Abstract

In this work, we propose a semi-supervised approach based on generative models to learn both feature representations and categories in an end-to-end manner. The learning process is guided by our proposed auxiliary task that performs assignments for the unlabeled data and regularizes the feature representations with the use of metric embedding methods. Our model is represented by a Gaussian Mixture Variational Autoencoder (GMVAE), in which, we model our categories with the Gumbel-Softmax distribution and we benefit from the autoencoder’s architecture to learn feature representations. Experimental results show the effectiveness of our method on three datasets: MNIST, Fashion-MNIST and SVHN.

1 Introduction

Semi-supervised learning aims to leverage limited amounts of labeled data, in conjunction with large amounts of unlabeled data to improve the model performance. In the last few years, Deep Neural Networks (DNNs) have been largely applied to solve this problem due to their ability of learning useful representations. The information of the unlabeled data can be incorporated into these networks through an unsupervised loss, pseudo-labels or other auxiliary tasks. Recently, Deep Generative Models (DGMs) have been widely used for semi-supervised learning. DGMs model complex high dimensional data by using latent variables. Numerous models are built on Variational Autoencoders (VAEs). For instance, Kingma et al. proposed the stacked generative model (M1+M2) whose latent space is the joint distribution over data and labels. Maaløe et al. introduced the auxiliary deep generative model (ADGM) which utilizes an extra set of auxiliary latent variables to improve the variational lower bound. Further, Maaløe et al. also propose the Skip Deep Generative Model (SDGM) which shows superior performance compared to an ADGM. Unlike these works, our probabilistic model is based on a GMVAE that does not require pre-training and compared to other GMVAE implementations, ours is a modification of the M2 model that considers deterministic feature representations. In addition to that, we use the Gumbel-Softmax distribution to approximate the discrete latent variable.

In this paper, we propose a semi-supervised approach that considers the use of deep generative models to learn feature representations that are guided by our auxiliary tasks in the form of loss functions. Unlike previous semi-supervised probabilistic methods, where the discrete latent variable is considered observable when using labeled data, we consider the complete model as unsupervised and we include the knowledge of the labeled data through our auxiliary tasks. Our total loss function is:

\[ \mathcal{L}_{total} = \mathcal{L}_{var} + \mathcal{L}_{aux}, \]  

where \( \mathcal{L}_{var} \) is the variational loss given by the generative model and \( \mathcal{L}_{aux} \) is our proposed auxiliary task loss. A general view of our proposed model is depicted in Fig. 1.
Figure 1: Illustration of the proposed model. Our encoder transforms the data into feature representations, which are used to infer a gaussian and categorical distribution. We take advantage of the small amount of labeled data to perform category assignments for the unlabeled data and regularize the feature space by using our auxiliary tasks.

Figure 2: Probabilistic graphical model of our approach. The node \( \hat{x} \) in the inference model represents a feature representation obtained from an encoder network.

2 Semi-supervised Learning using Deep Generative Models

For semi-supervised classification, Kingma et al. [11] proposed the stacked generative model M1+M2. This model is comprised of two approaches: a latent-feature discriminative model (M1) and a generative semi-supervised model (M2). The former is represented by a vanilla Variational Autoencoder (VAE) [9, 10] and is used to learn feature representations. The latter generates data from a discrete latent variable \( y \), represented by a categorical distribution, and a continuous variable \( z \), represented by a gaussian distribution. The M2 objective trains a discriminative network \( q_\phi(z|x,y) \), inference network \( q_\phi(z|x,y) \) and generative network \( p_\theta(x|z,y) \) by maximizing a variational lower bound. For labeled data, the class variable \( y \) is observed and \( z \) is the latent variable to be inferred. For unlabeled data both \( y \) and \( z \) are latent variables to be inferred.

