Unsupervised Data Augmentation

Qizhe Xie[1,2], **Zihang Dai**[1,2], **Eduard Hovy**[2], **Minh-Thang Luong**[1], **Quoc V. Le**[1]
[1] Google Brain, [2] Carnegie Mellon University
{qizhex, dzihang, hovy}@cs.cmu.edu, {thangluong, qvl}@google.com

Abstract

Despite its success, deep learning still needs large labeled datasets to succeed. Data augmentation has shown much promise in alleviating the need for more labeled data, but it so far has mostly been applied in supervised settings and achieved limited gains. In this work, we propose to apply data augmentation to unlabeled data in a semi-supervised learning setting. Our method, named Unsupervised Data Augmentation or UDA, encourages the model predictions to be consistent between an unlabeled example and an augmented unlabeled example. Unlike previous methods that use random noise such as Gaussian noise or dropout noise, UDA has a small twist in that it makes use of harder and more realistic noise generated by state-of-the-art data augmentation methods. This small twist leads to substantial improvements on six language tasks and three vision tasks even when the labeled set is extremely small. For example, on the IMDb text classification dataset, with only 20 labeled examples, UDA outperforms the state-of-the-art model trained on 25,000 labeled examples. On standard semi-supervised learning benchmarks, CIFAR-10 with 4,000 examples and SVHN with 1,000 examples, UDA outperforms all previous approaches and reduces more than 30% of the error rates of state-of-the-art methods: going from 7.66% to 5.27% and from 3.53% to 2.46% respectively. UDA also works well on datasets that have a lot of labeled data. For example, on ImageNet, with 1.3M extra unlabeled data, UDA improves the top-1/top-5 accuracy from 78.28/94.36% to 79.04/94.45% when compared to AutoAugment.

1 Introduction

Deep learning typically requires a lot of labeled data to succeed. Labeling data, however, is a costly process for each new task of interest. Making use of unlabeled data to improve deep learning has been an important research direction to address this costly process. On this direction, semi-supervised learning [Chapelle et al., 2009] is one of the most promising methods and recent works can be grouped into three categories: (1) graph-based label propagation via graph convolution [Kipf and Welling, 2016] and graph embeddings [Weston et al., 2012], (2) modeling prediction target as latent variables [Kingma et al., 2014], and (3) consistency / smoothness enforcing [Bachman et al., 2014, Laine and Aila, 2016, Miyato et al., 2018, Clark et al., 2018]. Among them, methods of the last category, i.e., based on smoothness enforcing, have been shown to work well on many tasks.

In a nutshell, the smoothness enforcing methods simply regularize the model's prediction to be less sensitive to small perturbations applied to examples (labeled or unlabeled). Given an observed example, smoothness enforcing methods first create a perturbed version of it (e.g., typically by adding artificial noise such as Gaussian noise or dropout), and enforce the model predictions on the two examples to be similar. Intuitively, a good model should be invariant to any small perturbations that do not change the nature of an example. Under this generic framework, methods in this category differ mostly in the perturbation function, i.e., how the perturbed example is created.

Preprint. Under review.

In our paper, we propose to use state-of-the-art data augmentation methods found in supervised learning as the perturbation function in the smoothness enforcing framework, extending prior works by Sajjadi et al. [2016], Laine and Aila [2016]. We show that better augmentation methods lead to greater improvements and that they can be used on many other domains. Our method, named Unsupervised Data Augmentation or UDA, minimizes the KL divergence between model predictions on the original example and an example generated by data augmentation. Although data augmentation has been studied extensively and has led to significant improvements, it has mostly been applied in supervised learning settings [Simard et al., 1998, Krizhevsky et al., 2012, Cubuk et al., 2018, Yu et al., 2018]. UDA, on the other hand, can directly apply state-of-the-art data augmentation methods on unsupervised data which is available at larger quantities and therefore has the potential to work much better than standard supervised data augmentation.

We evaluate UDA on a wide variety of language and vision tasks. On six text classification tasks, our method achieves significant improvements over state-of-the-art models. Notably, on IMDb, UDA with 20 labeled examples outperforms the state-of-the-art model trained on 1250x more labeled data. We also evaluate UDA on standard semi-supervised learning benchmarks on CIFAR-10 and SVHN. Our method achieves an error rate of 5.27% and 2.46% respectively, significantly outperforming the previous state-of-the-art method which has an error rate of 7.66% and 3.53%. Finally, we also find UDA to be beneficial when there is a large amount of supervised data. Specifically, on ImageNet, UDA leads to improvements of top-1 accuracy and top-5 accuracy from $78.28\%/94.36\%$ to $79.04\%/94.45\%$ when we use an external dataset with 1.3M unlabeled examples.

Our contributions, which will be presented in the rest of the paper, are as follows:

- First, we propose a training technique called TSA that effectively prevents overfitting when much more unsupervised data is available than supervised data.
- Second, we show that targeted data augmentation methods (such as AutoAugment) give a significant improvements over other untargeted augmentations.
- Third, we combine a set of data augmentations for NLPs, and show that our method works well there.
- Fourth, our paper show significant leaps in performance compared to previous methods in a range of vision and language tasks.
- Finally, we develop a method so that UDA can be applied even the class distributions of labeled and unlabeled data mismatch.

2 Unsupervised Data Augmentation (UDA)

In this section, we first formulate our task and then present the proposed method, UDA. Throughout this paper, we focus on classification problems and will use x to denote the input and $y(x)$ or simply y^* to denote its ground-truth prediction target. We are interested in learning a model $p_\theta(y \mid x)$ to predict y^* based on the input x, where θ denotes the model parameters. Finally, we will use L and U to denote the sets of labeled and unlabeled examples respectively.

2.1 Background: Supervised Data Augmentation

Data augmentation aims at creating novel and realistic-looking training data by applying a transformation to the input of an example, without changing the label / nature of the example.

