Assignment 7 in CSE 415, Winter 2024

by the Staff of CSE 415

This is due Wednesday, March 6 via Gradescope at 11:59 PM. Prepare a PDF file with your answers and upload it to Gradescope. The PDF file can created however you like. For example it can be from a scan of a printout of the assignment document onto which you have hand-written your answers. Or it can be from Word or Latex file with your answers. It can even be from photos of your handwritten answers on plain paper. You don't have to include the questions themselves, but it is fine to do so. In any case, it must be very clear to read, and it must be obvious and easy for each grader where to find your solutions to the exercises.

As with Assignment 4, this is an *individual work* assignment. Collaboration is not permitted.

Prepare your answers in a neat, easy-to-read PDF. If you choose to typeset your answers in Latex using the template file for this document, please put your answers in blue while leaving the original text black.

Do the following exercises. These are intended to take 15-30 minutes each if you know how to do them. Each is worth 20 points. The total of possible points is 100.

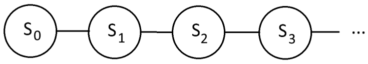
If corrections or clarifications to the problems have to be given, this will happen in the ED discussion forum under topic "Assignment 7."

Last name: Labbe, first name: Alexandre

Student number: 2377032

1 Markov Models

(20 points) Consider the Markov Model for the stock market shown below.



The transition probabilities for this model are given as:

S_t	S_{t+1}	$P(S_{t+1} \vert S_t)$
rising	rising	0.65
rising	falling	0.35
falling	rising	0.5
falling	falling	0.5

(a) (5 points) Assume $P(S_0 = \text{rising}) = 1.0$ and $P(S_0 = \text{falling}) = 0.0$. Using the miniforward algorithm, compute the $P(S_2)$ distribution.
$P(S_2 = \text{rising}) = 0.5975$
$P(S_2 = \text{falling}) = 0.4025$

(b) (2 points) Continuing with the miniforward algorithm, compute the $P(S_3)$ distribution.
$P(S_3 = \text{rising}) = 0.5896$
$P(S_3 = \text{falling}) = 0.4104$

(c) (3 points) Now assume $P(S_0 = \text{rising}) = 0.0$ and $P(S_0 = \text{falling}) = 1.0$. Compute the $P(S_2)$ distribution.
$P(S_2 = \text{rising}) = 0.5862$
$P(S_2 = \text{falling}) = 0.4138$

(d) (10 points) Compute the stationary distribution $P(S_\infty)$. Show your work.

$$\begin{aligned}
P(S_\infty = \text{falling}) &= P(\text{F}|\text{R}) \cdot P(S_\infty = \text{R}) + P(\text{F}|\text{F}) \cdot P(S_\infty = \text{F}) \\
&= 0.35 \cdot P(S_\infty = \text{R}) + 0.5 \cdot P(S_\infty = \text{F}) \\
&= 0.7 \cdot P(S_\infty = \text{R})
\end{aligned}$$

and

$$P(S_\infty = \text{falling}) + P(S_\infty = \text{rising}) = 1$$

so

$$\begin{aligned}
0.7 \cdot P(S_\infty = \text{rising}) + P(S_\infty = \text{rising}) &= 1 \\
P(S_\infty = \text{rising}) &= \frac{1}{1.7} \\
P(S_\infty = \text{falling}) &= \frac{0.7}{1.7}
\end{aligned}$$

Therefore,
$P(S_\infty = \text{rising}) = 0.588$
$P(S_\infty = \text{falling}) = 0.412$

2 D-Separation

(20 points) Consider the Bayes Net graph β below, which represents the topology of a web-server security model. Here the random variables have the following interpretations:

V = Vulnerability exists in web-server code or configs.

C = Complexity to access the server is high. (Passwords, 2-factor auth., etc.)

S = Server accessibility is high. (Firewall settings, and configs on blocked IPs are permissive).

A = Attacker is active.

L = Logging infrastructure is state-of-the-art.

