CS 165 Project Ideas

Prof. Anima Anandkumar

About the Document

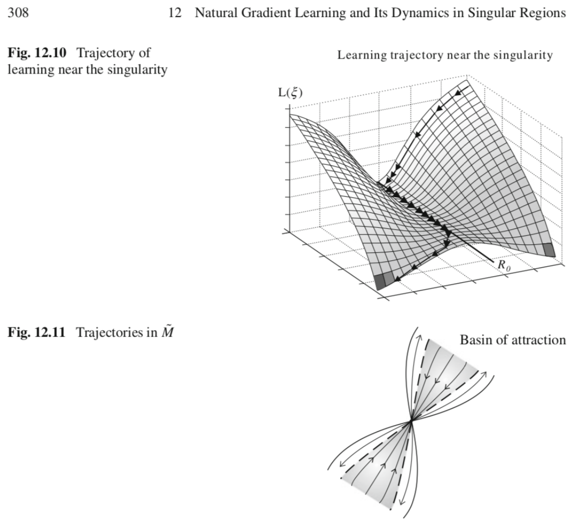
This document aims to provide some possible project ideas suggested by researchers in machine learning. Most of them are well defined problems which you will have a mentor guiding you throughout the project in order to get most out of CS 165 project task. These are also meant to give you some ideas if you are not sure what to do. You can always come up with your own project ideas too.

1 Optimization

1.1 Cubic Regularization on manifold

Mentor: Kamyar Azizzadenesheli (kazizzad@caltech.edu)

Introduction Main components of this particular problem are non-convex optimization, Riemann manifolds and cubic regularization. One of the main ingredient for the study of optimization problems and the analysis of convergence rates is the metric we chose to live in. Especially for non-convex problems, the choice of metric may significantly alter the geometry of the optimization landscape, where a smart choice of the metric results in a significant improvement in the optimization process. In his book, Shun-ichi Amari argues that the choice of Riemann metric under fisher information is a natural choice when we deal with expectations and comes up with natural gradient methods Fig. 1. He also argues that, mainly under a proper Riemann manifold, induced by Riemann metric, the saddle points collapse and become critical points; therefore it is natural to study the behavior of saddle points in different manifolds.



308 12 Natural Gradient Learning and Its Dynamics in Singular Regions

Fig. 12.10 Trajectory of learning near the singularity

Fig. 12.11 Trajectories in $\tilde{M}$

Figure 1: Figure from chapter 12 of Amari's book. Saddle manifold maps to a point

Cubic regularization is a novel second-order optimization method which studies the convergence rate to second order stationary points in a vast class of non-convex optimization problems under Euclidean metric space. Analyzing cubic regularization on the non-Euclidean manifold is still an open problem. The question of whether second-order methods are required for optimization of non-convex function after choosing a certain metric is also open.

Why it matters Solving non-convex problems is a prominent component for a variety of real-world problems, particularly machine learning problems. They abound from training deep neural networks, planning in sequential decision making to clustering and unsupervised learning problems. For the majority of these problems, in addition to finding the optimal solution, convergence rate to those solutions is also one of the primary concerns. The cubic regularization on smart choices of Riemann manifold provides more insight in the general problem of non-convex optimization and might provide faster convergence rate with the right choice of the manifold.

Project In this project, we aim to study the cubic regularization approach and simultaneously investigate the manifold optimization approach by mainly Amari. The goal is to develop principled understandings of cubic regularization on Riemannian manifold and study the convergence rate, the characteristics of the converged points, and geometry of saddle points.

References:

- Shun-ichi Amari *Chapter 12 of Information Geometry and Its Applications*
- Yurii Nesterov and B.T. Polyak *Cubic regularization of Newton method and its global performance*

2 Competitive Optimization

Mentor: Kamyar Azizzadenesheli (kazizzad@caltech.edu)

Introduction Competitive optimization is an optimization paradigm where mainly we are interested in solving min-max or max-min problems. Competitive optimization is a crucial component to game theory where we have a multi-agent setting if the agent competes against each other. Despite the prominent and principled importance of competitive optimization, we have limited knowledge in solving them. The main concern in game theory is mainly in characterizing the existence or properties of solution points rather than study of reaching them. In real world and practical problems, we are not only interested in the study of characterization of such points; but we are mainly interested in developing algorithms which can converge to such point.

