Semi-supervised Learning with Support Isolation by Small-Paced Self-Training

Zheng Xie, Hui Sun, Ming Li

National Key Laboratory for Novel Software Technology,
Nanjing University, Nanjing 210023, China
{xiez,sunh,lim}@lamda.nju.edu.cn

Abstract

In this paper, we address a special scenario of semi-supervised learning, where the label missing is caused by a preceding filtering mechanism, i.e., an instance can enter a subsequent process in which its label is revealed *if and only if* it passes the filtering mechanism. The rejected instances are prohibited to enter the subsequent labeling process due to economical or ethical reasons, making the support of the labeled and unlabeled distributions isolated from each other. In this case, semi-supervised learning approaches which rely on certain coherence of the labeled and unlabeled distribution would suffer from the consequent distribution mismatch, and hence result in poor prediction performance. In this paper, we propose a Small-Paced Self-Training framework, which iteratively discovers labeled and unlabeled instance subspaces with bounded Wasserstein distance. We theoretically prove that such a framework may achieve provably low error on the pseudo labels during learning. Experiments on both benchmark and pneumonia diagnosis tasks show that our method is effective.

1 Introduction

Semi-supervised learning (Chapelle, Schlkopf, and Zien 2006; Zhu et al. 2009), which aims to alleviate the huge cost of collecting labeled data by exploiting the relatively large amount of unlabeled data, is raised from real-world demands. Existing approaches utilize the unlabeled data for better modeling the data distribution through different ways, increasing the capability of semi-supervised learning in various scenarios (Bennett and Demiriz 1999; Nigam et al. 2000; Zhu, Ghahramani, and Lafferty 2003; Tarvainen and Valpola 2017; Berthelot et al. 2019).

Differing from semi-supervised learning, which usually considers the labeled data is sampled from the population distribution with no or neglectable shift, in specific situations, labeled data may be sampled from a different distribution other than the test distribution, and unlabeled data sampled from the test distribution can be used for improving learning. For example, domain adaptation (Ben-David et al. 2010; Hoffman et al. 2018; Qu et al. 2019) aims to build models with labeled and unlabeled data from two different but related (source and target) domains. Learning under sample selection bias (Quiñonero-Candela et al. 2008; Huang et al. 2006) aims to build models from the data where the selection of labeled data subjects to some bias or preference. The shift between labeled and unlabeled distributions is usually assumed to be of certain types, e.g., label shift, covariate shift, concept shift, etc.

In this paper, we focus on a specific type of problem, where the labeling process is not executed on random instances, but determined by some preceding filtering mechanism. Such a mechanism can be regarded as a deterministic classification model for predicting if an instance is qualified to enter the subsequent process, which includes the observation or production of its ground truth label. If the instance is rejected by the filtering model, the label remains unrevealed and will never be known. The filtering mechanism can be a set of rules, a group of experts, or a machine learning model, depending on the situation. Such situations can occur in various fields including financial, medical, marketing, etc., here we take the lung nodule diagnosis as an example:

> When a lung nodule is detected during a CT lung scan, the doctors decide if the nodule has to be surgically removed based on some treatment rules. If the nodule needs surgical removal, the nodule tissue can be collected during the surgery and then analyzed by the pathologists under a microscope. In such a case, the property of the tumor is observed. If the nodule is decided against surgical removal, the patient will have a conservative treatment, and the nodule property remains unrevealed since the nodule tissue is not available for biopsy. The doctors "filter" the data to be "labeled" according to the treatment rules, which makes the data suffer label missing for building machine learning models for other tasks like nodule classification.

Such a filtering mechanism makes the distribution of the labeled data different from the overall data distribution. A hard filtering boundary isolates the labeled distribution and the unlabeled distribution, making it difficult to learn the decision boundary for the target task on the unlabeled side, as shown in Figure 2. Here we remark that the problem we face can be regarded as some sort of sample selection bias, but the mainstream of research in this direction does not interested in such exceptional case that the labeled and unlabeled distribution do not overlap in their support. Instead, the condition that the support of biased labeled data

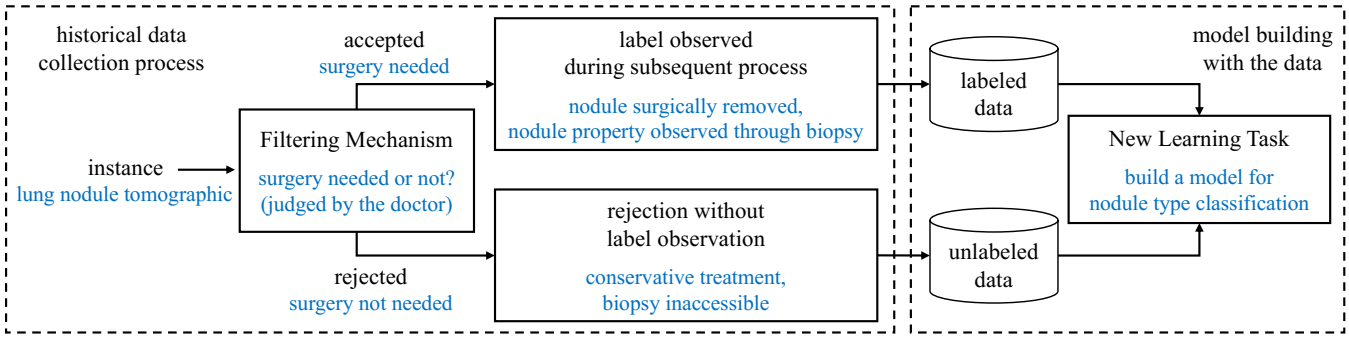
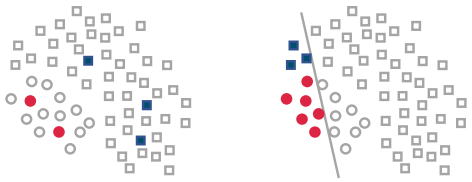


Figure 1: Demonstration of the labeling process governed by a filter.