Formally, let $q(\hat{x} \mid x)$ be the augmentation transformation from which one can draw augmented examples $\hat{x}$ based on an original example x. For an augmentation transformation to be valid, it is required that any example $\hat{x} \sim q(\hat{x} \mid x)$ drawn from the distribution shares the same ground-truth label as x, i.e., $y(\hat{x}) = y(x)$. Given a valid augmentation transformation, we can simply use the following objective to minimize the negative log-likelihood on augmented examples:

$$\min_\theta \mathcal{J}_{\text{da}}(\theta) = \mathop{\mathbb{E}}_{x,y^* \in L} \mathop{\mathbb{E}}_{\hat{x} \sim q(\hat{x}|x)} \left[-\log p_\theta(y^* \mid \hat{x}) \right]. \tag{1}$$

This objective can be equivalently seen as constructing an augmented labeled set from the original supervised set and then training the model on the augmented set. Therefore, the augmented set needs to provide additional supervised training signals / inductive biases to be more effective. How to design the augmentation transformation has thus become critical.

In recent years, there have been significant advancements on the design of data augmentations for NLP, vision and speech in supervised learning settings. For example, in question answering, QANet [Yu et al., 2018] employs a pair of machine translation systems to paraphrase a sentence. Employing the back-translation based augmentation has led to significant performance improvements [Yu et al., 2018]. For image classification, Cubuk et al. [2018] uses reinforcement learning to search for an "optimal" combination of image augmentation operations directly based on the validation performances, outperforming any manually designed augmentation procedure by a clear margin. Data augmentation has also been shown to work well on speech [Hannun et al., 2014, Park et al., 2019].

Despite the promising results, data augmentation is mostly regarded as the "cherry on the cake" which provides a steady but limited performance boost because these augmentations has so far only been applied to a set of labeled examples which is usually small. Motivated by this limitation, we develop UDA to apply effective data augmentations to unlabeled data, which is often in larger quantities.

2.2 Unsupervised Data Augmentation

As discussed in the introduction, a recent line of work in semi-supervised learning has been utilizing unlabeled examples to enforce smoothness of the model. The general form of these works can be summarized as follows:

- Given an input x, compute the output distribution $p_\theta(y \mid x)$ given x and a perturbed version $p_\theta(y \mid x, \epsilon)$ by injecting a small noise ϵ. The noise can be applied to x or hidden states or be used to change the computation process.
- Minimize some divergence between the two predicted distributions $\mathcal{D}\left(p_\theta(y \mid x) \| p_\theta(y \mid x, \epsilon)\right)$.

This procedure enforces the model to be insensitive to the perturbation ϵ and hence smoother with respect to changes in the input (or hidden) space.

In this work, we present a simple twist to the existing smoothness enforcing works and extend prior works on using data augmentation as perturbations [Sajjadi et al., 2016, Laine and Aila, 2016]. We propose to use state-of-the-art data augmentation targeted at different tasks as a particular form of perturbation and optimize the same smoothness enforcing objective on unlabeled examples. Specifically, following VAT [Miyato et al., 2018], we choose to minimize the KL divergence between the predicted distributions on an unlabeled example and an augmented unlabeled example:

$$\min_\theta \ \mathcal{J}_{\text{UDA}}(\theta) = \mathop{\mathbb{E}}_{x \in U} \mathop{\mathbb{E}}_{\hat{x} \sim q(\hat{x}|x)} \left[\mathcal{D}_{\text{KL}}\left(p_{\tilde{\theta}}(y \mid x) \| p_\theta(y \mid \hat{x}))\right)\right], \tag{2}$$

where $q(\hat{x} \mid x)$ is a data augmentation transformation and $\tilde{\theta}$ is a *fixed* copy of the current parameters θ indicating that the gradient is not propagated through $\tilde{\theta}$ as suggested by Miyato et al. [2018]. The data augmentation transformation used here is the same as the augmentations used in the supervised data augmentation such as back translation for texts and random cropping for images.

To use both labeled examples and unlabeled examples, we add the cross entropy loss on labeled examples and the unsupervised objective defined in Equation 2 with a weighting factor as our training objective, which is illustrated in Figure 1.

When compared to conventional perturbations such as Gaussian noise, dropout noise or affine transformations, we believe that data augmentations targeted at each task can serve as a more effective source of "noise". Specifically, using targeted data augmentation as the perturbation function has several advantages:

- **Valid / realistic perturbations**: In supervised data augmentation, state-of-the-art augmentation methods have the advantage of generating realistic augmented examples that share the same ground-truth labels with the original examples. When applied to unlabeled examples, the ground-truth labels of the augmented examples also remain the same as those of the original examples. Hence, it is safe to encourage the smoothness / consistency between predictions on the original unlabeled example and the augmented unlabeled example. In comparison, if the perturbation is generated by adding a large Gaussian noise to the input example, the input image might become indiscernible or the correct label of the augmented example might be different from that of the original example.

- **Diverse perturbations**: Data augmentation can generate a diverse set of samples since it can make large modifications to the input example without changing its label, while the perturbations such as Gaussian or Bernoulli noise only make local changes to the input example. Hence, encouraging
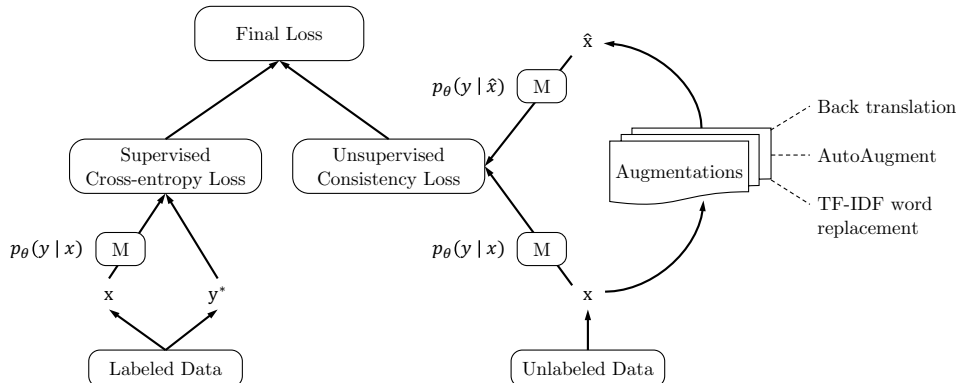
Figure 1: Training objective for UDA, where M is a model that predicts distribution $p_\theta(y \mid x)$ given x, and y^* is the ground-truth label.

smoothness / consistency between the original example and a diverse set of augmented examples can significantly improve the sample efficiency.

