A Survey on Deep Semi-supervised Learning

Xiangli Yang, Zixing Song, Irwin King, Fellow, IEEE, Zenglin Xu, Senior Member, IEEE

Abstract—Deep semi-supervised learning is a fast-growing field with a range of practical applications. This paper provides a comprehensive survey on both fundamentals and recent advances in deep semi-supervised learning methods from perspectives of model design and unsupervised loss functions. We first present a taxonomy for deep semi-supervised learning that categorizes existing methods, including deep generative methods, consistency regularization methods, graph-based methods, pseudo-labeling methods, and hybrid methods. Then we provide a comprehensive review of 52 representative methods and offer a detailed comparison of these methods in terms of the type of losses, contributions, and architecture differences. In addition to the progress in the past few years, we further discuss some shortcomings of existing methods and provide some tentative heuristic solutions for solving these open problems.

Index Terms—Deep semi-supervised learning, image classification, machine learning, survey

1 INTRODUCTION

Deep learning has been an active research field with abundant applications in pattern recognition [1], [2], data mining [3], statistical learning [4], computer vision [5], [6], natural language processing [7], [8], etc. It has achieved great successes in both theory and practice [9], [10], especially in supervised learning scenarios, by leveraging a large amount of high-quality labeled data. However, labeled samples are often difficult, expensive, or time-consuming to obtain. The labeling process usually requires experts’ efforts, which is one of the major limitations to train an excellent fully-supervised deep neural network. For example, in medical tasks, the measurements are made with expensive machinery, and labels are drawn from a time-consuming analysis of multiple human experts. If only a few labeled samples are available, it is challenging to build a successful learning system. By contrast, the unlabeled data is usually abundant and can be easily or inexpensive obtained. Consequently, it is desirable to leverage a large number of unlabeled data for improving the learning performance given a small number of labeled samples. For this reason, semi-supervised learning (SSL) has been a hot research topic in machine learning in the last decade [11], [12].

SSL is a learning paradigm associated with constructing models that use both labeled and unlabeled data. SSL methods can improve learning performance by using additional unlabeled instances compared to supervised learning algorithms, which can use only labeled data. It is easy to obtain SSL algorithms by extending supervised learning algorithms or unsupervised learning algorithms. SSL algorithms provide a way to explore the latent patterns from unlabeled examples, alleviating the need for a large number of labels [13]. Depending on the key objective function of the systems, one may have a semi-supervised classification, a semi-supervised clustering, or a semi-supervised regression. We provide the definitions as follows:

- **Semi-supervised classification.** Given a training dataset that consists of both labeled instances and unlabeled instances, semi-supervised classification aims to train a classifier from both the labeled and unlabeled data, such that it is better than the supervised classifier trained only on the labeled data.
- **Semi-supervised clustering.** Given a training dataset that consists of unlabeled instances, and some supervised information about the clusters, the goal of semi-supervised clustering is to obtain better clustering than the clustering from unlabeled data alone. Semi-supervised clustering is also known as constrained clustering.
- **Semi-supervised regression.** Given a training dataset that consists of both labeled instances and unlabeled instances, the goal of semi-supervised regression is to improve the performance of a regression algorithm from a regression algorithm with labeled data alone, which predicts a real-valued output instead of a class label.

In order to explain SSL clearly and concretely, we focus on the problem of image classification. The ideas described in this survey can be adapted without difficulty to other situations, such as object detection, semantic segmentation, clustering, or regression. Therefore, we primarily review image classification methods with the aid of unlabeled data in this survey.

Since the 1970s when the concept of SSL first came to the fore [14], [15], [16], there have been a wide variety of SSL methods, including generative models [17], [18], semi-supervised support vector machines [19], [20], [21], [22], graph-based methods [23], [24], [25], [26], and co-training [27]. We refer interested readers to [12], [28], which pro-
provide a comprehensive overview of traditional SSL methods. Nowadays, deep neural networks have played a dominating role in many research areas. It is important to adopt the classic SSL framework and develop novel SSL methods for deep learning settings, which leads to deep semi-supervised learning (DSSL). DSSL studies how to effectively utilize both labeled and unlabeled data by deep neural networks. A considerable amount of DSSL methods have been proposed. According to the most distinctive features in semi-supervised loss functions and model designs, we classify DSSL into five categories, i.e., generative methods, consistency regularization methods, graph-based methods, pseudo-labeling methods, and hybrid methods. The overall taxonomy used in this literature is shown in Fig. 1.

Some representative works of SSL were described in the early survey [12, 28], however, emerging technologies based on deep learning, such as adversarial training which generates new training data for SSL, have not been included. Besides, [13] focuses on unifying the evaluation indices of SSL, and [29] only reviews generative models and teacher-student models in SSL without making a comprehensive overview of SSL. Although [30] tries to present a whole picture of SSL, the taxonomy is quite different from ours. A recent review by Ouali et al. [31] gives a similar notion of DSSL as we do. However, it does not compare the presented methods based on their taxonomy and provide perspectives on future trends and existing issues. Summarizing both previous and the latest research on SSL, we survey the fundamental theories and compare the deep semi-supervised methods. In summary, our contributions are listed as follows.

- We provide a detailed review of DSSL methods and introduce a taxonomy of major DSSL methods, background knowledge, and various models. One can quickly grasp the frontier ideas of DSSL.
- We categorize DSSL methods into several categories, i.e., generative methods, consistency regularization methods, graph-based methods, pseudo-labeling methods, and hybrid methods, with particular genres inside each one. We review the variants on each category and give standardized descriptions and unified sketch maps.
- We identify several open problems in this field and discuss the future direction for DSSL.

This survey is organized as follows. In Section 2, we introduce SSL background knowledge, including assumptions in SSL, classical SSL methods, related concepts, and datasets used in various applications. Section 3 to Section 7 introduce the primary deep semi-supervised techniques, i.e., generative methods in Section 3, consistency regularization methods in Section 4, graph-based methods in Section 5, pseudo-labeling methods in Section 6, and hybrid methods in Section 7. In Section 8, we discuss the challenges in semi-supervised learning and provide some heuristic solutions and future directions for these open problems.

2 Background

Before presenting an overview of the techniques of SSL, we first introduce the notations. To illustrate the DSSL framework, we limit our focus on the single-label classification tasks which are simple to describe and implement. We refer interested readers to [32, 33, 34] for multi-label classification tasks. Let $X = \{X_L, X_U\}$ denote the entire data set, including a small labeled subset $X_L = \{x_i\}_{i=1}^{L}$ with labels $Y_L = \{y_1, y_2, \ldots, y_L\}$ and a large scale unlabeled subset $X_U = \{x_i\}_{i=1}^{U}$, and generally we assume $L \ll U$. We assume that the dataset contains $K$ classes and the first $L$ examples within $X$ are labeled by $\{y_i\}_{i=1}^{L} \in \{y^1, y^2, \ldots, y^K\}$. Formally, SSL aims to solve the following optimization problem:

$$
\min_{\theta} \sum_{x \in X_L, y \in Y_L} \mathcal{L}_s(x, y; \theta) + \alpha \sum_{x \in X_U} \mathcal{L}_u(x; \theta) + \beta \sum_{x \in X} \mathcal{R}(x; \theta),
$$

(1)

where $\mathcal{L}_s$ denotes the per-example supervised loss, e.g., cross-entropy for classification, $\mathcal{L}_u$ denotes the per-example unsupervised loss, and $\mathcal{R}$ denotes the per-example regularization, e.g., consistency loss or a designed regularization term. Note that unsupervised loss terms are often not strictly distinguished from regularization terms, as regularization terms are normally not guided by label information. Lastly, $\theta$ denotes the model parameters and $\alpha, \beta \in \mathbb{R}_{> 0}$ denotes the trade-off. Different choices of the unsupervised loss functions and regularization terms lead to different semi-supervised models. Note that we do not make a clear distinction between unsupervised loss and regularization.
terms in many cases. Unless particularly specified, the notations used in this paper are illustrated in TABLE 1.

Regarding whether test data are wholly available in the training process, semi-supervised learning can be classified into two settings: the transductive setting and the inductive learning setting. Transductive learning assumes that the unlabeled samples in the training process are exactly the data to be predicted, and the purpose of the transductive learning is to generalize over these unlabeled samples, while inductive learning supposes that the learned semi-supervised classifier will be still applicable to new unseen data. In fact, most graph-based methods are transductive while most other kinds of SSL methods are inductive.

2.1 Assumptions for semi-supervised learning

SSL aims to predict more accurately with the aid of unlabeled data than supervised learning that uses only labeled data. However, an essential prerequisite is that the data distribution should be under some assumptions. Otherwise, SSL may not improve supervised learning and may even degrade the prediction accuracy by misleading inferences. Following [12] and [28], the related assumptions in SSL include:

Self-training assumption. The predictions of the self-training model, especially those with high confidence, tend to be correct. We can assume that when the hypothesis is satisfied, those high-confidence predictions are considered to be ground-truth. This can happen when classes form well-separated clusters.

Co-training assumption. Different reasonable assumptions lead to different combinations of labeled and unlabeled data, and accordingly, different algorithms are designed to take advantage of these combinations. For example, Blum et al. [27] proposed a co-training model, which works under the assumptions: instance $x$ has two conditionally independent views, and each view is sufficient for a classification task.

Generative model assumption. Generally, it is assumed that data are generated from a mixture of distributions. When the number of mixed components, a prior $p(y)$ and a conditional distribution $p(x|y)$ are correct, data can be assumed to come from the mixed model. This assumption suggests that if the generative model is correct enough, we can establish a valid link between the distribution of unlabeled data and the category labels by $p(x, y) = p(y)p(x|y)$.

Cluster assumption. If two points $x_1$ and $x_2$ are in the same cluster, they should belong to the same category [28]. This assumption refers to the fact that data in a single class tend to form a cluster, and when the data points can be connected by short curves that do not pass through any low-density regions, they belong to the same class cluster [28]. According to this assumption, the decision boundary should not cross high-density areas but instead lie in low-density regions [28]. Therefore, the learning algorithm can use a large amount of unlabeled data to adjust the classification boundary.

Low-density separation. The decision boundary should be in a low-density region, not through a high-density area [28]. The low-density separation assumption is closely related to the cluster assumption. We can consider the clustering assumption from another perspective by assuming that the class is separated by areas of low density [28]. Since the decision boundary in a high-density region would cut a cluster into two different classes and within such a part would violate the cluster assumption.

Manifold assumption. If two points $x_1$ and $x_2$ are located in a local neighborhood in the low-dimensional manifold, they have similar class labels [28]. This assumption reflects the local smoothness of the decision boundary. It is well known that one of the problems of machine learning algorithms is the curse of dimensionality. It is hard to estimate the actual data distribution when volume grows exponentially with the dimensions in high dimensional spaces. If the data lie on a low-dimensional manifold, the learning algorithms can avoid the curse of dimensionality and operate in the corresponding low-dimension space.

2.2 Classical Semi-supervised learning Methods

In the following, we briefly introduce some representative SSL methods motivated from the above described assumptions.

In the 1970s, the concept of SSL first came to the fore [14], [15], [16]. Perhaps the earliest method has been established as self-learning — an iterative mechanism that uses initial labeled data to train a model to predict some unlabeled samples. Then the most confident prediction is marked as the best prediction of the current supervised model, thus providing more training data for the supervised algorithm, until all the unlabeled examples have been predicted.

Co-training [27] provides a similar solution by training two different models on two different views. Confident
predictions of one view are then used as labels for the other model. More relevant literature of this method also includes [36], [37], [38], etc.

Generative models assume a model \( p(x, y) = p(y)p(x|y) \), where the density function \( p(x|y) \) is an identifiable distribution, for example, polynomial, Gaussian mixture distribution, etc., and the uncertainty is the parameters of \( p(x|y) \). Generative models can be optimized by using iterative algorithms. [17], [18] apply EM algorithm for classification. They compute the parameters of \( p(x|y) \) and then classify unlabeled instances according to the Bayesian full probability formula. Moreover, generative models are harsh on some assumptions. Once the hypothetical \( p(x|y) \) is poorly matched with the actual distribution, it can lead to classifier performance degradation.

A representative example following the low-density separation principle is Transductive Support Vector Machines (TSVMs) [19], [20], [35], [39], [40]. As regular SVMs, TSVMs optimize the gap between decision boundaries and data points, and then expand this gap based on the distance from unlabeled data to the decision margin. To address the corresponding non-convex optimization problem, a number of optimization algorithms have been proposed. For instance, in [35], a smooth loss function substitutes the hinge loss of the TSVM, and for the decision boundary in a low-density space, a gradient descent technique may be used.