(a) No support isolation (b) Support isolation

Figure 2: Demonstration of a semi-supervised dataset with support isolation.

distribution covers the support of the population distribution is generally required, and the distribution density ratio has to be bounded (Shimodaira 2000; Huang et al. 2006; Quiñonero-Candela et al. 2008; Sugiyama, Krauledat, and Müller 2007). Such an issue also prevents us from solving it as a domain adaptation problem by regarding the labeled and unlabeled side as two domains, as it has been shown that learning invariant representations can be unhelpful under label shift and shift in the support (Ben-David and Urner 2012; Johansson, Sontag, and Ranganath 2019; Li et al. 2020; Zhao et al. 2019).

In this paper, we try to tackle the problem under the framework of semi-supervised learning. We propose Small-Paced Self-Training framework to address the problem. Self-training methods recently show great power on tasks including semi-supervised learning, domain adaptation, and unsupervised learning (Lee 2013; French, Mackiewicz, and Fisher 2018; Hu et al. 2017; Prabhu et al. 2020; Xie et al. 2021). Some recent theoretical results reveal the insights of self-training algorithms on specific scenarios, including gradual domain adaptation (Kumar, Ma, and Liang 2020), and self-training with consistency regularization (Wei et al. 2021). We modify self-training by adding a subset selection mechanism to ensure the pseudo-labeler models make provably low error. To be concrete, Small-Paced Self-Training framework selects a pseudo-labeled subset for training the pseudo-labeler models, and produces pseudo labels only on an unlabeled subset whose Wasserstein distance with the training set is bounded. Intuitively, this strategy learns the concept in a 'small-paced' way to avoid the performance degradation caused by the distribution mismatch. Our theoretical analysis shows that by restricting the Wasserstein distance of the training distribution and pseudo-labeled distribution, Small-Paced Self-Training produces pseudo-labels with low error provably. Our contributions are two folds:

1. We propose Small-Paced Self-Training framework for semi-supervised learning with support isolation problem, and theoretically show that our Small-Paced Self-Training helps the learning under support isolation.
2. We provide a practical algorithm of the Small-Paced Self-Training framework, and empirically show the effectiveness of our algorithm on benchmark and real-world tasks.

2 Problem Setup

Consider the problem of binary classification, let $P_{X,Y}$ denote the underlying data joint distribution over $\mathcal{X} \times \mathcal{Y}$, where $\mathcal{X} \subseteq \mathbb{R}^d$ is the feature space and $\mathcal{Y} = \{+1, -1\}$. Let P_X be the marginal distribution of X. In ordinary semi-supervised learning, the labeled data and unlabeled data

$$D_L = \{(x_i, y_i)\}_{i=1,\dots,n} \sim P_{X,Y}\,, \text{ and}$$
$$D_U = \{(x_j)\}_{j=n+1,\dots,n+m} \sim P_X\,,$$

are considered sampled i.i.d. from the same distribution P.

The problem we face is that a filtering mechanism governs the labeling process, making the sampling of labeled data and unlabeled data no longer i.i.d., but conditioned on the filter's decision. For an instance $X \sim P_X$, random variable $S = g(X)$ where $g : \mathcal{X} \to \{0, 1\}$ is the deterministic filter function which indicates if we are able to observe the label of X. Such filter function defines a partition $\{\mathcal{X}_L, \mathcal{X}_U\}$ of $\mathcal{X}$. The labels of the instances in subspace $\mathcal{X}_L = \{X \in \mathcal{X} | g(X) = 1\}$ are all observed and the instances in subspace $\mathcal{X}_U = \{X \in \mathcal{X} | g(X) = 0\}$ are all unlabeled. In this situation, the labeled set D_L and unlabeled set D_U are sampled from different conditional distributions:

$$D_L = \{(x_i, y_i)\}_{i=1,\dots,n} \sim P_{X,Y|S=1}\,, \text{ and}$$
$$D_U = \{(x_j)\}_{j=n+1,\dots,n+m} \sim P_{X|S=0}\,,$$

and the support of the two distributions are disjoint, or isolated. Particularly, in this paper, we consider the filtering function $g(\cdot)$ as a deterministic machine learning model, or a rule-based decision process. We do not require the knowledge of $g(\cdot)$ other than the dataset and labels.

In general, since $\mathcal{X}_L$ and $\mathcal{X}_U$ are disjoint, we obtain no knowledge on conditional probability $P_{Y|X}$ on $\mathcal{X}_U$ by learning on D_L, and thus the model cannot generalize to $\mathcal{X}_U$. However, the underlying structure of the data distribution may be captured to enable learning. In this paper, we assume the data distribution satisfies some assumptions on its connectivity and separability. These assumptions are commonly used in recent theory analysis for semi-supervised learning, unsupervised learning, and domain adaptation approaches (Wei et al. 2021; Liu, Wang, and Long 2021), and have been shown to hold for common data distribution including mixtures of isotropic Gaussians and mixtures of manifolds (Wei et al. 2021).

Definition 1 ((a, c)-expansion)**.** The class-conditional distribution P_i satisfies (a, c)-expansion if for all $V \subseteq \mathcal{X}$ with $P_i(V) \leq a$, the following holds:

$$P_i(\mathcal{N}(V)) \geq \min\{cP_i(V), 1\}\,, \tag{1}$$

where

$$\mathcal{N}(x) = \{x' \mid \|x - x'\|_2 \leq r\}\,, \tag{2}$$

$$\mathcal{N}(V) = \cup_{x \in V}\mathcal{N}(x)\,. \tag{3}$$

And if P_i satisfies (a, c)-expansion for both classes, then we say P satisfies (a, c)-expansion.

Definition 2 ((r, μ)-separation)**.** For a distribution P, an instance $x \sim P$, with at most probability μ, there exists $x' \sim P$ belongs to the different class of x and $x' \in \mathcal{N}(x)$.

Assumption 3 (Expansion)**.** We assume that the population distribution P satisfies $(0.5, c)$-expansion on $\mathcal{X}$ for some $c > 1$.

Assumption 4 (Separation)**.** We assume that the population distribution P satisfies (r, μ)-separation for some small $\mu > 0$.

