GOOD SEMI-SUPERVISED VAE REQUIRES TIGHTER EVIDENCE LOWER BOUND

Anonymous authors
Paper under double-blind review

ABSTRACT

Semi-supervised learning approaches based on generative models have now encountered 3 challenges: (1) The two-stage training strategy is not robust. (2) Good semi-supervised learning results and good generative performance can not be obtained at the same time. (3) Even at the expense of sacrificing generative performance, the semi-supervised classification results are still not satisfactory. To address these problems, we propose One-stage Semi-suPervised Optimal Transport VAE (OSPOT-VAE), a one-stage deep generative model that theoretically unifies the generation and classification loss in one ELBO framework and achieves a tighter ELBO by applying the optimal transport scheme to the distribution of latent variables. We show that with tighter ELBO, our OSPOT-VAE surpasses the best semi-supervised generative models by a large margin across many benchmark datasets. For example, we reduce the error rate from 14.41% to 6.11% on Cifar-10 with 4k labels and achieve state-of-the-art performance with 25.30% on Cifar-100 with 10k labels. We also demonstrate that good generative models and semi-supervised results can be achieved simultaneously by OSPOT-VAE.

1 INTRODUCTION

The rise of deep neural networks has led to breakthroughs in computer vision, natural language processing, and many other domains. Most of these models are trained on large labeled datasets via supervised learning. However, in many scenarios, although it is easy to acquire a large amount of the original data, obtaining corresponding labels is often very costly or even infeasible. Semi-supervised learning (Thomas, 2009) is proposed to address this problem by training classifiers with sufficient unlabeled data and a small fraction of labeled data.

Recent works on semi-supervised learning can be grouped into three categories: (1) disagreement based learning via data perturbation (Miyato et al., 2019) and consistency enforcing (Verma et al., 2019), (2) metric learning (Wu et al., 2018), (3) generative approaches via generative adversarial network (GAN) (Springenberg, 2016) and variational autoencoder (VAE) (Kingma et al., 2014). Compared with the first two categories, generative approaches have great advantages in interpretability. Based on the latent variable assumption (Doersch, 2016), the generative model has an explicit variational inference form, so it can learn the marginal probability distribution of the raw data as well as the conditional distribution of the latent variables given the input data, which makes predictions more reasonable. Besides, generative approaches not only learn the required classification representations, but also capture the semantics-disentangled factors that generate the data, making it easier to generalize to different tasks (Narayanaswamy et al., 2017).

However, in practice, semi-supervised generative approaches often encounter three major challenges: (1) The two-stage training process is not robust. Semi-supervised VAE (Kingma et al., 2014) needs to be trained carefully with a two-stage hierarchical strategy, while the training process of GAN is a two-stage adversarial game (Chrysos et al., 2019). (2) Good semi-supervised learning results and good generative performance can not be obtained at the same time. In GAN, good semi-supervised learning performance will lead to a mismatch between the generated results and the real data distribution (Dai et al., 2017). While in VAE, the evidence lower bound (ELBO) objective is irrelevant to the classification loss, making it difficult to learn from the labels directly (Narayanaswamy et al., 2017). (3) Even at the expense of sacrificing generative performance, the semi-supervised classification results are still not satisfactory. In practice, disagreement-based meth-
ods (Xie et al., 2019; Berthelot et al., 2019) have dramatically improved the state-of-the-art results on several standard datasets, surpassing generative approaches by a large margin. These challenges naturally raise a question: What limits the performance of generative approaches in semi-supervised learning?

In this work, we propose One-stage Semi-supervised Optimal Transport VAE (OSPOT-VAE) to address these challenges. OSPOT-VAE presents the following improvements: (1) a one-stage semi-supervised VAE model that unifies the generation and classification loss in one ELBO framework. (2) an estimation of the margin between true log-likelihood and the ELBO that exports a tighter evidence lower bound by applying optimal transport (Ambrosio & Gigli, 2013) scheme to the distribution of latent variables.

Our model has the following contributions:

- We show that OSPOT-VAE can be well trained with a direct one-stage strategy.
- We show that OSPOT-VAE can achieve both good generative performance and semi-supervised learning results simultaneously on a series of benchmark datasets.
- We point out that it is the large margin between the ELBO and the log-likelihood of the input data that limits the performance of semi-supervised VAE. Besides, we evaluate this assumption across many standard datasets and show that with the proposed tighter ELBO, OSPOT-VAE surpasses the best semi-supervised generative models by a large margin and achieves state-of-the-art performance on Cifar-100 with 10k labels.

2 Semi-Supervised Learning Methods

In supervised learning (SL), we are facing with training data that appears as input-target pairs \((X, y) \in D_L\), sampled from an unknown distribution \(p(X, y)\). Our goal is to learn a function \(f(X; \phi)\) parameterized by \(\phi\) that makes the correct inference \(y\) for unseen samples from \(p(X)\). While in semi-supervised learning (SSL), we can obtain an extra collection of unlabeled data \(X \in D_U\) sampled from the same distribution \(p(X)\). We hope to leverage the data from both \(D_L\) and \(D_U\) to achieve a more accurate model than what would have been obtained by only using \(D_L\).

In this section, we review some existing methods for SSL. We mainly focus on those who have reached state-of-the-art results, as well as generative approaches which are strongly connected with our model; the more comprehensive overview is beyond the scope of this paper, we refer readers to (Oliver et al., 2018).

2.1 Disagreement Based Learning

Disagreement-based learning refers to the general approaches of imposing disagreement among multiple learners on the same task or multiple predictions from a single learner. By eliminating the disagreement, we can enforce the generalization of the model on unseen data. A common technique for creating disagreement is data augmentation, which applies transformations or perturbations on the input data and leaves class semantics unchanged. For \(X \in D_U\), loss term can be derived as

\[
\|f(\text{Augment}(X); \phi) - f(X; \phi)\|_2^2
\]

(1)

where the Augment(X) is a stochastic function which can be obtained by image transformation (Xie et al., 2019), virtual adversarial training (Miyato et al., 2019), or mixup method (Verma et al., 2018)
Berthelot et al. [2019]. Another disagreement construction technique is to train multiple learners on the same dataset and utilize the loss
\[ ||f(X; \phi_1) - f(X; \phi_2)||^2_2 \] (2)
to enforce the predictive consistency of different models, for example, “Mean Teacher” (Tarvainen & Valpola [2017] and “Teacher Graph” (Luo et al. [2018]). The generalization of the models gets enhanced.