Graph-based methods rely on the geometry of the data induced by both labeled and unlabeled examples. This geometry is represented by an empirical graph \( \mathcal{G} = (V, E) \), where nodes \( V \) represent the training data points with \(|V| = n \) and edges \( E \) represent similarities between the points. By exploiting the graph or manifold structure of data, it is possible to learn with very few labels to propagate information through the graph [23], [24], [25], [26], [41], [42]. For example, Label propagation [41] is to predict the label information of unlabeled nodes from labeled nodes. Each node label propagates to its neighbors according to the similarity. At each step of a propagation, each node updates its label according to its neighbors’ label information. In the label propagation label, the label of the labeled data is fixed so that it propagates the label to the unlabeled data. The label propagation method can be applied to deep learning [43].

2.3 Related Learning Paradigms

There are many learning paradigms that can make use of an extra data source to boost learning performance. Based on the availability of labels or the distribution difference in the extra data source, there are several learning paradigms related to semi-supervised learning.

Transfer learning. Transfer learning [44], [45], [46] aims to apply knowledge from one or more source domains to a target domain in order to improve performance on the target task. In contrast to SSL, which works well under the hypothesis that the training set and the testing set are independent and identically distributed (i.i.d.), transfer learning allows domains, tasks, and distributions used in training and testing to be different but related.

Weakly-supervised learning. Weakly-supervised learning [47] relaxes the data dependence that requires ground-truth labels to be given for a large amount of training data set in strong supervision. There are three types of weakly supervised data: incomplete supervised data, inexact supervised data, and inaccurate supervised data. Incomplete supervised data means only a subset of training data is labeled. In this case, representative approaches are SSL and domain adaptation. Inexact supervised data suggests that the labels of training examples are coarse-grained, e.g., in the scenario of multi-instance learning. Inaccurate supervised data means that the given labels are not always ground-truth, such as in the situation of label noise learning.

Positive and unlabeled learning. Positive and unlabeled (PU) learning [48], [49] is a variant of positive and negative binary classification, where the training data consists of positive samples and unlabeled samples. Each unlabeled instance can be either the positive and negative class. During the training procedure, only positive samples and unlabeled samples are available. We can think of PU learning as a special case of SSL.

Meta-learning. Meta-learning [50], [51], [52], [53], [54], also known as “learning to learn”, aims to learn new skills or adapt to new tasks rapidly with previous knowledge and a few training examples. It is well known that a good machine learning model often requires a large number of samples for training. The meta-learning model is expected to adapt and generalize to new environments that have been encountered during the training process. The adaptation process is essentially a mini learning session that occurs during the test but has limited exposure to new task configurations. Eventually, the adapted model can be trained on various learning tasks and optimized on the distribution of functions, including potentially unseen tasks.

Self-supervised learning. Self-supervised learning [55], [56], [57] has gained popularity due to its ability to prevent the expense of annotating large-scale datasets. It can leverage input data as supervision and use the learned feature representations for many downstream tasks. In this sense, self-supervised learning meets our expectations for efficient learning systems with fewer labels, fewer samples, or fewer trials. Since there is no manual label involved, self-supervised learning can be regarded as a branch of unsupervised learning.

2.4 Datasets and applications

SSL has many applications across different tasks and domains, such as image classification, object detection, semantic segmentation, etc. in the domain of computer vision, and text classification, sequence learning, etc. in the field of Natural Language Processing (NLP). As shown in TABLE 2, we summarize some of the most widely used datasets and representative references according to the applications area. In this survey, we mainly discuss the methods applied to image classification since these methods can be extended to other applications, such as [58] applied consistency training to object detection, [59] modified Semi-GANs to fit the scenario of semantic segmentation. There are many works that have achieved state-of-the-art performance within different applications. Most of these methods share details of the implementation and source code, and we refer the interested readers to a more detailed review of the datasets and corresponding references in TABLE 2.
3 Generative methods

As discussed in Subsection 2.2, generative methods can learn the implicit features of data to better model data distributions. They model the real data distribution from the training dataset and then generate new data with this distribution. In this section, we review the deep generative semi-supervised methods based on the Generative Adversarial Network (GAN) framework and the Variational AutoEncoder (VAE) framework, respectively.

3.1 Semi-supervised GANs

A typical GAN [146] consists of a generator $G$ and a discriminator $D$ (see Fig. 2(2)). The goal of $G$ is to learn a distribution $p_G$ over data $x$ given a prior on input noise variables $p_z(z)$. The fake samples $G(z)$ generated by the generator $G$ are used to confuse the discriminator $D$. The discriminator $D$ is used to maximize the distinction between real training samples $x$ and fake samples $G(z)$. As we can see, $D$ and $G$ play the following two-player minimax game with the value function $V(G,D)$:

$$
\begin{align*}
\min_G \max_D V(D,G) &= \mathbb{E}_{x\sim p(x)}[\log D(x)] \\
& \quad + \mathbb{E}_{z\sim p_z}[\log (1 - D(G(z)))].
\end{align*}
$$

Since GANs can learn the distribution of real data from unlabeled samples, it can be used to facilitate SSL. There are many ways to use GANs in SSL settings. Inspired by [147], we have identified four main themes in how to use GANs for SSL, i.e., (a) re-using the features from the discriminator, (b) using GAN-generated samples to regularize a classifier, (c) learning an inference model, and (d) using samples produced by a GAN as additional training data.

A simple SSL approach is to combine supervised and unsupervised loss during training. [148] demonstrates that a hierarchical representation of the GAN-discriminator is useful for object classification. These findings indicate that a simple and efficient SSL method can be provided by combining an unsupervised GAN value function with a supervised classification objective function, e.g.,

$$
\mathbb{E}_{(x,y)\in X, y \neq \text{true class}} \log D(y|x).
$$

In the following, we review several representative methods of semi-supervised GANs.

CatGAN. Categorical Generative Adversarial Network (CatGAN) [149] modifies the GAN’s objective function to take into account the mutual information between observed examples and their predicted categorical class distributions. In particular, the optimization problem is different from the standard GAN (Eq. (2)). The structure is illustrated in Fig. 2(3). This method aims to learn a discriminator which distinguishes the samples into $K$ categories by labeling $y$ to each $x$, instead of learning a binary discriminator value function. Moreover, in the CatGAN discriminator loss function, the supervised loss is also a cross-entropy term between the predicted conditional distribution $p(y|x,D)$ and the true label distribution of examples. It consists of three parts: (1) entropy $H[p(y|x,D)]$ which to obtain certain category assignment for samples; (2) $H[p(y|G(z), D)]$ for uncertain predictions from generated samples; and (3) the marginal class entropy $H[p(y|D)]$ to uniform usage of all classes. The proposed framework uses the feature space learned by the discriminator for the final learning task. For the labeled data, the supervised loss is also a cross-entropy term between the conditional distribution $p(y|x,D)$ and the samples’ true label distribution.

CCGAN. Context-Conditional Generative Adversarial Networks (CCGAN) [150] is proposed to use an adversarial loss for harnessing unlabeled image data based on image in-painting. The architecture of the CCGAN is shown in Fig. 2(4). The main highlight of this work is context information provided by the surrounding parts of the image. The method trains a GAN where the generator is to generate pixels within a missing hole. The discriminator is to discriminate between the real unlabeled images and these in-painted images. More formally, $m \odot x$ as input to a generator, where $m$ denotes a binary mask to drop out a specified portion of an image and $\odot$ denotes element-wise multiplication. Thus the in-painted image $x_I = (1 - m) \odot x_G + m \odot x$ with generator outputs $x_G = G(m \odot x, z)$. The in-painted examples provided by the generator cause the discrimina-
Improved GAN. There are several methods to adapt GANs into a semi-supervised classification scenario. CAT-GAN [149] forces the discriminator to maximize the mutual information between examples and their predicted class distributions instead of training the discriminator to learn a binary classification. The classifier network can have \((K + 1)\) output units corresponding to \([y_1, y_2, \ldots, y_K, y_{K+1}]\), where the \(y_{K+1}\) represents the outputs generated by \(G\). Similar to SGAN, Improved GAN [151] solves a \((K + 1)\)-class classification problem. The structure of Improved GAN is shown in Fig. 2(5). Real examples for one of the first \(K\) classes and the additional \((K + 1)\)th class consisted of the synthetic images generated by the generator \(G\). This work proposes the improved techniques to train the GANs, i.e., feature matching, minibatch discrimination, historical averaging one-sided label smoothing, and virtual batch normalization, where feature matching is used to train the generator. It is trained by minimizing the discrepancy between features of the real and the generated examples classified to \(K\) real classes. The loss function for training the classifier becomes
\[
\max_D \mathbb{E}_{(x,y) \sim p(x,y)} \log p_D(y|x, y \leq K) + \mathbb{E}_{x \sim p(x)} \log p_D(y = K + 1|x),
\]
(3)
where the first term of Eq. (3) denotes the supervised cross-entropy loss, The last two terms of Eq. (3) are the unsupervised losses from the unlabeled and generated data, respectively.

GoodBadGAN. GoodBadGAN [153] realizes that the generator and discriminator in [152] may not be optimal simultaneously, i.e., the discriminator achieves good performance in SSL, while the generator may generate visually unrealistic samples. The structure of GoodBadGAN is shown in Fig. 2(5). The method gives theoretical justifications of why using bad samples from the generator can boost the SSL performance. Generally, the generated samples, along with the loss function (Eq. (3)), can force the boundary of the discriminator to lie between the data manifolds of different categories, which improves the generalization of the discriminator. Due to the analysis, GoodBadGAN learns a bad generator by explicitly adding a penalty term \(\mathbb{E}_{x \sim p(x)} \log p(x) \mathbb{1}[p(x) > \epsilon]\) to generate bad samples, where \(\mathbb{1}[\cdot]\) is an indicator function and \(\epsilon\) is a threshold, which ensures that only high-density samples are penalized while low-density samples are unaffected. Further, to guarantee the strong true-fake belief in the optimal conditions, a conditional entropy term \(\sum_{k=1}^{K} \log p_D(k|x)\) is added to
the discriminator objective function in Eq. (3).

**Localized GAN.** Localized GAN [154] focuses on using local coordinate charts to parameterize local geometry of data transformations across different locations manifold rather than the global one. This work suggests that Localized GAN can help train a locally consistent classifier by exploring the manifold geometry. The architecture of Localized GAN is shown in Fig. [2](6). Like the methods introduced in [152], [153], Localized GAN attempts to solve the $K + 1$ classification problem that outputs the probability of $x$ being assigned to a class. For a classifier, $\nabla x D(G(x, z))$ depicts the change of the classification decision on the manifold formed by $G(x, z)$, and the evolution of $D(\cdot)$ restricted on $G(x, z)$ can be written as

$$|D(G(x, z + \sigma z)) - D(G(x, z))|^2 \approx \|
abla x D(x)\|^2 \sigma z,$$

which shows that penalizing $\|
abla x D(x)\|^2$ can train a robust classifier with a small perturbation $\sigma z$ on a manifold. This probabilistic classifier can be introduced by adding $\sum_{k=1}^K \mathbb{E}_{x \sim p(x)} \|
abla x \log p(y = k|x)\|^2$, where $\nabla x \log p(y = k|x)$ is the gradient of the log-likelihood along with the manifold $G(x, z)$.

**CT-GAN.** CT-GAN [155] combines consistency training with WGAN [156] applied to semi-supervised classification problems. And the structure of CT-GAN is shown in Fig. [2](7). Following [157], this method also lays the Lipschitz continuity condition over the manifold of the real data to improve the improved training of WGAN. Moreover, CT-GAN devises a regularization over a pair of samples drawn near the manifold following the most basic definition of the 1-Lipschitz continuity. In particular, each real instance $x$ is perturbed twice and uses a Lipschitz constant to bound the difference between the discriminator’s responses to the perturbed instances $x', x''$. Formally, since the value function of WGAN is

$$\min_G \max_D \mathbb{E}_{x \sim p(x)} D(x) - \mathbb{E}_{z \sim p(z)} D(G(z)),$$

where $D$ is one of the sets of 1-Lipschitz function. The objective function for updating the discriminator include: (a) basic Wasserstein distance in Eq. (5), (b) gradient penalty $\nabla p|_{x}$ [157] used in the improved training of WGAN, where $\hat{x} = c x + (1-c) G(z)$, and (c) A consistency regularization $CT|_{x', x''}$. For semi-supervised classification, CT-GAN uses the Eq. (6) for training the discriminator instead of the Eq. (5), and then adds the consistency regularization $CT|_{x', x''}$.