Why it matters Competitive optimization abounds in many practical problems. Imagine we have two agents setting, e.g., two agents playing chess against each other, we train a generative adversarial network where we have a generator and discriminator, or adversarial attacks where some adversarial users might attach our Machine learning based web service (Of course this paradigm has many applications, but we just put some abstract ones).

Project For the simplest case, imagine we have two players where one is trying to maximize a given loss function and other one aims to minimize the very same loss function (zero sum game (the function needs not to be a loss in general)).

$$\min_{\theta} \max_{\rho} \ell(\theta, \rho)$$

We consider the optimization aspect of this problem and leave the statistical aspect for later. Can each player follow gradient descent and both converge to local Nash points? If yes what is the rate? Would applying optimistic mirror descent provide faster convergence? What is the set of constraints on the loss function to obtain convergent behavior?

In the second round, consider the stochastic version of the same problem. We aim to solve

$$\min_{\theta} \max_{\rho} \ \mathbb{E}_X \left[\ell(\theta, \rho, X)\right]$$

but we are just given samples of random variable X. Do we also converge under stochastic descent methods? What can we say about the convergent point?

References:

- Daskalakis and Panageas *The Limit Points of (Optimistic) Gradient Descent in Min-Max Optimization*
- Daskalakis et al. *Training GANs with Optimism*
- Heusel et al. *GANs Trained by a Two Time-Scale Update Rule Converge to a Local Nash Equilibrium*

3 Generalization

3.1 Mirror descent and its characterization

Mentor: Kamyar Azizzadenesheli, Navid Azizan (kazizzad, navid@caltech.edu)

Introduction We hear a lot that deep neural networks, despite having more parameters than data points, they mainly generalize well. In classical study Fig.2 we always consider that the as the error in training goes down the error in testing also goes down, but after some threshold, the testing error goes up. But this is not what we observe when we deploy deep neural networks.

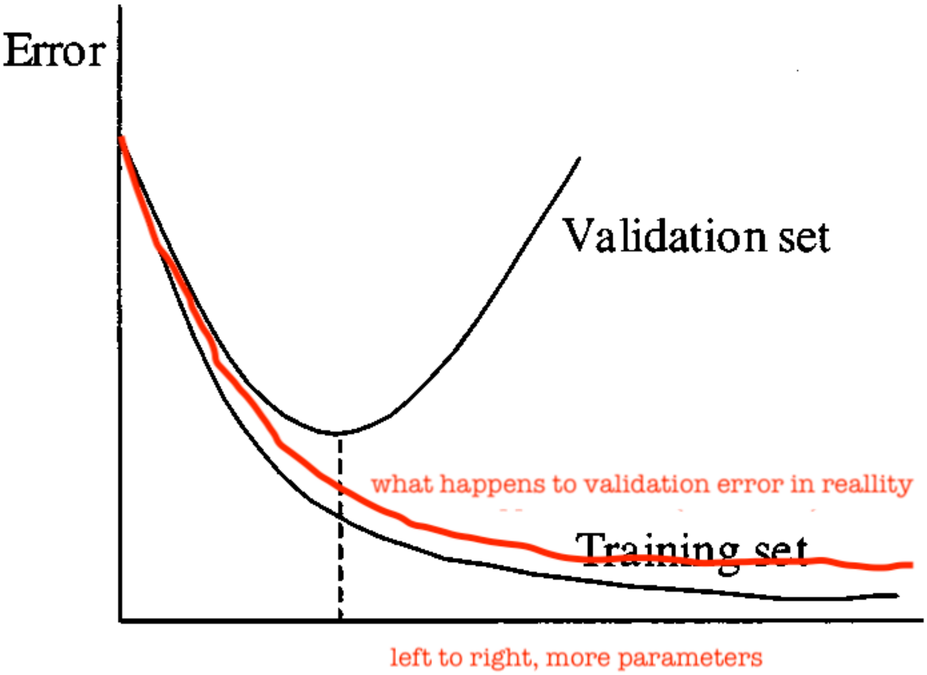


Figure 2: Generalization, what we have been told classically, and what we see

The hypothesis for what we observe is as follows; not only the capacity of function class we work with matters but also the algorithm we use to find our function also matters a lot. The deployed algorithms might search in a tiny subset of our function class and give us an implicit regularization. The topic of implicit regularization has been studied for a long time but we still do not have a clear answer what is happening with deep neural networks.