- **Targeted inductive biases**: As shown in AutoAugment [Cubuk et al., 2018], data augmentation policy can be directly optimized towards improving validation performance on each task. Such performance-oriented augmentation policy can learn to figure out the missing or most wanted training signal / inductive biases in an original labeled set. For example, it is shown that the best augmentation policies on CIFAR-10 mostly involve color-based transformations such as adjusting brightness, while on SVHN, the best augmentations involve geometric transformations such as shearing. In comparison, the perturbations in prior works on enforcing smoothness are fixed for different tasks and cannot provide targeted training signals / inductive biases. Note that the policies found by AutoAugment are optimized to improve model's performance in a supervised setting. We find that, in our semi-supervised setting, those policies also work well.

2.3 Augmentation Strategies for Different Tasks

As discussed in Section 2.1, data augmentation can be tailored to provide missing training signals specific to each task. We apply three kinds of augmentation strategies to different tasks in our experiments:

AutoAugment for Image Classification. We use the augmentation policies found, and open-sourced by AutoAugment for experiments on CIFAR-10, SVHN and ImageNet.[1] We also use Cutout [DeVries and Taylor, 2017] for CIFAR-10 and SVHN since it can be composed with AutoAugment to achieve improved performance in the supervised setting [Cubuk et al., 2018]. The augmentation policies inject task-specific inductive biases based on the invariance property of the task at hand.

Back translation for Text Classification. For sentiment classification datasets including IMDb, Yelp-2, Yelp-5, Amazon-2 and Amazon-5, we employ a back translation system [Sennrich et al., 2015, Yu et al., 2018] to paraphrase the training data. We train English-to-French and French-to-English translation models using the WMT 14 corpus. Similar to Edunov et al. [2018], we use random sampling to generate diverse translations and find it works well to set the Softmax temperature to 0.9 for decoding. Finally, since the parallel data in WMT 14 is for sentence-level translation while the

---

[1]https://github.com/tensorflow/models/tree/master/research/autoaugment

input examples in sentiment classification corpora are paragraphs, we perform back translation to each sentence instead of the whole paragraph.

TF-IDF based word replacing for Text Classification. While back translation is very good at maintaining a global semantics of the original sentence, there is no guarantee that it will keep certain words. However, some keywords are more informative than other words in determining the category, on DBPedia where the task is to predict the category of a Wikipedia page. Hence, we propose a new augmentation method called TF-IDF based word replacing that keeps those keywords while replacing other words.

Specifically, we get the IDF score for each word using the DBPedia training corpus and compute the TF-IDF score for each word in an example. Then we replace each word in the training example randomly based on its TF-IDF score. We set a high probability for replacing words with low TF-IDF scores and set a low probability for replacing words with high TF-IDF scores.

2.4 Training Signal Annealing

Since it is much easier to obtain unlabeled data than labeled data, in practice, we often encounter a situation where there is a large gap between the amount of unlabeled data and that of labeled data. To enable UDA to take advantage of as much unlabeled data as possible, we usually need a large enough model, but a large model can easily overfit the supervised data of a very limited size. To tackle this difficulty, we introduce a new training technique called Training Signal Annealing (TSA).

The main intuition behind TSA is to gradually release the training signals of the supervised examples as the model is trained on more and more unsupervised examples. Specifically, for each training step t, we set a threshold $\eta_t \leq 1$. When the probability of the correct category $p_\theta(y^* \mid x)$ of a labeled example is higher than the threshold η_t, we remove this example from the loss function and only train on other labeled examples in the minibatch. Formally, given a minibatch of labeled examples B, we replace the supervised objective with the following objective:

$$\min_\theta \frac{1}{Z} \sum_{x,y \in B} \left[-\log p_\theta(y \mid x) \, I(p_\theta(y \mid x) < \eta_t) \right], \tag{3}$$

where $I(\cdot)$ is the indicator function and $Z = \sum_{x,y \in B} I(p_\theta(y \mid x) < \eta_t)$ is simply a re-normalization factor. Effectively, the threshold η_t serves as a ceiling to prevent the model from over-training on examples that the model are already confident about.

Hence, when we gradually anneal η_t from $\frac{1}{k}$ to 1 during training with k being the number of categories, the model can only slowly receive supervisions from the labeled examples, largely alleviating the overfitting problem. To account for different ratios of unlabeled data and labeled data, we consider three particular schedules of η_t shown in Figure 2.
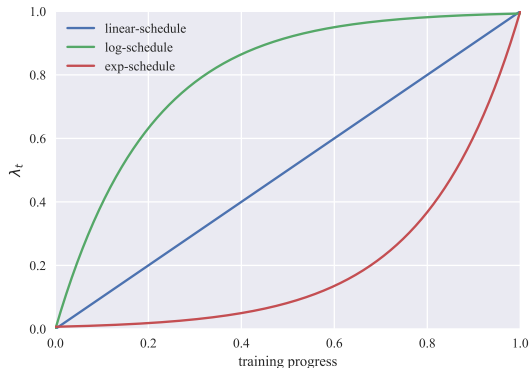

Figure 2: Three different schedules of TSA where λ_t is increased from 0 to 1. We simply set $\eta_t = \frac{1}{k} + \lambda_t * (1 - \frac{1}{k})$ so that η_t goes from $\frac{1}{k}$ to 1.

- **log-schedule** — the threshold n_t is increased most rapidly at the beginning of the training;
- **linear-schedule** — n_t is increased linearly as training progresses;

5

- **exp-schedule** — n_t is increased most rapidly at the end of the training.

Intuitively, for the case where the problem is relatively easy or the number of labeled examples is very limited, and the model can overfit very quickly, the exp-schedule is the most suitable one as the supervised signal is mostly released at the end of training. Following a similar logic, when the model is less likely to overfit (e.g., when we have abundant labeled examples), the log-schedule can serve well. We refer readers to Appendix A for a more detailed formulation of these schedules.

