Planning Confident Predictions for Semi-Supervised Learning

Eduardo H. P. Pooch
Ph.D. Student in Computer Science
Pontifícia Universidade Católica do Rio Grande do Sul
Porto Alegre, RS, Brazil
Email: eduardo.pooch@edu.pucrs.br

***Abstract*—In this project, we propose to develop a novel augmentation technique aimed at semi-supervised learning. The proposed method consists in searching for image augmentation policies that encourage more confident predictions during training. We will do that by modeling a Markov Decision Process and a search algorithm rewarded by larger confidence scores outputted by a neural network, enforcing entropy minimization, a technique used by multiple semi-supervised learning methods. We hope to extend a current state-of-the-art semi-supervised method by adding this new augmentation mechanism and evaluate its impact on image classification with limited supervision.**

1. Introduction

To train deep learning models in a supervised fashion, we need a significant amount of training data. However, in some scenarios, like in medical imaging medical imaging [1], there might be a lack of available annotated data. As data annotation is usually a manual procedure, to acquire a large dataset for computer vision like ImageNet [2] might get too costly when the people annotating the images need to be experts or if the annotation demands a lot of time.

Recently, research in semi-supervised learning for image classification had some considerable progress [3]. Methods based on consistency regularization and entropy minimization strategies such as Mean Teacher [4], and Unsupervised Data Augmentation (UDA) [5] achieve results comparable to supervised training but with only a fraction of the training samples. For instance, training a model on the SVHN dataset in a supervised fashion using all training data ($73,257$ labeled samples) results in an error rate of 2.59%, whereas training the same model with the UDA approach and only 250 labeled samples achieves an error rate of 2.72% [6].

In the **supervised learning** approach, the model learns based on known annotated examples. As the system is presented with input and output variables in the training set, it seeks to create a model representing this data distribution. Then, we extrapolate this model to infer the output variable of an unseen input sample. In the **semi-supervised learning** approach, besides labeled samples, we also have unlabeled samples that are within the same feature space $\mathcal{X}$, but whose output labels on the label space $\mathcal{Y}$ are unknown [7]. We can use the unlabeled samples in the training set alongside the labeled ones in order to improve the modeling of the function $m(x) : \mathcal{X} \rightarrow \mathcal{Y}$. Intuitively, the unlabeled samples provide important clues on the data distribution based on sample similarity, and they help to add robustness to the model by exploring this distribution [3].

Semi-supervised learning methods are mainly based on three assumptions: smoothness, low-density, and manifold [8]. The smoothness assumption states that if two samples x_1 and x_2 are close in the feature space, their labels y_1 and y_2 are probably the same. The low-density assumption states that the decision boundary of a classifier probably does not pass through high-density areas of the feature space. Finally, the manifold assumption says that samples located on the same low-dimensional feature space manifold probably have the same labels.

State-of-the-art semi-supervised learning methods implement both perturbation-based and entropy minimization techniques. Perturbation-based approaches rest on the smoothness assumption, implying that small perturbations on the input should not alter the model's prediction. This behavior does not depend on knowing the ground-truth label. Therefore, we can apply noise to input data points and use the distance between the output of clean and noisy input samples on the loss function, adjusting the model based on unlabeled data [8]. These methods take advantage of artificial neural networks because of their straightforward incorporation of additional terms on the objective optimization function. Entropy minimization approaches rest on the low-density assumption and encourages the model to make confident predictions even on unlabeled data in order to keep the decision boundary far from high-density areas.

Xie et al. [5] argue that the quality of the input noise plays a crucial role in perturbation-based semi-supervised learning methods. They propose Unsupervised Data Augmentation (UDA), which uses advanced data augmentation techniques to input noise on the training data. For image classification tasks, the authors propose using AutoAugment [9], an image augmentation method that searches for an optimal augmentation policy in a space of multiple image transformation functions. AutoAugment's objective is to find an augmentation policy that maximizes the accuracy of a predictive model in a labeled subset of the data. The found policy is then used by the method during the training of the

model.

The proposed approach is to model a search algorithm based on AutoAugment, but instead of using the accuracy as the reward, it rewards a maximum output probability score. This way, it enforces confident predictions and rests on the low-density assumption to achieve a better augmentation policy for semi-supervised learning, generating a new semi-supervised training method for image classification.