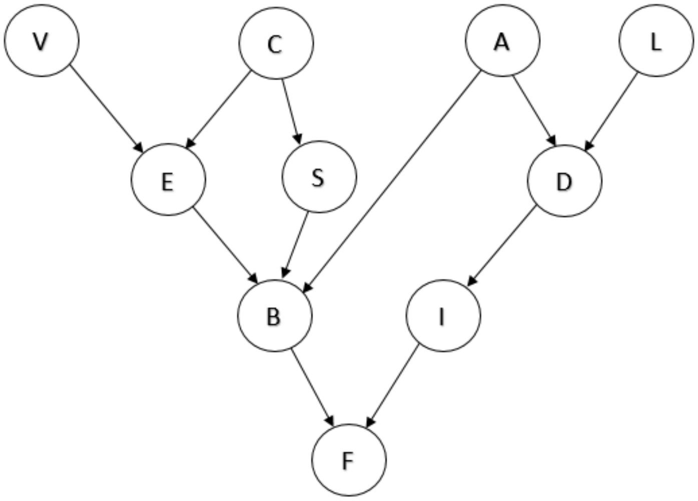
E = Exposure to vulnerability is high.

D = Detection of intrusion attempt.

B = Break-in; the web server is compromised.

I = Incident response is effective.

F = Financial losses are high (due to data loss, customer dissatisfaction, etc).



Let β' be the undirected graph obtained from β by removing the arrowheads from the edges of β. By an "undirected path" in β we mean any path in β'. A "loop-free" path is any path in which no vertex is repeated.

(a) (5 points) List all loop-free undirected paths from A to C in the graph β.

$A \to B \to S \to C$
$A \to B \to E \to C$
$A \to D \to I \to F \to B \to E \to C$
$A \to D \to I \to F \to B \to S \to C$

(b) (5 points) Suppose random variables F and S are observed, and no others are observed. Then which (if any) of those paths would be active paths? Justify your answer.

$A \to B \to E \to C$ Justification: ABE: collider-descendant, BEC: casual chain
$A \to D \to I \to F \to B \to E \to C$ Justification: ADI: casual chain, DIF: casual chain, IBF: collider observed, FBE: casual chain, BEC: casual chain

For each of the following statements, indicate whether (True) or not (False) the topology of the net guarantees that that the statement is true. If False, identify a path ("undirected") through which influence propagates between the two random variables being considered. (Be sure that the path follows the D-Separation rules covered in lecture.) The first one is done for you.

(c) $C \perp\!\!\!\perp A$: True (both are roots and no common descendants have been observed)

(d) (1 point) $B \perp\!\!\!\perp I \,|\, A$ False, BFI

(e) (1 point) $V \perp\!\!\!\perp D \,|\, E, B$ False, VECSBAD

(f) (1 point) $C \perp\!\!\!\perp D \,|\, A, I$ True

(g) (1 point) $C \perp\!\!\!\perp L \,|\, V, E, F, I$ True

(h) (1 point) $V \perp\!\!\!\perp F \,|\, E, B$ False, VECSBADIF

(i) (5 points) Suppose that the company hired an outside expert to examine the system and she determines that B, E, and I are true: a Break-in has occurred (the web server is compromised), Exposure to vulnerability is high, and Incident response is effective. Given this information, your job is to explain to management why getting additional information about C (Complexity to access the server is high) could have an impact on the probability of L (logging infrastructure is state-of-the-art). Give your explanation, for the manager of the company, using about 3 to 12 lines of text, which should be based on what you know about D-separation, applied to this situation. However, your explanation should not use the terminology of D-separation but be in plain English. (You can certainly use words like "influence", "probability", "given", but not "active path", "triple", or even "conditionally independent").

