

CS 5600/6600

Assignment 5

Vladimir Kulyukin
Department of Computer Science
Utah State University

September 28, 2019

Learning Objectives

1. Training and Testing NNs
2. Convolutional Nets

Introduction

I originally planned to have you design, implement, and test a few ConvNets on MNIST. Alas, I didn't get through all the material in Lecture 5 that I wanted to. So, we'll postpone ConvNets until the next assignment after we cover more ConvNet theory and go over a few `tflearn` coding samples in class. This assignment will be purely analytical. You'll read and write two one-page paper reports. You can also start working on Project 1 as you read and think about these papers.

Let me say a few words about analytical writing. Some of you may be new to this type of technical writing and may have some problems. I really enjoy reading most reports. I can tell right away that their authors took the time to read the assigned paper and think about it. They share their insights, ideas, and inspirations for future work even though they frankly admit that they cannot master all the technical details. The latter is perfectly understandable: some of you have more math background to rely on than others. But, the assigned papers have plenty of less technical points to write about. A few students just write a few sentences (literally – several bullet points) or short paragraphs. If you're one of them, try to put more thought into your writeups. In your writeups, you should discuss some concrete details from the assigned papers. If you don't do it, what evidence do I have that you've actually read them?

Problem 1 (2 points)

Read and write a one-page report on “ImageNet Classification with Deep Convolutional Neural Networks” by Krizhevsky, Sutskever, and Hinton. This is a relatively recent paper. It was published in 2012 and revived image classification research on large datasets. The paper discusses many practical issues that are applicable both to ANNs and ConvNets: overfitting, regularization, dropout, and GPU training. Pay attention to the results section and ask yourself impartially how much trust you as a researcher can place in them. Save your writeup in `cs5600_6600_F19_hw05_paper_01.pdf` and submit it in Canvas.

Problem 2 (3 points)

Read and write a one-page report on “Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images” by Nguyen, Yosinski, and Clune. This paper was published

in 2015. It started a new research venue on how one can prevent deep nets from being triggered into making mistakes. It's not as easy as it may seem at first sight. If we make a few changes in an image of a lion imperceptible to a human observer, the human observer will still classify the image as a lion, but not necessarily a trained convolutional network. This point implicitly raises two fundamental questions: 1) how much biological validity do deep nets really give us? and 2) how much trust can one put into a trained deep net? Save your writeup in `cs5600_6600_F19_hw05_paper_02.pdf` and submit it in Canvas.

What to Submit

1. `cs5600_6600_F19_hw05_paper_01.pdf`;
2. `cs5600_6600_F19_hw05_paper_01.pdf`.

Happy Reading, Thinking, and Writing!