Why it matters: Generalization theory prescribes on how to exploit our trained models on the data. They show us where we can trust and deploy our model, under what circumstances they break and if we use them how far things can go wrong. Therefore the study of generalization plays a main role in machine learning. In the recent year, the capability and representation power of deep learning methods have sparked a flurry of research interest as well as industries' where the statistical understanding of their behavior is one of the main barriers in justifying their potential capabilities.

Project: In this project, we study the intrinsic characterization of stochastic gradient descend (SGD) (or in general stochastic mirror descend (SMD)) to find the space that the SGD search over. Back in the 90s, Prof. Babak Hassibi showed how the stochastic gradient descend behaves for linear models. Recently, Navid showed how stochastic gradient descent behaves for a general class of functions and characterized the solution that SGD or SMD converge to.

In this project, we characterize the space of search by gradient descent. We also provide a study of algorithmic stability to finely offer a rigorous analysis of generalization in deep neural networks.

References:

- Azizan and Hassibi, *Stochastic Gradient/Mirror Descent: min-max Optimally and Implicit Regularization*

4 Domain Adaptation

4.1 Active learning and label shift

Mentor: Kamyar Azizzadenesheli, Angie Liu (kazizzad, anqiliu@caltech.edu)

Introduction Domain adaptation, roughly speaking, is a machine learning paradigm where the domain of training and testing are different. We usually denote the training domain as the source domain and the testing domain as the target domain. In the simplest case, we are given labeled samples from the source domain and unlabeled samples from the target domain. The question is can we learn to optimally do our ML job in target domain just by seeing labels samples from the source and unlabeled from the target? The answer is simply no unless we make some assumptions.

Some examples of domain adaptation In the most prominent vision data set, ImageNet, there are 1000 classes of different object, e.g., car, tree, and air-craft. We have the same number of car, tree, and aircraft in our training data set but in practice we barely see the same number of air-crafts as trees in daily base unless we work in an airport. Therefore, there is a shift from the source in the target distributions. For another example, consider we live in Pasadena and collect disease-symptoms data set to diagnose diseases from symptoms and imagine we do a great job in classification. Now we move to San Francisco. In San Francisco, there are more people who get cold than in Pasadena, i.e., the disease distribution has changed. The question is can we use the labeled data we collected in Pasadena (x, y) and record people's symptoms in San Francisco (x) (without going through the process of diagnosing their disease) and still do a great job in San Francisco?

We classify the domain adaptation problems to 4 cases: 1) arbitrary shift 2) covariate shift 3) label shift 4) no shift

The arbitrary shift is too general, no shift also is supervised learning. Therefore, we are interested in covariate shift and label shift in this project. Let P and Q denote the distribution in source and target domain respectively. In covariate shift setting, we have $P(Y|X) = Q(Y|X)$, but $P(X) \neq Q(X)$ where X is the covariate and Y is the label. In label shift scenario we have $P(X|Y) = Q(X|Y)$, but $P(Y) \neq Q(Y)$.

Why it matters Domain adaption is almost unavoidable in supervised learning type problems. There are bare situations where the training and testing distributions are actually the same. The diagnosing disease problem can be described as label shift problem, i.e., given a disease, e.g., harsh cold, the symptoms distribution is almost the same for people living in these two cities.

Bad news, we do not have an excellent way to approach covariate shift problems yet. Therefore it is a potential project.

Good news, we are relatively better in knowing how to approach label shift problems. Check out *Regularized Learning for Domain Adaptation under Label Shifts* by Azizzadenesheli et al.