Gaining information about the complexity, allows us to make assumptions about the server accessibility. Since both the presence of an Attacker and the server accessibility affect our belief of whether or not a break in has occured, but we know that there has been a break in, we can begin to make assumptions about the presence of an attacker based on what we learn about the server accessibility. In a somewhat similar fashion, since the presence of a break in affects our belief of an attacker being active, we can begin to make assumptions about the detection of an intrusion attempt. Normally, we would not be able to make assume that the presence of an attacker can change influence the belief in the logging infrastructure, but since the probability of the incident response being effective changes our belief in the ability to detect intruders, we can now confirm this notion for the same reason that we can assume that the server accessibility can affect the belief in the presence of an attacker.

3 Reinforcement Learning

Use the Markov Decision Process (MDP) diagram below to help you as you answer the following questions about Value Iteration and Q Learning.

A	B (-10)	C	D	E	F	G $(+10)$

(a) (10 points) Use Q Learning to estimate the true q values of this MDP given the observed state transitions below. For each state transition, indicate which q value is changing by giving the state and action associated with that value and giving its new value. You may wish to keep your own diagram of the current values while you work through the given transitions.

You may assume that at states $\{A, C, D, E, F\}$ there are two allowed actions, {Left, Right}, at states $\{B, G\}$, the only allowable action is the Exit action, and at the Terminal state there are no valid actions. Make sure to process the transitions in the order provided. All Q values are initialized to 0. Use a discount factor of $\gamma = 0.8$ and a learning rate of $\alpha = 0.5$.

Note that although a description of the MDP parameters are given in the next part of this question, Q Learning does not rely on knowing these parameters and this problem may not use the same rules and parameters.

State Transitions				New Q Values		
State (s)	Action (a)	New State (s')	Reward (r)	State	Action	Q(S,A)
A	Right	B	-1	A	Right	-0.5
B	Exit	Terminal	-10	B	Exit	-5
E	Right	D	-1	E	Right	-0.5
D	Right	E	-1	D	Right	-0.5
E	Right	F	-1	E	Right	-0.75
F	Right	G	-1	F	Right	-0.5
G	Exit	Terminal	10	G	Exit	5

(b) (10 points) Value Iteration:

Consider an MDP with the states shown in the diagram above. In this MDP, there are two allowable actions for non-goal states, {Left, Right}, whose intended effect is to move the agent to the state directly to the left or right of the current state respectively.

However, at each action with probability η (noise), the agent will instead move to the state in the opposite direction of its intended move. If at any point an action would move the agent to an invalid state, the agent instead will remain in place.

At states B and G, the only allowable action is the Exit action, which gives the reward indicated in the diagram and moves the agent to the Terminal state, which is a state with no allowable actions, indicating the end of the episode.

A few examples with $\eta = 0.3$: from state D, taking action Right, the agent will move to state E with probability 0.7 and will move to state C with probability 0.3. From state A, taking action Left, the agent will remain in state A with probability 0.7 and will move to state B with probability 0.3. From state B, the only allowed action is Exit, which gives reward -10.

Perform three iterations of value iteration on the MDP described above, using noise $\eta = 0.2$, discount $\gamma = 0.9$, and a living reward of 0.0. The initial values, V_0, for all the states are provided for you. Write the values V_i corresponding to each state in the boxes for that state for iterations $i = 1, 2, 3$.

V_0:

A: 0	B: 0	C: 0	D: 0	E: 0	F: 0	G: 0

V_1:

A 0	B -10	C 0	D 0	E 0	F 10	G 0

V_2:

A -1.8	B -10	C -1.8	D 0	E 7.2	F 10	G 7.2

V_3:

A -3.096	B -10	C -1.8	D 4.86	E 7.2	F 10	G 8.496

4 The Laws of Robotics

(20 points) In the 1940's, Isaac Asimov introduced a set of three laws to govern robot behavior:

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2. A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

(NOTE: You might also want to take a look at this cartoon `https://xkcd.com/1613/`)

For this question, you will read Asimov's short story *Liar!* linked here: `https://courses.cs.washington.edu/courses/cse415/24wi/uwnetid/misc/Asimov-Liar.pdf`.

It is one of Asimov's robot short stories that were collected together in the book *I, Robot*. After you have read the story, please answer the questions below.

