CPT_S 570

Machine Learning, Fall 2020

Homework # 4

Tayyab Munir

11716089

Question 1:

a)

It should be more intuitive to use state action-based reward function where different actions might end up giving different rewards. For example, in cricket game: $R(s)$: Bowler Just runs in and bowls. $R(s,a)$: Bowler runs in and bowls fast (more chance to get batsman out). It might be more suitable to use $R(s,a)$ type representation in this case.

b)

Finite Horizon Value Iteration algorithm in original form (In terms of state reward function) is given as:

$$V^{(o)}(s) = R(s)$$

$$V^{k+1}(s) = R(s) + \max_{a \epsilon A}\left[\sum_{s' \text{in S}} T(s,a,s')V^{(k-1)}\ (s)\right]$$

If we modify the MDP in terms of state action reward such that reward now depends on action at state "s" we can modify the MDP as:

$$V^{(k)}(s) = \max_{a \epsilon A}(R(s,a) + \sum_{s' in\ S} T(s,a,s')V^{(k-1)}(s)$$

c)

In state action reward type formulation MDP is given as:

$$V^{(k)}(s) = \max_{a \epsilon A}(R(s,a) + \sum_{s' in\ S} T(s,a,s')V^{(k-1)}(s)$$

$$V^{(k)}(s) = \max_{a \epsilon A}(R(s,a) + \max_{a \epsilon A} \sum_{s' in\ S} T(s,a,s')V^{(k-1)}(s)$$

Defining reward for state as:

$$R(s) = \max_{a \epsilon A} R(s,a)$$

We can now convert state action based MDP to equivalent State reward based MDP

$$V^{(k)}(s) = R(s) + \max_{a \epsilon A} \sum_{s' in\ S} T(s,a,s')V^{(k-1)}(s)$$

Question 2:

K_{th} order MDP depends upon current and "$k-1$" past states. Transition function for kth order MDP is defined as follows:

$$T(s_{k-1}, \ldots . s_1, a, s')$$

We can convert this representation to first order MDP by combining all k-states dictating the transition to form a master state:

$$S = [s_{k-1}, \ldots, s_1]'$$

Moreover, we can define new state as:

$$S_{new} = [s_{k-2}, \ldots, s_1, s_2]'$$

Transition matrix would now be defined by action such that state transitions from S to S_{new}.

Question 3:

$$V^{(k)}(s) = \max_{a \epsilon A}(R(s,a) + \sum_{s' in\ S} T(s,a,s')V^{(k-1)}(s)$$

If we include discount factor in the equation:

$$V^{(k)}(s) = \max_{a \epsilon A} \sum_{s' in\ S} T(s,a,s')R(s,a,s') + \gamma V(s')$$

Here γ is the discount factor $V(s')$ is the value of state s'.

Question 4:

Expressions for discounted value functions are given as follows:

$$V(s_0) = R(S_0) + \beta T(s_0, a, s_1)V(s_1)$$

$$V(s_1) = R(S_1) + \beta T(s_1, a, s_1)V(s_1)$$

a)

$$V(s_0) = 0 + 1 \times 1 \times V(s_1)$$

$$V(s_0) = V(s_1)$$

$$V(s_1) = 1 + (1)(1)V(s_1)$$

$$V(s_1) = 1 + V(s_1)$$

This system of equations is not solvable. Transition and reward functions are not well defined for part a.

b)

$$V(s_0) = 0 + 0.9 \times 1 \times V(s_1)$$

$$V(s_0) = 0.9V(s_1)$$

$$V(s_1) = 1 + (0.9)(1)V(s_1)$$

$$V(s_1) = 1 + 0.9V(s_1)$$

Solving these we get $V(s_0) = 9$ and $V(s_1) = 10$.

Question 5:

With the ever-increasing availability of data from diverse sources ethical questions regarding big data are becoming more pertinent because tools of big data are getting tightly woven into our daily life. Thus, there is a need to guide people doing big data research regarding responsible and ethical practices. Authors presented 10 rules first 5 of which focus on reducing potential public harm from big data practices. Next 5 rules present guidance regarding best practices in particular disciplines which can help data scientists contribute better to their domains.

First rule highlights the fact that data represents a group of people in some context. Practitioners should always assume that data impacts people directly unless proven otherwise. This helps in automatic consideration of this impact in research. Second rule states that privacy is not binary. It means that researchers should not assume only two classes as far as privacy is concerned. Sometimes even anonymous data can lead to unintended privacy issues. Giving importance to the context in which data is being presented is ethically very important. Third rule says that practitioners should always focus on making data as anonymous as possible. Neglection in this case can lead to unintended issues arising from re-identification of your data. Fourth rules say that practitioners should practice ethical data sharing. Collecting data in an environment that is not well regulated could lead to misleading conclusions once research is done on the collected data. Fifth rule says that practitioners should embrace both the strength and limitations of data. Many times, in research acknowledging messiness might be as important as getting good predictive results. Such approach leads to responsible research with positive contributions to the society.