The M1+M2 model uses hierarchical stochastic layers that Kingma et al. [11] were not able to train end-to-end, and thus relied on pre-training. The problem of hierarchical stochastic variables is due to the posterior collapse observed in \( z \) [17–20], where the distribution \( q_\phi(z|x,y) \) collapses to the prior \( p(z) \). To avoid this problem, Figueroa et al. [21] replaced the stochastic latent variable of the M1 model with a deterministic one. The posterior collapse is also observed in the latent variable \( y \), Shu et al. [22] performed an analysis of the M2 model for the problem of unsupervised clustering and found that it fails because the distribution \( q_\phi(y|x) \) collapses to the prior \( p(y) \). Similarly, Willetts et al. [23] found that this collapse also takes place over the subspace of unlabeled classes in the semi-supervised problem. To address this problem, Shu [24] proposed a modification of the M2 model, that explicitly models \( z \) as a Gaussian mixture conditioned on \( y \).

3 Probabilistic Model

Our probabilistic model is similar to the M1+M2 model proposed by Kingma et al. [11], in which, we replace the stochastic latent variable of the M1 model with a deterministic one to learn feature representations, in a similar way to that proposed by Figueroa et al. [21]. Thus, our learned representations are defined as \( \hat{x} = g(x) \), we use these representations as input to our probabilistic model. Our model is represented by a GMVVAE, which is based on the modification proposed by Shu [24].

3.1 Generative Model

We use two latent variables to model the data, the continuous variable \( z \) and the discrete variable \( y \), i.e., we have \( p_\theta(x,z,y) \). Our generative model is defined as \( p_\theta(x|z)p_\theta(z|y)p(y) \), cf. Fig. 25.

\[
p(y) = \text{Cat}(y|\pi),
\]

\[
p_\theta(z|y) = \mathcal{N}(z|\mu_\theta(y),\sigma_\theta^2(y)),
\]

\[
p_\theta(x|z) = \mathcal{N}(z|\mu_\theta(z),\sigma_\theta^2(z)) \text{ or } \mathcal{B}(z|\mu_\theta(z)),
\]

where \( p_\theta(x|z) \) is Gaussian (\( \mathcal{N} \)) or Bernoulli (\( \mathcal{B} \)) depending on whether \( x \) is continuous or discrete.
3.2 Variational Lower Bound

Computing the posterior \( p_\theta(z, y|x) \) is intractable, thus we approximate this posterior with a tractable one, \( q_\phi(z, y|x) \), by using variational inference [9]. Therefore, our inference model is defined as \( q_\phi(z|x, y)q_\phi(y|x) \), cf. Fig. 2a.

\[
\begin{align*}
q_\phi(y|x) &= \text{Cat}(y|\pi_\phi(\hat{x})), \\
q_\phi(z|x, y) &= \mathcal{N}(z|\mu_\phi(\hat{x}, y), \sigma_\phi^2(\hat{x}, y)),
\end{align*}
\]

where \( \text{Cat}(y|\pi_\phi(\hat{x})) \) is a categorical distribution that we approximate with the Gumbel-Softmax distribution [15, 16]. As aforementioned, we consider our probabilistic model as unsupervised, i.e., we require to infer both latent variables \( y \) and \( z \). Therefore, we optimize the model by maximizing the following lower bound:

\[
\log p_\theta(x) \geq \mathbb{E}_{q_\phi(y|x)} \left[ \mathbb{E}_{q_\phi(z|x, y)} \left[ \log p_\theta(x|z) \right] - KL(q_\phi(z|x, y)||p_\theta(z|y)) \right] - KL(q_\phi(y|x)||p(y))
\]

where the first term is given by the reconstruction loss \( (L_R) \), the second term is the mixture of gaussians loss \( (L_G) \) and the last term is denoted as the categorical loss \( (L_C) \). Therefore, our variational loss is defined as \( L_{va} = L_R + w_GL_G + w_CL_C \), where \( w_G \) and \( w_C \) are weights that specify the importance of the gaussian and categorical loss functions.

