On Coding Theory Adversarial Robustness

Omar Attia
School of Computer Science
University of Waterloo
Waterloo, ON, N2L 3G1
omar.attia@uwaterloo.ca

Abstract

Put here a brief summary of the project: what is it about, what are the related works, what is your execution plan, what do you expect to learn/contribute, and how are you going to evaluate your results. The proposal is expected to be 1 page (reference excluded), so be concise and to the point.

1 Introduction

In this section you are going to present a brief background and motivation of your project. Why is it interesting/significant? How does it relate to the course?

2 Related Works

Perform an initial review of relevant literature. Has your problem, or one of similar nature, been considered before? By whom? What are the differences or limitations (if any)?

3 Proposed Work

In this section please concisely describe what you are going to achieve in this project. E.g., formulate your problem precisely (mathematically), present the technical challenges (if any), discuss the tools or datasets that you will build on, state your goals, and come up with a plan for evaluation.

For your own sake, you might want to lay out a time line, so that you can keep a good track of your project.

Submitted to Introduction to Machine Learning (CS698, 2017 Fall). Do not distribute.

The report

Please summarize all your findings (empirical, algorithmic, theoretical) in a scientific report. I expect there is an introduction section, a background section, a main result section, and a conclusion section. Depending on your project, you may include an experimental section and/or discussion section. Please always give proper citations to prior work or results. Be precise and concise. I expect the report to be less than **8 pages** (references excluded).

Below are some suggested structures for the report. You do not have to follow any of them. Do what you think is best to summarize your project.

Option A (Literature survey)

- Introduction
  - What is the problem?
  - Why is it an important problem?
- Survey
  - Summarize the range of techniques by highlighting their strengths and weaknesses (i.e., the 6-10 papers that you read)
  - Tip: this summary should not be a laundry list of techniques with an independent paragraph for each technique
  - Suggestion: organize your summary based on desirable properties of the techniques
- Analysis
  - What is the state of the art?
  - Any open problem?
- Conlusion
  - What have you learned?
  - What future research do you recommend?

Option B (Empirical evaluation)

- Introduction
  - What is the problem?
  - Why is it an important problem?
- Techniques to tackle the problem
  - Brief review of previous work concerning this problem (i.e., the 3-6 papers that you read)
  - Brief description of the techniques chosen and why
- Empirical evaluation
  - Describe the datasets you tested on; justify their relevance
  - Compare empirically the techniques for complexity, performance, ease of use, etc.
- Conclusion
  - What is the best technique, in terms of what?
  - Is any technique good enough to declare the problem solved?
  - What future research do you recommend?

Option C (Algorithm design)

- Introduction
  - What is the problem?
  - Why can't any of the existing techniques effectively tackle this problem?
  - What is the intuition behind the technique that you have developed?
- Techniques to tackle the problem

  - Brief review of previous work concerning this problem (i.e., the 3-6 papers that you read)
  - Describe the technique that you developed
  - Brief description of the existing techniques that you will compare to
- Evaluation
  - Describe the datasets you tested on; justify their relevance
  - Analyze and compare (empirically or theoretically) your new approach to existing approaches
- Conclusion
  - Can your new technique effectively tackle the problem?
  - What future research do you recommend?

Option D (Theoretical analysis)

- Introduction
  - What is the problem or technique?
  - What properties did you analyze/prove about this problem or technique?
- Analysis
  - Brief survey of previous work concerning this problem (i.e., the 3-6 papers that you read)
  - Describe the analysis performed
- Conclusion:
  - What have you discovered about the technique analyzed?
  - What future research do you recommend?

Acknowledgement

Thank people who have helped or influenced you in this project.

References

[1] Shai Shalev-Shwartz and Shai Ben-David. *Understanding Machine Learning: From Theory to Algorithms*. Cambridge University Press, 2014.

[2] H. D. Block. The perceptron: A model for brain functioning. *Reviews of Modern Physics*, 34 (1):123–135, 1962.

[3] A. Novikoff. On convergence proofs for perceptrons. In *Symposium on Mathematical Theory of Automata*, pages 615–622, 1962.