(a) (1 points) Who was Isaac Asimov and what is his relevance to the field of Artificial Intelligence (answer in 3-4 sentences)?

Issac Asimov was a science fiction writer. He coined the term "robotics" and introduced the three laws of robotics. These laws are ethical principals for designing intelligent robots, which can be looked at as guidelines for designing artificial intelligence systems.

(b) (2 points) Explain why the robot was lying to the humans in the story.

The robot can read minds, therefore it is able to know what the humans want to hear and do not want to hear. The robot makes the assumption that telling a human something it does not want to hear, then it would be hurting the human. So, when the robot has garnered knowledge by reading the thoughts of other humans, and learns information about that a human does not want to hear, it does not tell the human the human the truth because it has assumed that telling the human the truth would be hurting it. The robot is acting in accordance to the first law of robotics, which takes priority over all other rules.

(c) (2) Do you think the robot behaved in accordance to the Laws of Robotics by lying or should it have realized that lying could also lead to harm being done (remember to explain your reasoning)?

I do think the robot was behaving in accordance to the Laws of Robotics. The robot made the assumption that telling the human something it does not want to hear, then it would be hurting the human. The robot had to make a decision, is lying or telling the truth more harmful to the human. It decided the truth was more harmful. Although I do not agree with this line of thought, I understand why the robot has adopted it. It decided early on that lying was better, and it had to stick by its line of reasoning and continue to lie to humans.

(d) (4 points) Brain-computer interfaces are an area of active research today. What are some beneficial applications of these technologies (if you look online to help you answer this question, please include citations)?

A beneficial application of these technologies is supplementing a compromised portion of a humans brain. If a human's brain is no longer, or never was, able to perform certain tasks, some would want to be able to supplement that function of the brain through brain-computer interfaces.

(e) (4 points) What are some concerns you would have with technology that could in some way "read" the user's mind (cite any references you consult)?

In a world where everything is becoming digital, where everything can be posted, where even the private information we store online is at risk of being made public, our thoughts are the only things we have left that we can keep private. For as long as we live, or until the introduction of mind reading technology, we have the right to keep our thoughts private. Our actions are rarely reflective of our thoughts. But does that even matter? After all it is only based upon our actions that our character can be judged upon. It should stay that way, allowing us to keep our thoughts private as they are ours and ours only.

(f) (1 points) Keeping in mind the requirement that the robot has to obey the Laws of Robotics, did you find the end of the story effective and/or convincing? Explain why or why not.

I did find the end of the story effective. The robot was put into a situation where it had two options, and both options would result in hurting a human. By following the orders of the humans (Law 2), it would hurt the humans. But by not following the orders, it was also hurting the human. The robot had no other option than to break.

(g) (3 points) If you were creating a mind-reading robot today, how might you try to program the robot to prevent such a catastrophic result? In your response, assume you are free to modify or eliminate the laws of robotics.

Following the sentiment I described earlier, I would not create a robot that could read minds. But in spirit of the question, I would allow the robot to read minds, but not to share the things it has learned to other people. I would allow the robot to communicate about thoughts only with the owner of the thoughts.

(h) (3 points) Did the approach you described above require modifications to or the elimination of the laws of robotics? Do you think constraints at the hardware (e.g. robot) level are the correct approach to take to ensuring ethical uses of technology? Explain why or why not.

I could implement my ideas by changing some of the laws of robotics. I would add an addendum to Law number 1, stating that sharing information that a human deems private is grounds for hurting the human. This would force the robot to not share private information because it would be harming the human. I do not think hardware constraints are the correct approach, I think this has to be done at the software level because if the software has no constraints, it could bypass the physical constraints in some ways.