Remark 5. The above problem setting belongs to a special case of *sample selection bias*, in which the sampling process of the labeled data subjects to some bias that can be described as a random rejection variable S. Let $S = 1$ represents the label is revealed and $S = 0$ represents the label is unrevealed. Then, the training set is sampled from $P_{X,Y|S=1}$ and the unlabeled set is sampled from P_X. Existing researches on this topic require the condition:

$$P(S = 1|X) > 0$$

holds on the region where $P(X) > 0$. With this condition, the propensity score function $s(X) = P(S = 1|X)$ can be modeled and used for reweighting the instances. In our setup, $P(S = 1|X) = g(X)$ is deterministic and ranging discrete in $\{0, 1\}$, and the goal is to build a model of $P(Y|X, S = 0)$ with the help of the unlabeled data. The existing line of research cannot be adapted to solve the problem of this paper.

Remark 6. Our problem setup is close to *domain adaptation*, where we have labeled data D_S from the source domain and unlabeled D_T from the target domain. Researches on this topic generally assume the class prior remains consistent in the two domains (or at least not vary significantly), and try to find a mapping function to map the source domain and the target domain into one same feature space. The problem we face is different to domain adaptation in two aspects: 1) in our setup, the class prior on the labeled and unlabeled side may vary arbitrarily, and their support does not overlap; and 2) there is not any conceptual reasonable invariant representation of the labeled and the unlabeled data. These differences make it difficult to adapt theories and practices to our setup (Zhao et al. 2019; Shu et al. 2018).

3 Small-Paced Self-Training

Standard self-training algorithms iteratively make predictions on the unlabeled data, and then add the confident predictions into the labeled set to refine the model. It is prone to failure when the labeled and unlabeled data distributions change significantly. We point out that 1) standard self-training typically uses all (pseudo-)labeled data, with or without weighting, to build the model for pseudo-labeling more instances, and 2) all the unlabeled instances are candidates for pseudo-labeling. Our proposed small-paced self-training differs from standard self-training in these two aspects.

3.1 Small-Paced Self-Training Framework

The main challenge of the problem is that the labeled distribution and the unlabeled distribution have disjoint support, hence when producing pseudo labels, the distribution discrepancy of $P_{X,Y|S=0}$ and $P_{X,Y|S=1}$ can be large, and the class prior between the two distributions can change arbitrarily.

To tackle this problem, the main idea of small-paced self-training is to 'break' the unlabeled distribution into small component distributions, so that at each iteration, we can find some labeled instances that the unlabeled ones are 'closed' to, and the model trained on the labeled instances can be provably adapted to the unlabeled ones. We use large margin models as the base model in each iteration. Intuitively, when unlabeled distribution drifts away from the labeled distribution only at a small pace, the unlabeled instances get close to the classification border but are unlikely to get across the border if the classifier has a large margin to the labeled instances.

Formally, at iteration t, we denote the subspace remaining unlabeled as $\mathcal{X}_U^{(t)}$ and the pseudo-labeled subspace as $\mathcal{X}_L^{(t)}$. Instead of training model with instances in $\mathcal{X}_L^{(t)}$ and generating pseudo-labels on instances in $\mathcal{X}_U^{(t)}$, we instead select a subset of $\mathcal{X}_L^{(t)}$ and a subset of $\mathcal{X}_U^{(t)}$, namely $\tilde{\mathcal{X}}_L^{(t)}$ and $\tilde{\mathcal{X}}_U^{(t)}$. We define the component distributions $P^{(t)} = P(x|x \in \tilde{\mathcal{X}}_L^{(t)})$ and $Q^{(t)} = P(x|x \in \tilde{\mathcal{X}}_U^{(t)})$. If all unlabeled data are pseudo-labeled in T iterations, we have:

$$P_{S=0} = P(x|x \in \bigcup_{t=1}^{T} \tilde{\mathcal{X}}_U^{(t)})\,. \tag{4}$$

Distribution distance. To make the pseudo-labels on $Q^{(t)}$ reliable, in iteration t, we want to find some labeled instances from some component distribution $P^{(t)}$, such that

the distributional distance between $P^{(t)}$ and $Q^{(t)}$ is small enough, and consequently the model f trained on $P^{(t)}$ can produce predictions on $Q^{(t)}$ with guaranteed performance. However, given the labeled and unlabeled distribution isolated in their supports, distribution distance measures like KL-divergence and JS-divergence cannot be defined. A reasonable choice here to consider is Wasserstein distance. In this paper, we use Wasserstein-infinity distance of the distributions:

$$W_\infty(P, Q) = \inf_T(\sup_x \|T(x) - x\|_2)\,, \tag{5}$$

$$T : \mathbb{R}^d \to \mathbb{R}^d\,, T_\# P = Q\,, \tag{6}$$

where $T_\# P$ denotes the push-forward measure of P by some measurable mapping T such that $T_\# P(A) = P(T^{-1}(A))$ for every set $A \subseteq \mathbb{R}^d$. Intuitively, W_∞ gives the upper bound of the distance of moving points to match the distribution P and Q. Let $\rho(P, Q)$ be the maximum W_∞ on the class conditional distributions:

$$\rho(P, Q) = \max_{y\in\{+1,-1\}}(W_\infty(P_{X|Y=y}, Q_{X|Y=y}))\,. \tag{7}$$

Such measure bounds the maximum moving distance of conditional mapping from Q to P.

Base models. We consider both linear and deep large margin models for classifying the component distributions. For linear base models $f(x) = w^\top x + b$, we optimize ramp loss with ℓ_2 regularization, which produces large margin classifiers and is shown robust to the outliers. Notice that although the entire dataset is not linearly separable, our algorithm breaks the whole dataset into separable subsets and produces reliable pseudo labels gradually, so that the linear base models do not restrict our algorithm to simple tasks. The ramp loss is formalized as:

$$\ell_r(z) = \min(\max(1 - z, 0), 1)\,. \tag{8}$$

For deep models, we use Large Margin Deep Networks (Elsayed et al. 2018) as the base models, which penalize the decision boundary going through the neighborhood of instance within distance δ:

$$\ell_m(x, y) = \max(0, \delta + y d_{f,x})\,, \tag{9}$$

where $d_{f,x}$ is the distance of instance x from the decision boundary:

$$d_{f,x} = \min_\xi \|\xi\|_2 \tag{10}$$

$$\text{s.t. } f(x + \xi) = 0\,. \tag{11}$$

Both linear and deep models we choose here enlarge the classification margin. For the linear model, by regularizing the $\|w\| \le R$ for some $\frac{1}{R} > \delta$, it penalizes the instances within the margin of distance at least δ from the classification border. For the deep model, the large margin loss also pushes the decision boundary away from the instances by a distance of at least δ.