2.2 Generative Approaches

In generative approaches, input X is supposed to have corresponding continuous and discrete latent variables, which we denote by z and c respectively.

Feature matching (FM) GANs (Salimans et al. [2016] Dai et al. [2017]) apply GANs to semi-supervised learning on K-classification tasks by specifying a (K+1)-class objective for the discriminator. Instead of binary classification, true samples are classified into the first K classes respectively and fake samples are classified into the (K+1)-th class. This target function achieves strong empirical results by matching the generator distribution with true data distribution and improves semi-supervised classification performance.

Semi-supervised VAEs (Kingma et al. [2014]; Narayanaswamy et al. [2017]) construct a probabilistic model parameterized by θ and φ describing the generation process of X by latent variables z and c:
\[ p(z) = \mathcal{N}(z; 0, I); \quad p(c) = \text{Mult}(c; K, \pi); \quad p_\theta(X|z, c) = f(X; z, c, \theta) \] (3)
where Mult(K, π) is the multinomial distribution with class K and parameter π. f(X; z, c, θ) is a suitable likelihood function, e.g., a Bernoulli or Gaussian distribution, parameterized by a non-linear transformation of the latent variables z and c. The class label y is treated as c if given. For the inference process, with the following hypothesis
\[ q_\phi(z, c|X) = q_\phi(z|X)q_\phi(c|X); \quad p(z, c|X) = p(z|X)p(c|X); \quad p(z, c) = p(z)p(c) \] (4)
evidence lower bound (ELBO) is used as objective to predict the posterior distribution of latent variables as follows (see Appendix A.1 for proof):
\[ \log p(X) \geq \mathbb{E}_{q_\phi(z, c|X)}[\log p_\theta(X|z, c)] - D_{KL}(q_\phi(z|X)||p(z)) - D_{KL}(q_\phi(c|X)||p(c)) = \text{ELBO} \] (5)
For the likelihood log p(X) is infeasible, VAE maximizes its evidence lower bound instead, which derives the loss function \( L(X; \phi, \theta) = -\text{ELBO} \). The predictions for the classification label y can be obtained from the inferred posterior distribution \( q_\phi(c|X) \). When class label y is not given, missing label sampling technique is used to sample from \( q_\phi(c|X) \) as
\[ \mathbb{E}_{q_\phi(c|X)} f(X; c, \theta) = \sum_{k=1}^{K} q_\phi(y_k|X) f(X; y_k, \theta) \] (6)
Here \( y_k \) represents a one-hot vector with 1 in k-th dimension. Utilizing this sampling method, the algorithmic complexity of VAE is proportional to K so it is computationally inefficient. Note that in objective (4), the label predictive distribution \( q_\phi(c|X) \) only contributes to the generative performance. To remedy this, existing models simply add a cross-entropy loss to the negative ELBO such that the distribution \( q_\phi(c|X) \) can also learn classification rules from the labeled data. The extended objective loss is
\[ \min_{\phi, \theta} \mathbb{E}_{X \sim \mathcal{D}_U} L(X; \phi, \theta) + \mathbb{E}_{(X, y) \sim \mathcal{D}_L} [L(X; c = y; \phi, \theta) - \log q_\phi(y|X)] \] (7)
Two-stage Training Strategy: In practice, (Kingma et al. [2014]) finds that directly training the one-stage objective (7) will lead to a bad semi-supervised learning result, so a two-stage training strategy is proposed to improve the model. The two-stage training strategy consists of two parts, M1 and M2. M1 means to learn a new continuous latent representation z1 first, and M2 means to train a semi-supervised model (7) with the embedding z1 from M1 instead of the raw data X. This M1+M2 strategy builds a deep VAE with two layers of random variables: \( p_\theta(X, z_1, z_2, c) = p_\theta(X|z_1)p_\phi(z_1|z_2, c)p(z_2)p(c) \), which can dramatically improve the performance of the inference \( q_\phi(c|X) \) but is not robust in training. Moreover, GAN’s training process can also be considered as two-stage with generator and discriminator competing with each other, and the two-stage adversarial game adds the difficulty in training.
3 ONE-STAGE SEMI-SUPERVISED OPTIMAL TRANSPORT VAE

In this section, we introduce our semi-supervised VAE framework, OSPOT-VAE. Firstly, we derive a one-stage loss function that unifies the generation and classification loss under one ELBO without introducing any additional auxiliary loss items like (7). Then, we analyze a phenomenon that good ELBO values do not guarantee good semi-supervised performance and propose the optimal transport estimation to deal with it. At last, combining the two parts, we give the detailed algorithm of OSPOT-VAE and discuss some problems in model optimization.

