Self-Supervised Wasserstein Pseudo-Labeling for Semi-Supervised Image Classification

Fariborz Taherkhani, Ali Dabouei, Sobhan Soleymani, Jeremy Dawson, Nasser M. Nasrabadi
West Virginia University
{ft0009, ad0046, ssoleyma} @ mix.wvu.edu, {jeremy.dawson, nasser.nasrabadi} @ mail.wvu.edu

Abstract

The goal is to use Wasserstein metric to provide pseudo labels for the unlabeled images to train a Convolutional Neural Networks (CNN) in a Semi-Supervised Learning (SSL) manner for the classification task. The basic premise in our method is that the discrepancy between two discrete empirical measures (e.g., clusters) which come from the same or similar distribution is expected to be less than the case where these measures come from completely two different distributions. In our proposed method, we first pre-train our CNN using a self-supervised learning method to make a cluster assumption on the unlabeled images. Next, inspired by the Wasserstein metric which considers the geometry of the metric space to provide a natural notion of similarity between discrete empirical measures, we leverage it to cluster the unlabeled images and then match the clusters to their similar class of labeled images to provide a pseudo label for the data within each cluster. We have evaluated and compared our method with state-of-the-art SSL methods on the standard datasets to demonstrate its effectiveness.

1. Introduction

CNN models have enabled breakthroughs in computer vision and machine learning. However, training a CNN model relies on a large-scale annotated datasets which are usually tedious and labor intensive to collect [38]. Considering the vast amounts of unlabeled data available on the web, the idea to use the unlabeled data without human effort to annotate them has become very appealing [77, 11]. In this work, we tackle the challenge of deep SSL, the task of which is to use the unlabeled data in conjunction with the labeled data to train a better CNN classifier. Conventionally, we are given a dataset $D = D_l \cup D_u$ where the data in $D_l$ are annotated by labels while the data in $D_u$ are not. The goal is to train a CNN classifier on the known categories in $D_l$ using the data in $D$. The test data involves only the classes that are present in $D_l$. The main challenge in SSL is to efficiently leverage the unlabeled $D_u$ to help learning on $D_l$. To make use of unlabeled data in the general setting of SSL challenge, there are two fundamental assumptions that must be taken into the consideration [11]: 1) We assume that labeled and unlabeled data come from the same or similar underlying distribution and there is no class distribution mismatch between the labeled and unlabeled sets. 2) We presume that the underlying distribution of data has some structure. SSL algorithms considers at least one of these structural assumptions: consistency, manifold and cluster.

In consistency assumption [5, 8, 9, 60, 66], data samples in a small neighbourhood have the same class label. In cluster assumption [53, 12, 75, 62], data tends to construct discrete clusters in some geometric sense, and data within the same cluster are more probably to have the same class label. In manifold assumption [49, 59, 70], data lie in the neighbourhood of a low-dimensional and well-defined manifold which can be classified by meaningful distances on the manifold. For all of these assumptions, it is important to consider the geometry of the data when designing an SSL method. For example, popular mean teacher [63] and π-model [39] leverage different data augmentations approaches, each of which uses a different strategy to explore the local geometry of the labeled data for generating new data.

Recently, the theory of Optimal Transport (OT) [57, 64] is used as a tool in machine learning algorithms to consider the geometry of the data. For example, the Wasserstein distance in OT uses the geometry of the metric space to provide a meaningful distance between two distributions even if the supports of these distributions do not overlap. This property of the Wasserstein distance has made it useful and practical for many computer vision and machine learning applications such as clustering [18, 37, 31, 46], generative models [4, 27], loss function [22], semi-supervised learning [61, 23, 69, 43, 62], and domain adaptation [16, 36, 58, 67, 19, 40].

In this work, we propose a new SSL method based on the Wasserstein metric which follows the general assumptions in SSL. Inspired by the effectiveness of Self-Supervised learning in many tasks including SSL [72, 35, 32], we first
pre-train our CNN using a self-supervised learning method, MoCo v2 [28, 13, 14]. This process potentially enforces a clustered structure in the feature space for the unlabeled data which motivates us to perform a clustering on the feature of unlabeled data and then infer a pseudo-label for them.

Specifically, using the self-supervised pre-training on the CNN, we make a cluster assumption about the unlabeled data in which clusters are identified by the Wasserstein barycenter of the unlabeled data. Then, we leverage the Wasserstein metric to match the clusters of unlabeled data to their most similar classes of labeled data to provide pseudo-labels for the unlabeled data. Here, the Wasserstein distance is a measure of similarity between two sets of data points where one of them contains labeled data while the other one consists of unlabeled data. This matching is based on the assumption that the labeled and unlabeled data within the same class have the same or similar distribution. Therefore, we would expect that the similarity between two sets of data which come from the same or similar distribution is more than the case where these sets of data come from completely two different distributions. Finally, depending on the matching, we infer a pseudo label for the unlabeled data within each cluster, which are used along with the initially labeled data to train our CNN classifier.

