CS 3600 Final exam

Due December 13, at 11:59pm Eastern

List any collaborations here: ____

Question 1. In each of the following questions, you will be given a scenario and be asked to consider whether a number of possible algorithms may or may not be well-suited to the task. One sentence should suffice for each. (1 point each)

1.a. A robot must navigate a collapsed mine to bring food and water to some survivors. If it falls down a shaft it will be destroyed. Air breezes are detectable nearby to most shafts, but breezes are sometimes too faint to be detected. Additionally, the rough terrain means that the robot's feet may slip and it may not always move forward at the intended pace. Explain why you should or should not use each of the following to reach the survivors:

i) A*: A* is not well-suited for this task because it may prioritize the shortest path, which could lead the robot down a shaft, posing a risk to its survival.

ii) A Markov Decision Process: Not well-suited for this scenario because it assumes perfect knowledge of the state, but uncertainties in air breezes make it challenging to have accurate information about the environment.

iii) A Partially-Observable Markov Decision Process: POMDP is well-suited for this task because it explicitly handles situations with imperfect information about the world state. Since it accounts for historical observations, the algorithm can detect the air breezes that have occurred.

iv) A Dynamic Bayes Network: Dynamic Bayes Network is not well-suited because it lacks specific mechanisms to handle uncertainties in observations.

v) A non-Dynamic Bayes Network: Similar to the Dynamic Bayes Network, a non-Dynamic Bayes Network is not well-suited because it does not adequately address uncertainties in observations, making it less effective in handling the complexities of the collapsed mine environment.

1.b. In the game of curling, the objective is to slide a stone down a sheet of ice and try to get it as close to the center of a target as possible. You release the stone at a particular velocity, however there are small imperfections in the ice. Explain why you should or should not use each of the following to predict where the stone will stop.

i) A*: A* should not be used for predicting where the stone will stop in curling because it is designed for solving search problems by finding the optimal path. Curling involves uncertainties due to imperfections in the ice, and A* does not inherently handle these uncertainties.

ii) A Markov Decision Process: MDP is not suitable for predicting the outcome of where the stone will stop in curling because it is more geared towards decision-making problems where the objective is to find the best sequence of actions to achieve a goal.

iii) A Partially-Observable Markov Decision Process: Not suitable for predicting outcomes, especially in the context of predicting where the stone will stop in curling. POMDP is more focused on decision-making under uncertainty.

iv) A Dynamic Bayes Network: Using DBN is a good choice for predicting where the stone will stop in curling since it is capable of handling uncertainties over time, making it suitable for generating a model based on past data and uncertainties present in curling, like imperfections in the ice.

v) A non-Dynamic Bayes Network: Not well-suited for predicting where the stone will stop in curling because it doesn't account for dynamic changes over time, such as variations in velocity.

1.c. Suppose you need to assemble a piece of Ikea furniture but lost the instructions. You need to figure out what order to assemble the pieces in, starting with a pile of parts. You have a very powerful computer that doesn't have the internet. Assume that since you will build the furniture according to the instructions generated, you will not have any problem identifying parts or applying each step. Explain why you should or should not use each of the following to create the sequence of steps to build the furniture:

i) A*: A* is suitable for this task as it is designed for finding the least number of steps (shortest path) needed to reach a goal.

ii) Reinforcement Learning: can be used if it has been trained with relevant furniture assembly data but does more than necessary.

iii) A Dynamic Bayes Network: DBN is suitable to be used as it can observe the state of the furniture in each step to make the correct decision of the next piece of assemble.

iv) A Perceptron: Not suitable to be used for furniture assembly since it is designed for classification tasks. Furniture assembly is more of a sequential planning and execution problem, which doesn't align with the task of a Perceptron.

1.d. Suppose you want to classifying rodents found on campus by species. There are 3 types of rodents (rat, shrew, or, mouse) that can be identified by inspecting size, color, tail length, whisker length, and size of front teeth. You must consider that any of these attributes can take on a range of values (e.g., a baby rat could be the size of a full-grown mouse). Explain why you should or should not use each of the following:

i) A*: A* should not be used for this classification problem because A* is designed for solving search problems

ii) A Markov Decision Process: Should not be used for classification purposes as MDP is typically applied in decision-making problems, and it is not a common choice for classification tasks.

iii) A Dynamic Bayes Network: DBN can be used for this classification task as it allows for the calculation of the overall probability of a rodent type by considering the joint probability of all the features listed.

iv) A Perceptron: A perceptron is a suitable choice for classification tasks because it can be used to correctly classify the three types of rodents by learning the appropriate weights and biases for each feature.