3.1 ONE-STAGE SEMI-SUPERVISED VAE

Following the notations and assumptions (3, 4) in Section 2.2 we derive our one-stage semi-supervised VAE. With the empirical distribution \( p_{emp}(X; D) = \frac{1}{|D|} \sum_{X \in D} 1_{X=x} \), we utilize the decomposition in [Zhao et al. 2017] and rewrite the second part of (5) into (proof in appendix A.2)

\[
\mathbb{E}_{p_{emp}(X)} D_{KL}(q_\phi(z|X)||p(z)) = I_{q_\phi(X; z)} + D_{KL}(q_\phi(z)||p(z)) \geq I_{q_\phi(X; z)}
\]

(8)

where \( q_\phi(z) = \frac{1}{|D|} \sum_{X \in D} q_\phi(z|x) \) and \( I_{q_\phi(X; z)} \) is the mutual information between \( X \) and \( z \). The left part of (8) equals to 0 when \( X \) and \( z \) are independent. This is undesirable, so \( I_{q_\phi(X; z)} \) can be regarded as the lower bound of controlled mutual information. The continuous variables in (8) can be easily extend to discrete variables \( c \). We can use \( I_z \) and \( I_c \) to denote the controlled information capacity and derive the objective for the unlabeled dataset \( \mathbb{D}_U \)

\[
\mathcal{L}_{\mathbb{D}_U}(X; \theta, \phi) = \mathbb{E}_{q_\phi(x|x; \theta, \phi)}[ -\log p_\theta(X, z, c)] + \beta_z D_{KL}(q_\phi(z|X)||p(z)) - I_z
\]

\(+ \beta_c D_{KL}(q_\phi(c|X)||p(c)) - I_c \)

(9)

where \( \beta, I_z, I_c \) are all hyper-parameters forcing the KL divergence term to match the mutual information capacities of \( z \) and \( c \).

For the labeled subset \( \mathbb{D}_L \), instead of directly employing class label \( y \) as sampled \( c \), we view it as the parameter of the true posterior distribution, i.e. \( p(c|X) = \text{Mult}(c; K, y) \) and derive the following one-stage ELBO form:

\[
\log p(X) = \log \mathbb{E}_{q_\phi(z|x), p(c|X)} \frac{p(X, z, c)}{q_\phi(z|X)p(c|X)} \geq \mathbb{E}_{q_\phi(z|x), p(c|X)} \log \frac{p(X, z, c)}{q_\phi(z|X)p(c|X)}
\]

\[= \mathbb{E}_{q_\phi(z|x), p(c|X)} [ \log p(X, z, c) + \log \frac{p(z)p(c)}{q_\phi(z|X)p(c|X)} ] = \mathbb{E}_{q_\phi(z|x), p(c|X)} \log p(X, z, c)
\]

\[- D_{KL}(q_\phi(z|X)||p(z)) - D_{KL}(p(c|X)||q_\phi(c|X)) + \mathbb{E}_{p(c|X)} \log \frac{p(c)}{q_\phi(c|X)} \]

(10)

Notice that \( D_{KL}(p(c|X)||q_\phi(c|X)) \) is equal to the common cross-entropy loss for \( y \) is a one-hot vector. In this respect, the margin between \( p(c|X) \) and \( q_\phi(c|X) \) can be significantly small when the suitable optimization method is chosen. This allows us to utilize the approximation \( p(c|X) \approx q_\phi(c|X) \) to modify \( \mathbb{E}_{p(c|X)} \log \frac{p(c)}{q_\phi(c|X)} \) in (10), resulting in a consist ELBO with \( \mathcal{L}_{\mathbb{D}_U}(X; \theta, \phi) \):

\[
\mathbb{E}_{p(c|X)} \log \frac{p(c)}{q_\phi(c|X)} \approx \text{when p(c|X)\approx q_\phi(c|X)} \mathbb{E}_{q_\phi(c|X)} \log \frac{p(c)}{q_\phi(c|X)} = D_{KL}(q_\phi(c|X)||p(c))
\]

(11)

Combining the ELBO form (10) of \( \mathbb{D}_L \) with the mutual information decomposition (8) and the approximation (11), the new objective for semi-supervised VAE is:

\[
\mathcal{L}_{\mathbb{D}_L}(X, y; \theta, \phi) = \mathbb{E}_{q_\phi(z|x), p(c|X)} [ -\log p_\theta(X|z, c) ] + \beta_z D_{KL}(q_\phi(z|X)||p(z)) - I_z
\]

\[+ \beta_c D_{KL}(q_\phi(c|X)||p(c)) - I_c + D_{KL}(p(c|X)||q_\phi(c|X)) \]

(12)

With (9) and (12), the objective for the entire dataset is now

\[
\min_{\theta, \phi} \mathbb{E}_{X \sim p_{emp}(X; \mathbb{D}_U)} \mathcal{L}_{\mathbb{D}_U}(X; \theta, \phi) + \mathbb{E}_{(X, y) \sim p_{emp}((X, y); \mathbb{D}_L)} \mathcal{L}_{\mathbb{D}_L}(X, y; \theta, \phi)
\]

(13)

This one-stage objective with a simple approximate transformation (9) unifies the generation loss as well as the target of SSL and results in improved performance of semi-supervised learning, which we demonstrate in Section 4.4.
In this scenario, the consistent optimization of ELBO will contribute no more to the expected margin between true log-likelihood and ELBO as (proof in appendix A.3):

\[
\int \int p(X) p(z|X)p(c|X) dz dc
\]

One phenomenon is that good ELBO values do not imply accurate inference. A typical example has been discussed in (Zhao et al., 2017). Here we mainly focus on the cause of this phenomenon and propose optimal transport estimation to alleviate this problem in semi-supervised learning. Following the work in (Rezende et al., 2014), we write down the closed form of the expected margin between true log-likelihood and ELBO as (proof in appendix A.3):

\[
\mathbb{E}_{p_{\text{emp}}(X)}[\log p(X) - \text{ELBO}] = \mathbb{E}_{p_{\text{emp}}(X)}[D_{KL}(q_\phi(z|X)||p(z|X)) + D_{KL}(q_\phi(c|X)||p(c|X))]
\]

Combined with the decomposition (8), it becomes possible by training the expected ELBO target on the approximation of ELBO. In this scenario, the consistent optimization of ELBO will contribute no more to the expected margin between true log-likelihood and ELBO as (proof in appendix A.3):

\[
\mathbb{E}_{p_{\text{emp}}(X)}[\log p(X) - \text{ELBO}] = \mathbb{E}_{p_{\text{emp}}(X)}[D_{KL}(q_\phi(z|X)||p(z|X)) + D_{KL}(q_\phi(c|X)||p(c|X))]
\]