Overall framework. Our framework requires the constructed component distributions at each step to meet the following conditions:

1. class prior consistent: $P_Y^{(t)} = Q_Y^{(t)}$;
2. small shifting: the distributional distance of labeled and unlabeled distributions is bounded, i.e., $\rho(P^{(t)}, Q^{(t)}) \le \delta$;
3. α^*-separation: $P^{(t)}$ and $Q^{(t)}$ satisfy α^*-separation for some small $\alpha^* > 0$, i.e., there exists some classifier f^* which can achieve low ramp loss on $P^{(t)}$ and $Q^{(t)}$.

The following theorem states that as long as the remaining unlabeled distribution contains instances from two classes, the component distributions that meet the above requirements exist.

Theorem 7. *Suppose the population distribution satisfies $(0.5, c)$-expansion and (r, μ)-separation. If $0 < P_Y(X|X \in \mathcal{X}_U^{(t)}) < 1$ for $Y \in \{+1, -1\}$, then $P^{(t)}$ and $Q^{(t)}$ that satisfy the class balanced, small shifting, and α^*-separation conditions exist.*

The proof of the Theorem 7 is provided in appendix. Based on this Theorem we can self-train the model till we cannot find any component distributions, and label the remainder unlabeled instances as some single class.

Practically, instead of explicitly finding the component distributions $P^{(t)}$ and $Q^{(t)}$, we select a pseudo-labeled instance set $\tilde{D}_{PL}^{(t)} \sim P^{(t)}$ and $\tilde{D}_U^{(t)} \sim Q^{(t)}$. Here we give an algorithmic summary of the small-paced self-training framework in Algorithm 1. We will first conduct theoretical analysis in Section 3.2 and then practical implementation of this framework in Section 4.

Algorithm 1: Small-Paced Self-Training Framework

repeat
  Choose subset $\tilde{D}_{PL}^{(t)} \sim P^{(t)}$ and $\tilde{D}_U^{(t)} \sim Q^{(t)}$.
  Train $f^{(t)}$ on $\tilde{D}_{PL}^{(t)}$ with a large margin.
  Select $\{x \in \tilde{D}_U^{(t)} | f(x) \ge \theta\}$ as the pseudo-labels.
until No unlabeled data remaining.

3.2 Theoretical Analysis

In this section, we conduct theoretical analysis of our small-paced self-training framework.

In step t, we regard the training subset $\tilde{D}_{PL}^{(t)}$ as drawn from $P^{(t)}$, and the generated pseudo-labeled instances $\tilde{D}_U^{(t)}$ as drawn from $Q^{(t)}$. Our algorithm makes sure that during the self-training process, $\rho(P^{(t)}, Q^{(t)}) \le \delta$, and the margin on B' is large, i.e., $f(B') > R$.

We next show that the small-paced self-training framework helps in learning. We first conduct some lemmas, and then give the main Theorem 11. The analysis is based on the linear base model case.

Lemma 8. *Given n samples D from a joint distribution P over inputs $\mathbb{R}^d$ and labels $\{-1, +1\}$, and suppose*

$\mathbb{E}_{X\sim P}[\|X\|_2^2] \leq B^2$. *Let* $\hat{f}$ *and* f^* *be the empirical and population minimizers of the ramp loss respectively:*

$$\hat{f} = \arg\min\, L(f, D)\,, \tag{12}$$

$$f^* = \arg\min\, L(f, P)\,, \tag{13}$$

where

$$L(f, D) = \sum_{x,y\in D} \left(\ell_r(yf(x))\right), \tag{14}$$

$$L(f, P) = \mathbb{E}_{X,Y\sim P}[\ell_r(Yf(X))]\,. \tag{15}$$

Then with probability at least $1-\delta$*,*

$$L(\hat{f}, P) - L(f^*, P) \leq \frac{4BR + \sqrt{2\log 2/\delta}}{\sqrt{n}}\,. \tag{16}$$

This lemma bounds the generalization error of a regularized linear classifier. The detailed proof is given in appendix, which follows the general analysis with Rademacher complexity.

Lemma 9. *If* f *is a linear model with* $\|w\| < R$*,* $\rho(P, Q) = \rho < \frac{1}{R}$*, and the class priors on* P *and* Q *are the same, i.e.,* $P(Y) = Q(Y)$*, then* $Err(f, Q) \leq \frac{2}{1-\rho R} L(f, P)$*.*

This lemma tells us that if we train a linear classifier f on P, the error rate on Q can be bounded by the ramp loss on P, even if the ramp loss $L(f, Q)$ can be large. Intuitively, since the shift between P and Q is small, and f is a large margin classifier trained on P, the sample from Q may go into the soft margin of f but is not likely to go across the border. The proof is given in appendix.

Lemma 10. *Given random variables* X*,* Y*,* Y' *with joint distribution* P*, where* X *denotes the instance, and* Y *and* Y' *denote the ground truth labels and the pseudo labels. If the probability of the pseudo label being incorrect* $P(Y \neq Y') \leq \epsilon$*, then for any* $f(x) = w^\top x + b$*, we have that* $L(f, P_X P_{Y|X}) < L(f, P_X P_{Y'|X}) + \epsilon$*.*

This lemma tells that if the pseudo labels have small error w.r.t. the true labels, then we can learn a classifier with low ramp loss by fitting the pseudo labels. The proof is given in appendix.