Consider the diagnosing diseases problem. We are given a set of $X's$ and $Y's$ from Pasadena and now given $X's$ from Puerto Rico after the Maria hurricane. Imagine right after the hurricane we have access to a limited number of doctors in the field that we can ask to diagnose a few patients for us in order to improve our classifier. Which patients should we query? We need to be strategic and the quarries are also expensive.

Project 1 In this project, we aim to deploy active learning to answer this question. We aim to actively sample people to diagnose such that we make our classifier better and better while following the principles developed in label shift.

References:

- Beygelzimer et al. *Importance Weighted Active Learning*
- Dasgupta and Langford, *A tutorial on Active Learning*

Project 2 Now consider a more realistic scenario in Puerto Rico. Consider a case where we also know how much each doctor, and each diagnosing process costs. Also, we have few field hospitals and can send a few people there. Also, we have access to helicopters to send people to the mainland. In addition, we have some estimate of the cost and the risks for each decision. Which patients should we query first? This problem is called cost sensitive active learning under label shift. In this project, we aim to extend the active learning and domain adaptation development and study the problem of cost-sensitive label shift active learning.

References

- Krishnamurthy et al. *Active Learning for Cost-Sensitive Classification*

4.2 Domain Adaptation with the Neural Rendering Model

Mentor: Tan M. Nguyen (mn15@rice.edu)

Introduction While deep learning's biggest successes in computer vision rely on massive datasets consisting of labeled images, its often costly or infeasible to acquire and annotate such voluminous data in practice. One promising solution is to train models on synthetic data, for which we know the true labels, and then deploy these models in real-world scenarios. Unfortunately, supervised learning techniques perform poorly when training and test distributions diverge. The subtle differences between real and synthetic data significantly degrade performance.

Methodology We propose to use the DrGANs in Section 6.1 for domain adaptation. Adversarial losses can be applied at both image pixel and latent code levels. In addition, we would like to propose an alternative to adversarial loss which takes geometry of data and latent codes into account.

Why it matters If this project succeeds, we can reduce the need of real labeled data in training deep learning models. As a result, deep learning models can be used in new domains and applications in which it is expensive and challenging to collect and annotate the data.

References

- Shrivastava and et al, Learning from Simulated and Unsupervised Images through Adversarial Training, CVPR 2017
- Ho, Nguyen, and et al, Neural Rendering Model: Joint Generation and Prediction for Semi-Supervised Learning, arXiv 2018

5 Reinforcement Learning/Imitation Learning

5.1 Benchmarking off-policy policy evaluation problem

Mentor: Hoang M. Le (hmle@caltech.edu)

Description of the Project Off-policy policy evaluation (OPE) is the setting where we try to estimate value of some policy having only access to data generated by some other behavior policy. OPE has important implication to real-world sequential decision making when exploration is either expensive or impractical due to cost or safety concerns. It is currently an active area of research with several new methods proposed in the last 3 years. Theoretical analyses of such approaches involve understanding the bias-variance trade-offs in reinforcement learning problems with possibly long horizon. Experimentally, most methods have been applied to small domains. Understanding how different methods perform for higher dimensional settings would be valuable.

References:

- Liu et al, Breaking the Curse of Horizon: Infinite-Horizon Off-Policy Estimation, NeurIPS 2018
- Thomas and Brunskill, Data-Efficient Off-Policy Policy Evaluation for Reinforcement Learning, ICML 2016
- Jiang and Li, Doubly Robust Off-policy Value Evaluation for Reinforcement Learning, ICML 2015

5.2 Hierarchical imitation and reinforcement learning for dialogue systems

Mentor: Hoang M. Le (hmle@caltech.edu)

Description of the Project Applying a combination of imitation and reinforcement learning to train a goal-oriented chat bot. The goal is well-specified depending on the domain (movie ticket booking, travel planning and reservation). Students can leverage existing datasets and implementations. The problem of natural language understanding and generation can be abstracted away, thus the focus would be on the algorithmic development into the core sequential decision making problem.