2. Related Work

2.1. Semi Supervised Learning for Deep Models

There are many SSL algorithms in the literature [78, 11, 52]. However, we briefly review the methods based on the pseudo-labeling and consistency regularization which have been incorporated with deep learning models.

**Pseudo-Labeling** was initially proposed in [41]. In SSL models based on the pseudo-labeling, the model usually relies on its own prior belief about the label of unlabeled data to obtain supplementary information over the course of training [41, 55, 21, 42, 34]. The main drawback of these methods is susceptibility to confirmation bias such that the model is confident about its incorrect prediction, and then overfits to incorrect pseudo-labels during the training [3]. Therefore, in these models, the incorrect pseudo-labels not only can not provide useful information during the training but also error of the model’s prediction is accumulated in the model and results in overfitting. This downside even gets worse in cases where the discrepancy between the domain of the unlabeled data is significant from that of labeled data.

**Consistency-based SSL models** perform based on the assumption that the model should be generally consistent with its predictions between a given data and its meaningfully-distorted versions [7]. This simple criterion on the models output has provided promising results in the SSL literature such as stochastic perturbations models [56], π-model [39], mean teacher [63], and virtual adversarial training (VAT) [47], Mixmatch [9], Remixmatch [8], and Fixmatch [60]. The primary idea in stochastic perturbations and π-model was initially proposed in [6] and is known as pseudo-ensembles. The pseudo-ensemble regularization techniques usually perform in such a way that under realistic perturbations of input $x: (x \sim x')$, the prediction of the model $g(x, \theta)$ should not vary drastically. This objective is achieved by considering a weighted loss term such as $d(g(x, \theta), g(x', \theta))$ during the training of model, where $d(., .)$ denotes MSE or KL divergence which calculates a distance or divergence between outputs of the prediction function. The main problem in pseudo-ensemble approaches, including π-model is that they highly depend on a likely unstable prediction, which can instantly deviate significantly over the course of training.

To solve this issue, two approaches including temporal ensembling [39] and mean teacher [63], were introduced to achieve a more stable target output $g'(x, \theta)$. In temporal ensembling, the model uses an exponentially accumulated average of outputs, $g(x, \theta)$, to produce a smooth and consistent target output while in mean teacher, the model uses a prediction function parametrized by an accumulated average of the model parameters $\theta$ during the training. Contrary to the stochastic perturbation methods mentioned earlier, VAT initially estimates a small perturbation $r$ to add it to $x$ which drastically changes the model prediction, $g(x, \theta)$. Then, a consistency regularization term, $d(g(x, \theta), g(x + r, \theta))$ is considered as a loss term during the training.

Following the advance in consistency regularization, and pseudo-labeling for SSL, MixMatch integrates data augmentation, consistency regularization [56], entropy minimization [26], and mixup [73]. ReMixMatch enhanced on MixMatch by including augmentation anchors and distribution alignment. Augmentation anchors are performs similar to pseudo-labeling. FixMatch which is the state-of-the-art and the most recent approach in this line of research combines consistency regularization, and pseudo-labeling with a threshold of confidence on the output of the model.

2.2. Self-Supervised Learning

The idea behind self-supervised learning (Self-SL) is to take large amount of readily and available unlabeled data and use it to understand itself [13, 14, 28, 50, 65]. Generally, the purpose of Self-SL for images is to create image representations that are semantically meaningful via pretext tasks that do not need human-annotations for a large training dataset. Pretex tasks usually guide the model towards learning meaningful representations that are covariant with image transformations such as rotations [25], and jigsaw transformations [50], and affine transformations [51, 74]. Recently, it has been shown that Self-SL approaches can be simply used to leverage all unlabeled data for learning and can be incorporated by SSL models [72, 35, 32]. For example, the
work in [72] demonstrated that integrating simple Self-SL losses such as rotation is useful for a SSL approach.