Theorem 11. *Given two distributions* P*,* Q *with* $\rho(P, Q) = \rho < \frac{1}{R}$*, and the class priors are the same, i.e.,* $P(Y) = Q(Y)$*. Let* f *be the pseudo-labeler model which is learned on pseudo-labeled distribution* $P_X P_{Y'|X}$ *with error probability* $P(Y \neq Y') \leq \epsilon$*. Then about the error of new pseudo labels on* Q *we have*

$$Err(f, Q) \leq \frac{2}{1-\rho R}(\alpha^* + \epsilon + \frac{4BR + \sqrt{2\log 2/\delta}}{\sqrt{n}})\,. \tag{17}$$

This theorem can be easily proved by combining the previous lemmas, and the detailed proof is given in appendix. This theorem tells us that by training a pseudo-labeler with data on P and pseudo-label with small error, the error rate of the pseudo-labels on Q can be bounded. With this theorem, we can bound the error rate of the pseudo labels at any step as follows.

Corollary 12. *Suppose* $(P^{(t)}, Q^{(t)})$ *for* $t = [T]$ *are selected component distributions that satisfy class balance, small shift, and linear separation. Letting* $\gamma = \frac{2}{1-\rho R}$*, then at step t, the new pseudo labels' error rate is bounded:*

$$Err(f^{(t)}, Q^{(t)}) \leq \gamma^t \left(\alpha^* + \frac{4BR + \sqrt{2\log 2/\delta}}{\sqrt{n}}\right). \tag{18}$$

4 Practical Implementation

In this section, we give a practical implementation of the framework in the agnostic scenario. The detailed algorithm description is shown in Algorithm 2.

Subset selection. We here describe how to find the instance set $\tilde{D}_{PL}^{(t)} \sim P^{(t)}$ for training and $\tilde{D}_U^{(t)} \sim Q^{(t)}$ for pseudo-labeling. The problem of finding such subsets with bounded W_∞ distance from two discrete distributions naturally corresponds to the problem of bipartite matching of instance pairs with a maximum distance limitation. We run bipartite graph matching between the pseudo-labeled and unlabeled data with edges between the nodes (x_L, x_U) that $d(x_L, x_U) < \delta$. The matched instances have empirical Wasserstein distance no larger than δ. If the base models are linear classifiers, an extra linear model $f_0(x) = w_0^\top x + b_0$ is trained on the pseudo-labels of the matched instances. By selecting an equal number of positive and negative instances with margin $\hat{y} f_0(x)$ from large to small while keeping $f_0(x_P) > f_0(x_N)$, we obtain a linear separable, class balanced training set $\tilde{D}_{PL}^{(t)}$. If the base models are deep models, we skip this step as deep models have stronger ability of fitting to separate the selected distribution. The pseudo-labeler model $f^{(t)}$ is then trained on $\tilde{D}_{PL}^{(t)}$ to enforce the margin on the training set. If the deep model is used, the model can be pre-trained on all pseudo-labels and then fine-tuned on the selected $\tilde{D}_{PL}^{(t)}$, as the pre-trainings will not decrease but may increase the generalization of the model on $Q^{(t)}$. The unlabeled instances in $\tilde{D}_U^{(t)}$ are fed into $f^{(t)}$, those predictions with large margin $|f^{(t)}(x_U)| > \theta$ will be accepted as pseudo-labeled data $\tilde{D}_U^{(t)}$.

Dynamic hyper-parameter choosing. The small-paced self-training requires the setting of hyper-parameter δ. Intuitively, δ controls the extent of the shift of the training $P^{(t)}$ and test distribution $Q^{(t)}$, and the smaller the distribution shifts, the better the model generalizes on $Q^{(t)}$. However, a small δ decreases the size of $\tilde{D}_{PL}^{(t)}$, making the model performance unreliable. To find a proper δ, we search from small to large in some interval $[\delta_-, \delta_+]$ containing δ. We start the algorithm from some small δ, and perform self-training only if the size of $\tilde{D}_{PL}^{(t)}$ reaches a lower limit number of instances. If the training data is too few, the δ is increased by a small step, and then the small-paced self-training algorithm continues. Notice that with δ going up, the geometric margin we require the pseudo labels also goes up correspondingly, thus the risk of introducing error is low. Generally, for datasets with normalized features, we search δ in $[0.1, 0.5]$.

Algorithm 2: Small-Paced Self-Training Algorithm

Let $t = 1$.
repeat
  Select $(\tilde{D}_{PL}^{(t)}, \tilde{D}_{U}^{(t)})$ by bipartite matching of $\big(D_{PL}^{(t)}, D_{U}^{(t)}, \{(x_L, x_U) | \|x_L - x_U\| < \delta\}\big)$.
  if $|\tilde{D}_{PL}^{(t)}| < n$ **then** increase δ, continue.
  (Deep Base Model) Pre-train $f^{(t)}$ with all pseudo-labeled data $D_{PL}^{(t)}$.
  (Deep Base Model) Fine-tune $f^{(t)}$ on $\tilde{D}_{PL}^{(t)}$.
  (Linear Base Model) Train $f^{(t)}$ on $\tilde{D}_{PL}^{(t)}$ with ramp loss and regularization $\|w\| < R$.
  Reject unconfident $\{x_U | f(x_U) < \theta\}$ from $\tilde{D}_{U}^{(t)}$, accept the reminder as the pseudo-labels.
  if $|\tilde{D}_{U}^{(t)}| = 0$ **then** decrease θ.
  Let $t \leftarrow t + 1$.
until No unlabeled data remaining.

Method	ACC	AUC	F1
MeanTeacher	0.902 (5.5%↓)	0.912 (4.3%↓)	0.887 (5.9%↓)
MixMatch	0.809 (9.4%↓)	0.833 (8.1%↓)	0.799 (9.2%↓)
FixMatch	0.966 (0.4%↓)	**0.967** (**0.5%**↓)	0.958 (**0.5%**↓)
CST	0.953 (0.5%↓)	0.953 (0.6%↓)	0.942 (0.6%↓)
Self-Training	0.921 (5.6%↓)	0.923 (5.1%↓)	0.917 (5.5%↓)
Small-Paced Self-Training (L)	0.919 (3.6%↓)	0.925 (2.8%↓)	0.942 (4.0%↓)
Small-Paced Self-Training (D)	**0.973** (**0.2%**↓)	**0.967** (**0.5%**↓)	**0.961** (0.8%↓)

Table 1: Results of the methods on CIFAR10 dataset. The leading numbers are the performance under support isolation, and the numbers in brackets are the percentage of the degradation, compared to the no-support-isolation case.

