CS 4376/5376

Midterm Exam

Tuesday, October 20

NAME: \_\_\_Oscar Galindo\_\_

Complete the exam and submit your work via blackboard no later than 3:00 PM. Scanned work is acceptable as long as it is legible. You may use a standard calculator and any of the reference materials from the class (lecture slides, readings, etc.), but are not allowed to consult with any other students or get other external aid. Please email me if you have any questions.

|  |  |  |
| --- | --- | --- |
| **Question** | **Points** | **Maximum** |
| **1** |  | **10** |
| **2** |  | **10** |
| **3** |  | **15** |
| **4** |  | **5** |
| **5** |  | **10** |
| **6** |  | **10** |
| **7** |  | **20** |
| **Total** |  | **80** |

**Question 1 (Probability Theory)**

Consider the following joint probability distribution over two events. Answer the following questions based on this table. **SHOW YOUR CALCULATIONS.**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Left | Center | Right |
| Top | 0.15 | 0.25 | 0 |
| Middle | 0 | 0.05 | 0.25 |
| Bottom | 0.1 | 0.05 | 0.15 |

a) What is the probability of Left or Bottom occurring, P(L v B)?

(0.15+0.1)+(0.1+0.05+0.15) – (repeated 0.1) = 0.45

b) What is the probability of Right and Top or Middle occurring,

P(C ^ (T v M))?

0.25 + 0.05 => 0.3

c) What are the marginal probabilities of the rows?

Top Row: 0.4 => 0.15+0.25

Middle Row: 0.3 => 0.05+0.25

Bottom Row: 0.3 => 0.1+0.05+0.15

d) What is the probability of Right given Bottom, P(R | B)?

P(R|B) = P(R^B)/P(B) = 0.15/0.15+0.05+0.1 => 0.15/0.3 => 0.5

e) What is the probability of Center or Right given Middle P((C v R) | M)?

P((CvR)|M) = P((CvR)^M)/P(M)=> P((M^C)v(M^R))/P(M) => (0.3)/0.3 => 1

**Question 2 (Reasoning about Evidence)**

a) You are using anomaly detection to try to detect whether a device on the network has been compromised by malware and may be acting as part of a botnet. On average, you believe that one in fifty devices on your network may be compromised. A network monitoring system generates an alert that indicates that a specific device has sent traffic to a blacklisted domain known to host botnet services. Based on the report, 10% of compromised devices send traffic to this domain, but only 0.5% of uncompromised devices do. After taking into account the evidence from the alert, what is the correct posterior belief that the device has been compromised? **SHOW YOUR CALCULATIONS.**

Diagram

Description automatically generated

A picture containing text, company name

Description automatically generated

Hypothesis: Device is compromised, Evidence: there is an alarm that goes off.

P(compromised) = 1/50 (Prior)

P(alert|compromised) = 0.1, P(alert|!compromised) = 0.05

P(compromised|alert) =? (We try to find this value)

P(compromised|alert) = P(alert|compromised) \* P(compromised)/P(alert) = P(alert|compromised)\*P(compromised) / P(alert|compromised)\*P(compromised) + P(alert|!compromised)P(!compromised) = 0.1\*0.02 / (0.1\*0.02+0.05\*(1-0.02)) = 0.002 / (0.002+0.049) = 0.03921

b) Briefly describe what a false positive and a false negative in this example would be (describe both types of error).

False Positive is when a device has set off an alert because it is communicating with the blacklisted domain but in reality, it hasn’t been compromised.

False Negative is when since the alert didn’t go off then the device the system says it is not compromised, but in reality it is compromised.

**Question 3 (Decision Theory)**

As a malware developer you are considering developing malware based on three different exploits. You only have time to develop one of the three exploits into working malware. The expected value of each exploit varies for different types of devices. Below are the expected values for three different types of devices. In addition, the probability of trying to infect each type of device is listed (i.e., how common the devices are).

|  |  |  |  |
| --- | --- | --- | --- |
|  | Device 1 | Device 2 | Device 3 |
| Exploit 1 | 0 | 2000 | 1000 |
| Exploit 2 | 5000 | 3000 | 0 |
| Exploit 3 | 10000 | 0 | 500 |

Devices frequencies:

Type 1: 0.05

Type 2: 0.2

Type 3: 0.75

a) Calculate the expected value of each type of exploit, and identify the exploit that maximizes expected utility.