**BiGAN.** Bidirectional Generative Adversarial Networks (BiGANS) [158] is an unsupervised feature learning framework. The architecture of BiGAN is shown in Fig. [2](8). In contrast to the standard GAN framework, BiGAN adds an encoder $E$ to this framework, which maps data $x$ to $z'$, resulting in a data pair $(x, z')$. The data pair $(x, z')$ and the data pair generated by generator $G$ constitute two kinds of true and fake data pairs. The BiGAN discriminator $D$ is to distinguish the true and fake data pairs. In this work, the value function for training the discriminator becomes,

$$\min_C \max_D \mathbb{E}_{(x, y) \sim p(x, y)} \left[ \mathbb{E}_{z \sim p(z)} \left[ \log D(x, z) \right] \right]$$

$$+ \mathbb{E}_{z \sim p(z)} \left[ \mathbb{E}_{x \sim p(x|z)} \left[ \log (1 - D(x, z)) \right] \right]$$

$$\log (1-D(G(z), z)),$$

which shows that penalizing $\|
abla \log p(y = k|x)\|^2$ can train a robust classifier with a small perturbation $\sigma z$ on a manifold. This probabilistic classifier can be introduced by adding $\sum_{k=1}^K \mathbb{E}_{x \sim p(x)} \|
abla x \log p(y = k|x)\|^2$, where $\nabla x \log p(y = k|x)$ is the gradient of the log-likelihood along with the manifold $G(x, z)$.

**ALL.** Adversarially Learned Inference (ALL) [159] is a GAN-like adversarial framework based on the combination of an inference network and a generative model. This framework consists of three networks, a generator, an inference network and a discriminator. The generative network $G$ is used as a decoder to map latent variables $z$ (with a prior distribution) to data distribution $x' = G(z)$, which can be formed as joint pairs $(x', z)$. The inference network $E$ attempts to encode training samples $x$ to latent variables $z' = E(x)$, and joint pairs $(x, z')$ are similarly drawn. The discriminator network $D$ is required to distinguish the joint pairs $(x, z')$ from the joint pairs $(x', z)$. As discussed above, the central architecture of ALL is regarded as similar to the BiGAN’s (see Fig. [2](9)). In semi-supervised settings, this framework adapts the discriminator network proposed in [152], and shows promising performance on semi-supervised benchmarks on SVHN and CIFAR 10. The objective function can be rewritten as an extended version similar to Eq. (6).
where $D$ obtains label information about unlabeled data from the classifier $C$ and forces the generator $G$ to generate the realistic image-label samples.

**Enhanced TGAN.** Based on the architecture of Triple GAN [162], Enhanced TGAN [163] modifies the Triple-GAN by re-designing the generator loss function and the classifier network. The generator generates images conditioned on class distribution and is regularized by class-wise mean feature matching. The classifier network includes two classifiers that collaboratively learn to provide more categorical information for generator training. Additionally, a semantic matching term is added to enhance the semantics consistency with respect to the generator and the classifier network. The discriminator $D$ learned to distinguish the labeled data pair $(x, y)$ from the synthesized data pair $(G(z), \hat{y})$ and predicted data pair $(x, \hat{y})$. The corresponding objective function is similar to Eq. (7), where $p(x, y)$ is sampling from the pre-specified distribution $p_g$, and $(x, \hat{y})$ denotes the predicted data pair determined by $p_r(x)$.

**MarginGAN.** MarginGAN [164] is another extension framework based on Triple GAN [162]. From the perspective of classification margin, this framework works better than Triple GAN when used for semi-supervised classification. The architecture of MarginGAN is presented in Fig. 2(10). MarginGAN includes three components like Triple GAN, a generator $G$ which tries to maximize the margin of generated samples, a classifier $C$ used for decreasing margin of fake images, and a discriminator $D$ trained as usual to distinguish real samples from fake images. This method solves the problem that performance is damaged due to the inaccurate pseudo label in SSL, and improves the accuracy rate of SSL.

**Triangle GAN.** Triangle Generative Adversarial Network (Δ-GAN) [162] introduces a new architecture to match cross-domain joint distributions. The architecture of the Δ-GAN is shown in Fig. 2(11). The Δ-GAN can be considered as an extended version of BiGAN [158] or ALI [159]. This framework is a four-branch model that consists of two generators $E$ and $G$, and two discriminators $D_1$ and $D_2$. The two generators can learn two different joint distributions by two-way matching between two different domains. At the same time, the discriminators are used as an implicit ternary function, where $D_2$ determines whether the data pair is from $(x, y')$ or from $(G(z), y)$, and $D_1$ distinguishes real data pair $(x, y)$ from the fake data pair $(G(z), y)$.

**Structured GAN.** Structured GAN [165] studies the problem of semi-supervised conditional generative modeling based on designated semantics or structures. The architecture of Structured GAN (see Fig. 2(12)) is similar to Triangle GAN [162]. Specifically, Structured GAN assumes that the samples $x$ are generated conditioned on two independent latent variables, i.e., $y$ that encodes the designated semantics and $z$ contains other variation factors. Training Structured GAN involves solving two adversarial games that have their equilibrium concentrating at the true joint data distributions $p(x, z)$ and $p(x, y)$. The synthesized data pair $(x', y)$ and $(x', z)$ are generated by generator $G(y, z)$, where $(x', y)$ mix real sample pair $(x, y)$ together as input for training discriminator $D(y, z)$ and $(x', z)$ blends the $E'$s outputs pair $(x, z')$ for discriminator $D(x, z)$.

**$R^3$-CGAN.** Liu et al. [166] propose a Class-conditional GAN with Random Regional Replacement ($R^3$-regularization) technique, called $R^3$-CGAN. Their framework and training strategy relies on Triangle GAN [162]. The $R^3$-CGAN architecture comprises four parts, a generator $G$ to synthesize fake images with specified class labels, a classifier $C$ to generate instance-label pairs of real unlabeled images with pseudo-labels, a discriminator $D_1$ to identify real or fake pairs, and another discriminator $D_2$ to distinguish two types of fake data. Specifically, CutMix [167], a Random Regional Replacement strategy, is used to construct two types of between-class instances (cross-category instances and real-fake instances). These instances are used to regularize the classifier $C$ and discriminator $D_1$. Through the minimax game among the four players, the class-specific information is effectively used for the downstream.

**Summary.** Comparing with the above discussed Semi-GANs methods, we find that the main difference lies in the number and type of the basic modules, such as generator, encoder, discriminator, and classifier. As shown in Fig. 2(1), we find the evolutionary relationship of the Semi-GANs models. Overall, CatGAN [149] and CCGAN [150] extend the basic GAN by including additional information in the model, such as category information and in-painted images. Based on Improved GAN [152], Localized GAN [154] and CT-GAN [155] consider the local information and consistency regularization, respectively. BiGAN [158] and ALI [159] learn an inference model during the training process by adding an Encoder module. In order to solve the problem that the generator and discriminator can not be optimal at the same time, Triple-GAN [161] adds an independent classifier instead of using a discriminator as a classifier.

### 3.2 Semi-supervised VAE

Variational AutoEncoders (VAEs) [168], [169] are flexible models which combine deep autoencoders with generative latent-variable models. The generative model captures representations of the distributions rather than the observations of the dataset, and defines the joint distribution in the form of $p(x, z) = p(z)p(x|z)$, where $p(z)$ is a prior distribution over latent variables $z$. Since the true posterior $p(z|x)$ is generally intractable, the generative model is trained with the aid of an approximate posterior distribution $q(z|x)$. The architecture of VAEs is a two-stage network, an encoder to construct a variational approximation $q(z|x)$ to the posterior $p(z|x)$, and a decoder to parameterize the likelihood $p(x|z)$. The variational approximation of the posterior maximizes the marginal likelihood, and the evidence lower bound (ELBO) may be written as

$$
\log p(x) = \log \mathbb{E}_{q(z|x)}[p(z)p(x|z)] - \mathbb{E}_{q(z|x)}[\log p(z)p(x|z)] - \log q(z|x) \tag{8}
$$

There are three reasons why latent-variable models can be useful for SSL: (a) It is a natural way to incorporate unlabeled data, (b) The ability to disentangle representations can be easily implemented via the configuration of latent variables, and (c) It also allows us to use variational neural methods. In the following, we review several representative latent variable methods for semi-supervised learning.
SSVAEs. SSVAEs denotes the VAE-based generative models with latent encoder representation proposed in [170]. The first one, i.e., the latent-feature discriminative model, referred to M1 [170], can provide more robust latent features with a deep generative model of the data. As shown in Fig. 3(1), \( p_0(x|z) \) is a non-linear transformation, e.g., a deep neural network. Latent variables \( z \) can be selected as a Gaussian distribution or a Bernoulli distribution. An approximate sample of the posterior distribution on the latent variable \( q_\theta(z|x) \) is used as the classifier feature for the class label \( y \). The second one, namely Generative semi-supervised model, referred to M2 [170], describes the data generated by a latent class variable \( y \) and a continuous latent variable \( z \), is expressed as \( p_0(x|z, y)p(z)p(y) \) (as depicted in Fig. 3(2)). \( p(y) \) is the multinomial distribution, where the class labels \( y \) are treated as latent variables for unlabeled data. \( p_0(x|z, y) \) is a suitable likelihood function. The inferred posterior distribution \( q_\theta(z|y, x) \) can predict any missing labels.

Stacked generative semi-supervised model, called M1+M2, uses the generative model M1 to learn the new latent representation \( z_1+M2 \), uses the generative model \( M1 \) to learn the new labels.

Learning the posterior distribution is intractable. Thus we define the approximation as \( q_\phi(a|x)q_\theta(z|y, x) \) and a classifier \( q_\phi(y|a, x) \). The auxiliary unit \( a \) actually introduces a class-specific latent distribution between \( x \) and \( y \), resulting in a more expressive distribution \( q_\phi(y|a, x) \).

Formally, [171] employs the similar variational lower bound \( \mathbb{E}_{q_\phi(a, z|x)}[\log p_\theta(a, x, y, z) − \log q_\phi(a, z|x, y)] \) on the marginal likelihood, with \( q_\phi(a, z|x, y) = q_\phi(a|x)q_\theta(z|y, x) \). Similarly, the unlabeled ELBO is \( \mathbb{E}_{q_\phi(a,y,z)}[\log p_\theta(a, x, y, z) − \log q_\phi(a, y, z|x)] \) with \( q_\phi(a, y, z|z) = q_\phi(z|y, x)q_\phi(y|a, x)q_\phi(a|z) \).

Interestingly, by reversing the direction of the dependence between \( x \) and \( a \), a model similar to the stacked version of M1 and M2 is recovered (Fig. 3(3)), with what the authors denote skip connections from the second stochastic layer and the labels to the inputs \( x \). In this case the generative model is affected, and the authors call this the Skip Deep Generative Model (SDGM). This model is able to be trained end to end using stochastic gradient descent (SGD) (according to the [171] the skip connection between \( z \) and \( x \) is crucial for training to converge). Unsurprisingly, joint training for the model improves significantly upon the performance presented in [170].

**Infinite VAE.** Infinite VAE [172] proposes a mixture model for combining variational autoencoders, a non-parametric Bayesian approach. This model can adapt to suit the input data by mixing coefficients by a Dirichlet process. It combines Gibbs sampling and variational inference that enables the model to learn the input’s underlying structures efficiently. Formally, Infinite VAE employs the mixing coefficients to assist SSL by combining the unsupervised generative model and a supervised discriminative model. The infinite mixture generative model as,

\[
p(c, \pi, x, z) = p(c|\pi)p_\alpha(\pi)p_\theta(x|c, z)p(z),
\]

where \( c \) denotes the assignment matrix for each instance to a VAE component where the VAE-i can best reconstruct instance \( i \). \( \pi \) is the mixing coefficient prior for \( c \), drawn from a Dirichlet distribution with parameter \( \alpha \). Each latent variable \( z_i \) in each VAE is drawn from a Gaussian distribution.