However, one phenomenon is that good ELBO values do not imply accurate inference. A typical example has been discussed in (Zhao et al., 2017). Here we mainly focus on the cause of this phenomenon and propose optimal transport estimation to alleviate this problem in semi-supervised learning. Following the work in (Rezende et al., 2014), we write down the closed form of the expected margin between true log-likelihood and ELBO as (proof in appendix A.3):

\[
\mathbb{E}_{p_{\text{emp}}(X)}[\log p(X) - \text{ELBO}] = \mathbb{E}_{p_{\text{emp}}(X)}[D_{KL}(q_\phi(z|X)||p(z|X)) + D_{KL}(q_\phi(c|X)||p(c|X))]
\]

3.2 Optimal Transport Estimation

To summarize the above, VAE aims to learn the useful representation \(q_\phi(z|X)\) and \(q_\phi(c|X)\) by reducing the KL divergence between the empirical distribution \(p_{\text{emp}}(X)\) and the model marginal \(p(X) = \int_p X p(X)p(z|X)p(c|X) dz dc\). Instead of minimizing \(D_{KL}(p_{\text{emp}}(X)||p(X))\) directly, VAE models use the expected negative ELBO mentioned in (5) as target via the following inequality

\[
D_{KL}(p_{\text{emp}}(X)||p(X)) \leq H(p_{\text{emp}}(X)) - \mathbb{E}_{p_{\text{emp}}(X)}[\text{ELBO}]
\]

Optimal transport estimation in Algorithm 1 takes advantage of this fact and returns the approximation of the margin \(D_{KL}(q_\phi(z|X)||p(z|X))\) and \(D_{KL}(q_\phi(c|X)||p(c|X))\)

**Algorithm 1** Optimal transport estimation ingests a batch of observation \(X\) as well as the representation \(q_\phi(z|X), q_\phi(c|X)\) inferred from the original VAE and returns the approximation of the margin \(D_{KL}(q_\phi(z|X)||p(z|X))\) and \(D_{KL}(q_\phi(c|X)||p(c|X))\)

**Input:**
- Batch of observation \(X\) sampled from \(p_{\text{emp}}(X)\);
- Inferred parameter \((\mu, \text{diag}(\sigma^2))\) of \(q_\phi(z|X) = \mathcal{N}(z; \mu, \text{diag}(\sigma^2))\);
- Inferred parameter \(\pi\) of \(q_\phi(c|X) = \text{Mult}(c; K, \pi)\);
- Hyperparameter \(\alpha\) for mixup vicinal distribution \(p_{\text{mixup}}(X)\)

**Output:**
- \(X\) sampled from \(p_{\text{mixup}}(X)\);
- Approximation of the residual \(D_{KL}(q_\phi(z|X)||p(z|X))\), \(L_{R_\alpha}\);
- Approximation of the residual \(D_{KL}(q_\phi(c|X)||p(c|X))\), \(L_{R_\alpha}\);
- \(X'\), \(\pi'\), \(\mu'\), \(\sigma'^2\) = RandomPermutation\((X, \pi, \mu, \sigma^2)\);
- \(\tilde{\mu} = \text{OptimalTransport}(\pi, \pi', \lambda)\);
- \((\tilde{\mu}, \tilde{\sigma}^2) = \text{OptimalTransport}(\mu, \sigma^2, \lambda)\);
- \(\bar{p}(\tilde{z}|X) = \mathcal{N}(\tilde{z}; \tilde{\mu}, \text{diag}(\tilde{\sigma}))\);
- \(\bar{p}(c|X) = \text{Mult}(c; K, \tilde{\pi})\);
- \(L_{R_\alpha} = D_{KL}(q_\phi(z|X)||\bar{p}(z|X))\);
- \(L_{R_\alpha} = D_{KL}(q_\phi(c|X)||\bar{p}(c|X))\)

**Return** \(X, L_{R_\alpha}, L_{R_\alpha}\)
The estimation of true posterior distributions. Following the work of Ambrosio & Gigli (2013), the transport scheme, we can calculate the distributions transformation could associate with the shortest-path transport in the latent space. Using the optimal one straight line Optimal Transport Scheme Algorithm 2 Under review as a conference paper at ICLR 2020

Proposition 3.1. The optimal transport scheme (17) between \( z_1 \sim \mathcal{N}(\mu_1, \text{diag}(\sigma_1^2)) \) and \( z_2 \sim \mathcal{N}(\mu_2, \text{diag}(\sigma_2^2)) \) with \( \lambda \in [0, 1] \) is

\[
\begin{align*}
\hat{\mu} &= \lambda \mu_1 + (1 - \lambda) \mu_2 \\
\hat{\sigma} &= \lambda \sigma_1 + (1 - \lambda) \sigma_2
\end{align*}
\]

Proposition 3.2. The KL divergence based optimal transport scheme between \( c_1 \sim \text{Mult}(K, \pi_1) \) and \( c_2 \sim \text{Mult}(K, \pi_2) \) with \( \lambda \in [0, 1] \) is

\[
\begin{align*}
\hat{\pi} &= \lambda \pi_1 + (1 - \lambda) \pi_2
\end{align*}
\]

Algorithm 2 yields the optimal transport estimation of the margin in (15), which leads to a tighter ELBO. In Section 4.2, we demonstrate that with this tighter ELBO, the inference performance of semi-supervised VAE is significantly improved on many benchmark datasets.

### 3.3 Optimization of OSPOT-VAE

Combining one-stage semi-supervised VAE and optimal transport estimation, we can get the complete OSPOT-VAE model. The full OSPOT-VAE algorithm is provided in Algorithm 2 and a schematic is shown in Figure 1. Note that the conditions for the approximations used in Algorithm 2 satisfy (1) \( q_\theta(c | X) \approx p(c | X) \) and (2) the VAE model already achieves a good ELBO. Therefore, warm-up schedule (Higgins et al. 2017) is used to set parameters \( I_z, I_c, \beta_x, \beta_e \) and \( w_{R_e}, w_{R_e} \). We list the details of “ELBOScheduler(t)” and “WeightScheduler(t)” in appendix A.5.