Question 2. (2 points) Suppose an autonomous car is driving down a road that is passing through a forest. The car strikes a pedestrian crossing a street. The pedestrian was dressed in a Halloween costume that made them look like an *Ent* (a walking, talking tree from The Lord of the Rings). It was raining at the time. The autonomous car uses only camera sensors. The car makes decisions using deep reinforcement learning. You have been called in to help investigate the crash.

You remember from CS 3600 that your professor told you there were four potential causes of errors. Explain how each type of error could have caused the crash using specific details from the scene.

Senor error: The camera sensors on the autonomous car experienced a malfunction or misinterpretation, leading to the car not being able to accurately distinguish the pedestrian from the background.

Effector error: The car correctly recognized the pedestrian and made the decision to brake. However, due to hardware malfunctions or mechanical issues, the braking system failed to execute the decision effectively.

Model error: The deep reinforcement learning lacks training to identify the pedestrian is a human and not an object, leading to the car to continue driving. The model may not have encountered enough diverse examples of pedestrians in Halloween costumes or similar scenarios during its training.

Wrong objective function: The model suffered from imitation learning with a flawed training set. If the training data included instances of cars crashing into pedestrians in rainy conditions, leading the model to imitate the behavior of crashing.

Question 3. (1 point). Consider the issue of prejudicial bias in machine learning models.

3.a. Explain how an imbalance of data for a particular feature can lead to prejudicial bias.

An imbalance of data for a specific feature can create prejudicial bias by causing the model to favor the majority while neglecting the minority. The model may then make inaccurate predictions for instances associated with the underrepresented group, resulting in biased outcomes.

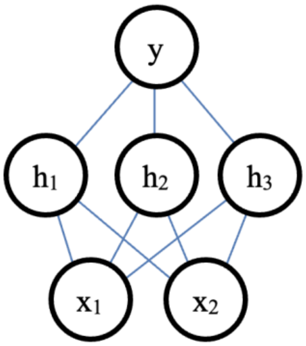
3.b. Suppose you have restricted the model's access to sensitive features but your red team discovers the potential for prejudicial bias still exists due to secondary features that cannot be removed. What technique might you use, and why might it work?

To mitigate potential prejudicial bias when sensitive features are restricted, adversarial tzxzraining can be employed. This technique introduces an adversarial component during training to identify and counteract biases in secondary features that cannot be removed. By training the model to resist biases, adversarial training can reduce the potential for prejudicial biases.

Question 4. Neural networks. Recall that the Rectified Linear Unit (ReLU) activation function is defined as:

$$ReLU(x) = \max(x,\ 0)$$

Consider the following neural network:



The activation function for all nodes are ReLUs. Neurons h_1, h_2, h_3, and y have a bias of -1. All weights, including the bias weights, are initialized to 0.1.

4.a. (1 point) x_1 and x_2 are input nodes. Suppose they are given the following values from one data point:

x_1 = 3.0
x_2 = 2.0

Compute the output activation of node y. (show work for partial credit)

output of y = ____.02_______

4a)

$h1_{in} = 3(.1)+2(.1)+(.1)(-1)=.4$
$h1_{out} = ReLU(h1in) = ReLU(.4)=.4$
$h2_{in} = 3(.1)+2(.1)+.1(-1)=.4$
$h2_{out} = ReLU(h2in)=ReLU(.4)=.4$
$h3_{in} = 3(.1)+2(.1)+.1(-1)=.4$
$h3_{out} = ReLU(h3_{in})= ReLU(.4)=.4$
$y_{in} = .4(.1)+.4(.1)+.4(.1)+.1(-1)=.02$
$y_{out} = ReLU(y_{in})=ReLU(.02)=.02$

4.b. (1 point) Suppose the target value should have been **0.0**. Using the loss function

$$L(target, output) = \frac{1}{2}(target - output)^2$$

and output of y that you computed from part 4.a, compute w_{x_1,h_1}, which is the weight between nodes x_1 and h_1, after back propagation. Use a learning rate of $\alpha = 0.5$.

w_{x_1,h_1}= __________.097______________

(Hint: you can verify your answer by using updated values for the weights in another forward pass to see if the output of y is closer to the target)

4b)

$$\frac{\partial L}{\partial W} = \frac{\partial}{\partial W}\left(\frac{1}{2}(y_{target} - y)\right) = y_{target} - y$$

$$\Delta y = ReLU'(y_{in})(y_{target} - y) = 1(0 - .02) = -.02$$

$$\Delta h_1 = ReLU'(y_{in})\, W_{h_1,y} \Delta y = 1(.1)\cdot(-.02) = -.002$$

$$W_{x_1,h_1} = W_{x_1,h_1} + \alpha X_{out} (\Delta_{h_1}) = .1 + .5(3)(-.002) = .097$$