Method	ACC	AUC	F1
MeanTeacher	0.774 (2.5%↓)	0.737 (3.7%↓)	0.650 (6.3%↓)
MixMatch	0.755 (**0.0%**↓)	0.724 (1.2%↓)	0.639 (2.0%↓)
FixMatch	0.783 (0.6%↓)	0.749 (0.7%↓)	0.672 (0.6%↓)
CST	0.763 (0.7%↓)	0.718 (1.5%↓)	0.626 (2.6%↓)
Self-Training	0.744 (0.6%↓)	0.653 (1.5%↓)	0.485 (3.6%↓)
Small-Paced Self-Training (L)	0.778 (0.8%↓)	0.760 (**0.4%**↓)	0.687 (**0.4%**↓)
Small-Paced Self-Training (D)	**0.796** (1.6%↓)	**0.768** (1.1%↓)	**0.697** (1.6%↓)

Table 2: Results of the methods on X-ray image classification task. The leading numbers are the performance under support isolation, and the numbers in brackets are the percentage of the degradation, compared to the no-support-isolation case.

5 Experiments

We verify the proposed small-paced self-training algorithm with linear base models (L) and deep base models (D), against several baselines on semi-supervised learning: **Mean Teacher** (Tarvainen and Valpola 2017), a semi-supervised learning approach that leverages the consistency of model outputs over different timestamp of the whole training. **MixMatch** (Berthelot et al. 2019), a holistic deep semi-supervised learning approach that combines multiple components from different SSL diagrams. **FixMatch** (Sohn et al. 2020), another recent holistic approach that combines consistency regularization and pseudo-labeling, which shown great ability on semi-supervised tasks. **Cycle Self-Training** (Liu, Wang, and Long 2021), a self-training variety designed for domain adaptation. Last, we compare standard **Self-Training** (Lee 2013) to show the small-paced restriction helps the learning process in our setup. All methods adopt ResNet-50 pre-trained on imagenet as the backbone; Small-Paced Self-Training (ours) and standard Self-training are not using image augmentation as the other methods do.

We compare the methods on commonly used `CIFAR10`, `CIFAR100` (Krizhevsky 2009) dataset and real-world X-ray pneumonia identification task (Kermany et al. 2018), which we refer to as `Pneumonia` hereinafter. On `CIFAR10`, we simulate the situation that we want to build a model to identify vehicles against animals, but the label collecting process is affected by a filter model built on automobile and dog images. Such situations commonly occur when we want to build a model for identification of some interesting object in real-world, but only has limited data to train an imperfect model at the start. For the pneumonia identification task, the X-ray images are collected from healthy children and children with pneumonia. The task is to identify the virus pneumonia patients, where the labeled data comes from the

patients who are formerly diagnosed with bacterial pneumonia. We describe the details of the datasets in appendix due to the tight space.

Performance under support isolation. The experimental results on `CIFAR10` and `Pneumonia` are shown in Tables 1 and 2. The results on `CIFAR100` are reported in appendix due to the page limit. It can be observed that Small-Paced Self-Training outperforms the baseline approaches when support isolation occurs in the datasets even without data augmentation techniques. The Small-Paced Self-Training algorithm with deep base models achieves better performance than using the linear models, while both algorithms achieve strong performance.

Impact of the support isolation. Yet the effect of the filtering mechanism can be regarded as some sort of distribution mismatch of the labeled and unlabeled data, the problem we try to address in this paper is one of the most severe cases. The main obstacle is that the support of the labeled data cannot cover the unlabeled data. To demonstrate the difficulty induced by the support isolation, we alter the `CIFAR10` and `Pneumonia` dataset used in the previous experiment by adding labels of 5% unlabeled data selected at random and removing the labels of the identical amount of labeled data. We denote this altered experiment setup as the *no-support-isolation* case. As the label rate remains unchanged and both labeling setup suffers from huge selection bias, ordinary semi-supervised learning approaches are affected hugely by the change of the distribution support. In Tables 1 and 2, we report the performance degradation when support isolation happens, compared to no support isolation case. The full results of the no-support-isolation case is contained in appendix. The Small-Paced Self-Training algorithms are shown to be impacted less from the support isolation problem than the standard self-training. Notice that Small-Paced Self-Training algorithms do not leverage image augmentation and consistency regularization techniques like all of the other baselines do, which are shown to be powerful for image-related tasks. The low performance degradation shows the effectiveness of the small-paced restriction.

6 Related Work

Semi-supervised learning (Chapelle, Schlkopf, and Zien 2006; Zhu et al. 2009) aims to improve learning by utilizing unlabeled data, traditionally can be classified as generative models (Shahshahani and Landgrebe 1994; Nigam et al. 2000), low density separation based methods (Joachims 1999; Chapelle, Chi, and Zien 2006; Li, Kwok, and Zhou 2010), graph based methods (Blum and Chawla 2001; Zhu, Ghahramani, and Lafferty 2003), and disagreement based methods (Blum and Mitchell 1998; Zhou and Li 2005). With the rise of deep neural networks in recent years, new approaches are proposed to exploit the power of stronger models for more challenging tasks. Consistency regularization methods are based on the concept that specific types of perturbations applied to an unlabeled instance should not change the model prediction (Rasmus et al. 2015; Zhang et al. 2018). Entropy minimization methods encourage the models to make confident predictions to avoid the decision boundary going near dense regions (Grandvalet and Bengio 2005). Deep generative models try to recover the data distribution for better feature learning (Kingma et al. 2014; Kumar, Sattigeri, and Fletcher 2017). Graph neural networks exploit the graphical structure of the data with neural networks (Scarselli et al. 2008; Kipf and Welling 2017; Li et al. 2016). Holistic models like MixMatch, FixMatch unify multiple strategies and components to achieve strong performance (Berthelot et al. 2019; Sohn et al. 2020).

The problem we address in this paper is also related to, yet different from, domain adaptation (Pan and Yang 2010), sample selection bias (Zadrozny 2004), and covariate shift (Shimodaira 2000). Domain adaptation aims to align source and target domains into one common representation space, so that the labeled source data can be helpful for building a model for the target domain without target label (Hoffman et al. 2018; Zhao et al. 2019; Li et al. 2020). Literature on sample selection bias and covariate shift problems employ importance reweighting or other techniques to compensate for the distribution density shift (Zadrozny 2004; Liu and Ziebart 2014; Shimodaira 2000; Sugiyama, Krauledat, and Müller 2007).