In Algorithm 2, we apply stochastic gradient descent (SGD) as optimizer, which needs to calculate the gradient \( \nabla_{\phi, \theta} L \). The target loss \( L \) consists of KL divergence and the expected log-likelihood. The derivation of KL divergence part has a closed form, while calculating the gradient...
Note that with \(20\) https://github.com/PaperCodeSubmission/OSPOT-VAE \(tained at the same time by OSPOT-V AE (Section 4.3). The source code is available at
additional application, we show that good generative models and semi-supervised results can be ob-
an ablation study to verify the contribution of the optimal transport estimation. As an addi-
compare with other state-of-the-art SSL models mentioned in Section 2. Besides, We provide
performance of OSPOT-V AE under “WideResNet” \(\text{Zagoruyko & Komodakis, 2016}\) backbone and
by comparing with other one-stage and two-stage V AE models. Then, we evaluate the per-
In Section 4.1, we show the validity of our one-stage semi-supervised V AE objective
experiments on 4 standard SSL benchmark datasets, that is, MNIST, SVHN, Cifar10, and Ci-
K with the class number
2014) and \(Jang et al., 2017\), using the reparameterization trick as
\[ \nabla_{\theta,\phi} E_{q_\phi(z|x)} \log p_\theta(x|z) = E_N(\epsilon;0,1) \nabla_{\theta,\phi} \log p_\theta(x|\mu + \sigma \cdot \epsilon) \]
\[ E_{\text{Gumble}(\epsilon;0,1)} \nabla_{\theta,\phi} \log p_\theta(x) \text{Softmax}(\frac{\log (\pi + \epsilon)}{\tau}) \rightarrow \nabla_{\theta,\phi} E_{q_\phi(z|x)} \log p_\theta(x|\epsilon)(\tau \rightarrow 0) \] (20)
Note that with (20), the algorithmic complexity of one-stage semi-supervised VAE is independent
with the class number \(K\), making it easier to extend to large-scale classification tasks.

## 4 EXPERIMENTS

In this section, we demonstrate the 3 contributions of our OSPOT-VAE model with sufficient
experiments on 4 standard SSL benchmark datasets, that is, MNIST, SVHN, Cifar10, and Cifar100. In Section 4.1, we show the validity of our one-stage semi-supervised VAE objective (13) by comparing with other one-stage and two-stage VAE models. Then, we evaluate the performance of OSPOT-VAE under “WideResNet” \(\text{Zagoruyko & Komodakis, 2016}\) backbone and compare with other state-of-the-art SSL models mentioned in Section 2. Besides, We provide an ablation study to verify the contribution of the optimal transport estimation. As an additional application, we show that good generative models and semi-supervised results can be obtained at the same time by OSPOT-VAE (Section 4.3). The source code is available at https://github.com/PaperCodeSubmission/OSPOT-VAE more details are available in Appendix A.6

### 4.1 ONE-STAGE SEMI-SUPERVISED VAE

We evaluate the effectiveness of the one-stage semi-supervised VAE objective on 2 standard bench-
marks, MNIST and SVHN. As for baseline models, we consider two VAE-based SSL models, which are one-stage disentangled VAE \(\text{Narayanaswamy et al., 2017}\) and two-stage VAE(M1+M2) \(\text{Kingma et al., 2014}\). For fairness, except the target loss functions, all models use the same structure as is used in M1+M2 \(\text{Kingma et al., 2014}\). The results are presented in Table 1, and our model achieves the best performance.
Table 3: Error in Cifar100. † and * have the same meaning as described in Table 2.

<table>
<thead>
<tr>
<th>BackBone Model</th>
<th>Cifar100(4k labels)</th>
<th>Cifar100(10k labels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WRN-28-2</td>
<td>[39.19]</td>
<td>[39.19]</td>
</tr>
<tr>
<td>GS-BadGAN†∗</td>
<td>45.11</td>
<td>37.16</td>
</tr>
<tr>
<td>LP∗ (Iscen et al. 2019)</td>
<td>42.73</td>
<td>35.92</td>
</tr>
<tr>
<td>OSPOT-VAE</td>
<td>[40.58(±0.48)]</td>
<td>[31.41(±0.21)]</td>
</tr>
<tr>
<td>WRN-28-10 MixMatch∗ (Berthelot et al. 2019)</td>
<td>25.88</td>
<td></td>
</tr>
<tr>
<td>OSPOT-VAE</td>
<td>[33.76(±0.53)]</td>
<td>[25.30(±0.31)]</td>
</tr>
</tbody>
</table>

Table 4: Ablation study with SVHN, Cifar10, and Cifar100.

<table>
<thead>
<tr>
<th>Methods</th>
<th>SVHN(1k labels)</th>
<th>Cifar10(4k labels)</th>
<th>Cifar100(10k labels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-stage VAE</td>
<td>10.53(±0.17)</td>
<td>18.26(±0.51)</td>
<td>38.62(±0.67)</td>
</tr>
<tr>
<td>Optimal transport estimation (with encoder only)</td>
<td>6.54(±0.62)</td>
<td>10.71(±0.44)</td>
<td>36.21(±0.29)</td>
</tr>
<tr>
<td>OSPOT-VAE</td>
<td>[5.79(±0.15)]</td>
<td>[8.51(±0.32)]</td>
<td>[31.41(±0.21)]</td>
</tr>
</tbody>
</table>

4.2 OSPOT-VAE

We compare the results of OSPOT-VAE with two categories of state-of-the-art models mentioned in Section 2. In all experiments, we use the “WideResNet-28” model or other deep models with a comparable amount of parameters as the backbone. The results in Table 2 demonstrate that our model outperforms most of the existing methods and surpasses state-of-the-art semi-supervised generative models (Dai et al. 2017) by a large margin. Notice that recently, data-augmentation based method, MixMatch, (Berthelot et al. 2019) achieves the absolute state-of-the-art results in all benchmarks. It uses pre-designed sophisticated data augmentation strategies for different datasets and outperforms our model. We list its results fairly as a comparison, while OSPOT-VAE surpasses it in Cifar100 dataset. Ablation Study: The OSPOT-VAE model consists of two parts: (1) a one-stage VAE objective and (2) an optimal transport estimation. In ablation study, we analyze the effect of each component in our model with the backbone “WideResNet-28-2”. To study the independent effects of transport estimation, we combine it with the encoder part of OSPOT-VAE to build a classifier with loss function $L_{Rc}$. The improved classification error rates in Table 4 show that, with optimal transport estimation, the posterior inference $q_\phi(c|X)$ gets closer to the true distribution $p(c|X)$. It indicates that our optimal transport estimation does reduce the gap between ELBO and the log-likelihood of the input data and yield a tighter ELBO, which leads to a better semi-supervised performance.