4.c. (1 point) Suppose at some point in the future of the neural network training the weights are:

$$w_{x_1,h_1} = w_{x_2,h_1} = w_{x_1,h_2} = w_{x_2,h_3} = w_{x_1,h_3} = w_{x_2,h_3} = w_{bias,h_1} = w_{bias,h_2} = w_{bias,h_3} = 0.08$$
$$w_{h_1,y} = w_{h_2,y} = w_{h_3,y} = w_{bias,y} = 0.09$$

Run a forward pass on the neural network using the following data:

$x_1 = 0.6$
$x_2 = 0.6$

Compute the output activation of node *y*. (show work for partial credit)

output of *y* = ____0_______

4c)

h1in = .6(.08)(2) + .08(-1) = .016
h1out = ReLU(h1in) = .016
h2in = .6(.08)(2) + .08(-1) = .016
h2out = ReLU(h2in) = .016
h3in = .6(.08)(2) + .08(-1) = .016
h3out = ReLu(h3in) = .016
yin = .016(.09)(3) + .09(-1) = -.086
yout = ReLU(yin) = ReLU(-.086) = 0

4.d. (1 point) Suppose the true target value is 1.0 for the data point in 4.c. Explain what will happen to the weights after the error from the output of y is backpropagated. (Hint: computing the back-propagation step may help though we don't require you to give us the new weights). Why is it different than what happened in 4.b.?

In 4.c, the weights are smaller than those in 4.a, while the bias remains unchanged at -1. In the calculation of network error for 4.c, where yin = -.086, the derivative of ReLU(yin) becomes 0 due to yin being negative. Consequently, this results in a network error of 0 during backpropagation, leading to no weight updates and hindering model improvement. Conversely, in 4.b, the model can continue updating weights during backpropagation as the network error is positive.

4.e. (1 point) It's not good for a network to be sensitive to the choice of a bias value. Instead of fiddling with the bias value, your professor, who is a genius,* has invented a new activation function called the Markified Linear Unit (MaLU), which is defined as:

$$g(x) = \begin{cases} x, & x > 0 \\ 0.001x, & x \leq 0 \end{cases}$$

Explain why the Markified Linear Unit will work better on the neural network above.

* Allegedly, it has not been confirmed.

The Markified Linear Unit ensures that even when x is less than 0, the derivative of g(x) is 0.001, unlike ReLU, where it's 0. This prevents the issue of the network error becoming 0 during backpropagation due to derivatives being 0, allowing the model to update its weights continuously for optimal results.

Question 5. In this question we look into modifications to the basic gradient descent technique.

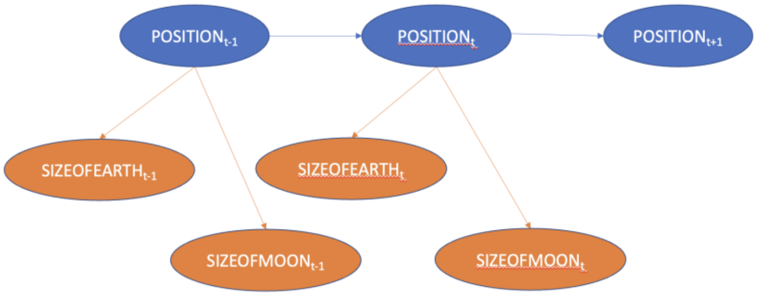
5.a. (1 point) Some more advanced gradient descent algorithms introduce the idea of "momentum" where a fraction of the delta of a weight from the previous iteration of back-propagation is added to the current delta of a weight from the current iteration of back-propagation. How does it help with the problem of local minima?

By adding a fraction of the delta of a weight from the previous iteration to the current delta, momentum allows the model to overcome getting stuck at local minima. This enables the optimization process to explore a larger space, facilitating the model's ability to escape local minima and converge towards a more optimum solution.

5.b. (1 point) Another advanced option for back-propagation is to use a decaying learning rate. The learning rate (alpha) starts relatively high and gets smaller after every epoch. What problem that we discussed in class does a decaying learning rate help with?

A decaying learning rate is helpful for finding the minimum and preventing oscillation. In a scenario with a constant learning rate, the model initially converges to the minimum, but during further iterations, it may oscillate around the minimum, failing to converge. This oscillation can be attributed to weight updates being too large, often caused by an excessively high learning rate. The decaying learning rate addresses this issue by maintaining a constant rate initially, ensuring fast convergence to the minimum. As the learning rate gradually decreases, it allows the model to fine-tune the weights, achieving convergence to the minimum without oscillation.