2. Technical approach

We intend to include the proposed augmentation method in a training framework based on UDA. UDA is a semi-supervised training method that uses one model $m(\cdot)$, which is updated by a combined loss function $\mathcal{L}_{comb}$. The combined loss is the sum of the task loss $\mathcal{L}_{task}$ with the consistency loss $\mathcal{L}_{cons}$. The task loss is a regular cross-entropy loss between the ground-truth labels y and the labels predicted by the model $m(x)$, which is only computed on labeled instances. The consistency loss is a KL-divergence between augmented ($\phi(u)$) and non-augmented (u) unlabeled data. A hyperparameter λ defines the weight of the consistency loss on the combined loss.

$$\mathcal{L}_{comb} = \mathcal{L}_{task} + \lambda \mathcal{L}_{cons} \tag{1}$$

$$\mathcal{L}_{task} = BCE(m(x), y) \tag{2}$$

$$\mathcal{L}_{cons} = log \frac{m(\phi(u))}{m(u)} \tag{3}$$

The proposed contribution of the project is to develop a novel augmentation mechanism ϕ in this semi-supervised framework. We aim to develop a Markov Decision Process (MDP) to search optimal augmentation policies. In this MDP, the states are the probability and magnitude values of each of the 16 image operation functions on the Python Image Library (PIL). The possible actions are to lower or increase the values of probability and magnitude of each image transformation function. Since we want to increase the confidence of the model, the reward would be the sum of the maximum output score probability of the model $m(.)$ on a subset of unlabeled data u, computing $\sum_i^n \max(m(\phi(u_i)))$.

This policy can be learned at each iteration of the model, based on a batch of samples, or learned offline on a subset of the data and then used during multiple iterations in case the proposed approach is too computationally expensive. We intend to evaluate the proposed approach by using common benchmarks of semi-supervised learning like the CIFAR-10 dataset [10] with only a subset of labeled samples of the dataset and compare it to current semi-supervised methods.

3. Project management

The final project is due in 5 weeks. Therefore we proposed the following schedule:

- Week 1: The first step of the project is to reproduce the UDA framework using a policy learned by AutoAugment;
- Week 2: Code the proposed MDP environment and study the best search algorithm for the proposed approach;
- Week 3: Implement the search algorithm on the proposed MDP using a static model and check if the generated scores are higher with the predicted augmentation policy.
- Week 4: Evaluate the computational cost and viability for the search to be online during training, then include the augmentation policy on the UDA framework, and evaluate the performance of the approach;
- Week 5: Report the results on the final paper.

4. Conclusion

At the end of this work, we expect to develop a novel semi-supervised learning approach that better encourages both consistency regularization through the UDA framework and entropy minimization through a novel augmentation mechanism that learns to enforce more confident predictions. We hope that this method can accomplish better results on semi-supervised learning, helping to advance the state-of-the-art in machine learning with limited supervision.

References

[1] G. Litjens, T. Kooi, B. E. Bejnordi, A. A. A. Setio, F. Ciompi, M. Ghafoorian, J. A. van der Laak, B. van Ginneken, and C. I. Sánchez, "A survey on deep learning in medical image analysis," *Medical Image Analysis*, vol. 42, pp. 60–88, dec 2017.

[2] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Advances in neural information processing systems*, 2012, pp. 1097–1105.

[3] G.-J. Qi and J. Luo, "Small data challenges in big data era: A survey of recent progress on unsupervised and semi-supervised methods," *arXiv preprint arXiv:1903.11260*, 2019.

[4] A. Tarvainen and H. Valpola, "Mean teachers are better role models: Weight-averaged consistency targets improve semi-supervised deep learning results," mar 2017. [Online]. Available: http://arxiv.org/abs/1703.01780

[5] Q. Xie, Z. Dai, E. Hovy, M.-T. Luong, and Q. V. Le, "Unsupervised data augmentation," *arXiv preprint arXiv:1904.12848*, 2019.

[6] D. Berthelot, N. Carlini, I. Goodfellow, N. Papernot, A. Oliver, and C. Raffel, "MixMatch: A Holistic Approach to Semi-Supervised Learning," may 2019. [Online]. Available: http://arxiv.org/abs/1905.02249

[7] X. Zhu and A. B. Goldberg, "Introduction to semi-supervised learning," *Synthesis Lectures on Artificial Intelligence and Machine Learning*, vol. 3, no. 1, pp. 1–130, 2009. [Online]. Available: https://doi.org/10.2200/S00196ED1V01Y200906AIM006

[8] J. E. van Engelen and H. H. Hoos, "A survey on semi-supervised learning," *Machine Learning*, Nov 2019. [Online]. Available: https://doi.org/10.1007/s10994-019-05855-6

[9] E. D. Cubuk, B. Zoph, D. Mane, V. Vasudevan, and Q. V. Le, "Autoaugment: Learning augmentation policies from data," *arXiv preprint arXiv:1805.09501*, 2018.

[10] A. Krizhevsky, G. Hinton *et al.*, "Learning multiple layers of features from tiny images," Citeseer, Tech. Rep., 2009.