Sixth rule states that there should always be an avenue for debate regarding ethical issues faced by data science practitioners in certain field. Moreover, bringing courses regarding ethical use of data in degree programs and training can be very productive. Seventh rule states that actively developing rules for big data research within a community is very important. It helps in getting representation from affected communities directly and can help in developing code of conduct that makes research community or business stake holders ethical contributors to society. Eighth rule focuses on encouraging auditability of data and developed models based on data. This would not only make better contributions but would also result in more ethical research practices. Ninth rule focuses on very important point that researchers should have broader picture in mind rather

than just some business benefits in case of industry or a bunch of citations in case of academia. Tenth rule discusses when one should put aside these rules because greater public good might be more important. Such scenarios can arise in case of emergencies like weather or medical catastrophes.

Question 6:

This paper extends the idea of Technical debt in software engineering terms to the domain of Machine learning. Technical debt in software engineering terms mean long-term costs incurred because of quickly moving in with a technical advancement. Authors highlight that goal should not only be to add new functionality, but a ML project must be able to add any future enhancements needed. The easier it is to make necessary modifications in future the lesser is technical debt and such a project is more maintainable.

Paying technical debt i.e., making improvements, adapting to changing system conditions over time etc. is necessary and deferring it would lead to compounding effects on a ML based system. Machine learning based systems are more prone to technical debt than traditional Software engineering systems because they have an additional data dependent framework apart from traditional code framework. Typical methods for paying off technical debt in software engineering terms are not as is applicable in Machine learning terms. The first section concerns with the how complex model erode boundaries. Authors state that strict abstraction boundaries that lead to maintainable and changeable codes in software engineering might be difficult to enforce in Machine learning. Authors discuss "Entanglement" issue regarding how changing one thing can lead to changing everything in machine learning context. One way to deal with this issue could be making ensembles but that also comes with the assumption that errors produced by individual learners are uncorrelated. Correction cascades also pose a big technical debt risk. ML projects are completed using cascading blocks and improving one could have harmful effects on system.

Another issue highlighted in this context is of undeclared customers. ML produced results are utilized by other users for solving own problems leading to hidden dependencies. In the next section authors highlight the point that data dependencies have potential to incur much more technical debt than code dependencies. The reason put forth is that it is easier to identify, detect and remove coding dependencies whereas it is not as simple in case of data dependencies. In the next section authors discuss about existence of hidden feedback loops in ML. Authors discuss how a ML program's output might be affecting itself. Authors call this direct dependency. Another mode of feedback loop could be a hidden one where two systems influence each other indirectly. Improvements or bugs in one could adversely affect the other system. In this section authors discuss the impacts of ML anti-patterns. They discuss that most ML projects follow high debt design patterns and depend on blocks like glue codes which are harder to tweak in real world when domain knowledge must be used to improve the ML systems. Authors also discuss about pipeline jungles where different ways to preprocess data like joining, different sampling steps can make a ML very different to interpret and improve in future. Dead experimental code paths are also highlighted as a key issue by authors in this context. In the last section authors discuss about configuration debt and how it can often take a backseat in terms of preference.

Authors conclude by summarizing about different ways to deal with technical debt and making it easier to make the necessary payments.

Question 7:

Machine learning reliability issues and production readiness issues are becoming extremely critical. This paper introduces a rubric to check Machine learning project for production readiness and reduce technical debt incurred in the long run. Authors explain that Testing and Monitoring for Machine learning is very important to ensure production readiness because performance on toy examples and offline datasets is not a good way to access production readiness. Authors specify 28 specific tests for accessing production readiness and monitoring field performance of ML systems. These tests can reduce the technical debt, reduce maintenance cost, and improve reliability of the systems. Authors suggest using each test as an assertion. First set of tests presented by authors concerns with data handling. Authors explain that machine learning testing is very complex because performance is highly dependent on data. Authors suggest that it is essential to analyze computational cost of features. It is also very important to take care about the requirements imposed on the data. Moreover, if feature can be added quickly it means that the ML project is more flexible and generalizable. Testing the code of features is also very important because such errors can go completely undetected. Second set of tests concern with the Machine learning model. Authors suggest that training should be auditable to improve reproducibility of a ML project. Furthermore, offline metrics that are normally not considered in modelling like user happiness should be correlated with model optimization metrics like least square loss. It is also essential to ensure that hyperparameters have been tuned because that can have great effect on model performance in terms of production readiness. Next set of tests concern with the ML infrastructure. Authors assert that testing a novel ML model for correctness is necessary and having just correct predictions does not justify adoption of a model. Authors state that since entire ML pipeline is integrated and each stage can produce errors, testing the whole pipeline is crucial. Moreover, it is necessary to ensure that a ML infrastructure allows easy debugging on simple example and, it should be easy to go back to previous version. Next set of tests deal with monitoring once the ML project has been deployed. Such tests include dealing with issues like data hold leading to anomalous predictions or detecting problems in the dataset that could lead to problems with production success of ML project. At the end authors introduce a way to use these tests to come up with a rubric that could be used to improve reliability and technical debt.