3 Experiments

We apply UDA to a variety of language tasks and vision tasks. Specifically, we show experiments on six text classification tasks in Section 3.1. Then, in Section 3.2, we compare UDA with other semi-supervised learning methods on standard vision benchmarks, CIFAR-10 and SVHN. Lastly, we evaluate UDA on ImageNet in Section 3.3 and provide ablation studies for TSA and augmentation methods in Section 3.4. Due to the space limit, we only present the information necessary to compare the empirical results at this moment and refer readers to the code for implementation details.[2]

3.1 Text Classification Experiments

Datasets. We conduct experiments on six language datasets including IMDb, Yelp-2, Yelp-5, Amazon-2, Amazon-5 and DBPedia [Maas et al., 2011, Zhang et al., 2015], where DBPedia contains Wikipedia pages for category classifications and all other datasets are about sentiment classifications on different domains. In our semi-supervised setting, we set the number of supervised examples to 20 for binary sentiment classification tasks including IMDb, Yelp-2 and Amazon-2. For the five-way classification datasets Yelp-5 and Amazon-5, we use 2,500 examples (i.e., 500 examples per class). Finally, although DBPedia has 14 categories, the problem is relatively simpler. Hence, we set the number of training examples to 140 (i.e., 10 examples per class). For unlabeled data, we use the whole training set for DBPedia and the concatenation of the training set and the unlabeled set for IMDb. We obtain large datasets of Yelp reviews and Amazon reviews [McAuley et al., 2015] as the unlabeled data for Yelp-2 Yelp-5, Amazon-2 and Amazon-5.[3]

Experiment settings. We adopt the Transformer model [Vaswani et al., 2017] used in BERT [Devlin et al., 2018] as our baseline model due to its great performances on many tasks. Then, we consider four initialization schemes. Specifically, we initialize our models either with (a) random Transformer, (b) BERT base, (c) BERT large or (d) BERT large fine-tuned on in-domain unlabeled data. The latter finetuning strategy is motivated by the fact that ELMo [Peters et al., 2018] and ULMFiT [Howard and Ruder, 2018] show that fine-tuning language models on domain specific data can lead to performance improvements. In all these four settings, we compare the performance with and without UDA.

We truncate the input to 512 subwords since BERT is pretrained with a maximum sequence length of 512. We increase the dropout rate on the attention and the hidden states to 0.2, when we use a random initialization. All experiments are performed on a v3-32 Cloud TPU v2 Pod.

Results. The results for text classification are shown in Table 1 with three key observations.

- Firstly, UDA consistently improves the performance regardless of the model initialization scheme. Most notably, even when BERT is further finetuned on in-domain data, UDA can still significantly reduce the error rate from 6.50% to 4.20% on IMDb. This result shows that the benefit UDA provides is complementary to that of unsupervised representation learning and they can be combined to produce the best empirical results.
- Secondly, with a significantly smaller amount of supervised examples, UDA can offer decent or even competitive performances compared to the SOTA model trained with full supervised data. In particular, on binary sentiment classification tasks, with only 20 supervised examples, UDA outperforms the previous SOTA trained on full supervised data on IMDb and gets very close on Yelp-2 and Amazon-2.

---

[2]Code will be released.

[3]https://www.kaggle.com/yelp-dataset/yelp-dataset, http://jmcauley.ucsd.edu/data/amazon/

6

Fully supervised baseline						
Datasets (# Sup examples)	IMDb (25k)	Yelp-2 (560k)	Yelp-5 (650k)	Amazon-2 (3.6m)	Amazon-5 (3m)	DBpedia (560k)
Pre-BERT SOTA	*4.32*	2.16	29.98	3.32	34.81	0.70
BERT$_{LARGE}$	4.51	*1.89*	*29.32*	*2.63*	*34.17*	*0.64*

Semi-supervised setting							
Initialization	**UDA**	IMDb (20)	Yelp-2 (20)	Yelp-5 (2.5k)	Amazon-2 (20)	Amazon-5 (2.5k)	DBpedia (140)
Random	✗	43.27	40.25	50.80	45.39	55.70	41.14
	✓	25.23	8.33	41.35	16.16	44.19	7.24
BERT$_{BASE}$	✗	27.56	13.60	41.00	26.75	44.09	2.58
	✓	5.45	2.61	33.80	3.96	38.40	1.33
BERT$_{LARGE}$	✗	11.72	10.55	38.90	15.54	42.30	1.68
	✓	4.78	2.50	33.54	3.93	37.80	1.09
BERT$_{FINETUNE}$	✗	6.50	2.94	32.39	12.17	37.32	-
	✓	**4.20**	**2.05**	**32.08**	**3.50**	**37.12**	-

Table 1: Error rates on text classification datasets. BERT$_{FINETUNE}$ denotes BERT$_{LARGE}$ fine-tuned on in-domain unlabeled data. We do not pursue further experiments for BERT$_{FINETUNE}$ on DBPedia since fine-tuning BERT on DBPedia does not result in better performance than BERT$_{LARGE}$ in our preliminary experiments. This is probably due to the fact that DBPedia is on the Wikipedia domain and BERT is already trained on the whole Wikipedia corpus. In the fully supervised settings, the pre-BERT SOTAs include ULMFiT [Howard and Ruder, 2018] for Yelp-2 and Yelp-5, DPCNN [Johnson and Zhang, 2017] for Amazon-2 and Amazon-5, Mixed VAT [Sachan et al., 2018] for IMDb and DBPedia.

- Finally, we also note that five-category sentiment classification tasks turn out to be much more difficult than their binary counterparts and there still exists a clear gap between UDA with 500 labeled examples per class and BERT trained on the entire supervised set. This suggests a room for further improvement in the future.

3.2 Comparison with semi-supervised learning methods

Experiment settings. Following the standard semi-supervised learning setting, we compare UDA with prior works on CIFAR-10 [Krizhevsky and Hinton, 2009] and SVHN [Netzer et al., 2011]. Oliver et al. [2018] provided evaluation results of prior works with the same architecture and evaluation scheme, hence we follow their settings and employ Wide Residual Networks [Zagoruyko and Komodakis, 2016] with depth 28 and width 2 as our baseline model. To strictly enforce that UDA does not use extra supervised data, we use the same examples which AutoAugment finds its optimal policy on, since AutoAugment finds the optimal policies also using 4,000 supervised examples in CIFAR-10 and 1,000 supervised examples in SVHN. For hyperparameter tuning, we follow Oliver et al. [2018] and only tune the learning rate and hyperparameters for our unsupervised objective. Since there are many more unlabeled examples than labeled examples, we use a larger batch size for the unsupervised objective. For example, in our CIFAR-10 experiments, we use a batch size of 32 for the supervised loss and use a batch size of 960 for the unsupervised loss. We report the average performance and the standard deviation for ten runs.