4 Auxiliary Tasks

Our main objective is to guide the learning process of our probabilistic model to perform semi-supervised classification. To achieve it, we propose two auxiliary tasks in the form of loss functions: the assignment loss \( (L_A) \) and the metric embedding loss \( (L_M) \). The first one considers the feature representations of the data to learn category assignments, and the second one regularizes the feature representations with the use of metric embedding methods. Therefore, our auxiliary task loss is given by \( L_{aux} = w_AL_A + w_ML_M \), where the weights \( w_A \) and \( w_M \) define the importance of each task.

4.1 Assignment Loss

Our first auxiliary task assigns labels to the unlabeled data. In order to do it, we use the distance-weighted \( k \)-nearest neighbor \((k-NN) \) on the feature space, i.e., we compare the features of the unlabeled data, \( \hat{x}_u \), with the features of the labeled data, \( \hat{x}_l \), and assign the label based on the contribution or weight of each of the \( k \) nearest neighbors. The assigned label for each unlabeled data is given by:

\[
y = \arg\max_j \sum_{(x_i, y_i) \in D_k} w_i \times I(j = y_i),
\]

where \( y \) is the assigned label, \( D_k \) is the set of the \( k \) closest samples, \( w_i \) is the weight of the \( i \) sample and is given by \( 1/\text{distance}(\hat{x}_u, \hat{x}_l) \). A similar assignment process was proposed by Hoffer et al. [26] and Figueroa et al. [8] but they considered only the nearest neighbor \((1-NN) \). Once we obtained the assignments for the unlabeled data, we teach our network about these assignments with the cross-entropy loss that we denote as Assignment Loss \( (L_A) \).

4.2 Metric Embedding Loss

Our second auxiliary task regularizes the feature space. In order to do it, we use metric learning methods [27,28] on the feature space, in such a way that the distance between features that belong to the same category should be smaller than features of different categories. In our experiments, we use the lifted structured loss [23], but any metric learning method can be used. This loss function is applied after the assignment process because it requires all the data labeled. We denote this loss as the Metric Embedding Loss \( (L_M) \).
We run our method with...

We evaluate our method on three image datasets. MNIST [29]: a dataset containing a total of 70,000 handwritten digits with 60,000 training and 10,000 testing samples, each being a 28 × 28 image. SVHN [30]: consists of 99,289 house number digits with 73,257 training and 26,032 testing samples of size 3 × 32 × 32. There is an additional extra set of 531,131 samples for training. However, we do not consider this additional set in our experiments. Fashion-MNIST [31]: This dataset has the same number of images and the same image size of MNIST, but it is more complicated. Instead of digits, it consists of various types of fashion products. For image pre-processing, we normalize the image intensities to be in the range of [0, 1] for all the datasets, and consequently use the sigmoid function in the last layer of the decoder. We use the pre-defined train/test splits of each data set, from the training set we consider 80% for training and 20% for validation. Furthermore, we randomly chose 100 labeled examples for MNIST and Fashion-MNIST, and 1000 for SVHN and Fashion-MNIST that are fixed for the whole training phase. We ensure that all classes have the same number of labeled images.

Table 1: Semi-supervised test error (%) benchmarks on MNIST, SVHN and Fashion-MNIST for randomly and evenly distributed labeled data. The results with (*) on top use an additional extra set for training.

<table>
<thead>
<tr>
<th>Method</th>
<th>MNIST</th>
<th>SVHN</th>
<th>Fashion-MNIST</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>100</td>
<td>1000</td>
<td>100</td>
</tr>
<tr>
<td>M1+T SVM [11]</td>
<td>11.82 (± 0.25)</td>
<td>55.33 (± 0.11)</td>
<td>-</td>
</tr>
<tr>
<td>M1+M2 [11]</td>
<td>3.33 (± 0.14)</td>
<td>36.02 (± 0.10)</td>
<td>-</td>
</tr>
<tr>
<td>SS-Clustering [8]</td>
<td>1.66 (± 0.20)</td>
<td>20.66 (± 1.09)</td>
<td>-</td>
</tr>
<tr>
<td>SDGM [12]</td>
<td>1.32 (± 0.07)</td>
<td>16.61* (± 0.24)</td>
<td>-</td>
</tr>
<tr>
<td>ADGM [12]</td>
<td>0.96 (± 0.02)</td>
<td>22.86*</td>
<td>-</td>
</tr>
<tr>
<td>Proposed</td>
<td>1.94 (± 0.49)</td>
<td>14.78 (± 0.40)</td>
<td>26.88 (± 0.86)</td>
</tr>
</tbody>
</table>