**Disentangled VAE.** Disentangled VAE [173] attempts to learn disentangled representations using partially-specified graphical model structures and distinct encoding aspects of the data into separate variables. It explores the graphical model for modeling a general dependency on observed and unobserved latent variables with neural networks, and a stochastic computation graph [174] is used to infer with and train the resultant generative model. For this purpose, importance sampling estimates are used to maximize the lower
bound of both the supervised and semi-supervised likelihoods. Formally, this framework considers the conditional probability \( q_{θ}(z|x) \), which has a factorization \( q_{θ}(y,z|x) = q_{θ}(y|x,z)q_{θ}(z|x) \) rather than \( q_{θ}(y,z|x) = q_{θ}(z|x,y)q_{θ}(y|x) \) in \( 170 \), which means we can no longer compute a simple Monte Carlo estimator by sampling from the unconditional distribution \( q_{θ}(z|x) \). Thus, the variational lower bound for the variational bound is expanded below,

\[
\mathbb{E}_{q_{θ}(z|x,y)}[\log p_{θ}(x|y,z)p(y)p(z) - q_{θ}(y,z|x)]. \tag{13}
\]

---

**SDVAE.** Semi-supervised Disentangled VAE (SDVAE) \( 175 \) incorporates the label information to the latent representations by encoding the input disentangled representation and non-interpretable representation. The disentangled variable captures categorical information, and the non-interpretable variable consists of other uncertain information from the data. As shown in Fig. \( 3(5) \), SDVAE assumes the disentangled variable \( v \) and the non-interpretable variable \( u \) are independent condition on \( x \), i.e., \( q_{θ}(u,v|x) = q_{θ}(u|x)q_{θ}(v|x) \). This means that \( q_{θ}(v|x) \) is the encoder for the disentangled representation, and \( q_{θ}(u|x) \) denotes the encoder for non-interpretable representation. Based on those assumptions, the variational lower bound is written as:

\[
\mathbb{E}_{q_{θ}(u|z,q(v|x))}[\log p(x|u,v)p(v)p(u) - \log q(u|x)q(v|x)]. \tag{14}
\]

**ReVAE.** Reparameterized VAE (ReVAE) \( 176 \) develops a novel way to encode supervised information, which can capture label information through auxiliary variables instead of latent variables in the prior work \( 170 \). The graphical model is illustrated in Fig. \( 3(6) \). In contrast to SS-VAEs, ReVAE captures meaningful representations of data with a principled variational objective. Moreover, ReVAE carefully designed the mappings between auxiliary and latent variables. In this model, a conditional generative model \( p_{θ}(z|y) \) is introduced to address the requirement for inference at test time. Similar to \( 170 \) and \( 171 \), ReVAE treats \( y \) as a known observation when the label is available in the supervised setting, and as an additional variable in the unsupervised case. In particular, the latent space can be partitioned into two disjoint subsets under the assumption that label information captures only specific aspects.

**Summary.** As the name indicates, Semi-supervised VAE applies the VAE architecture for handling SSL problems. An advantage of these methods is that meaningful representations of data can be learned by the generative latent-variable models. The basic framework of these Semi-supervised VAE methods is M2 \( 170 \). On the basis of the M2 framework, ADGM \( 171 \) and ReVAE \( 176 \) consider introducing additional auxiliary variables, although the roles of the auxiliary variables in the two models are different. Infinite VAE \( 172 \) is a hybrid of several VAE models to improve the performance of the entire framework. Disentangled VAE \( 173 \) and SDVAE \( 175 \) solve the semi-supervised VAE problem by different disentangled methods. Under semi-supervised conditions, when a large number of labels are unobserved, the key to this kind of method is how to deal with the latent variables and label information.

## 4 Consistency Regularization

In this section, we introduce the consistency regularization methods for semi-supervised deep learning. In these methods, a consistency regularization term is applied to the final loss function to specify the prior constraints assumed by researchers. Consistency regularization is based on the manifold assumption or the smoothness assumption, and describes a category of methods that the realistic perturbations of the data points should not change the output of the model \( 13 \). Consequently, consistency regularization can be regarded to find a smooth manifold on which the dataset lies by leveraging the unlabeled data \( 177 \).

The most common structure of consistency regularization SSL methods is the Teacher-Student structure. As a student, the model learns as before, and as a teacher, the model generates targets simultaneously. Since the model itself generates targets, they may be incorrect and then used by themselves as students for learning. In essence, the consistency regularization methods suffer from confirmation bias \( 68 \), a risk that can be mitigated by improving the target’s quality. Formally, following \( 178 \), we assume that dataset \( X \) consists of a labeled subset \( X_l \) and an unlabeled subset \( X_u \). Let \( θ' \) denote the weight of the target, and \( θ \) denotes the weights of the basic student. The consistency constraint is defined as:

\[
\mathbb{E}_{x \in X} \mathcal{R}(f(θ, x), τ_ξ) = \mathbb{E}_{x \in X} \mathcal{R}(f(θ', x), τ_ξ) \tag{15}
\]

where \( f(θ, x) \) is the prediction from model \( f(θ) \) for input \( x \), \( τ_ξ \) is the consistency target of the teacher. \( \mathcal{R}(·, ·) \) measures the distance between two vectors and is usually set to Mean Squared Error (MSE) or KL-divergence. Different consistency regularization techniques vary in how they generate the target. There are several ways to boost the target \( τ_ξ \) quality. One strategy is to select the perturbation rather than additive or multiplicative noise carefully. Another technique is to consider the teacher model carefully instead of replicating the student model.

**Ladder Network.** Ladder Network \( 65 \), \( 179 \) is the first successful attempt towards using a Teacher-Student model that is inspired by a deep denoising AutoEncoder. The structure of the Ladder Network is shown in Fig. \( 3(1) \). In Encoder, noise \( ζ \) is injected into all hidden layers as the corrupted feedforward path \( x + ζ \xrightarrow{Encoder} \hat{z}_1 \xrightarrow{Decoder} \hat{z}_2 \) and shares the mappings \( f(·) \) with the clean encoder feedforward path \( x \xrightarrow{Encoder} \hat{z}_1 \xrightarrow{Decoder} \hat{z}_2 \). The decoder path \( \hat{z}_1 \xrightarrow{Decoder} \hat{z}_2 \xrightarrow{Decoder} g(·) \) consists of the denoising functions \( g(·) \) and the unsupervised denoising square error \( \mathcal{R} \) on each layer consider as consistency loss between \( \hat{z}_1 \) and \( z_i \). Through latent skip connections, the ladder network is differentiated from regular denoising AutoEncoder. This feature allows the higher layer features to focus on more abstract invariant features for the task. Formally, the ladder network unsupervised training loss \( L_u \) or the consistency loss is computed as the MSE between the activation of the clean encoder \( z_i \) and the reconstructed activations \( \hat{z}_i \). Generally, \( L_u \) is

\[
\mathbb{E}_{x \in X} \mathcal{R}(f(θ, x), g(f(θ, x + ζ))). \tag{16}
\]

**Π Model.** Unlike the perturbation used in Ladder Network, Π Model \( 66 \) is to create two random augmentations of a sample for both labeled and unlabeled data. Some techniques with non-deterministic behavior, such as randomized data augmentation, dropout, and random max-pooling, make an input sample pass through the network
Architecture as the student model with exponential moving average similar to the student and teacher. The student model is a regular model in Fig. 4(4). Mean Teacher consists of two models called student and teacher. The structure of Mean Teacher is shown in Fig. 4(5). This technique aims to generate an adversarial transformation of a sample, which can change the model prediction. Specifically, the adversarial training technique is used to find the optimal adversarial perturbation $\gamma$ of a real input instance $x$ such that $\gamma \leq \delta$. Afterward, the consistency constraint is applied between the model’s output of the original input sample and the perturbed one, i.e.,

$$E_{x \in X} R(f(\theta, x, \gamma), g(\theta, x + \gamma_{adv})).$$

which minimizes the difference between the two predictions.

**Temporal Ensembling.** Temporal Ensembling [67] is similar to the II Model, which forms a consensus prediction under different regularization and input augmentation conditions. The structure of Temporal Ensembling is shown in Fig. 4(3). It modifies the II Model by leveraging the Exponential Moving Average (EMA) of past epochs predictions. In other words, while II Model needs to forward a sample twice in each iteration, Temporal Ensembling reduces this computational overhead by using EMA to accumulate the predictions over epochs as $\mathcal{T}_Z$. Specifically, the ensemble outputs $Z_i$ is updated with the network outputs $z_i$ after each training epoch, i.e., $Z_i \leftarrow \alpha Z_i + (1 - \alpha) z_i$, where $\alpha$ is a momentum term. During the training process, the $Z$ can be considered to contain an average ensemble of $f(\cdot)$ outputs due to Dropout and stochastic augmentations. Thus, consistency loss is:

$$E_{x \in X} R(f(\theta, x, \zeta_1), EMA(f(\theta, x, \zeta_2))).$$

**Mean Teacher.** Mean Teacher [68] averages model weights using EMA over training steps and tends to produce a more accurate model instead of directly using output predictions. The structure of Mean Teacher is shown in Fig. 4(4). Mean Teacher consists of two models called student and teacher. The student model is a regular model similar to the II Model, and the teacher model has the same architecture as the student model with exponential moving average of the student weights. Then Mean Teacher applied a consistency constraint between the two predictions of student and teacher:

$$E_{x \in X} R(f(\theta, x, \zeta), f(EMA(\theta), x, \zeta')).$$

**VAT.** Virtual Adversarial Training [180] proposes the concept of adversarial attack for consistency regularization. The structure of VAT is shown in Fig. 4(5). This technique aims to generate an adversarial transformation of a sample, which can change the model prediction. Specifically, the adversarial training technique is used to find the optimal adversarial perturbation $\gamma$ of a real input instance $x$ such that $\gamma \leq \delta$. Afterward, the consistency constraint is applied between the model’s output of the original input sample and the perturbed one, i.e.,

$$E_{x \in X} R(f(\theta, x, \gamma), g(\theta, x + \gamma_{adv})).$$

**Dual Student.** Dual Student [178] extends the Mean Teacher model by replacing the teacher with another student. The structure of Dual Student is shown in Fig. 4(6). The two students start from different initial states and are optimized through individual paths during training. The authors also defined a novel concept, “stable sample”, along with a stabilization constraint to avoid the performance bottleneck produced by a coupled EMA Teacher-Student model. Hence, their weights may not be tightly coupled, and each learns its own knowledge. Formally, Dual Student checks whether $x$ is a stable sample for student $i$:

$$C^i_x = \{ p^i_x = p^i_x \} \land \{ M^i_x > \xi \} \land \{ M^i_x > \xi \} ,$$

where $M^i_x = \| f(\theta^i, x) \|_{\infty}$, and the stabilization constraint:

$$L^i_{sta} = \{ \epsilon^i > \epsilon^i \} \land \{ R(f(\theta^i, x), f(\theta^i, x)) \} \land \{ C^i = C^i \} \land \{ C'/R(f(\theta^i, x), f(\theta^i, x)) \} \text{ otherwise} .$$

**SWA.** Stochastic Weight Averaging (SWA) [181] improves generalization than conventional training. The aim is
to average multiple points along the trajectory of stochastic gradient descent (SGD) with a cyclical learning rate and seek much flatter solutions than SGD. The consistency-based SWA [182] observes that SGD fails to converge on the consistency loss but continues to explore many solutions with high distances apart in predictions on the test data. The structure of SWA is shown in Fig. 9(7). The SWA procedure also approximates the Teacher-Student approach, such as II Model and Mean Teacher with a single model. The authors propose fast-SWA, which adapts the SWA to the optimization of dropout weights in each cycle. Generally, the consistency loss can be rewritten as follows:

$$\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x), f(SWA(\theta), x, \zeta)).$$ \hspace{1cm} (23)

**VAaD.** In VAT, the adversarial perturbation is defined as an additive noise unit vector applied to the input or embedding spaces, which has improved the generalization performance of SSL. Similarly, Virtual Adversarial Dropout (VAaD) [183] also employs adversarial training in addition to the II Model. The structure of VAaD is shown in Fig. 9(8). Following the design of II Model, the consistency constraint of VAaD is computed from two different dropped networks: one dropped network uses a random dropout mask, and the other applies adversarial training to the optimized dropout network. Formally, $f(\theta, x, \epsilon)$ denotes an output of a neural network with a random dropout mask, and the consistency loss incorporating adversarial dropout is described as:

$$\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x, \epsilon^\ast), f(\theta, x, \epsilon^{adv})),$$ \hspace{1cm} (24)

where $\epsilon^{adv} = \arg\max_{\epsilon, |\epsilon| \leq H} R(f(\theta, x, \epsilon^\ast), f(\theta, x, \epsilon)); f(\theta, x, \epsilon^{adv})$ represents an adversarial target; $\epsilon^{adv}$ is an adversarial dropout mask; $\epsilon^\ast$ is a sampled random dropout mask instance; $\delta$ is a hyperparameter controlling the intensity of the noise, and $H$ is the dropout layer dimension.