Self-training, also known as pseudo-labeling, is a type of method that trains models according to the previous prediction on the unlabeled data (Lee 2013; Grandvalet and Bengio 2005). It is drawing increasing attention, as it shows great effectiveness in semi-supervised learning, domain adaptation, and other related tasks (Sohn et al. 2020; French, Mackiewicz, and Fisher 2018; Hu et al. 2017). Though the idea of self-training can date back a very long time, there is little progress in the theoretical understanding of self-training type of algorithms until recent years. Kumar, Ma, and Liang (2020) conducted theoretical analysis for self-training of linear models in the scenario of gradual domain adaptation. Wei et al. (2021) theoretically analyzed the self-training with input-consistency regularization, provided improved understanding for applying self-training algorithms with deep learning models.

7 Conclusion

We study the semi-supervised learning problem where the label missing is caused by a proceeding filtering mechanism. Such filtering mechanism dominated label collecting process leads to the isolation of the support of the labeled and unlabeled data distributions, making the problem more difficult than usual. In this case, the standard self-training approach suffers from overconfidence on instances far away from the current knowledge boundary. We propose Small-Paced Self-Training to tackle this problem, which gradually pushes the knowledge boundary. We show that by leveraging a small-paced restriction, the algorithm can produce reliable pseudo labels on the overall dataset. The provided selection algorithm may not be the only way to enjoy the theoretical guarantee, there might be more effective algorithms being developed based on the idea of limiting the distributional distance for self-training.

Acknowledgements

This research was supported by NSFC (62076121, 61921 006).

References

Ben-David, S.; Blitzer, J.; Crammer, K.; Kulesza, A.; Pereira, F.; and Vaughan, J. W. 2010. A Theory of Learning from Different Domains. *Machine Learning*, 79(1-2): 151–175.

Ben-David, S.; and Urner, R. 2012. On the Hardness of Domain Adaptation and the Utility of Unlabeled Target Samples. In *23rd International Conference on Algorithmic Learning Theory*, volume 7568 of *Lecture Notes in Computer Science*, 139–153.

Bennett, K.; and Demiriz, A. 1999. Semi-Supervised Support Vector Machines. In *Advances in Neural Information Processing Systems*, volume 11.

Berthelot, D.; Carlini, N.; Goodfellow, I.; Papernot, N.; Oliver, A.; and Raffel, C. A. 2019. MixMatch: A Holistic Approach to Semi-Supervised Learning. In *Advances in Neural Information Processing Systems*, volume 32.

Blum, A.; and Chawla, S. 2001. Learning from Labeled and Unlabeled Data Using Graph Mincuts. In *Proceedings of the 18th International Conference on Machine Learning*, 19–26.

Blum, A.; and Mitchell, T. 1998. Combining Labeled and Unlabeled Data with Co-training. In *Proceedings of the Eleventh Annual Conference on Computational Learning Theory*, 92–100.

Chapelle, O.; Chi, M.; and Zien, A. 2006. A Continuation Method for Semi-Supervised SVMs. In *Proceedings of the Twenty-Third International Conference on Machine Learning*, 185–192.

Chapelle, O.; Schlkopf, B.; and Zien, A. 2006. *Semi-Supervised Learning*. The MIT Press.

Elsayed, G.; Krishnan, D.; Mobahi, H.; Regan, K.; and Bengio, S. 2018. Large Margin Deep Networks for Classification. In *Advances in Neural Information Processing Systems*, volume 31.

French, G.; Mackiewicz, M.; and Fisher, M. 2018. Self-Ensembling for Visual Domain Adaptation. In *International Conference on Learning Representations*.

Grandvalet, Y.; and Bengio, Y. 2005. Semi-supervised Learning by Entropy Minimization. In *Advances in Neural Information Processing Systems*, volume 17.

Hoffman, J.; Tzeng, E.; Park, T.; Zhu, J.; Isola, P.; Saenko, K.; Efros, A. A.; and Darrell, T. 2018. CyCADA: Cycle-Consistent Adversarial Domain Adaptation. In *Proceedings of the 35th International Conference on Machine Learning*, volume 80, 1994–2003.

Hu, W.; Miyato, T.; Tokui, S.; Matsumoto, E.; and Sugiyama, M. 2017. Learning Discrete Representations via Information Maximizing Self-Augmented Training. In *Proceedings of the 34th International Conference on Machine Learning*, 1558–1567.

Huang, J.; Smola, A. J.; Gretton, A.; Borgwardt, K. M.; and Schölkopf, B. 2006. Correcting Sample Selection Bias by Unlabeled Data. In *Advances in Neural Information Processing Systems*, 601–608.

Joachims, T. 1999. Transductive Inference for Text Classification Using Support Vector Machines. In *Proceedings of the 16th International Conference on Machine Learning*, 200–209.

Johansson, F. D.; Sontag, D. A.; and Ranganath, R. 2019. Support and Invertibility in Domain-Invariant Representations. In *The 22nd International Conference on Artificial Intelligence and Statistics*, volume 89, 527–536.

Kermany, D. S.; et al. 2018. Identifying Medical Diagnoses and Treatable Diseases by Image-Based Deep Learning. *Cell*, 172(5): 1122–1131.e9.

Kingma, D. P.; Mohamed, S.; Jimenez Rezende, D.; and Welling, M. 2014. Semi-supervised Learning with Deep Generative Models. In *Advances in Neural Information Processing Systems*, volume 27.

Kipf, T. N.; and Welling, M. 2017. Semi-Supervised Classification with Graph Convolutional Networks. In *International Conference on Learning Representations*.

Krizhevsky, A. 2009. Learning Multiple Layers of Features from Tiny Images. Technical report.

Kumar, A.; Ma, T.; and Liang, P. 2020. Understanding Self-Training for Gradual Domain Adaptation. In *Proceedings of the 37th International Conference on Machine Learning*, volume 119, 5468–5479.