3. Wasserstein Distance

For any subset \( \theta \subset \mathbb{R}^d \), assume that \( P(\theta) \) represents the space of Borel probability measures on \( \theta \). The Wasserstein space of order \( k \in [1, \infty) \) of probability measures on \( \theta \) is defined as follows: \( P_k(\theta) = \{ P \in P(\theta) : \int ||x||^k dP(x) < \infty \} \), where \( ||.|| \) is the Euclidean distance in \( \mathbb{R}^d \). Let \( x \sim P \in P(\theta), y \sim Q \in P(\theta) \) and \( J(P, Q) \) denote all the joint distributions \( J \) for \( (x, y) \) on \( \theta \times \theta \) that have marginals \( P \) and \( Q \) for \( x \) and \( y \), respectively, and also assume that \( \delta(x, y) \) is a distance measure between two instances \( x \) and \( y \). Then, the Wasserstein distance is defined as follows:

\[
W_k(P, Q) = \left( \inf_{J \in J(P, Q)} \int \delta(x, y)^k dJ(x, y) \right)^{1/k},
\]

where \( k \geq 1 \). In case \( k = 1 \), this is also called the Earth Mover distance. The term \( J(x, y) \) can be considered as a plan that transports a unit of mass from location \( x \) to another location \( y \) such that the marginal constraints are satisfied. The minimizer \( J^* \) in Eq. (1) is called the optimal transport plan. In the case where transporting cost of a unit of mass from \( x \sim P \) to \( y \sim Q \) is equal to \( \delta(x, y)^k \), then \( W_k(P, Q) \) is the minimum expected transportation cost. The Kantorovich-Rubinstein dual theorem [64] indicates that in the special case where \( k = 1 \), the Wasserstein distance has a closed form of an integral probability metric as follows:

\[
W_1(P, Q) = \sup_{\|f\|_L \leq 1} \mathbb{E}_{x \sim P}[f(x)] - \mathbb{E}_{x \sim Q}[f(x)],
\]

where the supremum is over all 1-Lipschitz functions \( f : \mathcal{X} \rightarrow \mathbb{R} \), and Lipschitz semi-norm is defined as follows: \( \|f\|_L = \sup \|f(x) - f(y)\|/\delta(x, y) \).

4. Wasserstein Barycenter

Wasserstein Barycenter was initially introduced by [1], and provided an efficient role in clustering methods based on OT [18, 37, 31, 46]. Let \( \theta \) denote a Polish space, and \( P(\theta) \) represent the space of probability measures on this space. Moreover, let’s assume that we are given \( M \geq 1 \) probability measures \( P_1, P_2, ..., P_M \in P(\theta) \) with finite second moments, then the Wasserstein barycenter of these measures is defined as follows:

\[
B(\bar{P}) = \inf_{\bar{P} \in P(\theta)} \frac{1}{M} \sum_{i=1}^{M} W_2^2(\bar{P}, P_i),
\]

it has been demonstrated by [2] that the problem of exploring Wasserstein barycenter on the space of \( P(\theta) \) in Eq. (3) boils down to search only on a reduced space \( \mathcal{O}_r(\theta) \) where \( r = \sum_{i=1}^{M} e_i - M + 1 \) and \( e_i \) is the number of elements in \( P_i \) for all \( 1 \leq i \leq M \). Moreover, several practical and effective algorithms have been recently proposed in [1, 18, 68] that provide proper local solutions for the Wasserstein barycenter problem over the space of \( \mathcal{O}_r(\theta) \). These algorithms such as the one in [18] have been a building block for many interesting clustering algorithms based on OT such as [31].

5. Proposed Method

Here, we describe the outline of our SSL method. Our SSL model contains three steps as follows: in step (1), we initially pre-train our CNN using a self-SL method on the unlabeled data and then fine-tune it using the initially labeled data. This operation potentially encourages the CNN model to construct cluster structure when representing the data. For example, in Self-SL based on contrastive learning paradigm [28, 13, 14], the goal is to learn similarities/dissimilarities such that the model is able to understand that the similar data should be closer to each other while dissimilar data should be far away from each other in terms of their representations. Therefore, pre-training the CNN motivates us to make a cluster assumption on the unlabeled data and then annotate each cluster with a unique pseudo-label.

In step (2), we use Wasserstein distance as a metric of similarity between two discrete probability measures to match each cluster of the unlabeled data to the most similar class of the labeled data for pseudo-labeling (see Fig. 1). This pseudo-labeling is based on the SSL assumption in which the labeled and unlabeled data within the same class should come from the same or similar distribution. Thus, we would expect that the similarity between two clouds of data which come from the same or similar distribution is more than the case where these clouds come from completely two different distributions.

Finally, in step (3), we use the unlabeled data annotated with the pseudo labels obtained from step (2) in conjunction
with the initially labeled data to train our CNN classifier.

5.1. Self-Supervised Learning and Clustering via Wasserstein Barycenter

As discussed earlier, in step (1), we initially pre-train our CNN model using a Self-SL paradigm on the unlabeled data to make a cluster assumption for them. Here, we use MoCo v2 Self-SL [14] as it is a strong and efficient Self-SL method. Specifically, we use SimCLR [13] style data augmentation for the unlabeled images in the contrastive loss, and follow the implementation details in MoCo v2 where we use two-layers MLP on the top of the last feature layer to map image features to a 128 dimensions, and then use a momentum updated model to calculate the key features in the memory bank.