**WCP.** A novel regularization mechanism for training deep SSL by minimizing the Worse-case Perturbation (WCP) is presented by Zhang et al. [69]. The structure of WCP is shown in Fig. 9(9). WCP considers two forms of WCP regularizations – additive and DropConnect perturbations, which impose additive perturbation on network weights and make structural changes by dropping the network connections, respectively. Instead of generating an ensemble of randomly corrupted networks, the WCP suggests enhancing the most vulnerable part of a network by making the most resilient weights and connections against the worst-case perturbations. It enforces an additive noise on the model parameters $\zeta$, along with a constraint on the norm of the noise. In this case, the WCP regularization becomes:

$$\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x), g(\theta + \zeta, x)).$$ \hspace{1cm} (25)

The second perturbation is at the network structure level by DropConnect, which drops some network connections. Specifically, for parameters $\theta$, the perturbed version is $(1 - \alpha)\theta$, and the $\alpha = 1$ denotes a dropped connection while $\alpha = 0$ indicates an intact one. By applying the consistency constraint, we have

$$\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x), f((1 - \alpha)\theta, x)).$$ \hspace{1cm} (26)

**UDA.** UDA stands for Unsupervised Data Augmentation [184] for image classification and text classification. The structure of UDA is shown in Fig. 9(10). This method investigates the role of noise injection in consistency training and substitutes simple noise operations with high-quality data augmentation methods, such as AutoAugment [185], RandAugment [186] for images, and Back-Translation [187, 188] for text. Following the consistency regularization framework, the UDA [184] extends the advancement in supervised data augmentation to SSL. As discussed above, let $f(\theta, x, \zeta)$ be the augmentation transformation from which one can draw an augmented example $(x, \zeta)$ based on an original example $x$. The consistency loss is:

$$\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x), f(\theta, x, \zeta)),$$ \hspace{1cm} (27)

where $\zeta$ represents the data augmentation operator to create an augmented version of an input $x$.

**Summary.** The core idea of consistency regularization methods is that the output of the model remains unchanged.

| Methods          | Techniques                  | Transformations                  | Consistency Constraints               |
|------------------|----------------------------|----------------------------------|---------------------------------------|
| Ladder Network   | Additional Gaussian Noise   | input                            | $\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x), f(\theta, x + \zeta))$ |
| II Model         | Different Stochastic Augmentations | input                           | $\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x, \zeta_1), f(\theta, x, \zeta_2))$ |
| Ensembling       | Different Stochastic Augmentation | predictions                    | $\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x, \zeta_1), f(\theta, x, \zeta_2), \text{EMA}(f(\theta, x, \zeta_1)))$ |
| Mean Teacher     | Different Stochastic Augmentation | input, predictions              | $\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x, \zeta), f(\text{EMA}(\theta), x, \zeta))$ |
| VAT              | Adversarial perturbation    | input                            | $\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x), f(\theta, x, \zeta^{adv}))$ |
| Dual Student     | Stable sample and stabilization constraint | input, weights                  | $\mathbb{E}_{x \in \mathcal{X}} R(f(\text{STA}(\theta, x_i), \zeta_1), f(\text{STA}(\theta, x_j), \zeta_2))$ |
| SWA              | Stochastic Weight Averaging | input, weights                   | $\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x), f(\text{STA}(\theta), x, \zeta))$ |
| VAaD             | Adversarial perturbation and Stochastic Augmentation | input, weights                   | $\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x, \epsilon^\ast), f(\theta, x, \epsilon^{adv}))$ |
| UDA              | AutoAugment/RandAugment for image; Back-Translation for text | input                           | $\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x), f(\theta, x, \zeta))$ |
| WCP              | Additive perturbation on network weights, DropConnect perturbation for network structure | input, network structure       | $\mathbb{E}_{x \in \mathcal{X}} R(f(\theta, x), g(\theta + \zeta, x))$ |
under realistic perturbation. As shown in TABLE 3, Consistency constraints can be considered at three levels: input dataset, neural networks and training process. From the input dataset perspective, perturbations are usually added to the input examples: additive noise, random augmentation, or even adversarial training. We can drop some layers or connections for the networks, as WCP [69]. From the training process, we can use SWA to make the SGD fit the consistency training or EMA parameters of the model for some training epochs as new parameters.

5 Graph-based methods

Graph-based semi-supervised learning (GSSL) has always been a hot subject for research with a vast number of successful models [189], [190], [191] because of its wide variety of applicability. The basic assumption in GSSL is that a graph can be extracted from the raw dataset where each node represents a training sample, and each edge denotes some similarity measurement of the node pair. In this section, we review graph embedding SSL methods, and the principal goal is to encode the nodes as small-scale vectors representing their role and the structure information of their neighborhood.

For graph embedding methods, we have the formal definition for the embedding on the node level. Given the graph $G(V, E)$, the node that has been embedded is a mapping result of $f_x : v \mapsto z_v \in \mathbb{R}^d, \forall v \in V$ such that $d \ll |V|$, and the $f_x$ function retains some of the measurement of proximity, defined in the graph $G$.

The unified form of the loss function is shown as Eq. (28) for graph embedding methods.

$$L(f_x) = \sum_{(x,y) \in X} (x, y, f_x) + \alpha \sum_{z \in X} R(x, f_x), \quad (28)$$

where $f_x$ is the embedding function.

Besides, we can divide graph embedding methods into shallow embedding and deep embedding based on the use or not use of deep learning techniques. The encoder’s function, as a simple lookup function based on node ID, is built with shallow embedding methods including DeepWalk [192], LINE [193] and node2vec [194], whereas the deep embedding encoder is far more complicated, and the deep learning frameworks have to make full use of node attributes.

As deep learning progresses, recent GSSL research has switched from shallow embedding methods to deep embedding methods in which the $f_x$ embedding term in the Eq. (28) is focused on deep learning models. Two classes can be identified among all deep embedding methods: AutoEncoder-based methods and GNN-based methods.

5.1 AutoEncoder-based methods

AutoEncoder-based approaches also differ as a result of using a unary decoder rather than a pairwise method. More precisely, every node, $i$, is correlated to a neighborhood vector $s_i \in \mathbb{R}^{|V|}$. The $s_i$ vector contains $i$’s similarity with all other graph nodes and acts as a high-dimensional vector representation of $i$ in the neighborhood. The aim of the auto-encoding technique is to embed nodes using hidden embedding vectors like $s_i$ in so as to reconstruct the original information from such embeddings (Fig. 5[1]):

$$\text{Dec}(\text{Enc}(s_i)) = \text{Dec}(z_i) \approx s_i, \quad (29)$$

In other words, the loss for these methods takes the following form:

$$L = \sum_{i \in V} \| \text{Dec}(z_i) - s_i \|_2^2, \quad (30)$$

SDNE. Structural deep network embedding (SDNE) is developed by Wang et al. [195] by using deep autoencoders to maintain the first and second-order network proximities. This is managed by optimizing the two proximities simultaneously. The process utilizes highly nonlinear functions to obtain its embedding. This framework consists of two parts: unsupervised and supervised. The first is an autoencoder to identify an embedding for a node to rebuild the neighborhood. The second is based on Laplacian Eigenmaps [196], which imposes a penalty when related vertices are distant from each other.

DNGR. (DNGR) [197] combines random surfing with autoencoders. The model includes three components: random surfing, positive pointwise mutual information (PPMI) calculation, and stacked denoising autoencoders. The random surfing design is used to create a stochastic matrix equivalent to the similarity measure matrix in HOPE [198] on the input graph. The matrix is transformed into a PPMI matrix and fed into a stacked denoising autoencoder to obtain the embedding. The PPMI matrix input ensures that the autoencoder model captures a higher proximity order. The use of stacked denoising autoencoders also helps make the model robust in the event of noise in the graph, as well as in seizing the internal structure needed for downstream tasks.

GAE & VGAE. Both MLP-based and RNN-based strategies only consider the contextual information and ignore the feature information of the nodes. To encode both, GAE [199] uses GCN [200]. The encoder is in the form,

$$\text{Enc}(A, X) = \text{GraphConv}(\sigma(\text{GraphConv}(A, X))), \quad (31)$$

where GraphConv($\cdot$) is a graph convolutional layer defined in [200], $\sigma(\cdot)$ is the activation function and $A, X$ are adjacency matrix and attribute matrix respectively. The decoder of GAE is defined as

$$\text{Dec}(z_u, z_v) = z_u^T z_v. \quad (32)$$

Variational GAE (VGAE) [199] learns about the distribution of the data in which the variation lower bound $L$ is optimized by reconstructing the adjacency matrix.

$$L = E_{q(z|X, A)}[\log p(A|Z)] - KL[q(Z|X, A)||p(Z)], \quad (33)$$

where $KL[q(\cdot)||p(\cdot)]$ is the Kullback-Leibler divergence between $q(\cdot)$ and $p(\cdot)$. Moreover, we have

$$q(Z|X, A) = \prod_{i=1}^{N} \mathcal{N}(z_i | \mu_i, \text{diag}(\sigma_i^2)), \quad (34)$$

and

$$p(A|Z) = \prod_{i=1}^{N} A_{ij} \sigma(z_i \top z_j) + (1 - A_{ij}) \left(1 - \sigma(z_i \top z_j)\right). \quad (35)$$
5.2 GNN-based methods

Several updated, deep embedding strategies are designed to resolve major autoencoder-based method disadvantages by building certain specific functions that rely on the local community of the node but not necessarily the whole graph (Fig. 5(5)). The GNN, which is widely used in state-of-the-art deep embedding approaches, can be regarded as a general guideline for the definition of deep neural networks on graphs.

Like other deep node-level embedding methods, a classifier is trained to predict class labels for the labeled nodes. Then it can be applied to the unlabeled nodes based on the final, hidden state of the GNN-based model. Since GNN consists of two primary operations: the aggregate operation and the update operation, the basic GNN is provided, and then some popular GNN extensions are reviewed with a view to enhancing each process, respectively.

**Summary.** It should be noted from Eq. (29) that the encoder unit does depend on the specific $s_i$ vector, which gives the crucial information relating to the local community structure of $v_i$. TABLE 4 sums up the main components of these methods, and their architectures are compared as Fig. 5.

**Basic GNN.** As Gilmer et al. [201] point out, the critical aspect of a basic GNN is that the benefit of neural message passing is to exchange and update messages between each node pair by using neural networks.

More specifically, a hidden embedding $h_u^{(k)}$ in each neural message passing through the GNN basic iteration is updated according to message or information from the neighborhood within $\mathcal{N}(u)$ according to each node $u$. This general message can be expressed according to the update rule:

$$h_u^{(k+1)} = \text{Update}^{(k)} \left( h_u^{(k)}, \text{Aggregate}^{(k)} \left( \left\{ h_v^{(k)}, \forall v \in \mathcal{N}(u) \right\} \right) \right)$$

$$= \text{Update}^{(k)} \left( h_u^{(k)}, m_{\mathcal{N}(u)}^{(k)} \right),$$

(36)

where

$$m_{\mathcal{N}(u)}^{(k)} = \text{Aggregate}^{(k)} \left( \left\{ h_v^{(k)}, \forall v \in \mathcal{N}(u) \right\} \right).$$

(37)

It is worth noting that the functions Update and Aggregate must generally be differentiable in Eq. (36). The new state is generated in accordance with Eq. (36) when the neighborhood message is combined with the previous hidden embedding state. After a number of iterations, the last hidden embedding state converges so that each node’s final status is created as the output. Formally, we have, $z_u = h_u^{(K)}$, $\forall u \in V$.

The basic GNN model is introduced before reviewing many other GNN-based methods designed to perform SSL tasks. The basic version of GNN aims to simplify the original GNN model, proposed by Scarselli et al. [202].

The basic GNN message passing is defined as:

$$h_u^{(k)} = \sigma \left( W_{\text{self}}^{(k)} h_u^{(k-1)} + W_{\text{neigh}}^{(k)} \sum_{v \in \mathcal{N}(u)} h_v^{(k-1)} + b^{(k)} \right),$$

(38)

where $W_{\text{self}}^{(k)}$, $W_{\text{neigh}}^{(k)}$ are trainable parameters and $\sigma$ is the activation function. In principle, the messages from the neighbors are summarized first. Then, the neighborhood information and the previously hidden node results are integrated by an essential linear combination. Finally, the joint information uses a nonlinear activation function. It is worth noting that the GNN layer can be easily stacked together following Eq. (38). The last layer’s output in the GNN model is regarded as the final node embedding result to train a classifier for the downstream SSL tasks.