5 Experiments

5.1 Datasets

We evaluate our method on three image datasets. MNIST [29]: a dataset containing a total of 70,000 handwritten digits with 60,000 training and 10,000 testing samples, each being a 28 × 28 image. SVHN [30]: consists of 99,289 house number digits with 73,257 training and 26,032 testing samples of size 3 × 32 × 32. There is an additional extra set of 531,131 samples for training. However, we do not consider this additional set in our experiments. Fashion-MNIST [31]: This dataset has the same number of images and the same image size of MNIST, but it is more complicated. Instead of digits, it consists of various types of fashion products. For image pre-processing, we normalize the image intensities to be in the range of [0, 1] for all the datasets, and consequently use the sigmoid function in the last layer of the decoder. We use the pre-defined train/test splits of each data set, from the training set we consider 80% for training and 20% for validation. Furthermore, we randomly chose 100 labeled examples for MNIST and Fashion-MNIST, and 1000 for SVHN and Fashion-MNIST that are fixed for the whole training phase. We ensure that all classes have the same number of labeled images.

5.2 Implementation Details

We employ convolutional neural networks to represent our encoder and decoder networks and fully connected multilayer networks to infer our latent variables. Our inference and generative models are parameterized by three neural networks: gaussians model \( q_\phi(z|x, y) \), categorical model \( q_\phi(y|x) \) and generative model \( p_\theta(x|z, y) \). Detailed model architectures can be found in Appendix A.

For training we use Adam [32] optimizer with a learning rate of 0.001. We iterate for 200 epochs and at each epoch we consider a different random permutation of our data. We use a batch size of 200 for MNIST and Fashion-MNIST, and 400 for SVHN. Half of the batch is composed by labeled data that is randomly selected. The feature size \( f_{x,z} \) is 100 for both MNIST and SVHN, and 200 for Fashion-MNIST, the gaussian size \( g_{x,z} \) is 100 for MNIST, 150 for SVHN and 50 for Fashion-MNIST; we use 5 nearest neighbors in the assignment process for MNIST and 3 for SVHN and Fashion-MNIST. The weights of the auxiliary tasks are \( w_A = 5 \) and \( w_M = 3 \) for SVHN, \( w_A = w_M = 1 \) for MNIST and \( w_A = 1 \) and \( w_M = 0.1 \) for Fashion-MNIST. The margin used in the metric embedding loss is 2 for MNIST, 0.5 for SVHN and 1 for Fashion-MNIST. We use the mean square error in the reconstruction loss for all the datasets. Finally, we smooth the temperature used in Gumbel-Softmax from 1 to 0.5 in the first 50 epochs. All the hyperparameters were found in the validation set using random search.

5.3 Quantitative Results

We run our method with 5 random seeds and report the average performance. All the results of the related works were reported from the original papers. The character ‘*’ means that results for that metric or setup were not executed. We compared our method with probabilistic generative models applied to semi-supervised classification.

As we can see in Table 1 for the MNIST dataset, our method obtained comparable results with SDGM [12] and ADGM [12], which are models that use skip connections between the input data and all the latent variables in the inference model. We can see the effectiveness of our method on the
Table 2: Semi-supervised test error (%) of our probabilistic model when we train it only with the assignment loss ($L_A$) and jointly with the metric embedding loss ($L_M$) on the MNIST, SVHN and Fashion-MNIST datasets.

