Introduction to RL - final project's guideline

Dr. Teddy Lazebnik

2.8.2023

This document outlines the objectives of the project and how it will be evaluated. It is short as I give you as much space to be creative with your projects as possible.

The Task

The task is simple - write in English a 2400-6000 word document summarizing an academic manuscript focusing on cyber security. Afterward, prepare a presentation based on this document and present it in class. You can either pick one, send me an email and get it approved or choose one from the list below. Please try to make sure you do not pick the same project as other members of the course so it would be interesting in the last session when you present your work. Notice, that as part of the document preparation, you will have to implement the RL model in the manuscript you picked.

Document guideline

The report should be structured as follows, and answer the questions below. **Structure**: Title, authors, abstract (up to 250 words), introduction, related work, paper review, project implementation, your results, conclusion and applications, references. You can change it if you have a good reason but I would be careful with such a decision. The Introduction outlines shortly the relevance and usage of the reviewed work, the main features and how they are implemented, how they used the concepts we learn in class, and any additional points you feel are important for the reader before the main part of the body. The related work section includes **other** works (not the reviewed work) and their connection to the reviewed work. The idea is that you shortly tell the reader what is the more general context of the work in the field. For example, if this is an email server (SMTP server) the related work is how SMTP is working and its evolution over time. The paper review section is just the review - this should be the longest section. Make sure you answer the main questions such as the novelty and uniqueness of the work, the objective and features it has, what methodology it uses, how developers can use it, what limitations one can have with this work, and how one can use it in integration with other projects. Finally, the conclusion and application section in your own thoughts and ideas on how **you** or anyone else can use the new knowledge of the reviewed work to solve **similar** objectives. The last section is your real place to be creative and extend the scope and improve the quality of the work. In particular, you should show in code how you used the project in a realistic scenario.

For the "project implementation" and "your results" parts you need to implement the RL model the manuscript you review is suggesting. You need to reproduce the results of the paper to the least. If you can present any additional (and interesting) result(s), a 5 points bonus would be provided.

Make sure you properly cite the relevant references in the document. Of note, less than 10 references will be strange... This is not "a must" but think about it. Please cite appropriately - if you are not sure how, just check out any of my papers (or any other CS/Math academic manuscript). Make sure you cite any claim you make - especially if it is something about trends, numbers, or a comparison of computational models.

I really suggest writing the document in TEX and overleaf.com in particular. However, if you prefer, you can use Word/Docs - just be aware it will be harder for you to manage the citations and make the document look nice.

Document guideline

You should prepare an 10 minutes presentation (10-25 slides) based on the document you presented. Feel free to be creative with your presentation, it is only 15% of the score and the idea is that it will be informative and fun to hear you out by your peers. To make it easier for your first time preparing such a presentation, you should follow the following flow:

- Title slide - make it cool, it has a lot of screen time.
- Agenda - please avoid this, you will all have the same agenda.
- Paper review - provide the motivation of the paper. State clearly the task they aim to solve and the solution. State clearly the novelty of the solution and its limitations.
- Solution development review - Show how you reproduce the solution. What are the main classes that you used? have you taken advantage of ready code published by the authors? Any challenges you had in the process?
- Graphs! Results! Cool videos! - This is the place for visuals, make the audience impressed by the RL agent you trained.
- Summary and "Take home message" - final one or two slides with personal remarks and thoughts about the project. This is the place for you to show your creativity.
- Final slide - Summarize the main points from the slides. Please at all costs, avoid the "thank you" or "questions?" type of slides.

Several additional important comments. First, if you show a slide with a large volume of text the body will read it and I reduce you 1 point for each such slide. Second, if you present a graph without clear labels on the axis (or the plot itself), no one would understand the graph and I will reduce you 2 points for each such graph. Third, if you show a slide with only a picture that is not super related to the subject, I will reduce you 3 points for each such slide - I am sorry, you are not Steve Jobs and even he did not perform this trick well 100% of the time. Finally, if you add smarty-pants jokes (which are actually funny) into the presentation, I will give you 5 points bonus.

Q&A

Question: We want to do this work in groups... May we?
Answer: Of course! Up to three (3) students are allowed to be in a single group. That said, please note that if someone just writes his/her name and you would come to complain - I will not help you. As such, choose your co-authors wisely.

Question: Can we get an extension to the project submission?
Answer: Thanks for asking - No.

Question: ¡Insert a really good personal reason here¿. Can we get an extension on the project submission?
Answer: Wow - this is indeed a sad personal story. If the head of the department is OK with that, so am I. Please asked him to send me an email with his decision.

Question: Can you help us with the code?
Answer: No. I know this is hard, but you will never learn if you would not overcome it yourself. As such, I cross my fingers for you.

Question: I sent an email and did not get an answer yet - what should I do?
Answer: Thank you for asking. I have an algorithm for this case. If less than 2 business days have passed - wait. If more than 2 business days and this is the first time, write another polite email. If 2 business days have passed from your second email, CC the head of the department and use a sad smiley in the title of the email. If you get to this case, I am probably dead, you are expected to find out where is my office and bring flowers (I like blue ones).

Score

The score will be assessed by the following factors:

Document

- How well the related work is done, mapping the location of the reviewed work among the other works in the field.
- How well the problem is defined and formalized
- How well the novelty of the reviewed work is defined
- How well the methodology is explained and demonstrated
- How well the results and conclusions are analyzed and put into practice context - this is the main part, to be honest.

Presentation

- How well it has been presented - does the idea was clear? do you make it fun and informative?
- Flow and content - how well did you follow the required flow and presented the content accurately?
- Presentation design and structure