As previously mentioned, GNN models have all sorts of variants that try to some degree boost their efficiency and robustness. All of them, though, obey the Eq. (36) neural message passing structure, regardless of the GNN version explored previously.

**GCN.** As mentioned above, the most simple neighborhood aggregation operation only calculates the sum of the neighborhood encoding states. The critical issue with this approach is that nodes with a large degree appear to derive a better benefit from more neighbors compared to those with a lower number of neighbors.

One typical and straightforward approach to this problem is to normalize the aggregation process depending on the central node degree. The most popular method is to use the following symmetric normalization Eq. (39) employed by Kipf et al. [200] in the graph convolutional network (GCN) model as Eq. (39).

$$m_{\mathcal{N}(u)} = \sum_{v \in \mathcal{N}(u)} \frac{h_v}{\sqrt{\left| \mathcal{N}(u) \right| \left| \mathcal{N}(v) \right|}}$$

(39)

GCN fully uses the uniform neighborhood grouping technique. Consequently, the GCN model describes the up-
**TABLE 4** Summary of AutoEncoder-based Deep Graph Embedding Methods

| Method   | Encoder | Decoder | Similarity Measure | Loss Function | Time Complexity |
|----------|---------|---------|-------------------|---------------|-----------------|
| SDNE     | MLP     | MLP     | $s_u$             | $\sum_{u \in V} \| \text{Dec} \left( z_u \right) - s_u \|_2$ | $O(\|V\|\|E\|)$ |
| DNCR     | MLP     | MLP     | $s_u$             | $\sum_{u \in V} \| \text{Dec} \left( z_u \right) - s_u \|_2$ | $O(\|V\|\|E\|)$ |
| GAE      | GCN     | $z_u$   | $A_{uv}$          | $\sum_{u \in V} \| \text{Dec} \left( z_u \right) - A_{uv} \|_2$ | $O(\|V\|\|E\|)$ |
| VGAE     | GCN     | $z_u$   | $A_{uv}$          | $E_{q(z|X,A)} \left[ \log p(A|z) - KL[q(z|X,A)||p(z)] \right]$ | $O(\|V\|\|E\|)$ |

The date function as Eq. (40). As it is indirectly specified in the update function, no aggregation operation is defined.

$$h_u^{(k)} = \sigma \left( W^{(k)} \sum_{v \in N(u) \cup \{u\}} \frac{h_v}{\sqrt{|N(u)||N(v)|}} \right)$$  

A vast range of GNN variants is available to boost SSL performance from various aspects [203, 204]. Li et al. [205] were the first to have a detailed insight into the performance and lack of GCN in SSL tasks. Subsequently, GCN extensions for SSL started to propagate [206, 207, 208, 209, 210].

**GAT.** In addition to more general ways of set aggregation, another common approach for improving the aggregation layer of GNNs is to introduce a set of attention mechanisms. The basic theory is to give each neighbor a weight or value of significance which is used to weight the influence of this neighbor during the aggregation process. The first GNN to use this focus was Cucurull et al.’s Graph Attention Network (GAT), which uses attention weights to describe a weighted neighboring amount:

$$m_{N(u)} = \sum_{v \in N(u)} \alpha_{u,v} h_v,$$  

where $\alpha_{u,v}$ denotes the attention on neighbor $v \in N(u)$ when we are aggregating information at node $u$. In the original GAT paper, the attention weights are defined as

$$\alpha_{u,v} = \exp \left( a^T \left[ Wh_u + Wh_v \right] \right) / \sum_{v' \in N(u)} \exp \left( a^T \left[ Wh_u + Wh_{v'} \right] \right),$$  

where $a$ is a trainable attention vector, $W$ is a trainable matrix, and denotes the concatenation operation.

**GraphSAGE.** Over-smoothing is an obvious concern for GNN. Over-smoothing after several message iterations is almost unavoidable as the node-specific information is “washed away.” The use of vector concatenations or skip connections, which both preserve information directly from the previous rounds of the update, is one fair way to lessen this concern. For general purposes, $\text{Update}_{\text{base}}$ denotes a basic update rule.

One of the simplest updates in GraphSage [212] for skip connection uses a concatenation vector to contain more node-level information during a messages passing process:

$$\text{Update} \left( h_u, m_{N(u)} \right) = \left[ \text{Update}_{\text{base}} \left( h_u, m_{N(u)} \right) \right] \oplus h_u,$$  

where the output from the basic update function is concatenated with the previous layer representation of the node. The critical observation is that this designed model is encouraged to detach information during the message passing operation.

**GGNN.** Parallel to the above work, researchers also are motivated by the approaches taken by recurrent neural networks (RNNs) to improve stability. One way to view the GNN message propagation algorithm is to gather an observation from neighbors of the aggregation process and then change each node’s hidden state. In this respect, specific approaches can be used explicitly based on observations to check the hidden states of RNN architectures.

For example, one of the earliest GNN variants which put this idea into practice is proposed by Li et al. [213], in which the update operation is defined as Eq. (44)

$$h_u^{(k)} = \text{GRU} \left( h_u^{(k-1)}, m_{N(u)}^{(k)} \right),$$  

where GRU is a gating mechanism function in recurrent neural networks, introduced by Kyunghyun Cho et al. [214]. Another related approach would be similar improvements based on the LSTM architecture [215].

**Summary.** The main point of graph-based models for DSSL is to perform label inference on a constructed similarity graph so that the label information can be propagated from the labeled samples to the unlabeled ones by incorporating both the topological and feature knowledge. Moreover, the involvement of deep learning models in GSSL helps generate more discriminative embedding representations that are beneficial for the downstream SSL tasks, thanks to the more complex encoder functions.

### 6 Pseudo-labeling methods

The pseudo-labeling methods differ from the consistency regularization methods in that the consistency regularization methods usually rely on consistency constraint of rich data transformations. In contrast, pseudo-labeling methods rely on the high confidence of pseudo-labels, which can be added to the training data set as labeled data. There are two main patterns, one is to improve the performance of the whole framework based on the disagreement of views or multiple networks, and the other is self-training, in particular, the success of self-supervised learning in unsupervised domain makes some self-training self-supervised methods realized.

#### 6.1 Disagreement-based models

The idea of disagreement-based SSL is to train multiple learners for the task and exploit the disagreement during the learning process [216]. In such model designs, two or three different networks are trained simultaneously and label unlabeled samples for each other.

**Deep co-training.** Co-training [27] framework assumes each data $x$ in the dataset has two different and complementary views, and each view is sufficient for training a good
classifier. Because of this assumption, Co-training learns two different classifiers on these two views (see Fig. 6(1)). Then the two classifiers are applied to predict each view’s unlabeled data and label the most confident candidates for the other model. This procedure is iteratively repeated till unlabeled data are exhausted, or some condition is met (such as the maximum number of iterations is reached).

Let $v_1$ and $v_2$ as two different views of data such that $x = (v_1, v_2)$. Co-training assumes that $C_1$ as the classifier trained on View-1 $v_1$ and $C_2$ as the classifier trained on View-2 $v_2$ have consistent predictions on $X$. In the objective function, the Co-training assumption can be model as:

$$L_{ct} = H(\frac{1}{2}(C_1(v_1) + C_2(v_2))) - \frac{1}{2}(H(C_1(v_1)) + H(C_2(v_2))), \tag{45}$$

where $H(\cdot)$ denotes the entropy, the Co-training assumption is formulated as $C(x) = C_1(v_1) = C_2(v_2), \forall x = (v_1, v_2) \sim X$. On the labeled dataset $X_L$, the supervised loss function can be the standard cross-entropy loss

$$L_s = H(y, C_1(v_1)) + H(y, C_2(v_2)), \tag{46}$$

where $H(p, q)$ is the cross-entropy between distribution $p$ and $q$.

The key to the success of Co-training is that the two views are different and complementary. However, the loss function $L_{ct}$ and $L_s$ only ensure the model tends to be consistent for the predictions on the dataset. To address this problem, $[217]$ forces to add the View Difference Constraint to the previous Co-training model, and formulated as:

$$\exists \mathcal{X}' : C_1(v_1) \neq C_2(v_2), \forall x = (v_1, v_2) \sim \mathcal{X}', \tag{47}$$

where $\mathcal{X}'$ denotes the adversarial examples of $\mathcal{X}$, thus $\mathcal{X}' \cap \mathcal{X} = \emptyset$. In the loss function, the View Difference Constraint can be model by minimizing the cross-entropy between $C_2(x)$ and $C_1(g_2(x))$, where $g(\cdot)$ denotes the adversarial examples generated by the generative model. Then, this part loss function is:

$$L_{dif}(x) = H(C_1(x), C_2(g_1(x))) + H(C_2(x), p_1(g_2(x))). \tag{48}$$

Some other research works also explore to apply co-training into neural network model training. For example, $[218]$ treats the RGB and depth of an image as two independent views for object recognition. Then, co-training is performed to train two networks on the two views. Next, a fusion layer is added to combine the two-stream networks for recognition, and the overall model is jointly trained. Besides, in sentiment classification, $[219]$ considers the original review and the automatically constructed anonymous reviews as two opposite sides of one review and then apply the co-training algorithm. One crucial property of $[219]$ is that two views are opposing and therefore associated with opposite class labels.

**Tri-Net.** Tri-net $[220]$, a deep learning-based method inspired by the tri-training $[221]$. The tri-training learns three classifiers from three different training sets, which are obtained by utilizing bootstrap sampling. The framework (as shown in Fig. 6(2)) of tri-net can be intuitively described as follows. Output smearing $[222]$ is used to add random noise to the labeled sample to generate different training sets and help learn three initial modules. The three models then predict the pseudo-label for unlabeled data. With the predictions of two modules for unlabeled instances consistent, the pseudo-label is considered to be confident and stable. The labeled sample is added to the training set of the third module, and then the third module is fine-tuned on the augmented training set. During the augmentation process, the three modules become more and more similar, so the three modules are fine-tuned on the training sets respectively to ensure diversity. Formally, the output smearing is used to construct three different training sets $\{C_{di} = (x_i, \tilde{y}_i^j), j = 1, 2, 3\}$ from the initial labeled set $X_L$. Then tri-net can be initialized by minimizing the sum of standard softmax cross-entropy loss function from the three training sets,

$$\begin{align*}
\mathcal{L} &= \frac{1}{L} \sum_{i=1}^{L} \left\{ \mathcal{L}_g(M_1(M_S(x_i)), \tilde{y}_i^1) + \mathcal{L}_g(M_2(M_S(x_i)), \tilde{y}_i^2) \\
&+ \mathcal{L}_g(M_3(M_S(x_i)), \tilde{y}_i^3) \right\}, \tag{49}
\end{align*}$$

where $\mathcal{L}_g$ is the standard softmax cross-entropy loss function; $M_S$ denote a shared module, and $M_1, M_2, M_3$ are the three different modules; $M_j(M_S(x_i)), j = 1, 2, 3$ denotes the outputs of the shared features generated by $M_S$. In the whole procedure, the unlabeled sample can be pseudo-labeled by the maximum posterior probability,

$$y = \arg\max_{k \in \{1, 2, ..., K\}} \left\{ p(M_1(M_S(x)) = k|x) + p(M_2(M_S(x)) = k|x) + p(M_3(M_S(x)) = k|x) \right\}.$$ 

**Summary.** The disagreement-based SSL methods exploit the unlabeled data by training multiple learners, and the
“disagreement” among these learners is crucial. When the data has two sufficient redundancy and conditional independence views, Deep Co-training \cite{217} improves the disagreement by designing a View Difference Constraint. Tri-Net \cite{220} obtains three labeled datasets by bootstrap sampling and trains three different learners. These methods in this category are less affected by model assumptions, non-convexity of the loss function and the scalability of the learning algorithms.

### 6.2 Self-training models

Self-training algorithm leverages the model’s own confident predictions to produce the pseudo labels for unlabeled data. In other words, it can add more training data by using existing labeled data to predict the labels of unlabeled data.

**EntMin.** Entropy Minimization (EntMin) \cite{223} is a method of entropy regularization, which can be used to realize SSL by encouraging the model to make low-entropy predictions for unlabeled data and then using the unlabeled data in a standard supervised learning setting. In theory, entropy minimization can prevent the decision boundary from passing through a high-density data points region, otherwise it would be forced to produce low-confidence predictions for unlabeled data.