Expected Utility (Exploit1) = 0.05\*0 + 2000\*0.2+0.75\*1000 => 400+750=> 1150

Expected Utility (Exploit2) = 0.05\*5000 + 3000\*0.2 + 0\*0.75 => 250+600 => 850

Expected Utility (Exploit3) = 0.05\*10,000 + 0.2\*0 + 0.75\*500 => 500+375 => 875

Choose Exploit 1 since it has the highest expected utility.

b) Calculate the maxmin value of each exploit, and identify the exploit that maximizes the minimum utility.

Exploit 1: Min(0,2000,1000) = 0

Exploit 2: Min(5000,3000,0) = 0

Exploit 3: Min(10000,0,500) = 0

Since the three possible exploits could not generate any utility then the

Minimums are equal to zero, hence we choose

c) Calculate the regret (opportunity loss) table, and identify the exploit that minimizes the maximum regret.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Device 1 | Device 2 | Device 3 |
| Exploit 1 | 0 | 2000 | 1000 |
| Exploit 2 | 5000 | 3000 | 0 |
| Exploit 3 | 10000 | 0 | 500 |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Device 1 | Device 2 | Device 3 |
| Exploit 1 | 10,000 | 1000 | 0 |
| Exploit 2 | 5000 | 0 | 1000 |
| Exploit 3 | 0 | 3000 | 5000 |

Maximum regrets per exploit:

Exploit 1: 10,000

Exploit 2: 5,000

Exploit 3: 5,000

If we want to minimize the maximum regrets, we choose either exploit 2 or 3 as their maximum regrets are similar.

d) Calculate the expected value of perfect information for this scenario.

Type 1: 0.05

Type 2: 0.2

Type 3: 0.75

Expected Utility (Exploit1) = 0.05\*0 + 2000\*0.2+0.75\*1000 => 400+750=> 1150

Expected Value of Perfect Information = 0.05\*10,000 + 3000\*0.2 + 1000\*0.75 = 500 + 600 + 750 = 1850

EVPI = 1850 – 1150 = 700

**Question 4 (Bounding Losses)**

You are selling security insurance services to a small business and wish to know how to price your policy. In particular, you will reimburse the client for the costs of any attack up to a limit of $5,000,000. You know based on your data that attacks that result in more than $2,000,000 of damage occur during a given year no more than 10% of the time, and attacks with damage between $500,000 and $2,000,000 occur no more than 20% of the time. How much should you charge the client on a yearly basis to ensure that you do not lose money on the insurance policy in expectation? Note that your information is incomplete, so you should make pessimistic assumptions where necessary to GUARANTEE your profits.

**Assumptions:**

* **The 10% of the time the attack costs more than $2M it will stay in the range $2M-$5M range**
* **The 20% of the time the cost lies on the range $500,000 to $2M**
* **Between $0 to $500,000 we will assume we have to pay $500,000 due to a pessimistic assumption (70%).**

**Estimates (Pessimistic View):**

* Expected Value ($2M-$5M) = 0.1 \* -$5M = -$500,000
* Expected Value ($500,000-$2M) = 0.2 \* -$2M = -$400,000
* Expected Value ($500,000) = 0.7 \* -$500,000 = -$350,000
* Expected Cost based on probabilities: -$1.25M
* Hence, we should at least charge $1.25M to every client since we expect the cost of providing insurance to every client to be around $1.25M

**Question 5 (Dynamic Programming)**

Consider an MDP with four states, labeled S1, S2, S3, and S4. The current values of the states are listed below. There are two actions that can be taken from state S1, labeled A1 and A2. The current policy is to choose each action with probability 0.5. The transition probabilities and immediate rewards are also listed below. The discount rate is 1.