We compare UDA with Pseudo-Label [Lee, 2013], an algorithm based on self-training, Virtual adversarial training (VAT) [Miyato et al., 2018], an algorithm that generates adversarial Gaussian noise perturbations on input, Π-Model [Laine and Aila, 2016], which combines simple input augmentation with hidden state perturbations, Mean Teacher [Tarvainen and Valpola, 2017], which enforces model parameter smoothness, ICT [Verma et al., 2019] and mixmixup [Hataya and Nakayama, 2019] which enforce interpolation smoothness similar to mixup [Zhang et al., 2017] and LGA + VAT [Jackson and Schulman, 2019], an algorithm based on gradient similarity.

Datasets	CIFAR-10 (4k)	SVHN (1k)
Supervised	$20.26 \pm .38$	$12.83 \pm .47$
AutoAugment*	14.1	8.2
Pseudo-Label	$17.78 \pm .57$	$7.62 \pm .29$
Π-Model	$16.37 \pm .63$	$7.19 \pm .27$
Mean Teacher	$15.87 \pm .28$	$5.65 \pm .47$
VAT	$13.86 \pm .27$	$5.63 \pm .20$
VAT + EntMin	$13.13 \pm .39$	$5.35 \pm .19$
LGA + VAT	$12.06 \pm .19$	$6.58 \pm .36$
mixmixup	10	-
ICT	$7.66 \pm .17$	$3.53 \pm .07$
UDA	$\mathbf{5.27 \pm .11}$	$\mathbf{2.46 \pm .17}$

Table 2: Comparison with existing methods on CIFAR-10 and SVHN with $4,000$ and $1,000$ examples respectively. All compared methods use a common architecture WRN-28-2 with 1.4M parameters except AutoAugment* which uses a larger architecture WRN-28-10. The results for Pseudo-Label [Lee, 2013], Π-Model [Laine and Aila, 2016], Mean Teacher [Tarvainen and Valpola, 2017] and VAT (VAT) [Miyato et al., 2018] are reproduced by Oliver et al. [2018]. We also compare with recently proposed models ICT [Verma et al., 2019], LGA+VAT [Jackson and Schulman, 2019] and mixmixup [Hataya and Nakayama, 2019].

Results. The results are shown in Table 2. When compared with the previous SOTA model ICT [Verma et al., 2019], UDA reduces the error rate from 7.66% to 5.27% on CIFAR-10 and from 3.53% to 2.46% on SVHN, marking a relative reduction of 31.2% and 30.3%, respectively. Note that the difference of UDA and VAT is essentially the perturbation process. While the perturbations produced by VAT often contain high-frequency artifacts that do not exist in real images, data augmentation in UDA mostly generates diverse and realistic examples. Hence, the performance difference between UDA and VAT shows the superiority of data augmentation based perturbation, echoing our discussion in Section 2.2.

In addition, it is worth mentioning that though not used in this work, more advanced architectures such as PyramidNet+ShakeDrop could further boost the SOTA performance. But for fair comparison with the existing methods, we only consider WRN-28-2 here. The results in AutoAugment [Cubuk et al., 2018] are not comparable here also due to using a more advanced architecture.

3.3 ImageNet experiments

In previous sections, all datasets we consider have a relatively small number of training examples and classes. In addition, we only use in-domain unlabeled data in previous experiments, where the class distribution of the unlabeled data always match with that of labeled data. In order to further test whether UDA can still excel on larger and more challenging datasets, we conduct experiments on ImageNet [Deng et al., 2009] with about 1.28M images from 1,000 target classes. We also develop a method to apply UDA on out-of-domain unlabeled data, which leads to performance improvements when we use the whole ImageNet as the supervised data.

Experiment settings. While ImageNet is much more challenging than datasets considered earlier, the number of labeled examples in ImageNet is also substantially larger. Therefore, to provide a more informative evaluation, we conduct experiments on two settings with different numbers of supervised examples: (a) We use ImageNet-10% which keeps roughly 10% of the supervised data while using all other ImageNet data as unlabeled data, (b) Secondly, we consider the fully supervised scenario where we keep all images in ImageNet as supervised data and obtain extra unlabeled data from the JFT dataset [Hinton et al., 2015, Chollet, 2017]. We employ ResNet-50 [He et al., 2016b] as our baseline model.

Using out-of-domain unlabeled data. Ideally, we would like to make use of out-of-domain unlabeled data since it is usually much easier to collect a large amount of out-of-domain unlabeled data, but the class distributions of out-of-domain data are usually mismatched with those of in-domain

data. Due to the mismatched class distributions, using out-of-domain unlabeled data can hurt the performance than not using it [Oliver et al., 2018].

To obtain images relevant to the ImageNet domain, we use our baseline model ResNet-50 trained on ImageNet to infer the labels of images in the JFT dataset and pick out 1.3M images (equally distributed among classes) that the model is most confident about. Specifically, for each category, we sort all images based on the classified probabilities of being in that category and select the top $1,300$ images with the highest probabilities.

Additional training techniques. Due to the large number of categories involved in ImageNet, we observe that the predicted distributions on unlabeled examples and augmented unlabeled examples, i.e., $p_{\tilde{\theta}}(y \mid x)$ and $p_{\theta}(y \mid \hat{x})$, tend to be over-flat across categories, especially in the ImageNet-10% setting where there are limited training examples. Consequently, the unsupervised training signal from the KL divergence is relatively weak and thus gets dominated by the supervised part. Therefore, we find it helpful to sharpen the predicted distribution produced on unlabeled examples. Specifically, we employ the following three techniques:

- **Entropy minimization**: We add an entropy term to the overall objective and regularize the predicted distribution on augmented examples $p_{\theta}(y \mid \hat{x})$ to have a low entropy.

- **Softmax temperature control**: We also employ a straightforward solution that controls the temperature of Softmax when computing the prediction on the original example $p_{\tilde{\theta}(y|x)}$. Specifically, $p_{\tilde{\theta}(y|x)}$ is computed as $\mathrm{Softmax}(l(x)/\tau)$ where $l(x)$ denotes the logits and τ is the temperature. A lower temperature corresponds to a sharper distribution.

- **Confidence-based masking**: We also find it to be helpful to mask out examples that the current model is not confident about. Specifically, in each minibatch, the unsupervised loss term is computed only on examples whose highest probability $\max_y p_{\tilde{\theta}(y|x)}$ is greater than a threshold.