**Pseudo-label.** Pseudo-label \cite{224} proposes a simple and efficient formulation of training neural networks in a semi-supervised fashion, in which the network is trained in a supervised way with labeled and unlabeled data simultaneously. As illustrated in Fig. \ref{fig:method}(3), the model is trained on labeled data in a usual supervised manner with a cross-entropy loss. For unlabeled data, the same model is used to get predictions for a batch of unlabeled samples. The maximum confidence prediction is called a pseudo-label, which has the maximum predicted probability.

That is, the pseudo-label model trains a neural network with the loss function $L$, where:

$$
L = \frac{1}{n} \sum_{m=1}^{n} \sum_{i=1}^{K} R(y_i^m, f_i^m) + \alpha(t) \frac{1}{n'} \sum_{m=1}^{n'} \sum_{i=1}^{K} R(y_i^m, f_i^m),
$$

where $n$ is the number of mini-batch in labeled data for SGD, $n'$ for unlabeled data, $f_i^m$ is the output units of $m$’s sample in labeled data, $y_i^m$ is the label of that, $y_i^m$ for unlabeled data, $y_i^m$ is the pseudo-label of that for unlabeled data, $\alpha(t)$ is a coefficient balancing the supervised and unsupervised loss terms.

**Noisy Student.** Noisy Student \cite{225} proposes a semi-supervised method inspired by knowledge distillation \cite{226} with equal-or-larger student models. The framework is shown in Fig. \ref{fig:method}(4). The teacher EfficientNet \cite{227} model is first trained on labeled images to generate pseudo labels for unlabeled examples. Then a larger EfficientNet model as a student is trained on the combination of labeled and pseudo-labeled examples. These combined instances are augmented using data augmentation techniques such as RandAugment \cite{228}, and model noise such as Dropout and stochastic depth are also incorporated in the student model during training. After a few iterations of this algorithm, the student model becomes the new teacher to relabel the unlabeled data and this process is repeated.

**S$^4$L.** Self-supervised Semi-supervised Learning (S$^4$L) \cite{229} tackles the problem of SSL by employing self-supervised learning \cite{230} techniques to learn useful representations from the image databases. The architecture of S$^4$L is shown in Fig. \ref{fig:method}(5). The conspicuous self-supervised techniques are predicting image rotation \cite{231} and exemplar \cite{232, 233}. Predicting image rotation is a pretext task that anticipates an angle of the rotation transformation applied to an input example. In S$^4$L, there are four rotation degrees \{$0^\circ, 90^\circ, 180^\circ, 270^\circ$\} to rotate input images. The S$^4$L-Rotation loss is the cross-entropy loss on outputs predicted by those rotated images. S$^4$L-Exemplar introduces an exemplar loss which encourages the model to learn a representation that is invariant to heavy image augmentations. Specifically, eight different instances of each image are produced by inception cropping \cite{234}, random horizontal mirroring, and HSV-space color randomization as in \cite{232}. Following \cite{230}, the loss term on unsupervised images uses the batch hard triplet loss \cite{235} with a soft margin.

**MPL.** In the SSL, the target distributions are often generated on unlabeled data by a shaped teacher model trained on labeled data. The constructions for target distributions are heuristics that are designed prior to training, and cannot adapt to the learning state of the network training. Meta Pseudo Labels (MPL) \cite{236} designs a teacher model that assigns distributions to input examples to train the student model. Throughout the course of the student’s training, the teacher observes the student’s performance on a held-out validation set, and learns to generate target distributions so that if the student learns from such distributions, the student will achieve good validation performance. The training procedure of MPL involves two alternating processes. As shown in Fig. \ref{fig:method}(6), the teacher $g_\theta(x)$ produces the conditional class distribution $g_\theta(x)$ to train the student. The pair $(x, g_\theta(x))$ is then fed into the student network $f_\theta(x)$ to update its parameters $\theta$ from the cross-entropy loss. After the student network updates its parameters, the model evaluates the new parameters $\theta'$ based on the samples from the held-out validation dataset. Since the new parameters of the student depend on the teacher, the dependency allows us to compute the gradient of the loss to update the teacher’s parameters.

**EnAET.** Different from the previous semi-supervised methods and S$^4$L \cite{229}, EnAET \cite{237} trains an Ensemble of Auto-Encoding Transformations to enhance the learning ability of the model. The core part of this framework is that EnAET integrates an ensemble of spatial and non-spatial transformations to self-train a good feature representation \cite{238}. EnAET incorporates four spatial transformations and a combined non-spatial transformation. The spatial transformations are Projective transformation, Affine transformation, Similarity transformation and Euclidean transformation. The non-spatial transformation is composed of different colors, contrast, brightness and sharpness with four strength parameters. As shown in Fig. \ref{fig:method}(7), EnAET learns an encoder $E: x \rightarrow E(x), t(x) \rightarrow E(t(x))$ on an original instance and its transformations. Meanwhile, a decoder $D: [E(x), E(t(x))] \rightarrow \hat{t}$ is learned to estimate $\hat{t}$ of input transformation. Then, we can get an AutoEncoding
Transformation (AET) loss,
\[ L_{AET} = \mathbb{E}_{x,t(x)}[D[E(x), E(t(x))] - t(x)], \]
and EnAET adds the AET loss to the SSL loss as a regularization term. Apart from the AET loss, EnAET explore a pseudo-labeling consistency by minimizing the KL divergence between \( P(y|x) \) on an original sample \( x \) and \( P(y|t(x)) \) on a transformation \( t(x) \).

SimCLRv2. SimCLRv2 \(^{239}\) modifies SimCLR \(^{240}\) for SSL problems. Following the paradigm of supervised fine-tuning after unsupervised pretraining, SimCLRv2 uses unlabeled samples in a task-agnostic way, and shows that a big (deep and wide) model can surprisingly effective for semi-supervised learning. As shown in Fig. 6(8), the SimCLRv2 can be summarized in three steps: unsupervised or self-supervised pre-training, supervised fine-tuning on 1% or 10% labeled samples, and self-training with task-specific unsupervised pre-training, supervised fine-tuning. As shown in Fig. 6(8), the SimCLRv2 (deep and wide) model can surprisingly effective for semi-labeled samples in a task-agnostic way, and shows that a big SSL problems. Following the paradigm of supervised fine-tuning, SimCLRv2 learns representations by maximizing the contrastive learning loss labeled examples. In the pre-training step, SimCLRv2 learns representations by maximizing the contrastive learning loss labeled examples. In the pre-training step, SimCLRv2 learns representations by maximizing the contrastive learning loss labeled examples. In the pre-training step, SimCLRv2 learns representations by maximizing the contrastive learning loss labeled examples. In the pre-training step, SimCLRv2 learns representations by maximizing the contrastive learning loss labeled examples. In the pre-training step, SimCLRv2 learns representations by maximizing the contrastive learning loss labeled examples. In the pre-training step, SimCLRv2 learns representations by maximizing the contrastive learning loss labeled examples.

ICT. Interpolation Consistency Training (ICT) \(^{27}\) regularizes SSL by encouraging the prediction at an interpolation of two unlabeled examples to be consistent with the interpolation of the predictions at those points. The architecture is shown in Fig. 6(1). The low-density separation assumption inspires this method, and Mixup can achieve a broad margin decision boundaries. It is done by training the model \( f(\theta) \) to predict \( \text{Mix}_\lambda(y_j, y_k) \) at location \( \text{Mix}_\lambda(x_j, x_k) \) with the Mixup operation: \( \text{Mix}_\lambda(a, b) = \lambda a + (1 - \lambda) b \). In semi-supervised settings, ICT extends Mixup by training the model \( f(\theta, x) \) to predict the "fake label" \( \text{Mix}_\lambda(f(\theta, x), f(\theta, x_k)) \) at location \( \text{Mix}_\lambda(x_j, x_k) \). Moreover, the model \( f_\theta \) predicts the fake label \( \text{Mix}_\lambda(f_\theta(x), f_\theta(x_k)) \) at location \( \text{Mix}_\lambda(x_j, x_k) \), where \( \theta^* \) is a moving average of \( \theta \), like \(^{68}\), for a more conservation consistent regularization. Thus, the ICT term is

\[ E_{x \in \mathcal{X}} R(f(\theta, \text{Mix}_\lambda(x_i, x_j)), \text{Mix}_\lambda(f(\theta^*, x_i), f(\theta^*, x_j)). \]

MixMatch. MixMatch \(^{71}\) combines consistency regularization and entropy minimization in a unified loss function. This model operates by producing pseudo-labels for each unlabeled instance and then training the original labeled data with the pseudo-labels for the unlabeled data using fully-supervised techniques. The main aim of this algorithm is to create the collections \( \mathcal{X}'_L \) and \( \mathcal{X}'_U \), which are made up of augmented labeled and unlabeled samples that were generated using Mixup. Formally, MixMatch produces an augmentation of each labeled instance \( (x_i, y_i) \) and \( K \) weakly augmented version of each unlabeled instance \( (x_j) \) with \( k \in \{1, \ldots, K\} \). Then, it generates a pseudo-label \( \tilde{y}_j \) for each \( x_j \) by computing the average prediction across the \( K \) augmentations. The pseudo-label distribution is then sharpened by adjusting temperature scaling to get the final pseudo-label \( \tilde{y}_j \). After the data augmentation, the batches of augmented labeled examples and unlabeled with pseudo-label examples are combined, then the whole group is shuffled. This group is divided into two parts: the first \( L \) samples were taken as \( \mathcal{W}_L \), and the remaining taken as \( \mathcal{W}_U \). The group \( \mathcal{W}_L \) and the augmented labeled batch \( \tilde{X}_L \) are fed into the Mixup algorithm to compute examples \( (x', y') \) where \( x' = \lambda x_1 + (1 - \lambda) x_2 \) for \( \lambda \sim \text{Beta}(\alpha, \alpha) \). Similarly, Mixup is applied between the remaining \( \mathcal{W}_U \) and the augmented unlabeled group \( \tilde{X}_U \). MixMatch conducts traditional fully-supervised training with a standard cross-entropy loss for a supervised dataset and a mean square error for unlabeled data given these mixed-up samples.

ReMixMatch. ReMixMatch \(^{72}\) extends MixMatch \(^{71}\) by introducing distribution alignment and augmentation anchoring. Distribution alignment encourages the marginal distribution of aggregated class predictions on unlabeled

\[ \tilde{x} = \lambda x_i + (1 - \lambda) x_j, \quad \tilde{y} = \lambda y_i + (1 - \lambda) y_j, \]
where \( (x_i, y_i) \) and \( (x_j, y_j) \) are two instances from the training data, and \( \lambda \in [0, 1] \). Therefore, Mixup extends the training data set by a hard constraint that linear interpolations of samples should lead to the linear interpolations of the corresponding labels.

7 HYBRID METHODS
Hybrid methods combine ideas from the above-mentioned methods such as pseudo-label, consistency regularization and entropy minimization for performance improvement. Moreover, a learning principle, namely Mixup \(^{241}\), is introduced in these hybrid methods. It can be considered as a simple, data-agnostic data augmentation approach, a convex combination of paired samples and their respective labels. Formally, Mixup constructs virtual training examples,
Augmentation anchoring replaces the consistency regularization component of MixMatch. This technique generates multiple strongly augmented versions of input and encourages each output to be close to predicting a weakly-augmented variant of the same input. A variant of AutoAugment [185] dubbed “CTAugment” is also proposed to produce strong augmentations, which learns the augmentation policy alongside the model training. As the procedure of ReMixmatch presented in Fig. 7(3), an “anchor” is generated by applying weak augmentation to a given unlabeled example and then $K$ strongly-augmented versions of the same unlabeled example using CTAugment.

DivideMix. DivideMix [73] presents a new SSL framework to handle the problem of learning with noisy labels. As shown in Fig. 7(4), DivideMix proposes co-divide, a process that trains two networks simultaneously. For each network, a dynamic Gauss Mixed Model (GMM) is fitted on the loss distribution of each sample to divide the training set into labeled data and unlabeled data. The separated data sets are then used to train the next epoch’s networks. In the follow-up SSL process, co-refinement and co-guessing are used to improve MixMatch [71] and solve the problem of learning with noisy labels.