After pre-training, we use the Wasserstein metric to perform a clustering on the unlabeled features extracted from the network. Following the previous clustering method based on OT [18, 37, 31, 46], here we relate the clustering algorithm to the problem of exploring Wasserstein barycenter of the unlabeled data to find the clusters underlying them. The K-means objective is an optimization problem that has come up in the quantization problem [54].

Given $n$ unlabeled data $\{x_1, \ldots, x_n\} \in \mathbb{R}^d$, suppose that these data are grouped into $k$ clusters where $k \geq 1$. The K-means algorithm aims to find a set $C$ which contains $k$ elements $\{c_1, \ldots, c_k\}$ that minimizes the following objective:

$$
F(C) = \inf \frac{1}{n} \sum_{i=1}^{n} D^2(x_i, C),
$$

(4)

let $P_n = \frac{1}{n} \sum_{i=1}^{n} \delta_{x_i}$ be a probability measure where $\delta_{x_i}$ is the Dirac function on $x_i$. Then, problem (4) is equal to exploring a probability measure $Q$ with $k$ finite atoms that minimizes the following objective:

$$
B(Q) = \inf_{Q \in \mathcal{Q}_n(\theta)} \frac{1}{n} \sum_{i=1}^{n} W^2_2(Q, P_n),
$$

(5)

this optimization problem can also be thought as a Wasserstein barycenter problem when $M = 1$ in Eq. (3). From this perspective, as introduced by [18], the algorithm for exploring the Wasserstein barycenter is an alternative for the well-known Loyd’s algorithm to obtain local minimum for the K-means. In this work, we use [18] to find the Wasserstein barycenter of the unlabeled data for clustering.

5.2. Matching Clusters to Classes via WGAN

After clustering the unlabeled data, in step (2), we follow the cluster assumption in SSL where data within the same cluster more likely should have the same class label. Moreover, in the general setting of SSL, data within the same class in both labeled and unlabeled sets have the same or similar distribution. Therefore, by considering the Wasserstein distance as a metric of similarity between two discrete probability measures, label of each cluster can be predicted based on the closest Wasserstein distance that the cluster has with a class of labeled data in the labeled set. This is because we would expect that the similarity between two sets of data coming from the same or similar distribution is more than the case where they come from completely two different distributions. Since we usually deal with large scale datasets, and CNN model is usually trained by stochastic gradient descent, we follow the standard training procedure, and use an approach based on gradient descent [4, 58, 24] to compute the Wasserstein distance.

Suppose that $P_i = \frac{1}{n_i} \sum_{j=1}^{n_i} \delta_{x_{ij}}$ denotes a labeled discrete measure which is constructed by labeled data $x_{ij}$ belonging to the $i$-th class; and $Q_i = \frac{1}{n_i} \sum_{j=1}^{n_i} \delta_{x'_{ij}}$ denotes an unlabeled discrete measure which is constructed by unlabeled data $x'_{ij}$ belonging to the $i$-th cluster. In step (2) of our algorithm, we aim to match each of $Q_1, \ldots, Q_k$ to one of the labeled measures $P_1, \ldots, P_c$, so that we can infer a label for each cluster. Therefore, we use the empirical Wasserstein distance as a measure of similarity between each pair $(Q_i, P_j)$ to match the pairs. For example, if the labeled measure $P_m$ is the closest measure to the unlabeled measure $Q_i$, we annotate the data within the $i$-th cluster with label $m$.

In our SSL method, we use the CNN pre-trained via Self-SL to extract the feature for a given sample. Given an image $x \in \mathbb{R}^{m \times n}$, the CNN as a function $f_n: \mathbb{R}^{m \times n} \rightarrow \mathbb{R}^d$ with parameters $\theta_n$ maps sample $x$ to a d-dimensional representation. Inspired by the Wasserstein Generative Adversarial Network (WGAN) [4], we use a critic layer to compute the Wasserstein distance between each pair $(Q_i, P_j)$. Given a feature $z = f_n(x)$ obtained by the CNN, the critic layer in our model learns a function $f_c: \mathbb{R}^d \rightarrow \mathbb{R}$ with parameters $\theta_c$ that maps a feature to a real number. Therefore, the Wasserstein distance between two discrete measures $P_i$ and $Q_j$, where $z = f_n(x), x' = f_n(x'), x \in P_i$ and $x' \in Q_j$ can be calculated by using Eq. (2) as follows:

$$
W_i(P_i, Q_j) = \sup_{||f_c||_{\text{Lipschitz}} \leq 1} \mathbb{E}_{P_i} [f_c(z)] - \mathbb{E}_{Q_j} [f_c(z')]
$$

(6)