References:

- Le et al, Hierarchical Imitation and Reinforcement Learning, ICML 2018
- Peng et al, Composite Task-Completion Dialogue Policy Learning via Hierarchical Deep Reinforcement Learning, NAACL 2017

5.3 Object recognition as a reinforcement learning problem

Mentor: Hoang M. Le (hmle@caltech.edu)

Description of the Project This project aims to tackle the issue of exploration in a natural image context. The overall goal, as usual, is to identify the object presented in the natural image (for example from ImageNet or Cifar). Initially, the image is unknown to the learning agent (essentially a black screen). Simulating the idea of active scanning and attention, we'd apply the constraint that at each time step, the learning agent can only choose a small patch of the image to reveal the pixels behind the patch. And the goal is to be able to identify the object behind the screen in as few steps as possible. This is similar to a game in the RL context, but we will focus on the practical issue of object recognition.

References:

- Bahdanau et al, An Actor-Critic Algorithm for Sequence Prediction, ICLR 2017
- Zhang et al, Actor-Critic Sequence Training for Image Captioning, NeurIPS 2017

5.4 Regularizing reinforcement learning with partial expert feedback

Mentor: Hoang M. Le (hmle@caltech.edu)

Description of the Project Reinforcement and imitation learning are two paradigms to tackle sequential decision making problems. However, they fundamentally have different objective functions. One way to connect the two objectives is to view one as a regularization objective of the other. The question of interest here is can we show theoretically and experimentally the benefit of regularizing RL problems with limited expert feedback. Theoretical analyses may involve understanding the statistical properties of regularizing policy classes. Experimentally, one could implement ideas in domains such as car driving from openAI gym, or TORCS.

References:

- Le et al., Batch Policy Learning under Constraints (in submission - talk to Hoang Le about the algorithm)
- Ross and Bagnell, Reinforcement and Imitation Learning via Interactive No-Regret Learning
- Sun et al, Provably Efficient Imitation Learning from Observation Alone, NeurIPS 2018 Workshop on Imitation Learning for Robotics

6 Generative Modeling

6.1 DrGAN: Deep Rendering Generative Adversarial Networks

Mentor: Tan M. Nguyen (mn15@rice.edu)

Introduction A recent interest in generative modeling is to develop invertible deep generative models. The likelihood of these models can be exactly computed while their inference has the form of a neural network and is, therefore, efficient. Among the invertible deep generative models is the Neural Rendering Model (NRM). The hallmark of the NRM is that its inference matches the architecture of a convolutional neural network (CNN). This advantage does not only provide a probabilistic framework to study CNNs but also allows the NRM to achieve state-of-the-art results in semi-supervised learning. However, since the NRM employs a large amount of auxiliary latent variables to compensate for the loss of information in CNNs, image generation in the NRM is challenging. The NRM indeed fails to generate realistic-looking images.

Methodology We propose to combine the Generative Adversarial Networks (GANs) and the NRM into a new generative probabilistic model, namely the Deep Rendering Generative Adversarial Model (DrGAN), which achieves good performance on both semi-supervised learning and image generation. In particular, DrGAN inherits the zero-sum game framework from GANs, but uses the NRM's generation and inference processes as its generator and discriminator, respectively.

Why it matters The adversarial loss allows DrGAN to sample the latent variables which yield in realistic-looking images. Furthermore, the generator and discriminator in DrGAN share weights, and thus DrGAN uses less parameters compared to other GANs, which potentially results in faster and more stable training.

References

- Goodfellow and et al, Generative Adversarial Nets, NIPS 2014
- Ho, Nguyen, and et al, Neural Rendering Model: Joint Generation and Prediction for Semi-Supervised Learning, arXiv 2018

6.2 Generative Scattering Networks

Mentor: Tan M. Nguyen (mn15@rice.edu)

Introduction Scattering networks have been used to solve inverse problems in various geophysical applications including earthquake detection and fault evolution forecasting. Since labeled data is rarely available in the field of geophysics, it is unclear what objective loss to train the scattering networks should be. Various objective losses have been proposed, but most of them are not mathematically grounded.

