or false. No explanation is required. No partial credit will be given.

1. (2pts) $\mathbf{AF}(y \leq 2)$.
2. (2pts) $\mathbf{EFAX}(y = 1)$.

Ignore the pseudocode and let p, q be propositions. $\vee$ means "OR" in Boolean algebra.

3. (4pts) Decide the two properties are equivalent or not.
    - Property 1: $\mathbf{AF}(p \vee q)$.
    - Property 2: $\mathbf{AF}(p) \vee \mathbf{AF}(q)$.

   If yes, explain why they are equivalent; otherwise, draw a computation tree that satisfies one property but does not satisfy the other property.

5 Weakly-Hard Constraints (12pts)

We use a weakly-hard constraint (m, k) to constrain the input of a system. A weakly-hard constraint (m, k) means that there are at most m bad events for any k consecutive events.

1. (4pts) If a system with $(m, k) = (1, 3)$ is unsafe, can it imply that the system with $(m, k) = (1, 2)$ is unsafe? If yes, prove it; otherwise, provide an example.

2. (4pts) If a system with $(m, k) = (1, 2)$ is safe, can it imply that the system with $(m, k) = (2, 10)$ is safe? If yes, prove it; otherwise, provide an example.

3. (4pts) If a system with $(m, k) = (2, 10)$ is safe, can it imply that the system with $(m, k) = (1, 2)$ is safe? If yes, prove it; otherwise, provide an example.