<table>
<thead>
<tr>
<th>Auxiliary Task</th>
<th>MNIST</th>
<th>SVHN</th>
<th>Fashion-10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_A$</td>
<td>10.16</td>
<td>58.77</td>
<td>29.98</td>
</tr>
<tr>
<td>$L_A + L_M$</td>
<td>1.94</td>
<td>14.78</td>
<td>26.88</td>
</tr>
</tbody>
</table>

Table 3: Clustering performance, ACC(%) and NMI(%), on MNIST and Fashion-MNIST.

<table>
<thead>
<tr>
<th>Method</th>
<th>MNIST</th>
<th>Fashion-10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ACC</td>
<td>NMI</td>
</tr>
<tr>
<td>GMVAE [13]</td>
<td>82.31</td>
<td>-</td>
</tr>
<tr>
<td>IDEC [33]</td>
<td>88.06</td>
<td>86.72</td>
</tr>
<tr>
<td>VaDE [14]</td>
<td>94.46</td>
<td>87.60</td>
</tr>
<tr>
<td>JULE-RC [34]</td>
<td>96.40</td>
<td>91.30</td>
</tr>
<tr>
<td>DEPICT [35]</td>
<td>96.50</td>
<td>91.70</td>
</tr>
<tr>
<td>DualAuto [36]</td>
<td>97.80</td>
<td>94.10</td>
</tr>
<tr>
<td>Proposed (Avg.)</td>
<td>92.46</td>
<td>88.16</td>
</tr>
<tr>
<td>Proposed (Best)</td>
<td>97.36</td>
<td>93.44</td>
</tr>
</tbody>
</table>

SVHN dataset, where we outperformed all the probabilistic methods without the use of the additional extra training set. We also reported results for the Fashion-MNIST, where we did not get as good results as MNIST because this is a harder dataset.

Besides the comparison with state-of-the-art methods, we performed an ablation study over the auxiliary tasks. To do so, we trained our probabilistic model only with the assignment loss ($L_A$) and with both assignment loss ($L_A$) and metric embedding loss ($L_M$). Table 2 shows the results of this study, we can see that with the assignment loss we are able to obtain reasonable results on MNIST and Fashion-MNIST. However, it is not very useful on the SVHN dataset. Recall that this loss depends on the feature representations to obtain assignments for classification. Therefore, if the feature representations are not learned properly, the assignment loss will misclassify the data.

According to the results, regularizing the feature space with the metric embedding loss is of great importance to improve the performance of our model and achieve competitive results.

5.3.1 Unsupervised Clustering

Our proposed model can be applied to clustering. To do so, we train our probabilistic model without labeled data. We examine the clustering performance on the MNIST and Fashion-MNIST datasets. For this task, we consider a different set of hyperparameters. We use a batch size of 64 for both datasets. The feature size ($f_{sz}$) is 100 for MNIST and 200 for Fashion-MNIST, the gaussian size ($g_{sz}$) is 150 for MNIST and 50 for Fashion-MNIST. Finally, the weight of the gaussian loss ($w_G$) is set to 5. We train our models with the binary cross entropy loss for reconstruction. This set of hyperparameters gives us better results than those used in the semi-supervised task.

We evaluate our clustering results with two metrics commonly used in the literature, clustering accuracy (ACC) and normalized mutual information (NMI) [37]. We report the average and best results of 5 random seeds. We compare our method with probabilistic generative models [13, 14] and models that use convolutional networks [33–36]. As we can see in Table 3, our average results are competitive with the state-of-the-art and the best results outperform different methods. Compared to probabilistic generative models, our model outperforms the GMVAE proposed by Dilokthanakul et al. [14] and our best run outperforms VaDE [14] on the MNIST and Fashion-MNIST datasets, these methods are very related to us because they also model the data with a mixture of gaussians.