By considering the parameterized class of critic functions $f_c$ are all 1-Lipschitz, we can then calculate the empirical Wasserstein distance by maximizing the critic loss $L_w$ with respect to parameters $\theta_c$ as follows:

$$
L_w(P_i, Q_j) = \frac{1}{|P_i|} \sum_{x \in P_i} f_c(f_n(x)) - \frac{1}{|Q_j|} \sum_{x' \in Q_j} f_c(f_n(x')).
$$

(7)

Now, we need to force the Lipschitz constraint. In WGAN [4], it is suggested to clip the weights of critic layer in a compact interval $[-c, c]$ after each gradient update. However,
weight clipping causes some issues including capacity underuse, and exploding problems or gradient vanishing [27]. Therefore, we use the technique used [27] to force a gradient penalty $L_{\text{grad}}$ for critic parameters $\theta_c$ as follows:

$$L_{\text{grad}}(\hat{z}) = (\| \nabla_{\hat{z}} f_c(\hat{z}) \|_2 - 1)^2,$$

where the features $\hat{z}$ on which to penalize the gradients are the features of the labeled and unlabeled data, and also the random points along the line between labeled and unlabeled pairs. Therefore, we can approximate the Wasserstein distance by optimizing the following objective:

$$W_1(\mathcal{P}_i, \mathcal{Q}_j) = \max_{\theta_c} (L_w - \alpha L_{\text{grad}}),$$

where $\alpha$ is a coefficient that balances between $L_w$ and $L_{\text{grad}}$.

### 5.3. Total Loss for Training the CNN

In step (3), we remove two-layers MLP from top of the last feature layer which we used for Self-SL, and then place a softmax layer for the classification task. In this step, we modify the decision making process to decide which classes are predicted for each training sample. Thus, we used the supervised softmax layer to output the probability of each class. In this step, we remove two-layers MLP from top of the CNN. Therefore, we can approximate the Wasserstein distance by optimizing the following objective:

$$W_1(\mathcal{P}_i, \mathcal{Q}_j) = \max_{\theta_c} (L_w - \alpha L_{\text{grad}}),$$

where $\alpha$ is a coefficient that balances between $L_w$ and $L_{\text{grad}}$.

### Algorithm 1 Self-Supervised Wasserstein Pseudo-Labeling

**input**: $X_l, X_u, \alpha, \lambda, \beta_1, \beta_2, b, k, m$

1. **initialize**: critic layer $\theta_c$ with $\mathcal{N}(0, 0.001)$.
2. **pretrain** $\theta_n$ using MoCo v2 Self-SL.
3. **repeat**
   4. $Z_l = \{z_i\}_{i=1}^m$, $Z_u = \{z_i\}_{i=1}^m$: where $z_i = f_n(x_i)$.
   5. $\{Q_1, ..., Q_k\} \leftarrow$ cluster $Z_u$ to $k$ groups.
   6. $\{P_1, ..., P_c\} \leftarrow$ cluster $Z_l$ to $c$ classes.
   7. for each $Q_j$ and $P_j$ do
      8. for $i = 1, ..., s$ do
         9. choose a batch: $\{x_i\}_{i=1}^b \subset P_j$, $\{x_i\}_{i=1}^b \subset Q_i$.
         10. $z_i' = f_n(x_i')$, $z_i = f_n(x_i)$.
         11. $\hat{z} \leftarrow \{z_i', z_i, \hat{z}\}$: take sample $\hat{z}$ randomly on lines between $z_i'$ and $z_i$ pairs.
         12. $\theta_c \leftarrow \theta_c + \beta_1 \nabla_{\theta_c} [L_w(z', \hat{z}) + \alpha L_{\text{grad}}(\hat{z})].$
      13. **end for**
      14. $S(i, j) \leftarrow L_w(P_i, Q_j)$, by Eq. (7)
   15. **end for**
   16. $\{y_i\}_{i=1}^m \leftarrow$ pseudo label data within each cluster $Q_j$ with the most similar class (i.e., argmin $S(i, j)$).
   17. **repeat**
      18. choose a batch: $\{x_i\}_{i=1}^b \subset X_u \cup X_l$.
      19. $\theta_n \leftarrow \theta_n - \beta_2 \nabla_{\theta_n} \left[ L(\theta_n, x, x', y, y') \right]$, by Eq. (10).
   20. **until** for an epoch
   21. **until** $\theta_n$ converge

### 6. Experiments

We carry out empirical analysis to show the effectiveness and benefit of our SSL algorithm over other state-of-the-art methods [55, 41, 66, 63, 9, 8, 60]. Here, we perform following studies: 1) We report results for supervised-baseline where the CNN is only trained by initially labeled data, this is because the goal of SSL is to greatly improve the supervised-baseline. 2) We change number of the labeled and unlabeled data and report the results as an efficient SSL method should still perform well even by using a small number of labeled data and extra amount of unlabeled data. 3) We replace our OT-base clustering method with the popular k-means and report the results to demonstrate the importance of the Wasserstein metric in our SSL algorithm. 4) We conduct an analysis on the clustering resolution (i.e., $k$ in Alg 1) to see its importance in our model.