FixMatch. FixMatch [242] combines consistency regularization and pseudo-labeling while vastly simplifying the overall method. The key innovation comes from the combination of these two ingredients, and the use of a separate weak and strong augmentation in the consistency regularization approach. Given an instance, only when the model predicts a high-confidence label can the predicted pseudo-label be identified as ground-truth. As shown in Fig. 7(5), given an instance $x_j$, FixMatch firstly generates pseudo-label $\hat{y}_j$ for weakly-augmented unlabeled instances $\hat{x}_j$. Then, the model trained on the weakly-augmented samples is used to predict pseudo-label in the strongly-augmented version of $x_j$. In FixMatch, weak augmentation is a standard flip-and-shift augmentation strategy, randomly flipping images horizontally with a probability. For strong augmentation, there are two approaches which are based on [185], i.e., RandAugment [228] and CTAugment [72]. Moreover, Cutout [243] is followed by either of these strategies.

Summary. As discussed above, the hybrid methods unite the most successful approaches in SSL, such as pseudo-labeling, entropy minimization and consistency regularization, and adapt them to achieve state-of-the-art performance. In TABLE 5, we summarize some techniques that can be used in consistency training to improve model performance.

### 8 Challenges and Future Directions

Although exceptional performance and achieved promising DSSL progress, there are still several open research questions for future work. We outline some of these issues and future directions below.

Theoretical analysis. Existing semi-supervised approaches predominantly use unlabeled samples to generate constraints and then update the model with labeled data and these constraints. However, the internal mechanism of DSSL and the role of various techniques, such as data augmentations, training methods and loss functions, etc., are not clear. Generally, there is a single weight to balance the supervised and unsupervised loss, which means that all unlabeled instances are equally weighted. However, not all unlabeled data is equally appropriate for the model in practice. To counter this issue, [244] considers how to use a different weight for every unlabeled example. For consistency regularization SSL, [182] investigates how loss...
geometry interacts with training process. [245] experimentally explores the effects of data augmentation and labeled dataset size on pre-training and self-training, as well as the limitations and interactions of pre-training and self-training. [246] analyzes the property of the consistency regularization methods when data instances lie in the neighborhood of low-dimensional manifolds, especially in the case of efficient data augmentations or perturbations schemes.

**Incorporation of domain knowledge.** Most of the SSL approaches listed above can obtain satisfactory results only in ideal situations in which the training dataset meets the designed assumptions and contains sufficient information to learn an insightful learning system. However, in practice, the distribution of the dataset is unknown and does not necessarily meet these ideal conditions. When the distributions of labeled and unlabeled data do not belong to the same one or the model assumptions are incorrect, the more unlabeled data is utilized, the worse the performance will be. Therefore, we can attempt to incorporate richer and more reliable domain knowledge into the model to mitigate the degradation performance. Recent works focusing on this direction have proposed [247], [248], [249], [250], [251] for DSSL.

**Learning with noisy labels.** In this survey, models discussed typically consider the labeled data is generally accurate to learn a standard cross-entropy loss function. An interesting consideration is to explore how SSL can be performed for cases where corresponding labeled instances with noisy initial labels. For example, the labeling of samples may be contributed by the community, so we can only obtain noisy labels for the training dataset. One solution to this problem is [252], which augments the prediction objective with consistency where the same prediction is made given similar percepts. Based on graph SSL, [253] introduces a new $L_1$-norm formulation of Laplacian regularization inspired by sparse coding. [254] deals with this problem from the perspective of memorization effects, which proposed a learning paradigm combining co-training and mean teacher.

**Imbalanced semi-supervised learning.** The problem of class imbalance is naturally widespread in real-world applications. When the training data is highly imbalanced, most learning frameworks will show bias towards the majority class, and in some extreme cases, may completely ignore the minority class [255], as a result, the efficiency of predictive models will be significantly affected. Nevertheless, to handle the semi-supervised problem, it is commonly assumed that training dataset is uniformly distributed over all class labels. Recently, more and more works have focused on this problem. [256] aligns pseudo-labels with the desirable class distribution in the unlabeled data for SSL with imbalanced labeled data. Based on graph-based semi-supervised methods, [257] copes with various degrees of class imbalance in a given dataset.

**Robust semi-supervised learning.** The common of the latest state-of-the-art approaches is the application of consistency training on augmented unlabeled data without changing the model predictions. One attempt is made by VAT [180] and VAdaD [183]. Both of them employ adversarial training to find the optimal adversarial example. Another promising approach is data augmentation (adding noise or random perturbations, CutOut [243], RandomErasing [258], HideAndSeek [259] and GridMask [260]), especially advanced data augmentation, such as AutoAugment [185], RandAugment [228], CTAugment [72], and Mixup [241] which also can be considered as a form of regularization.

**Safe semi-supervised learning.** In SSL, it is generally accepted that unlabeled data can help improve learning performance, especially when labeled data is scarce. Although it is remarkable that unlabeled data can improve learning performance under appropriate assumptions or conditions, some empirical studies [261], [262], [263] have shown that the use of unlabeled data may lead to performance degeneration, making the generalization performance even worse than a model learned only with labeled data in real-world applications. Thus, safe semi-supervised learning approaches are desired, which never significantly degrades learning performance when unlabeled data is used.

9 **Conclusion**

Deep semi-supervised learning is a promising research field with important real-world applications. The success of deep learning approaches has led to the rapid growth of DSSL techniques. This survey provides a taxonomy of existing DSSL methods, and groups DSSL methods into five categories: Generative models, Consistency Regularization models, Graph-based models, Pseudo-labeling models, and Hybrid models. We provide illustrative figures to compare the differences between the approaches within the same category. Finally, we discuss the challenges of DSSL and some future research directions that are worth further studies.

**Acknowledgment**

This paper was partially supported by the National Key Research and Development Program of China (No. 2018AAA0100204), and a key program of fundamental research from Shenzhen Science and Technology Innovation Commission (No. JCYJ2020109113403826).

**References**

1. J. Padmanabhan and J. M. J. Premkumar, “Advanced deep neural networks for pattern recognition: An experimental study,” in ScCPaR, ser. Advances in Intelligent Systems and Computing, vol. 614. Springer, 2016, pp. 166–175.

2. K. Yun, A. Huyen, and T. Li, “Deep neural networks for pattern recognition,” CoRR, vol. abs/1809.09645, 2018.

3. Q. Zhang, L. T. Yang, Z. Chen, and P. Li, “A survey on deep learning for big data,” Inf. Fusion, vol. 42, pp. 146–157, 2018.

4. T. Tran, T. Pham, G. Carneiro, L. J. Palmer, and I. D. Reid, “A bayesian data augmentation approach for learning deep models,” in NIPS, 2017, pp. 2797–2806.

5. A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” Commun. ACM, vol. 60, no. 6, pp. 84–90, 2017.

6. K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in CVPR. IEEE Computer Society, 2016, pp. 770–778.

7. J. Devlin, M. Chang, K. Lee, and K. Toutanova, “BERT: pre-training of deep bidirectional transformers for language understanding,” in NAACL-HLT. Association for Computational Linguistics, 2019, pp. 4171–4186.

8. A. Torfi, R. A. Shirvani, Y. Keneshloo, N. Tavvaf, and E. A. Fox, “Natural language processing advancements by deep learning: A survey,” CoRR, vol. abs/2003.01200, 2020.

9. I. J. Goodfellow, Y. Bengio, and A. C. Courville, Deep Learning, ser. Adaptive computation and machine learning. MIT Press, 2016.
[10] Y. LeCun, Y. Bengio, and G. E. Hinton, "Deep learning," *Nat.*, vol. 521, no. 7553, pp. 436–444, 2015.

[11] O. Chapelle, B. Schölkopf, and A. Zien, "Introduction to semi-supervised learning," in *Semi-Supervised Learning*. The MIT Press, 2006, pp. 1–72.

[12] X. Zhu and A. B. Goldberg, *Introduction to Semi-Supervised Learning*, ser. Synthesis Lectures on Artificial Intelligence and Machine Learning. Morgan & Claypool Publishers, 2009.

[13] A. Oliver, A. Odena, C. Raffel, E. D. Cubuk, and I. J. Goodfellow, "Realistic evaluation of deep semi-supervised learning algorithms," in *NeurIPS*, 2018, pp. 3239–3250.

[14] A. K. Agrawala, "Learning with a probabilistic teacher," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1227–1246, 1993.

[15] O. Chapelle, B. Schölkopf, and A. Zien, Eds., *Semi-Supervised Learning*. Morgan & Claypool Publishers, 2009.

[16] D. J. Miller and H. S. Uyar, "A mixture of experts classifier with feedback," in *NeurIPS*, 2018, pp. 6227–6234.

[17] Y. LeCun, "Reading digits in natural images with unsupervised feature learning," in *NIPS Workshop on Deep Learning and Unsupervised Feature Learning*, 2011.
[48x66]

[84x512] D. Vitale, P. Ferragina, and U. Scaiella, “Classification of short

[50x704] L. Zhang and G. Qi, “WCP: worst-case perturbations for semi-

[70x357] CVPR

[494x445]. IEEE Computer

[497x694]. IEEE Computer

[535x316], vol. 115, no. 3, pp. 211–252, 2015.

[134x385], vol. 115, no. 3, pp. 211–252, 2015.

[135x612] M. Nießner, “Scannet: Richly-annotated 3d reconstructions

[176x239]. IEEE Computer Society, 2017, pp.

[209x157]. IEEE, 2019, pp. 1931–

[266x275]. IEEE

[278x758] 22

[278x140]. ACL

[556x758]

[334x48] NIPS

[334x528] Computer Society, 2009, pp. 1–8.

[334x372] CVPR

[334x372] semi-supervised semantic image segmentation using stochastic

[334x408] CVPR

[334x417] dilated convolution: A simple approach for weakly- and semi-

[334x445] ICCV

[334x445] for semantic image segmentation,” in

[334x454] and semi-supervised learning of a deep convolutional network

[334x473] 1495–1503.

[334x537]. IEEE, 2019, pp. 7283–7292.

[334x621], ser. Lecture Notes in Computer Science, vol. 5302.

[396x584], vol. 33, no. 5, pp. 978–994, 2011.

[432x85], vol. abs/1908.05724, 2019.

[494x445]. IEEE Computer

[497x694]. IEEE Computer

[515x168] AAAI

[535x316], vol. 115, no. 3, pp. 211–252, 2015.

[540x658]. IEEE

[546x140] ACL

[556x758] 22

[562x140].

[562x344], 2012, pp. 830–839.

[598x584], vol. 33, no. 5, pp. 978–994, 2011.

[608x279]. IEEE, 2020, pp. 12 712–12 722.

[613x621], ser. Lecture Notes in Computer Science, vol. 5302.

[623x722], vol. 27, no. 1, pp. 349–364, 2018.

[633x248]. IEEE Computer Society, 2017, pp.

[646x239]. IEEE Computer Society, 2015, pp. 1635–1643.

[676x239]. IEEE, 2019, pp. 7283–7292.

[682x184]. IEEE, 2020, pp.

[693x157]. IEEE, 2019, pp. 1931–

[704x184]. IEEE, 2020, pp.

[715x279]. IEEE, 2020, pp. 12 712–12 722.

[720x621], ser. Lecture Notes in Computer Science, vol. 5302.

[730x722], vol. 27, no. 1, pp. 349–364, 2018.

[742x248]. IEEE Computer Society, 2017, pp.

[752x239]. IEEE Computer Society, 2015, pp. 1635–1643.

[763x184]. IEEE, 2020, pp.

[774x157]. IEEE, 2019, pp. 1931–

[785x184]. IEEE, 2020, pp.

[796x157]. IEEE, 2019, pp. 1931–

[807x184]. IEEE, 2020, pp.

[818x157]. IEEE, 2019, pp. 1931–

[829x184]. IEEE, 2020, pp.
[259] K. K. Singh, H. Yu, A. Sarmasi, G. Pradeep, and Y. J. Lee, “Hide-and-seek: A data augmentation technique for weakly-supervised localization and beyond,” CoRR, vol. abs/1811.02545, 2018.

[260] P. Chen, S. Liu, H. Zhao, and J. Jia, “Gridmask data augmentation,” CoRR, vol. abs/2001.04086, 2020.

[261] A. Singh, R. D. Nowak, and X. Zhu, “Unlabeled data: Now it helps, now it doesn’t,” in NIPS. Curran Associates, Inc., 2008, pp. 1513–1520.

[262] T. Yang and C. E. Priebe, “The effect of model misspecification on semi-supervised classification,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 10, pp. 2093–2103, 2011.

[263] N. V. Chawla and G. I. Karakoulas, “Learning from labeled and unlabeled data: An empirical study across techniques and domains,” J. Artif. Intell. Res., vol. 23, pp. 331–366, 2005.