Question 8:

In the keynote speech by Kate Crawford, The Trouble with Bias, she centers her attention to the inflection point of machine learning and computing in 20th century. Although we have seen and experienced the vast platform of technological rush, nevertheless, this is also the crossroad where biased stereotypes can be found like word embedding, machine vision systems, language processing etc. Bias is the new underrated digital web that highlights gender classification, racist segregation, and racial disparity in the intelligence system. Terms are glossed on search engines for classification, areas are colored by companies to prioritize service and, worst of all, softwares are developed to determine future criminals in which the common poles suggest racism.

Since Machine Learning is a huge business, it affects people on a larger scale today, so biases are more likely to propagate in the field. This bias has been called a core problem of the digital world. For this reason, the motto of ML has digressed from 'Neutral Data' to 'Neutralized Data' but the solution to execute bias is something that needs to be rendered via multiple aspects. Calling bias, a technical nuance is only as much of a prejudiced perspective as the core problem itself is. To tackle this aspect, structural bias needs to be dealt with first, as that is the darkest bias present, because it is more of a social issue than a technical issue. Though we are constantly convinced that this issue has been dealt with, but the truth is that it is not.

Coming down to the origin of the word 'bias', we can notice the gradual change in the annotation of the word to suit the political and cultural reference. Even when looked into different subjects, 'bias' has a different meaning that causes the common man to never comprehend the true situation of being 'biased'. Moreover, this social stratification and prejudice made its way into Machine Learning.

So, the real problem of bias in ML comes with the harms of Allocation and Representation and the Politics of Classification. The harm of allocation happens when resources are allocated according to biases like reinforcing the subjugation of identities according to race, class and color. When allocation is structured in such a manner that people are technologically classified, their representation at a global level is also harmed. Although allocation is an immediate action, but the representation based on it has a long-term effect. One example is the stereotype of gender stratification and recognition of human beings as a single race. Data mostly does not recognize every face structure and color as it is specifically designed to recognize certain color and face structure. It further develops into labelling people according to what kind of data is fed to the machine. Denigration and under-representation are also harmful outcomes of the same process.

The most common technical responses to the problem of bias are to remove the inaccurate terms, blacklist the accusers, scrub down the data to neutral, give equal representation or spread awareness. The problem remains at the root cause when we try to address neutrality or demographics because then what is neutrality and according to which definition neutrality is neutral.

The probable root cause of bias is Classification amongst humans based on social, cultural, and religious notions. Classification initially started from the beginning of time but with modernization, classification also changed in its meaning depending on what is more socially acceptable. For example, till 2015 homosexuality was considered a mental disorder and today it is still considered a criminalized activity in a lot of countries. This is how classification affects in the long term.

To address the problem, we need to work on finishing classification at a global level.

Question 9:

In the video, In the Age of AI, the importance of artificial intelligence is elaborated with numerous examples. In every culture there is always a mind enhancing complex game like Goo or Chess which work on strategies. When such games are fed to AI, the system does not only marshal a vast amount of data, but it can also design new strategies based on already fed information. It's more like mimicking the human brain to open new windows of intelligence. This shows how AI algorithms usher in a new world of efficiency that can also be full of division.

China and USA are the two biggest AI competitors. Although US is ahead in technology because it stepped in the field years before, but China has a bigger consumer market of AI because of a larger scale of data and users of the system. When the users are more and the data is bigger, then AI can determine the behavior and needs of humans, like anyone looking for loan or what does it mean if a person keeps their mobile battery charged. This can have multiple outcomes, both good and bad, like the government can use the data to punish people for not abiding by rules or vice versa. Today China is like a Petri dish of Capitalism and technology.

Apart from gathering data, AI can also be used to self-drive cars and trucks to avoid accidents caused by human errors. At certain points, AI is also considered as the savior of mankind when it comes up with early diagnoses and better cures and treatments for illnesses like cancer. With better and early diagnoses, it can also be determined which patient requires which treatment and which patient will develop a disease later.

The problem lies with the other side of the coin, which suggests that AI can be a threat as well because it can easily displace humans like the labor force disruption will take place, human intelligence will be replaced and altogether the cognitive process. Although it cannot be estimated exactly how many jobs will extinguish in coming years, nevertheless it will happen and has already started. Automation has replaced human work. This decline in human work force has also brought a decline in the income although the scale of production has increased dramatically. This in turn has created a gap between the rich and the poor. The progressive middle class will eventually finish off, either there will be the top 1% who will own all the capital or there will the 99% who will not own anything.

AI uses algorithms to create a surveillance capitalism whose purpose is to gather as much data as possible about every individual. For example, if you ask Siri about the weather, it can decipher your temperature, cold or cough with your single question. Same is done with social media applications, every piece of information is very spied on and every outlet of AI is actually a surveillance of every human being. There are almost 58 countries, which have already become part of China's global digital system by using their AI system in forms like mobile phones, networks, devices etc.

To conclude, the war technological between USA and China will force the third world countries to take sides as to whose AI system should they use because that would mean to whom do you want your data to go to. This in turn will create a scenario of Cold War between the two superpowers and that will not be a good thing to happen.