4.3 GENERATIVE PERFORMANCE

$\mathbb{E}_{p_{\text{data}}(X)}$ measures the margin between the true data distribution and the distribution learned by generation models (Doersch 2016). By comparing the $\mathbb{E}_{p_{\text{data}}(X)}$ value of pure unsupervised VAE and our semi-supervised VAE model under the same “WideResNet-28-2” backbone, we demonstrate that good generative models and semi-supervised results can be obtained at the same time in OSPOT-VAE. The results in Table 5 show that the data generative distribution learned by our OSPOT-VAE model is as good as the pure VAE model. Further generated results are available in appendix A.7.

5 CONCLUSION

In this work, we pointed out that it was the large margin between ELBO and the true log-likelihood of the raw data that limits the performance of semi-supervised VAE. To this end, we introduced OSPOT-VAE, a one-stage generative model that unified the classification and generation objective and achieved a tighter ELBO by optimal transport estimation. We demonstrated our assertion through extensive experiments, and our semi-supervised results significantly outperform former state-of-the-art generative SSL methods by a large margin on Cifar10 and Cifar100.
REFERENCES


A APPENDIX

A.1 BASIC INEQUALITY OF ELBO

Proposition A.1. The Basic inequality of ELBO is
\[
\log p(\mathbf{X}) \geq \mathbb{E}_{q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X})}[\log p_\theta(\mathbf{X}|\mathbf{z}, \mathbf{c})] - D_{KL}(q_\phi(\mathbf{z}|\mathbf{X})||p(\mathbf{z})) - D_{KL}(q_\phi(\mathbf{c}|\mathbf{X})||p(\mathbf{c}))
\]
proof

\[
\log p(\mathbf{X}) = \log \int_{\mathbf{z}, \mathbf{c}} q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X}) \frac{p(\mathbf{X}, \mathbf{z}, \mathbf{c})}{q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X})} = \log \mathbb{E}_{q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X})} \frac{p(\mathbf{X}, \mathbf{z}, \mathbf{c})}{q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X})} \\
\geq \mathbb{E}_{q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X})} \log \frac{p(\mathbf{X}, \mathbf{z}, \mathbf{c})}{q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X})} \\
= \int_{\mathbf{z}, \mathbf{c}} q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X}) \log \frac{p(\mathbf{z}, \mathbf{c})}{q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X})} + \int_{\mathbf{z}, \mathbf{c}} q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X}) \log p_\theta(\mathbf{X}|\mathbf{z}, \mathbf{c}) \\
= -D_{KL}(q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X})||p(\mathbf{z}, \mathbf{c})) + \mathbb{E}_{q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X})}[\log p_\theta(\mathbf{X}|\mathbf{z}, \mathbf{c})] \\
= \text{with assumption (3,4)} \mathbb{E}_{q_\phi(\mathbf{z}, \mathbf{c}|\mathbf{X})}[\log p_\theta(\mathbf{X}|\mathbf{z}, \mathbf{c})] - D_{KL}(q_\phi(\mathbf{z}|\mathbf{X})||p(\mathbf{z})) - D_{KL}(q_\phi(\mathbf{c}|\mathbf{X})||p(\mathbf{c}))
\]

A.2 DECOMPOSITION OF ELBO IN INFO-VAE

Proposition A.2. The expected ELBO with empirical distribution satisfies
\[
\mathbb{E}_{p_{emp}(\mathbf{X})} D_{KL}(q_\phi(\mathbf{z}|\mathbf{X})||p(\mathbf{z})) = I_{q_\phi}(\mathbf{X}; \mathbf{z}) + D_{KL}(q_\phi(\mathbf{z})||p(\mathbf{z}))
\]
proof

\[
\mathbb{E}_{p_{emp}(\mathbf{X})} D_{KL}(q_\phi(\mathbf{z}|\mathbf{X})||p(\mathbf{z})) = \int_{\mathbf{X}} p_{emp}(\mathbf{X}) \int_{\mathbf{z}} q_\phi(\mathbf{z}|\mathbf{X}) \frac{q_\phi(\mathbf{z}|\mathbf{X})}{p(\mathbf{z})} d\mathbf{z} d\mathbf{X} \\
= \int_{\mathbf{X}} p_{emp}(\mathbf{X}) \int_{\mathbf{z}} q_\phi(\mathbf{z}, \mathbf{X}) \frac{q_\phi(\mathbf{z}|\mathbf{X})}{q_\phi(\mathbf{z})} d\mathbf{z} d\mathbf{X} + \int_{\mathbf{X}} p_{emp}(\mathbf{X}) \int_{\mathbf{z}} q_\phi(\mathbf{z}|\mathbf{X}) \frac{q_\phi(\mathbf{z})}{p(\mathbf{z})} d\mathbf{z} d\mathbf{X} \\
= \int_{\mathbf{X}} \int_{\mathbf{z}} q_\phi(\mathbf{z}, \mathbf{X}) \log \frac{q_\phi(\mathbf{z}, \mathbf{X})}{q_\phi(\mathbf{z}) p_{emp}(\mathbf{X})} d\mathbf{z} d\mathbf{X} + D_{KL}(q_\phi(\mathbf{z})||p(\mathbf{z})) \\
= I_{q_\phi}(\mathbf{X}; \mathbf{z}) + D_{KL}(q_\phi(\mathbf{z})||p(\mathbf{z}))
\]
A.3 The equation form of ELBO