Following the compared methods, we have been consistent in CNN network and used the ‘WRN-28-2’ [71], including leaky ReLU nonlinearities [45] and batch normalization [33]. We performed our experiments on the widely used CIFAR-10/100 [38], SVHN [48], and ImageNet [20] datasets. We note that in all of our experiments, we consider the general SSL setting where the labeled and unlabeled data coming the same or similar distribution, and a given unlabeled data belongs to one of the classes in the labeled set and there is no class distribution mismatch. Furthermore, for each of aforementioned datasets, we split the training set into two different sets of labeled and unlabeled data. We make sure that all classes are balanced such that each class should have the same number of labeled data.

For training, we set hyperparameter $\lambda$ to 0.7 in all of our experiments. We use the regular SGD optimizer with momentum 0.9, and weight decay $10^{-4}$. We set the learning rate $\beta_2$ in Alg 1 to $3 \times 10^{-3}$ in all of our experiment. The batch size in the experiments (b in Alg 1) is set to 128. We note that our batch size for training the CNN (b) is different from the batch size that we map the unlabeled data to the labeled data (m in Alg 1). The batch size for mapping the unlabeled data to the labeled data is the size of initially labeled data ($|X_l|$. In other words, each time, we select $|X_l|$ unlabeled data to cluster them. Then, we use WGAN to map these clusters to the groups of data formed by $X_l$. 12271
The parameters of the network ($\theta_n$ in Alg 1) are initialized by pre-training via MoCo v2 Self-SL [14]. Here, we follow the implementation details from MoCo-v2 but we use a memory bank of size 16384. We initialized the parameters of the critic layer ($\theta_c$ in Alg 1) by sampling randomly from $\mathcal{N}(0, 0.001)$. The critic layer parameters usually requires around 10 epochs ($s$ in Alg 1) to converge in our experiments but we set it to 20 epochs for a sufficient optimization guarantee for the parameters of the critic layer. For training the critic layer, the learning rate is also set to $\beta_1 = 3 \times 10^{-3}$. Note that during the training of the critic layer, we penalize the gradients not only at CNN outputs for the unlabeled and labeled data points but also at random points along the line between pairs of labeled and unlabeled data points. The coefficient $\alpha$ is set to 10 as is suggested in [27].

In our experiments, we use the regular data augmentation and standard data normalization techniques. Specifically, for SVHN, we converted and normalized pixel intensity values of the images to floating point values in the range of [-1, 1]. For the data augmentation, we only applied random translation by up to 2 pixels. For CIFAR-10/100, we used global contrast normalization. The data augmentation on CIFAR-10/100 are random translation by up to 2 pixels, random horizontal flipping, and Gaussian input noise with standard deviation 0.15.

### 6.1. Comparison

The goal in SSL is essentially to obtain a better performance when we use the unlabeled data compared to the case where we use the labeled data alone. Thus, we report the error rate of our ‘WRN-28-2’ for cases where we only use a limited amount of labeled data (i.e., Supervised in Table 1), and the case where we leverage the unlabeled data using our SSL method called Self-Supervised Wasserstein Pseudo Labeling (SSWPL) in Table 1. Furthermore, we report the performance of the other SSL methods including $\pi$ model [55], Pseudo-Labeling [41], UDA [66], MT [63], MixMatch [9], ReMixMatch [8], and FixMatch [60] in Table 1. For comparison, we chose 250, and 4000 labeled images for CIFAR-10, 2500, and 10000 labeled images for CIFAR-100, 250, and 1000 labeled images for SVHN. Here, the remaining images of the training set are used as the unlabeled images to train the network. We ran our SSL methods over 5 times with different random splits of labeled and unlabeled sets for each dataset, and we reported the mean and standard deviation of the test error rate in Table 1. The results on CIFAR-10/100 and SVHN datasets in Table 1 demonstrate the potential of SSWPL for using the unlabeled data in comparison to other