Results. As shown in Table 3, for the 10% supervised data setting, UDA improves the top-1 and top-5 accuracy from 55.09% to 68.66% and from 77.26% to 88.52% respectively. As for the setting using the entire ImageNet as supervised data shown in Table 4, when compared with AutoAugment, UDA improves the baseline top-1 accuracy from 78.28% to 79.04% and improves the top-5 accuracy from 94.36% to 94.45%, with only 1.3M more unlabeled data. We expect that there will be further improvements with more unlabeled data, which we leave as future works.

Model	top-1 / top-5 accuracy
ResNet-50	55.09 / 77.26
UDA	**68.66 / 88.52**

Table 3: Accuracy on ImageNet-10% with image size 224. We use the training set of the ImageNet dataset as the unlabeled data.

Model	top-1 / top-5 accuracy
ResNet-50	77.28 / 93.73
AutoAugment	78.28 / 94.36
UDA	**79.04 / 94.45**

Table 4: Accuracy on ImageNet with image size 331. We use the ImageNet dataset and another 1.3M unlabeled images from the JFT dataset as the unlabeld data.

3.4   Ablation studies

Finally, we provide analysis of when and how to use TSA and effects of different augmentation methods for researchers and practitioners.

Ablations on Training Signal Annealing (TSA). We study the effect of TSA on two tasks with different amounts of unlabeled data: (a) Yelp-5: on this text classification task, we have about 6M unlabeled examples while only having 2.5k supervised examples. We do not initialize the network by BERT in this study to rule out factors of having a pre-trained representation, (b) CIFAR-10: we have 50k unlabeled examples while having 4k labeled examples.

The comparison is shown in Table 5. As can be seen from the table, on Yelp-5, where there is a lot more unlabeled data than supervised data, TSA reduces the error rate from 50.81% to 41.35%

when compared to the baseline without TSA. More specifically, the best performance is achieved when we choose to postpone releasing the supervised training signal to the end of the training, i.e, exp-schedule leads to the best performance.

On the other hand, linear-schedule is the sweet spot on CIFAR-10 in terms of the speed of releasing supervised training signals, where the amount of unlabeled data is not a lot larger than that of supervised data.

Ablations on Augmentation methods. Targeted augmentation methods such as AutoAugment have been shown to lead to significant performance improvements in supervised learning. In this study, we would like to first study whether targeted augmentations are also effective when applied to unlabeled data and whether improvements of augmentations in supervised learning can lead to improvements in our semi-supervised learning setting.

Firstly, as shown in Table 6, if we apply the augmentation policy found on SVHN by AutoAugment to CIFAR-10 (denoted by Switched Augment), the error rate increases from 5.10 to 5.59, which demonstrate the effectiveness of targeted data augmentations. Further, if we remove AutoAugment and only use Cutout, the error rate increases to 6.42. Finally, the error rate increases to 16.17 if we only use simple cropping and flipping as the augmentation. On SVHN, the effects of different augmentations are similar. These results show the importance of applying augmentation methods targeted at each task to inject the most needed inductive biases.

We also observe that the effectiveness of augmentation methods on supervised learning settings transfers to our semi-supervised settings. Specifically, in the fully supervised learning settings, Cubuk et al. [2018] also show that AutoAugment improves upon Cutout and that Cutout is more effectively than basic augmentations, which aligns well with the observations in semi-supervised settings. In our preliminary experiments for sentiment classifications, we have also found that, both in supervised learning settings and unsupervised learning settings, back-translation works better than simple word dropping or word replacing.

TSA schedule	Yelp-5	CIFAR-10
✗	50.81	5.67
log-schedule	49.06	5.41
linear-schedule	45.41	**5.10**
exp-schedule	**41.35**	7.25

Table 5: Ablation study for Training Signal Annealing (TSA) on Yelp-5 and CIFAR-10. The shown numbers are error rates.

Augmentation	CIFAR-10	SVHN
Cropping & Flipping	16.17	8.27
Cutout	6.42	3.09
Switched Augment	5.59	2.74
AutoAugment	**5.10**	**2.22**

Table 6: Ablation study for data augmentation methods. Switched Augment means to apply the policy found by AutoAumgent on SVHN to CIFAR-10 and vice versa.

4   Related Work

Due to the long history of semi-supervised learning (SSL), we refer readers to [Chapelle et al., 2009] for a general review. More recently, many efforts have been made to renovate classic ideas into deep neural instantiations. For example, graph-based label propagation [Zhu et al., 2003] has been extended to neural methods via graph embeddings [Weston et al., 2012, Yang et al., 2016] and later graph convolutions [Kipf and Welling, 2016]. Similarly, with the variational auto-encoding framework and reinforce algorithm, classic graphical models based SSL methods with target variable being latent can also take advantage of deep architectures [Kingma et al., 2014, Maaløe et al., 2016, Yang et al., 2017]. Besides the direct extensions, it was found that training neural classifiers to classify out-of-domain examples into an additional class [Salimans et al., 2016] works very well in practice. Later, Dai et al. [2017] shows that this can be seen as an instantiation of low-density separation.

Most related to our method is a line of work that enforces classifiers to be smooth with respect to perturbations applied to the input examples or hidden representations. As explained earlier, works in this family mostly differ in how the perturbation is defined: Pseudo-ensemble [Bachman et al., 2014] directly applies Gaussian noise; Π-Model [Laine and Aila, 2016] combines simple input augmentation with hidden state noise; VAT [Miyato et al., 2018, 2016] defines the perturbation by approximating the

direction of change in the input space that the model is most sensitive to; Cross-view training [Clark et al., 2018] masks out part of the input data; Sajjadi et al. [2016] combines dropout and random max-pooling with affine transformation applied to the data as the perturbations. In comparison, we propose to utilize state-of-the-art data augmentations to produce diverse and realistic perturbed examples that lead to better performance and higher data efficiency.

Also related to our work is the field of data augmentation research. Besides the conventional approaches and two data augmentation ideas mentioned in Section 2.1, back translation [Sennrich et al., 2015, Edunov et al., 2018] and dual learning [He et al., 2016a, Cheng et al., 2016] can be regarded as performing data augmentation on monolingual data and have also been shown to improve the performance on machine translation. Moreover, a recent approach MixUp [Zhang et al., 2017] goes beyond data augmentation from a single data point and performs interpolation of data pairs to achieve augmentation.