Kumar, A.; Sattigeri, P.; and Fletcher, T. 2017. Semi-supervised Learning with GANs: Manifold Invariance with Improved Inference. In *Advances in Neural Information Processing Systems*, volume 30.

Lee, D. 2013. Pseudo-Label: The Simple and Efficient Semi-Supervised Learning Method for Deep Neural Networks. In *Workshop on challenges in representation learning, ICML*.

Li, B.; Wang, Y.; Che, T.; Zhang, S.; Zhao, S.; Xu, P.; Zhou, W.; Bengio, Y.; and Keutzer, K. 2020. Rethinking Distributional Matching Based Domain Adaptation. *arXiv preprint arXiv:2006.13352*.

Li, Y.; Tarlow, D.; Brockschmidt, M.; and Zemel, R. 2016. Gated Graph Sequence Neural Networks. In *International Conference on Learning Representations*.

Li, Y.-F.; Kwok, J. T.; and Zhou, Z.-H. 2010. Cost-sensitive Semi-Supervised Support Vector Machine. In *Proceedings of the Twenty-Fourth AAAI Conference on Artificial Intelligence*, 500–505.

Liu, A.; and Ziebart, B. 2014. Robust Classification Under Sample Selection Bias. In *Advances in Neural Information Processing Systems*, volume 27.

Liu, H.; Wang, J.; and Long, M. 2021. Cycle Self-Training for Domain Adaptation. In *Advances in Neural Information Processing Systems*, volume 34, 14.

Nigam, K.; McCallum, A. K.; Thrun, S.; and Mitchell, T. 2000. Text Classification from Labeled and Unlabeled Documents Using EM. *Machine Learning*, 39(2): 103–134.

Pan, S. J.; and Yang, Q. 2010. A Survey on Transfer Learning. *IEEE Transactions on Knowledge and Data Engineering*, 22(10): 1345–1359.

Prabhu, V.; Khare, S.; Kartik, D.; and Hoffman, J. 2020. SENTRY: Selective Entropy Optimization via Committee Consistency for Unsupervised Domain Adaptation. *CoRR*, abs/2012.11460.

Qu, X.; Zou, Z.; Cheng, Y.; Yang, Y.; and Zhou, P. 2019. Adversarial Category Alignment Network for Cross-domain Sentiment Classification. In *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics*.

Quiñonero-Candela, J.; Sugiyama, M.; Schwaighofer, A.; and Lawrence, N. D., eds. 2008. *Dataset Shift in Machine Learning*. The MIT Press.

Rasmus, A.; Berglund, M.; Honkala, M.; Valpola, H.; and Raiko, T. 2015. Semi-supervised Learning with Ladder Networks. In *Advances in Neural Information Processing Systems*, volume 28.

Scarselli, F.; Gori, M.; Tsoi, A. C.; Hagenbuchner, M.; and Monfardini, G. 2008. The Graph Neural Network Model. *IEEE Transactions on Neural Networks*, 20(1): 61–80.

Shahshahani, B. M.; and Landgrebe, D. A. 1994. The Effect of Unlabeled Samples in Reducing the Small Sample Size Problem and Mitigating the Hughes Phenomenon. *IEEE Transactions on Geoscience and Remote Sensing*, 32(5): 1087–1095.

Shimodaira, H. 2000. Improving Predictive Inference under Covariate Shift by Weighting the Log-Likelihood Function. *Journal of Statistical Planning and Inference*, 90(2): 227–244.

Shu, R.; Bui, H. H.; Narui, H.; and Ermon, S. 2018. A DIRT-T Approach to Unsupervised Domain Adaptation. In *International Conference on Learning Representations*.

Sohn, K.; Berthelot, D.; Carlini, N.; Zhang, Z.; Zhang, H.; Raffel, A. C.; Cubuk, D. E.; Kurakin, A.; and Li, C.-L. 2020. FixMatch: Simplifying Semi-Supervised Learning with Consistency and Confidence. In *Advances in Neural Information Processing Systems*, volume 33.

Sugiyama, M.; Krauledat, M.; and Müller, K.-R. 2007. Covariate Shift Adaptation by Importance Weighted Cross Validation. *Journal of Machine Learning Research*, 8(35): 985–1005.

Tarvainen, A.; and Valpola, H. 2017. Mean Teachers are Better Role Models: Weight-Averaged Consistency Targets Improve Semi-Supervised Deep Learning Results. In *Advances in Neural Information Processing Systems*, volume 30.

Wei, C.; Shen, K.; Chen, Y.; and Ma, T. 2021. Theoretical Analysis of Self-Training with Deep Networks on Unlabeled Data. In *International Conference on Learning Representations*.

Xie, S. M.; Kumar, A.; Jones, R.; Khani, F.; Ma, T.; and Liang, P. 2021. In-N-Out: Pre-Training and Self-Training using Auxiliary Information for Out-of-Distribution Robustness. In *International Conference on Learning Representations*.

Zadrozny, B. 2004. Learning and Evaluating Classifiers under Sample Selection Bias. In *Proceedings of the 21st International Conference on Machine Learning*, 114.

Zhang, H.; Cisse, M.; Dauphin, Y. N.; and Lopez-Paz, D. 2018. mixup: Beyond Empirical Risk Minimization. In *International Conference on Learning Representations*.

Zhao, H.; des Combes, R. T.; Zhang, K.; and Gordon, G. J. 2019. On Learning Invariant Representations for Domain Adaptation. In *Proceedings of the 36th International Conference on Machine Learning*, volume 97, 7523–7532.

Zhou, Z.-H.; and Li, M. 2005. Tri-Training: Exploiting Unlabeled Data Using Three Classifiers. *IEEE Transactions on Knowledge and Data Engineering*, 17(11): 1529–1541.

Zhu, X.; Ghahramani, Z.; and Lafferty, J. 2003. Semi-Supervised Learning Using Gaussian Fields and Harmonic Functions. In *Proceedings of the 20th International Conference on Machine Learning*, 912–919.

Zhu, X.; Goldberg, A. B.; Brachman, R.; and Dietterich, T. 2009. *Introduction to Semi-Supervised Learning*. Morgan and Claypool Publishers.