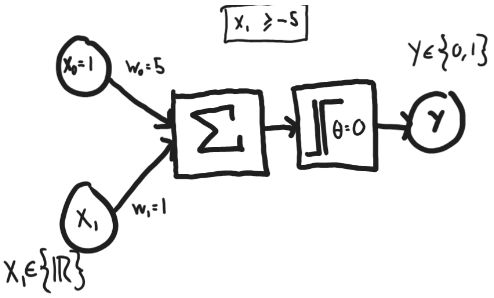
5 Perceptrons

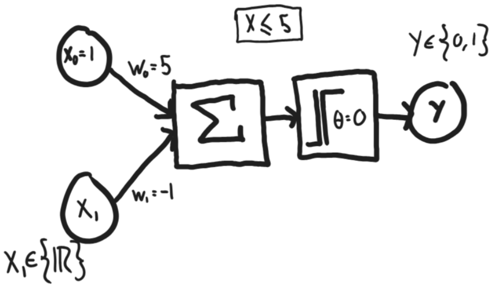
(20 points) In this question we'll assume that perceptrons should output 1 if $\sum_{i=0}^{n} w_i x_i \geq 0$ and 0 otherwise. The weight w_0 is called the bias weight, and x_0 is called the bias input and it is always equal to 1.

(a) (4 points) Assuming there will be two inputs x_1 and x_2, each with possible values in $\{0, 1\}$, give values for a triple of weights $\langle w_0, w_1, w_2 \rangle$ such that the corresponding perceptron would act as a NOR gate for the two inputs. (Again, weight w_0 is the bias weight.) Note that a NOR gate outputs 1 when both its inputs are 0; it outputs 0 otherwise.

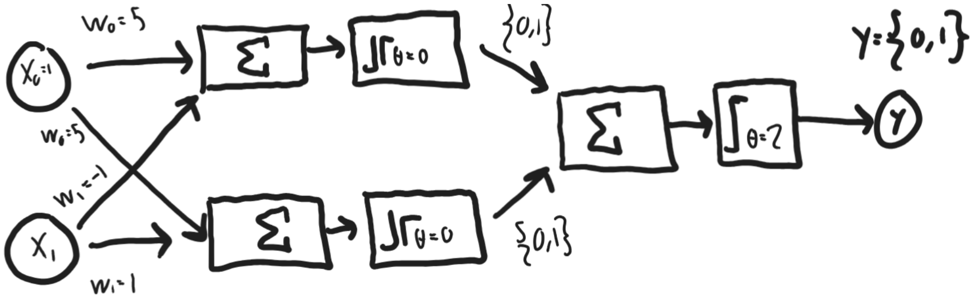
$\langle 1, -2, -2 \rangle$

(b) (4 points) Draw a perceptron, with weights, that accepts a single integer x_1 and outputs 1 if and only if the input is greater than or equal to -5. Be sure to include x_0 (the bias input of value 1) and its weight w_0 in your diagram. Draw another perceptron that outputs 1 if and only if the input is less than or equal to 5.





(c) (4 points) Using the previous perceptrons, create a two-layer perceptron that outputs 1 if $|x| \leq 5$, and 0 otherwise.



(d) (4 points) Suppose we want to train a perceptron to compare two numbers x_1 and x_2 and produce output $y = 1$ provided that x_2 exceeds x_1 by at least 7. Assume that the initial weight vector is: $\langle w_0, w_1, w_2 \rangle = \langle 1, -1, -1 \rangle$. Consider a first training example: $(\langle x_1, x_2 \rangle, y) = (\langle 3, 11 \rangle, 1)$. This says that with inputs 3, and 11, the output y should be 1, since 11 exceeds 3 by 8. What will be the new values of the weights after this training example has been processed one time? Assume the learning rate is 2.

$\langle w_0, w_1, w_2 \rangle = \langle 3, 5, 21 \rangle$.

(e) (4 points) Continuing with the last example, now suppose that the next step of training involves a different training example: $(\langle 2, 8 \rangle, 0)$. The output for this example should be 0, since 8 does not exceed 2 by at least 7. Starting with the weights already learned in the first step, determine what the adjusted weights should be after this new example has also been processed once.

$\langle w_0, w_1, w_2 \rangle = \langle 2, 3, 13 \rangle$.