Apart from semi-supervised learning, unsupervised representation learning offers another way to utilize unsupervised data. Collobert and Weston [2008] demonstrated that word embeddings learned by language modeling can improve the performance significantly on semantic role labeling. Later, the pre-training of word embeddings was simplified and substantially scaled in Word2Vec [Mikolov et al., 2013] and Glove [Pennington et al., 2014]. More recently, Dai and Le [2015], Radford et al. [2018], Peters et al. [2018], Howard and Ruder [2018], Devlin et al. [2018] have shown that pre-training using language modeling and denoising auto-encoding leads to significant improvements on many tasks in the language domain. In Section 3.1, we show that the proposed method and unsupervised representation learning can complement each other and jointly yield the state-of-the-art results.

5 Conclusion

In this paper, we show that data augmentation and semi-supervised learning are well connected: better data augmentation can lead to significantly better semi-supervised learning. Our method, UDA, employs highly targeted data augmentations to generate diverse and realistic perturbations and enforces the model to be smooth with respect to these perturbations. We also propose a technique called TSA that can effectively prevent UDA from overfitting the supervised data, when a lot more unlabeled data is available. For text, UDA is very effective in low-data regime where state-of-the-art performance is achieved on IMDb with only 20 examples. For vision, UDA reduces error rates by more than 30% in heavily-benchmarked semi-supervised learning setups. Lastly, UDA can effectively leverage out-of-domain unlabeled data and achieve improved performances on ImageNet where we have a large amount of supervised data.

Acknowledgements

References

Philip Bachman, Ouais Alsharif, and Doina Precup. Learning with pseudo-ensembles. In *Advances in Neural Information Processing Systems*, pages 3365–3373, 2014.

Olivier Chapelle, Bernhard Scholkopf, and Alexander Zien. Semi-supervised learning (chapelle, o. et al., eds.; 2006)[book reviews]. *IEEE Transactions on Neural Networks*, 20(3):542–542, 2009.

Yong Cheng, Wei Xu, Zhongjun He, Wei He, Hua Wu, Maosong Sun, and Yang Liu. Semi-supervised learning for neural machine translation. *arXiv preprint arXiv:1606.04596*, 2016.

François Chollet. Xception: Deep learning with depthwise separable convolutions. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1251–1258, 2017.

Kevin Clark, Minh-Thang Luong, Christopher D Manning, and Quoc V Le. Semi-supervised sequence modeling with cross-view training. *arXiv preprint arXiv:1809.08370*, 2018.

Ronan Collobert and Jason Weston. A unified architecture for natural language processing: Deep neural networks with multitask learning. In *Proceedings of the 25th international conference on Machine learning*, pages 160–167. ACM, 2008.

Ekin D Cubuk, Barret Zoph, Dandelion Mane, Vijay Vasudevan, and Quoc V Le. Autoaugment: Learning augmentation policies from data. *arXiv preprint arXiv:1805.09501*, 2018.

Andrew M Dai and Quoc V Le. Semi-supervised sequence learning. In *Advances in neural information processing systems*, pages 3079–3087, 2015.

Zihang Dai, Zhilin Yang, Fan Yang, William W Cohen, and Ruslan R Salakhutdinov. Good semi-supervised learning that requires a bad gan. In *Advances in Neural Information Processing Systems*, pages 6510–6520, 2017.

Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. Imagenet: A large-scale hierarchical image database. In *2009 IEEE conference on computer vision and pattern recognition*, pages 248–255. Ieee, 2009.

Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv preprint arXiv:1810.04805*, 2018.

Terrance DeVries and Graham W Taylor. Improved regularization of convolutional neural networks with cutout. *arXiv preprint arXiv:1708.04552*, 2017.

Sergey Edunov, Myle Ott, Michael Auli, and David Grangier. Understanding back-translation at scale. *arXiv preprint arXiv:1808.09381*, 2018.

Awni Hannun, Carl Case, Jared Casper, Bryan Catanzaro, Greg Diamos, Erich Elsen, Ryan Prenger, Sanjeev Satheesh, Shubho Sengupta, Adam Coates, et al. Deep speech: Scaling up end-to-end speech recognition. *arXiv preprint arXiv:1412.5567*, 2014.

Ryuichiro Hataya and Hideki Nakayama. Unifying semi-supervised and robust learning by mixup. *ICLR The 2nd Learning from Limited Labeled Data (LLD) Workshop*, 2019.

Di He, Yingce Xia, Tao Qin, Liwei Wang, Nenghai Yu, Tie-Yan Liu, and Wei-Ying Ma. Dual learning for machine translation. In *Advances in Neural Information Processing Systems*, pages 820–828, 2016a.

Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778, 2016b.

Geoffrey Hinton, Oriol Vinyals, and Jeff Dean. Distilling the knowledge in a neural network. *arXiv preprint arXiv:1503.02531*, 2015.

Jeremy Howard and Sebastian Ruder. Universal language model fine-tuning for text classification. In *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, volume 1, pages 328–339, 2018.

Jacob Jackson and John Schulman. Semi-supervised learning by label gradient alignment. *arXiv preprint arXiv:1902.02336*, 2019.

Rie Johnson and Tong Zhang. Deep pyramid convolutional neural networks for text categorization. In *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, volume 1, pages 562–570, 2017.

Durk P Kingma, Shakir Mohamed, Danilo Jimenez Rezende, and Max Welling. Semi-supervised learning with deep generative models. In *Advances in neural information processing systems*, pages 3581–3589, 2014.

Thomas N Kipf and Max Welling. Semi-supervised classification with graph convolutional networks. *arXiv preprint arXiv:1609.02907*, 2016.

Alex Krizhevsky and Geoffrey Hinton. Learning multiple layers of features from tiny images. Technical report, Citeseer, 2009.

Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. In *Advances in neural information processing systems*, pages 1097–1105, 2012.

Samuli Laine and Timo Aila. Temporal ensembling for semi-supervised learning. *arXiv preprint arXiv:1610.02242*, 2016.

Dong-Hyun Lee. Pseudo-label: The simple and efficient semi-supervised learning method for deep neural networks. In *Workshop on Challenges in Representation Learning, ICML*, volume 3, page 2, 2013.

Lars Maaløe, Casper Kaae Sønderby, Søren Kaae Sønderby, and Ole Winther. Auxiliary deep generative models. *arXiv preprint arXiv:1602.05473*, 2016.

Andrew L Maas, Raymond E Daly, Peter T Pham, Dan Huang, Andrew Y Ng, and Christopher Potts. Learning word vectors for sentiment analysis. In *Proceedings of the 49th annual meeting of the association for computational linguistics: Human language technologies-volume 1*, pages 142–150. Association for Computational Linguistics, 2011.