Question 6. (1 point) Suppose you are an astronaut on the way to the moon. Unfortunately, your radar has gone out and you have lost contact with Mission Control on Earth. You want to be able to estimate your current position and predict when you will get to the lunar orbital insertion point so you can fire your thrusters and enter orbit. You figure your current position is related to the observable size of the Earth and the Moon from your position (as you get farther from Earth it looks smaller; as you get closer to the Moon it looks bigger). Your observations aren't perfect, but you remember from CS 3600 that a Dynamic Bayesian Network can be used to estimate unobservable features—like your position in space—from imperfect observations. This is the Dynamic Bayesian Network you come up with, along with the conditional probability tables (not shown):



You decide to implement a particle filter to estimate your future position. This DBN is a bit different from the ones studied in class. What step in the particle filtering algorithm has to change to account for this network, and how must it be changed? You do not have to derive any equations.

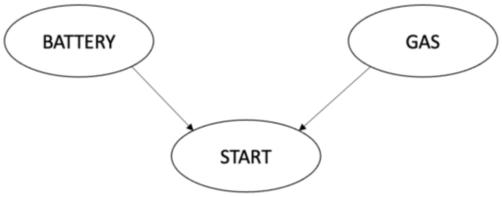
The step in the particle filtering algorithm that needs to change is the sensor model. Unlike the simplified model studied in class where the sensor model typically involves one piece of evidence, in this case, there are two pieces of evidence: the size of the Earth and the size of the Moon. Therefore, the sensor model needs to be adapted to handle the two-evidence scenario. Weights assigned to particles should consider both pieces of evidence, factoring in the observable sizes of both the Earth and the Moon for a more accurate estimation of the astronaut's position in space.

Question 7. (1 point) Someone develops an AI system that takes an image of you and makes it look more professional so that you can add it your LinkedIn account or résumé. For example, it will make your clothes look more expensive, remove blemishes and dirt from your face, make your hair look professionally and expensively groomed, and change the background to look like you are sitting in a well-furnished, private office. But this service needs a very big server and costs with high energy and maintenance costs. Thus, the service costs $500 for a set of 5 pictures. What principle from our class discussion on societal implications must be considered, and why.

The principle from our class discussion on societal implications that must be considered is fairness. The elevated service cost may contribute to economic inequalities, restricting access based on financial means. Additionally, there is a potential for bias to be introduced by the service.

Question 8: Consider the following Bayesian network that models components of a car.

- BATTERY: The car's battery is working (true or false)
- GAS: The car's gas tank has gas (true or false)
- START: The engine will start (true or false).



The engine will not start when the car is out of gas or if the battery is not working. If the car has gas and the battery is working there is an 80% chance that the car will start. History suggests that the battery works 70% of the time and that the car has gas 60% of the time.

8.a. (1 pt.) Fill out the conditional probability tables:

BATTERY	P(BATTERY)
T	.7
F	.3

GAS	P(GAS)
T	.6
F	.4

BATTERY	GAS	P(START=T | BATTERY, GAS)	P(START=F | BATTERY, GAS)
T	T	.8	.2
T	F	0	1
F	T	0	1
F	F	0	1

8.b. (2 pts.) Suppose you know that the car doesn't start. Use the definition of independence to prove or show that BATTERY and GAS not independent on each other when the car is observed to not start. Recall that dependence means that when one variable changes its value, then the distribution over the values of the other variable changes. Show your work to receive any partial credit.

Hint: Variables A and B are independent if P(A, B) == P(A)P(B). But we have an extra variable, C with a *given* value that must be factored in.

8 b)

To prove that battery & gas are not independent:

$P(\text{battery}, \text{gas} \mid \text{start}=F) \neq P(\text{battery} \mid \text{start}=F) \cdot P(\text{gas} \mid \text{start}=F)$

2 causes of car not starting

$P(\text{start}=F \mid \text{battery}=F, \text{gas}=F) = 1$

If, $P(\text{battery} \mid \text{start}=F) = P(X)$

$P(\text{gas} \mid \text{start}=F) = P(Y)$

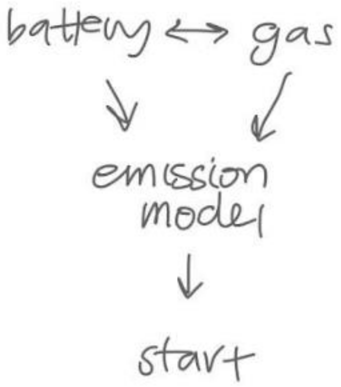
$\therefore P(\text{battery} \mid \text{start}=F) \cdot P(\text{Gas} \mid \text{start}=F) = P(X) \cdot P(Y)$

$P(\text{battery}, \text{gas} \mid \text{start}=F) \neq P(X)P(Y)$

conclusion: battery & gas are not independent when car is observed not to start

8.c. (1 pt.) Given your answer to 3.b and the fact that the car doesn’t start, explain how you could use a voltmeter on the battery to predict whether the gas tank is empty. Draw a new Bayesian Network that illustrates how the test works. [Hint: your network should now have 4 nodes, and the new node should be an emission model]

8c)


battery
gas
emission model
start