Calculate the Q-values for each action and the value of the state for the current policy. Finally, give the new optimal action. **Show your work.**

Initial Values

S1: 5 S2: 20

S3: 10 S4: 5

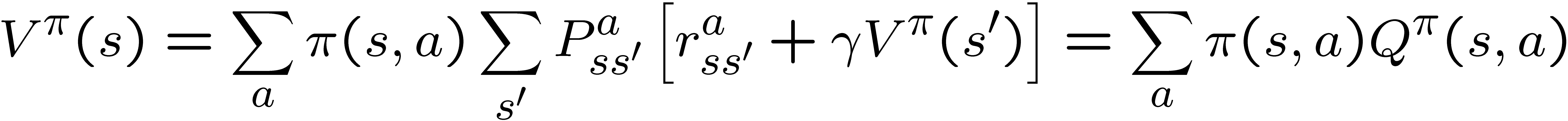
Transition Reward Probability

S1 A1 S4 10 0.2

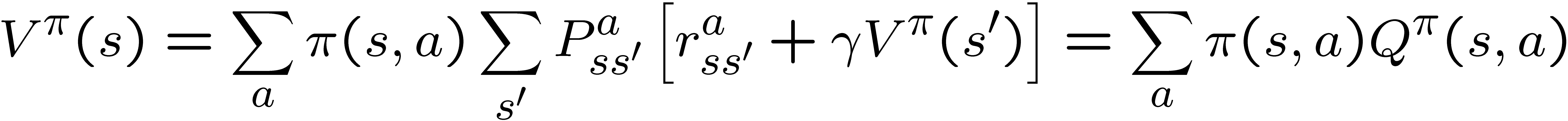
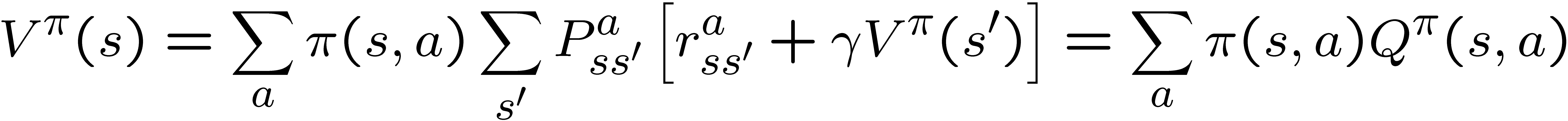
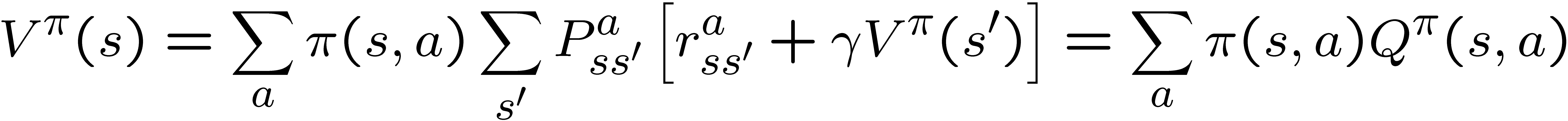
S1 A1 S3 5 0.8

S1 A2 S3 15 0.5

S1 A2 S2 10 0.5



Hence:



**Q(S1, A1):** Q(S1,A1) = 0.2\*[10+1(5)]+0.8\*[5+1(10)] = 15

**Q(S1, A2):** Q(S1,A2) = 0.5\*[15 + 1(10)]+0.5\*[10+1(20)] = 0.5\*25 + 0.5\*30 = 12.5+15 = 27.5

**V(S1):** 0.5\*15 + 0.5\*27.5 = 21.25

**Optimal action: Action 2 because it has the greatest value.**

**Question 6 (Temporal Difference Learning)**

a) Consider a simple MDP with three states and the initial value estimates shown in the table below. Let the discount rate λ = 0.5 and learning rate α= 0.1. Perform the temporal differences (TD) learning updates for the transitions shown and record the updated values for all states in the columns provided in the table.

Transition 1: S1 –> A3 –> S3 with reward rt = 5

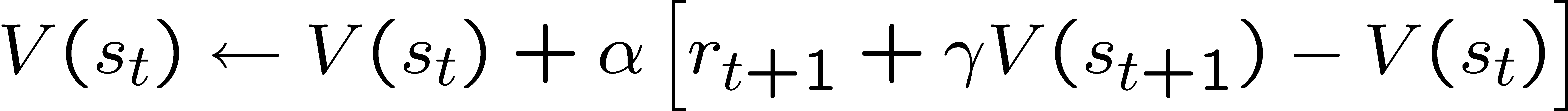
Transition 2: S3 –> A1 –> S2 with reward rt = 2

Transition 3: S2 –> A2 –> S1 with reward rt = 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| State | Initial Value | After Transition 1 | After Transition 2 | After Transition 3 |
| S1 | 4 | 4.2 | 4.2 | 4.2 |
| S2 | 8 | 8 | 8 | 7.71 |
| S3 | 2 | 2 | 2.4 | 2.4 |