**Proposition A.3.** The expected margin between the true log-likelihood \( E_{p_{emp}}(X) \log p(X) \) and \( E_{p_{emp}}(X) \) ELBO is
\[
E_{p_{emp}}(X) \log p(X) - \text{ELBO} = E_{p_{emp}}(X) [D_{KL}(q_\phi(z|X)||p(z|X)) + D_{KL}(q_\phi(c|X)||p(c|X))]
\]

**proof**

We just need to prove the following equation
\[
\log p(X) - \text{ELBO} = D_{KL}(q_\phi(z|X)||p(z|X)) + D_{KL}(q_\phi(c|X)||p(c|X))
\]
and the proof under assumption (3, 4) is
\[
\log p(X) = \int_{z,c} q_\phi(z|X) q_\phi(c|X) \log p(X) dz dc = \int_{z,c} q_\phi(z|X) q_\phi(c|X) \log \frac{p(X, z, c)}{p(z|X)p(c|X)} dz dc
\]
\[
= E_{q_\phi(z|X)} q_\phi(c|X) \log \frac{p(X, z, c)}{p(z|X)p(c|X)} + \int_{z,c} q_\phi(z|X) q_\phi(c|X) \log \frac{q_\phi(z|X) q_\phi(c|X)}{p(z|X)p(c|X)}
\]
\[
= \text{ELBO} + D_{KL}(q_\phi(z|X)||p(z|X)) + D_{KL}(q_\phi(c|X)||p(c|X))
\]

A.4 Optimal Transport Scheme

**Proposition A.4.**

1. The optimal transport scheme (17) between \( z_1 \sim \mathcal{N}(\mu_1, \text{diag}(\sigma_1^2)) \) and \( z_2 \sim \mathcal{N}(\mu_2, \text{diag}(\sigma_2^2)) \) with \( \lambda \in [0, 1] \) is
   \[
   \mu = \lambda \mu_1 + (1 - \lambda) \mu_2 \\
   \sigma = \lambda \sigma_1 + (1 - \lambda) \sigma_2
   \]
   \[
   (A.1)
   \]

**proof**

Utilizing the conclusions in [Kuang & Tabak, 2017], the closed form of optimal transport from one multi-normal distribution \( \mathcal{N}(z_1; \mu_1, \Sigma_1) \) to another normal distribution \( \mathcal{N}(z_2; \mu_2, \Sigma_2) \) is
\[
z \rightarrow T(z) = \mu_2 + T(z - \mu_1); \quad T = \Sigma_1^{-\frac{1}{2}}(\Sigma_1^{\frac{1}{2}} \Sigma_2 \Sigma_1^{\frac{1}{2}})^{\frac{1}{2}} \Sigma_1^{-\frac{1}{2}}
\]
Utilize the diag matrix assumption, the optimal transport theme with \( \lambda \) is
\[
z_\lambda = (1 - \lambda)z_1 + \lambda T(z_1) \\
T = \text{diag}(\sigma_1/\sigma_2)
\]
\[
(A.2)
\]
Utilize (A.2), we can get (A.1) as
\[
z_\lambda \sim \mathcal{N}(\mu, \text{diag}(\sigma^2)); \quad \mu = \lambda \mu_1 + (1 - \lambda) \mu_2; \quad \sigma = \lambda \sigma_1 + (1 - \lambda) \sigma_2
\]
\[
(A.2)
\]

2. The KL divergence based optimal transport scheme between \( c_1 \sim \text{Mult}(K, \pi_1) \) and \( c_2 \sim \text{Mult}(K, \pi_2) \) with \( \lambda \in [0, 1] \) is
   \[
   \tilde{\pi} = \lambda \pi_1 + (1 - \lambda) \pi_2
   \]
   \[
   (A.3)
   \]

**proof**

As the definition (17) has no closed-form solution for multinomial distribution, we use KL divergence instead. The KL divergence based optimal transport target \( c_\lambda \sim \text{Mult}(K, \tilde{\pi}) \) between two multinomial distribution \( c_1 \sim \text{Mult}(K, \pi_1) \) and \( c_2 \sim \text{Mult}(K, \pi_2) \) with \( \lambda \in [0, 1] \) satisfy
\[
\min \lambda D_{KL}(\pi_1||\tilde{\pi}) + (1 - \lambda) D_{KL}(\pi_2||\tilde{\pi}) \quad s.t. \quad \sum_{i=1}^{K} \tilde{\pi}_i = 1
\]
\[
(A.4)
\]
The Lagrange multiplier form of (A.4) is
\[
\mathcal{L}(\tilde{\pi}; t) = \lambda D_{KL}(\pi_1||\tilde{\pi}) + (1 - \lambda) D_{KL}(\pi_2||\tilde{\pi}) + t * (\sum_{i=1}^{K} \tilde{\pi}_i - 1)
\]
Table 6: Schedule Parameters

