Unsupervised Aggregation of Deep Models

Amirhossein Afsharrad
Introduction

• **Ensemble Models:** a group of algorithms focusing on aggregating multiple base learners to outperform each individual learner

• **Black-Box Models:** models that we only have access to their input-output pairs

• **Goal:** aggregation of deep black-box models in an *unsupervised* manner
Problem Statement

- $X_1, \ldots, X_M$: unlabelled samples (images)
- $K$ local classifiers
- $Y^k_m$: label of the $k$th model to the $m$th input
- $Z_1, \ldots, Z_M$: hidden true labels
- Goal: Estimate $Z_1: M$ by observing $X_1: M$ and $Y^1: K_1: M$
Dataset

- CIFAR10
- ImageNet
- Animal and Non-Animal binary classification

\[
\begin{align*}
Z &= 1 \\
Z &= 0
\end{align*}
\]
Mathematical Model

Model Introduction

• Model 1: Uniform Error Model
  • The $k$th model makes a prediction error with probability $\epsilon_k$
  • Maximum Likelihood Problem:
    \[
    \max_{Z_1, \ldots, Z_M} \sum_{k=1}^{K} \sum_{m=1}^{M} \log \mathbb{P}(Y_k^m | Z_m)
    \]

• Model 2: Non-Uniform Error Model
  • The $k$th model makes a prediction error with probability $\epsilon_k(X)$ for the input vector $X$
  • Maximum Likelihood Problem:
    \[
    \max_{Z_1, \ldots, Z_M} \sum_{k=1}^{K} \sum_{m=1}^{M} \log \mathbb{P}(Y_k^m | Z_m, X_m)
    \]
Mathematical Model

Problem Formulation

• Model 1: Uniform Error Model

  Since we do not know $\epsilon_k$, we jointly maximize over $\epsilon, Z_{1:M}$:

  $\max_{\epsilon_1,\ldots,\epsilon_K} \max_{Z_1,\ldots,Z_M} \sum_{k=1}^K \sum_{m=1}^M \log \mathbb{P}(Y_{km}^k \mid Z_m)$

  • Solving this problem is exponential in $M$, instead we use Expectation Maximization:

    Until Convergence:
    1. Fix $Z$, and maximize over $\epsilon$
    2. Fix $\epsilon$, and maximize over $Z$

• Model 2: Non-Uniform Error Model

  Since we do not know $\epsilon_k$, we jointly maximize over $\epsilon, Z_{1:M}$:

  $\max_{\epsilon_1(\cdot),\ldots,\epsilon_K(\cdot)} \max_{Z_1(\cdot),\ldots,Z_M} \sum_{k=1}^K \sum_{m=1}^M \log \mathbb{P}(Y_{km}^k \mid Z_m, X_m)$

  • Solving this problem is exponential in $M$, instead we use Expectation Maximization:

    Until Convergence:
    1. Fix $Z$, and maximize over $\epsilon$
    2. Fix $\epsilon(\cdot)$, and maximize over $Z$
Mathematical Model
Comparing the Two Models

• Why do we need to introduce the non-uniform model?
  
The error depends on the input

1. There are easy and hard examples

2. Models can be specialized
   A specific example can be easy for one model but difficult for another
Results

• Ideal (Synthetic) Setting

• Local models having different overall accuracy

• $c_k(X)$ varies with $X$
  
  • maj: simple majority voting
  
  • EM0: uniform error model
  
  • EM: non-uniform error model

![Classification Accuracy for $K = 5$ with $N = 100$ Iterations](image)
Results

- Ideal (Synthetic) Setting
- Local models having different overall accuracy
- $e_k(X)$ does not vary with $X$ (uniform error model holds)
Results

- Realistic Setting
- 5 convolutional neural networks

**Problem:** pixel-wise distance of images is not a good measure

**Solution:**

1. Color histogram / HOG
2. Auto-Encoders

![Classification Accuracy](chart.png)

Classification Accuracy for \( K = 5 \) with \( N = 100 \) Iterations
Results

- Realistic Setting
- 5 convolutional neural networks
- $\epsilon_k(X)$ varies with $X$
- Auto-encoders used to create $\hat{X}$ from $X$, then we estimate $\epsilon_k(\hat{X})$
Conclusion and Future Works

• We studied a novel approach to combine black-box deep models and outperform majority voting for model aggregation.

• Future directions:
  • Non-binary classification
  • More complicated models (RNNs)
  • Finding theoretical guarantees for the proposed algorithms