Show your work:

λ = 0.5, α= 0.1



Transition 1:

V(S1) = 4 + 0.1[5+0.5(2)-4] => 4 + 0.1[2] => 4.2

Transition 2:

V(S3) = 2 + 0.1[2+0.5(8)-2] = 2 + 0.1[4] = 2.4

Transition 3:

V(S2) = 8 + 0.1[3+0.5(4.2)-8] = 8 + 0.1[-2.9] = 7.71

b) What is necessary for an agent using Q-learning to converge to the optimal policy?

That we update each (state, action) pair indefinitely.

**Question 7 (Short Answer)**

a) Briefly describe some types of decisions where it would make sense to use a worst-case decision criterion (e.g., maxmin), and some types of decisions where it would make sense to maximize expected value. What are the best arguments for each type of criteria?

* Worst-Case decision criterion is appropriate to be used when we try to minimize impacts even if they occur. For example, how much data will be lost if a data breach was to occur, how quickly can a service be restored when an attack happens, what is the monetary cost of having an attack.

Best Argument: We will like to be sure that the worst of my weaknesses is just as good as one of my smaller strengths. In this case I think the best argument is that you want to play safe, reduce risk.

* Maximize Expected Value criterion is appropriate to be used when we try to look at the world and think that the worst will not happen, we say that among all outcomes even though the worst can and sometimes happens we decide to say it will “likely” not. Decisions that support this rationale is like a small business buying mid-level security software since the small business might not have the kind of attacks that the Federal Reserve, or other bigger institutions might have. This also applies to decisions where you say do you want to buy insurance in such product? Maybe not since the use you will give to that product is small almost negligible. In both cases you worst case can happen, a huge attack could be directed to you, or the thing you bought breaks, but again not likely.

Best Argument: I want to make sure that on average I have a specific result, if I maximize the average then I will likely do good in the long run.

b) Describe the main idea of the Bellman equation; what does this equation say, and why is it important?

* The main idea of the Bellman equation is to assign some kind of measurement of the value we can expect to find when we reach the state. It is important because it allows us to decide between what states to visit when we are faced with options, if we knew, for example one state will provide you with a small value, and another with a high value then we immediately know what our decision should be.

c) Define both ordinal preferences and utility functions. What is the theoretical connection between them, and how can this justify using utility functions in decision making?

* The theoretical connection is preferences on comparable decisions, it is that we can decide what do we prefer to happen, for example we can decide that I prefer to receive a free cup of coffee from Starbucks than having to pay for it. The difference between both is that one attempts to quantify the degree of preference (utility functions) by using quantities (i.e. 0.5,1,2,etc.) and the other leaves them as simple comparisons between things (which do have an order of what we prefer to happen) since it does not make sense to ask how many more times do I prefer to receive a free cup of coffee from Starbucks than having to pay for it. So, a justification to use either, but certainly even more in the case of utility functions is that we can at any given time quantify and decide what we prefer, this translates into deciding between actions which do drive the behavior of agents.

d) Give three reasons why formalizing decisions and using decision theoretic solution concepts to analyze them might be desirable for cyber security decisions.

* Reason 1: Uncertainty
  + In the logic of uncertainty, we don’t have an idea of how the environment (i.e. the world) will interact in the future with our system so we ought to make decisions with our previous experience, which requires that we actually maybe have a backwards looking notion of what could I have done better, maybe bought a software instead of another? In this case the concept of regret could help.
* Reason 2: Cost
  + In the logic of cost, we are interested in analyzing, for example, what analyst to hire, what software to buy. So, by dealing with cost we often have to decide on what complexities/scenarios are we protecting against for example do we want to buy software for simple or more complex cybersecurity attacks? In this case we could analyze our choice with the concept of utility and that way choose infrastructures or people who maximize our utility.
* Reason 3: Develop a clear plan of action
  + In the context of planning we could map possible states that will incur in some costs, use of time to address an attack. For example, what will we like to do first get hold of the sequestered servers or will we like to immediately increase the capacity of the portion of the system that works? For this case we can create agents that automatically make such decisions for us based on specific values assigned to the different situation in which our systems might be found in. In a cybersecurity context this would be helpful because our agent will now what to do to protect our system.