<table>
<thead>
<tr>
<th></th>
<th>MNIST</th>
<th>SVHN(one-stage)</th>
<th>SVHN</th>
<th>Cifar10</th>
<th>Cifar100</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(h_{\text{max}})</td>
<td>(t_{\text{max}})</td>
<td>(h_{\text{max}})</td>
<td>(t_{\text{max}})</td>
<td>(h_{\text{max}})</td>
</tr>
<tr>
<td>(\beta_z)</td>
<td>30</td>
<td>50</td>
<td>1</td>
<td>175</td>
<td>1e-3</td>
</tr>
<tr>
<td>(\beta_c)</td>
<td>30</td>
<td>50</td>
<td>1</td>
<td>175</td>
<td>1</td>
</tr>
<tr>
<td>(I_z)</td>
<td>17.5</td>
<td>50</td>
<td>50</td>
<td>175</td>
<td>1280</td>
</tr>
<tr>
<td>(I_c)</td>
<td>17</td>
<td>50</td>
<td>50</td>
<td>175</td>
<td>2.3</td>
</tr>
<tr>
<td>(w_{R_z})</td>
<td>(\)</td>
<td>(\)</td>
<td>(\)</td>
<td>(\)</td>
<td>(1e-3)</td>
</tr>
<tr>
<td>(w_{R_c})</td>
<td>(\)</td>
<td>(\)</td>
<td>(\)</td>
<td>(\)</td>
<td>(\)</td>
</tr>
</tbody>
</table>

and the related KKT conditions are

\[
\frac{\partial L(\bar{\pi}, t)}{\partial \bar{\pi}} = t - \lambda \pi_1 + (1 - \lambda) \pi_2 = 0
\]

\[
t \ast \left( \sum_{i=1}^{K} \bar{\pi}_i - 1 \right) = 0
\]

(A.5)

Solve the equation (A.5), we can get the closed form of \(\bar{\pi}\) as

\[
\bar{\pi} = \lambda \pi_1 + (1 - \lambda) \pi_2
\]

A.5 Schedule Analysis

The warm-up scheduler aims to slowly increase the parameters until they reach their maximum. For a certain hyperparameter \(h\), there are 2 parameters control its warm-up process, the target value \(h_{\text{max}}\) and the total epoch \(t_{\text{max}}\) to reach the target value. We use the exponential function to get the middle value \(h_t\) as

\[
h_t = h_{\text{max}} \times \exp \left[ -5 \times (1 - \min(1, t/t_{\text{max}}))^2 \right]
\]

(A.6)

The curve of (A.6) is shown in Figure 2 and we list the scheduler parameters of 4 benchmark datasets, i.e. MNIST, SVHN, Cifar10, Cifar100, in Table 6.
Table 7: Details of Training Process

<table>
<thead>
<tr>
<th></th>
<th>MNIST</th>
<th>SVHN(one-stage)</th>
<th>SVHN</th>
<th>Cifar10</th>
<th>Cifar100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latent Dim($z/c$)</td>
<td>10/10</td>
<td>32/10</td>
<td>128/10</td>
<td>128/10</td>
<td>128/100</td>
</tr>
<tr>
<td>Mutual Info($z/c$)</td>
<td>17.5/17.0</td>
<td>50/50</td>
<td>1280/2.3</td>
<td>200/2.3</td>
<td>1280/4.6</td>
</tr>
<tr>
<td>loss of $-\log p_\theta(X</td>
<td>c,z)$</td>
<td>BCE</td>
<td>BCE</td>
<td>MSE</td>
<td>MSE</td>
</tr>
<tr>
<td>$\alpha$ of $p_{mixup}(X)$</td>
<td>_</td>
<td>Adam</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>learning rate</td>
<td>5e-4</td>
<td>1e-3</td>
<td>0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lr scheduler(decay ratio)</td>
<td>_</td>
<td>_</td>
<td>every 50 epoch after 200-th epoch(0.5)</td>
<td><a href="0.2">500,600,650</a></td>
<td></td>
</tr>
<tr>
<td>weight decay</td>
<td>0</td>
<td>0</td>
<td>5e-4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A.6 DETAILS OF TRAINING PROCESS

Here we list some important items need to set in the training process for different process. We classify these items into 2 categories: (1) items related to the loss function and (2) items related to the optimization strategy. The details are as follows and we list the exact value in Table 7.

1. Items related to the loss function

- **Latent dim**
  The latent dim of discrete variable $c$ is the same as the number of classifications, that is, $K$. For continuous variable $z$, the latent dim is determined by experiments.

- **Mutual information**
  We find the value of continuous mutual information will affect the generative performance, but have little impact on semi-supervised learning results, so we choose a suitable value to get the best generative performance. For discrete information, we choose the value in the ideal scene, that is, $I_c = \log(K)$.

- **Calculation of $E_{q_\phi(z|x),q_\phi(c|x)} - \log p_\theta(X|c,z)$**
  $p_\theta(X|c,z)$ has two forms: (1) normal distribution with $N(f_\theta(c,z),I)$ and (2) multinomial distribution with $\text{Mult}(\text{dim}(X),f_\theta(c,z))$. For the two forms, the loss function of $-\log p_\theta(X|c,z)$ is mean square error (MSE) and binary cross entropy (BCE) respectively. We use reparameterization trick in (20) to approximate expectation, and the sampling frequency is 1.

- **$\alpha$ of $p_{mixup}(X)$**
  The $\beta(\alpha,\alpha)$ for mixup vicinal distribution will strongly affect SSL performance. We set it to 2 in all experiments.

2. Items related to the optimization strategy

- **Optimizer**
  In one-stage VAE, we use Adam. In OSPOT-VAE, we use SGD with momentum 0.9.

- **Learning rate**
  We set the initial learning rate to 0.1 in OSPOT-VAE, which obtains best SSL performance.

- **The scheduler of adjusting learning rate**
  We decay the learning ratio in some milestones with the specified decay rate.

- **Weight decay**
  Weight decay controls the strength of $L_2$ regularization.

We also list some standard training curves on benchmark datasets in Figure 3 and 4.
Figure 3: The training curves of Cifar10.
Left: classification performance. Right: $E_{q_{\phi}(z|X)q_{\phi}(c|X)} - \log p_{\theta}(X|c, z)$

Figure 4: The training curves of Cifar100.
Left: classification performance. Right: $E_{q_{\phi}(z|X)q_{\phi}(c|X)} - \log p_{\theta}(X|c, z)$

A.7 Generative Performance

Following figures 5-7 show the generation performance of our OSPOT-VAE.

Figure 5: The generative performance of OSPOT-VAE in MNIST and SVHN
Figure 6: Compare the generative performance of pure VAE and OSPOT-VAE in Cifar10

Figure 7: Compare the generative performance of pure VAE and OSPOT-VAE in Cifar100