<table>
<thead>
<tr>
<th>Datasets</th>
<th>CIFAR-10</th>
<th>CIFAR-100</th>
<th>SVHN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>250</td>
<td>4000</td>
<td>250</td>
</tr>
<tr>
<td>Supervised</td>
<td>56.85 ± 1.34</td>
<td>19.74 ± 0.23</td>
<td>24.95 ± 0.49</td>
</tr>
<tr>
<td>$\pi$ model [55]</td>
<td>54.26 ± 3.97</td>
<td>14.01 ± 0.38</td>
<td>18.96 ± 1.92</td>
</tr>
<tr>
<td>Pseudo-Labeling [41]</td>
<td>49.78 ± 0.43</td>
<td>16.09 ± 0.28</td>
<td>20.21 ± 1.09</td>
</tr>
<tr>
<td>UDA [66]</td>
<td>8.82 ± 1.08</td>
<td>4.88 ± 0.18</td>
<td>5.69 ± 2.76</td>
</tr>
<tr>
<td>MT [63]</td>
<td>32.32 ± 2.30</td>
<td>9.19 ± 0.19</td>
<td>3.57 ± 0.11</td>
</tr>
<tr>
<td>MixMatch [9]</td>
<td>11.05 ± 0.86</td>
<td>6.42 ± 0.10</td>
<td>3.98 ± 0.23</td>
</tr>
<tr>
<td>ReMixMatch [8]</td>
<td>5.44 ± 0.05</td>
<td>4.72 ± 0.13</td>
<td>2.92 ± 0.48</td>
</tr>
<tr>
<td>FixMatch [60]</td>
<td>5.07 ± 0.33</td>
<td>4.31 ± 0.15</td>
<td>2.86 ± 0.24</td>
</tr>
<tr>
<td>SSWPL (k-means)</td>
<td>9.62 ± 0.47</td>
<td>7.74 ± 0.73</td>
<td>30.19 ± 0.35</td>
</tr>
<tr>
<td>SSWPL</td>
<td>4.11 ± 0.15</td>
<td>3.18 ± 0.09</td>
<td>26.52 ± 0.45</td>
</tr>
</tbody>
</table>

Table 1. Comparing test error between SSWPL and different baselines and SSL methods.
state-of-the-art SSL algorithms.

6.2. Self-SL Contribution on Clustering

As discussed in step (1), we pre-train our CNN model using Self-SL method and then form the clusters on the unlabeled data. Here, we evaluate the importance of the Self-SL on the clustering performance in our model. This is because one may assume that pre-training of the CNN on the initially labeled data can also enforce a clustered structure in the feature space for the unlabeled data, so it is important to know the benefit of using Self-SL on the clustering performance which plays an essential role in our model. Therefore, we conducted experiments to compare two different cases where in case (1), we fine-tune the network using initially labeled data without considering the Self-SL while in case (2) we consider the Self-SL for clustering. To compare these two cases and indicate the positive influence of the Self-SL on clustering, we changed the number of initially labeled data in the training set and reported the number of accurately predicted pseudo labels using our SSL method in case (1) and (2) on the remaining unlabeled training data. The significant gap between case (1) and case (2) which are respectively indicated by SSWPL and w/o Self-SL in Fig. 2 show that for CIFAR-10/100 and SVHN datasets, the labels predicted by our SSL method on the unlabeled training data are more accurate in case (1) than case (2), which means that the entire CNN network can benefit from Self-SL.

6.3. Analysis in Limited Label Regime

Here, we investigate that how changing the amount of initially labeled data increase the accuracy of our SSL algorithm in the very limited label scenario, and also at which point our SSL algorithm can recover the performance of training when using all of the labeled data in the dataset. To conduct this evaluation, we moderately increase the number of labeled samples during the training and report the performance of our SSL algorithm on the testing set. In this study, we ran our SSL algorithm over 5 times with different random splits of labeled and unlabeled sets for each dataset, and reported the mean and standard deviation of the error rate in Fig. 3. The results indicate that the performance of our SSL method on CIFAR-10/100 and SVHN inclines to converge as the number of initially labeled data increases.

6.4. Varying Number of the Clusters

We evaluate the role of the clustering resolution on the error rate of SSWPL. In this study, we use 500, 1000, and 4000 labeled images from the training sets of SVHN, CIFAR-10, and CIFAR-100 datasets, respectively. We change the number of the clusters in our model, and evaluate error of the model on the validation set. The results on SVHN and CIFAR-10/100 datasets in Fig. 4 demonstrate that as we increase the number of the clusters in our model, the model can benefit from it but performance of the model inclines to degrade as we largely perform over-clustering. The reason can be interpreted by SSL models based on consistency regularization [76, 44, 5]. In other words, if we significantly perform over-clustering, we basically disregard the local geometry or structure of the data when mapping clusters to the label classes using the Wasserstein metric which is not useful in SSL as we neglect the local consistency.

Furthermore, in our other studies, instead of using the Wasserstein metric in the K-means objective for clustering the unlabeled data, we used the generic K-means in SSWPL and reported the test error rate in Table. 1. We call this baseline as SSWPL (K-means). The compared results between SSWPL and SSWPL (K-means) on SVHN, and CIFAR-10/100 datasets in Table. 1 demonstrate advantage of leveraging the Wasserstein-metric in the K-means objective for our SSL model.