Julian McAuley, Christopher Targett, Qinfeng Shi, and Anton Van Den Hengel. Image-based recommendations on styles and substitutes. In *Proceedings of the 38th International ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 43–52. ACM, 2015.

Tomas Mikolov, Ilya Sutskever, Kai Chen, Greg S Corrado, and Jeff Dean. Distributed representations of words and phrases and their compositionality. In *Advances in neural information processing systems*, pages 3111–3119, 2013.

Takeru Miyato, Andrew M Dai, and Ian Goodfellow. Adversarial training methods for semi-supervised text classification. *arXiv preprint arXiv:1605.07725*, 2016.

Takeru Miyato, Shin-ichi Maeda, Shin Ishii, and Masanori Koyama. Virtual adversarial training: a regularization method for supervised and semi-supervised learning. *IEEE transactions on pattern analysis and machine intelligence*, 2018.

Yuval Netzer, Tao Wang, Adam Coates, Alessandro Bissacco, Bo Wu, and Andrew Y Ng. Reading digits in natural images with unsupervised feature learning. 2011.

Avital Oliver, Augustus Odena, Colin A Raffel, Ekin Dogus Cubuk, and Ian Goodfellow. Realistic evaluation of deep semi-supervised learning algorithms. In *Advances in Neural Information Processing Systems*, pages 3235–3246, 2018.

Daniel S Park, William Chan, Yu Zhang, Chung-Cheng Chiu, Barret Zoph, Ekin D Cubuk, and Quoc V Le. Specaugment: A simple data augmentation method for automatic speech recognition. *arXiv preprint arXiv:1904.08779*, 2019.

Jeffrey Pennington, Richard Socher, and Christopher Manning. Glove: Global vectors for word representation. In *Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP)*, pages 1532–1543, 2014.

Matthew E Peters, Mark Neumann, Mohit Iyyer, Matt Gardner, Christopher Clark, Kenton Lee, and Luke Zettlemoyer. Deep contextualized word representations. *arXiv preprint arXiv:1802.05365*, 2018.

Alec Radford, Karthik Narasimhan, Tim Salimans, and Ilya Sutskever. Improving language understanding by generative pre-training. *URL https://s3-us-west-2. amazonaws. com/openai-assets/research-covers/languageunsupervised/language understanding paper. pdf*, 2018.

Devendra Singh Sachan, Manzil Zaheer, and Ruslan Salakhutdinov. Revisiting lstm networks for semi-supervised text classification via mixed objective function. 2018.

Mehdi Sajjadi, Mehran Javanmardi, and Tolga Tasdizen. Regularization with stochastic transformations and perturbations for deep semi-supervised learning. In *Advances in Neural Information Processing Systems*, pages 1163–1171, 2016.

Tim Salimans, Ian Goodfellow, Wojciech Zaremba, Vicki Cheung, Alec Radford, and Xi Chen. Improved techniques for training gans. In *Advances in neural information processing systems*, pages 2234–2242, 2016.

Rico Sennrich, Barry Haddow, and Alexandra Birch. Improving neural machine translation models with monolingual data. *arXiv preprint arXiv:1511.06709*, 2015.

Patrice Y Simard, Yann A LeCun, John S Denker, and Bernard Victorri. Transformation invariance in pattern recognition—tangent distance and tangent propagation. In *Neural networks: tricks of the trade*, pages 239–274. Springer, 1998.

Antti Tarvainen and Harri Valpola. Mean teachers are better role models: Weight-averaged consistency targets improve semi-supervised deep learning results. In *Advances in neural information processing systems*, pages 1195–1204, 2017.

Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. In *Advances in neural information processing systems*, pages 5998–6008, 2017.

Vikas Verma, Alex Lamb, Juho Kannala, Yoshua Bengio, and David Lopez-Paz. Interpolation consistency training for semi-supervised learning. *arXiv preprint arXiv:1903.03825*, 2019.

Jason Weston, Frédéric Ratle, Hossein Mobahi, and Ronan Collobert. Deep learning via semi-supervised embedding. In *Neural Networks: Tricks of the Trade*, pages 639–655. Springer, 2012.

Zhilin Yang, William W Cohen, and Ruslan Salakhutdinov. Revisiting semi-supervised learning with graph embeddings. *arXiv preprint arXiv:1603.08861*, 2016.

Zhilin Yang, Junjie Hu, Ruslan Salakhutdinov, and William W Cohen. Semi-supervised qa with generative domain-adaptive nets. *arXiv preprint arXiv:1702.02206*, 2017.

Adams Wei Yu, David Dohan, Minh-Thang Luong, Rui Zhao, Kai Chen, Mohammad Norouzi, and Quoc V Le. Qanet: Combining local convolution with global self-attention for reading comprehension. *arXiv preprint arXiv:1804.09541*, 2018.

Sergey Zagoruyko and Nikos Komodakis. Wide residual networks. *arXiv preprint arXiv:1605.07146*, 2016.

Hongyi Zhang, Moustapha Cisse, Yann N Dauphin, and David Lopez-Paz. mixup: Beyond empirical risk minimization. *arXiv preprint arXiv:1710.09412*, 2017.

Xiang Zhang, Junbo Zhao, and Yann LeCun. Character-level convolutional networks for text classification. In *Advances in neural information processing systems*, pages 649–657, 2015.

Xiaojin Zhu, Zoubin Ghahramani, and John D Lafferty. Semi-supervised learning using gaussian fields and harmonic functions. In *Proceedings of the 20th International conference on Machine learning (ICML-03)*, pages 912–919, 2003.

A Training Signal Annealing (TSA) Schedules

Suppose T is the total number of training steps and t is the current training step. Suppose k is the number of possible target categories. η_t is computed as follows for the three schedules:

- **log-schedule**: $\eta_t = (1 - \exp(-\frac{t}{T} * 5)) * (1 - \frac{1}{k}) + \frac{1}{k}$
- **linear-schedule**: $\eta_t = \frac{t}{T} * (1 - \frac{1}{k}) + \frac{1}{k}$
- **exp-schedule**: $\eta_t = \exp((\frac{t}{T} - 1) * 5) * (1 - \frac{1}{k}) + \frac{1}{k}$

The log-schedule does not use the log function, but the shape of the curve resembles log function.