Methodology We propose a new generative model whose inference matches the scattering network's architecture. Our model learns from unlabeled data by optimizing the data log-likelihood. We evaluate the model on the tremor signal detection task. Tremors are used to detect and forecast earthquakes.

Why it matters If our model can learn to predict earthquake from unlabeled geophysical data and the physics are ultimately shown to scale from the laboratory to the field, researchers will have the potential to improve earthquake hazard assessments that could save lives and billions of dollars in infrastructure.

References

- Bruna and Mallat, Invariant Scattering Convolution Networks, PAMI 2013
- Angles and Mallat, Generative networks as inverse problems with scattering transforms, ICLR 2018
- Machine Learning for Geophysical & Geochemical Signals Workshop, NeurIPS 2018
- LANL Earthquake Prediction

6.3 Active Learning with Deep Generative Models

Mentor: Tan M. Nguyen (mn15@rice.edu)

Introduction Data likelihood estimated from deep generative models such as the variational autoencoders and pixel recurrent neural networks can potentially be used in various active learning applications. However, it is nebulous how to use the data likelihood from these generative models to actively select samples for training convolution neural networks (CNNs). This is partly because there is no clear connection between CNNs and these aforementioned deep generative models. Thus, likelihood from those models do not necessarily associate with the distribution learned by the CNNs.

Methodology The Neural Rendering Model (NRM) is a recently developed deep generative model whose inference matches the architecture of convolutional neural networks (CNNs). In other words, if CNNs estimate the posterior $p(y|x)$, then the likelihood $p(x|y)$ can be computed from the NRM. Thus, the NRM's density estimation can be used in conjuction with CNNs in an active learning setting. In this project, we would like to explore using the likelihood estimated from the NRM for active learning in the corresponding CNN.

Why it matters Training CNNs requires a large amount of labeled data. Our active learning approach will reduce the number of samples needed to train CNNs, which results in faster training with potentially better accuracy. These advantages help reduce the cost of data collection/annotation and lower the amount of computational resources needed for training large-scale CNNs.

References

- Shen and et al, Deep Active Learning for Named Entity Recognition, ICLR 2018
- Rob Nowak and Sanjoy Dasgupta's talk at the Simons Institute (https://simons.berkeley.edu/talks/ dasgupta-01-24-2017-1)
- Nalisnic and et al, Do Deep Generative Models Know What They Don't Know?, ICLR 2019
- Ho, Nguyen, and et al, Neural Rendering Model: Joint Generation and Prediction for Semi-Supervised Learning, arXiv 2018

7 Efficient Machine Learning

7.1 Energy Efficient Neural Networks via Born Again Approach

Mentor: Tan M. Nguyen (mn15@rice.edu)

Introduction Various pruning and skipping methods have been developed to reduce the computational and memory cost of convolutional neural networks (CNNs) at both training and deployment. These methods usually trade off between accuracy and efficiency and often result in compact networks with a slight decrease in performance. We would like to overcome this performance degradation.

Methodology Recently, born again networks (BANs) have been proposed to improve the networks accuracy via a sequence of knowledge distillation re-trainings. In particular, in addition to being optimized for the task of interest, a BAN learns to match the activations of a teacher network which has the same architecture. We propose to combine pruning and skipping with knowledge distillation in BANs to improve the accuracy-efficiency trade-off.

Why it matters Efficient and yet accurate neural networks are highly demanded in edge computing on resource-constrained platforms including mobile and wearable devices. If our project succeeds, it will facilitate the development of deep learning-powered Internet of Things (IoT) devices, which promise to dramatically revolutionize the way we live and work by enhancing our ability to recognize, analyze, and classify the world around us.

References

- Furlanello and et al, Born Again Neural Networks, ICML 2018
- Wang and et al, SkipNet: Learning Dynamic Routing in Convolutional Networks, ECCV 2018
- Han and et al, Deep Compression: Compressing Deep Neural Networks with Pruning, Trained Quantization and Huffman Coding, ICLR 2016
- Wang, Nguyen, and et al, EnergyNet: Energy-Efficient Dynamic Inference, NeurIPS workshop 2018