6.5. Results on ImageNet

We also conducted an experiment on the large-scale ImageNet dataset to evaluate the performance of our model when using unlabeled unlabeled data in a very limited label regime.
Following the prior work [60, 66], we also used a ResNet-50 architecture and RandAugment [17] data augmentation technique to conduct our experiments. Here, we set the number of the clusters in our method to the number of classes (i.e., 1000). We used 10% of the training set as our initially labeled data and the remaining as the unlabeled data. We ran our model 3 times and reported the mean and standard deviation of top-1 (top-5) error rate. The supervised-baseline top-1 (top-5) error rate using 10% of the training data is $45.64\pm0.83\%$ ($24.67\pm0.32$) while for our SSL model (i.e., SSWPL), FixMatch[60], and UDA [66] are $26.46\pm0.44\%$ ($9.14\pm0.26\%$), $28.54\pm0.52\%$ ($10.87\pm0.28\%$), and $31.22\%$ ($11.2\%$), respectively. These results indicate the efficiency and potential of our SSL method compared to other effective SSL approaches for the large-scale datasets.

6.6. Limitation, discussion and Future Work

As mentioned earlier, in this study we consider the general setting of SSL in the literature [78, 11, 52] where there is no class distribution mismatch and the main assumption is that the labeled and unlabeled data coming from the same or similar distribution. Specifically, every given unlabeled data should belong to one of the classes which present in the labeled set. However, the work [52] in Sec. 4.4 showed that using unlabeled data from the mismatched classes essentially has a negative impact on the performance of the studied SSL approaches compared to the case where these approaches do not use any unlabeled data at all. Likewise, our method would also hurt the performance when using the unlabeled data from the mismatched classes. This is because our method will provide a pseudo-label for the unlabeled data whether they belong to the mismatched classes or not. Thus in such a case, our model predicts high confident but incorrect labels for the unlabeled data within the mismatched classes and then use them for training which causes a confirmation bias problem [3]. However, pre-training the network using the Self-SL approach on the unlabeled data as we used in our method potentially can cluster the unlabeled data from mismatched classes as good as the unlabeled data which are not from mismatched classes. Therefore, in such a case, we can perform the clustering approach on the entire data and then disregards the clusters which contain the unlabeled data from mismatched classes during the training. There are many methods in the literature [10, 29, 30, 15] that are proposed to detect out of distribution samples which we can potentially use them to detect out of distribution clusters. We will consider this study as our future work.

7. Conclusion

We proposed a new SSL algorithm that uses the Wasserstein distance and Self-SL technique to provide pseudo labels for the unlabeled data to train a CNN classifier in an SSL fashion. In this work, after pre-training the CNN model using a Self-SL method, we made a cluster assumption about the unlabeled data and then used their Wasserstein barycenter to explore the clusters underlying them. In the next step, we used the Wasserstein GAN to match each of the clusters to the most similar class of labeled data so we can provide a unique label for the data within each cluster. Finally, we used all the unlabeled data annotated by pseudo labels in conjunction with the initially labeled data to train our CNN model. In this study, we conducted empirical analysis to demonstrate the potential and efficiency of our SSL algorithm for leveraging the unlabeled data when labels are limited over the course of training.

References

[50x205][15] Yanbei Chen, Xiatian Zhu, Wei Li, and Shaogang Gong. Semi-
[50x377][11] Olivier Chapelle, Bernhard Schölkopf, and Alexander Zien.
[50x240][14] Xinlei Chen, Haoqi Fan, Ross Girshick, and Kaiming He. Im-
[50x286][13] Ting Chen, Simon Kornblith, Mohammad Norouzi, and Ge-
[50x331][12] Olivier Chapelle, Jason Weston, and Bernhard Schölkopf.
[50x423][10] Markus M Breunig, Hans-Peter Kriegel, Raymond T Ng, and
[55x480][9] David Berthelot, Nicholas Carlini, Ian Goodfellow, Nicolas
[55x582][7] Mikhail Belkin, Partha Niyogi, and Vikas Sindhwani. Mani-
[55x536][8] David Berthelot, Nicholas Carlini, Ekin D Cubuk, Alex
[69x183]AAAI Joint Conference on Neural Networks (IJCNN), pages 1–8.
[25] Spyros Gidaris, Praveer Singh, and Nikos Komodakis. Unsu-
[32] Chao Huang, Hui Tang, Wei Fan, Yuan Xiao, Dingjun Hao, Zhen Qian, Demetri Terzopoulos, et al. Self-supervised, semi-supervised, multi-context learning for the combined classification and segmentation of medical images (student abstract). In...


