

Refining Adversarial Training Methods Using Game Theory

15-400 Project Milestone Report

Akhil Nadigatla

27 April 2021

1 Major Changes

While we would have loved to provide and prove some theorems for the phenomenon seen during the workings of the last milestone, we have run of time and we are still working on some of the core experiments that we hope to present during the Meeting of the Minds.

2 Accomplishments

No significant accomplishments were made during this milestone. We have been running new and repetitions of the experiments during this time in preparation for the final presentation.

3 Meeting Fourth Milestone

As aforementioned, not much of interest has happened during this milestone. A significant portion of the time was spent deciding what more we can do in this limited time for the project. We may try to explore what the perturbation model should be for this ensemble training method, but that may have to be pushed to the summer if time does not permit.

4 Surprises

No real surprises were experienced during this milestone.

5 Looking Ahead

Our main focus now is deciding what more can be done in the next couple of days and what exactly to show during the Meeting of the Minds presentation.

6 Revisions to Future Milestones

No revisions made to future milestones.

7 Resources Needed

No additional resources are needed on my end.