5.4 Qualitative Results

Besides classification, we also evaluated the generative part of our model. Fig. 3 shows how our model can generate random images for each category. Fig. 4 depicts the feature representations of all the datasets using t-SNE [38], we reduced the dimensionality of the feature representations to 2D and plot the test sets. Different colors indicate ground-truth classes. We can see that for MNIST and SVHN datasets we obtained a good separability of the categories. However, for Fashion-MNIST the separability is not very clear because some samples of different categories are mixed.
6 Conclusions

In this paper, we proposed a semi-supervised method that combines the variational loss given by a GMV AE with our proposed auxiliary tasks that assign labels to the unlabeled data and regularize the feature space using metric embedding methods. Our approach is not restricted to GMV AE and can be applied to other models like M2 [11] or ADGM [12]. Experimental results show that our approach can obtain competitive results by adding loss functions that drive the learning process of our generative model. One problem of the current version of our approach is the fact that we require to change the weights of some loss functions in order to get good results. Future work focuses on the application of methods to avoid posterior collapse like InfoVAE [39]. Furthermore, we can improve the assignment process using more complex techniques.

References


Appendix

A Network Architectures

Table 4 provides a description of the encoder architecture used to learn feature representations, \( \hat{x} = g(x) \). The discriminative network \( q_{\phi}(y|\hat{x}) \), is given by the set of linear layers: \( f_{sz} - f_{sz} - c \), where \( f_{sz} \) is the feature size of \( \hat{x} \), \( c \) is the number of classes, the output vector is given by the Gumbel-Softmax distribution. The architecture of the inference network \( q_{\phi}(z|\hat{x}, y) \), is \( (f_{sz} + c) - z_{sz} - z_{sz} - z_{sz} \), where the input is the concatenation of the features and categories, \( z_{sz} \) is the size of the gaussian latent variable, its output vector is given by the reparameterization trick of the gaussian distribution. The architecture of \( p_{\theta}(z|y) \) is given by two linear layers for \( \mu \) and \( \sigma^2 \) respectively. All the linear layers are followed by Leaky ReLU non-linearity. Finally, the architecture of the generative model \( p_{\theta}(x|z) \) is given in Table 5.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>layer1</th>
<th>layer2</th>
<th>layer3</th>
<th>layer4</th>
<th>layer5</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>(16@5, 1, 1)</td>
<td>(32@5, 1, 1)</td>
<td>(64@4, 2, 2)</td>
<td>(128@4, 2, 2)</td>
<td>( f_{sz}@5, 1, 1 )</td>
</tr>
<tr>
<td>SVHN</td>
<td>(16@5, 1, 1)</td>
<td>(32@5, 1, 1)</td>
<td>(64@4, 2, 2)</td>
<td>(128@4, 2, 2)</td>
<td>( f_{sz}@6, 1, 1 )</td>
</tr>
<tr>
<td>Fashion-10</td>
<td>(16@5, 1, 1)</td>
<td>(32@5, 1, 1)</td>
<td>(64@4, 2, 2)</td>
<td>(128@4, 2, 2)</td>
<td>( f_{sz}@5, 1, 1 )</td>
</tr>
</tbody>
</table>

Table 5: Neural Network Architecture of \( p_{\theta}(x|z) \): The input is a vector of size \( f_{sz} \). All the layers are followed by Batch Normalization and ReLU non-linearity. Convolutional layers are specified as (filters@filterSize, stride, padding). The output is an image.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>layer1</th>
<th>layer2</th>
<th>layer3</th>
<th>layer4</th>
<th>layer5</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST</td>
<td>(128@5, 1, 1)</td>
<td>(64@4, 2, 2)</td>
<td>(32@4, 2, 2)</td>
<td>(16@5, 1, 1)</td>
<td>(1@5, 1, 1)</td>
</tr>
<tr>
<td>SVHN</td>
<td>(128@6, 1, 1)</td>
<td>(64@4, 2, 2)</td>
<td>(32@4, 2, 2)</td>
<td>(16@5, 1, 1)</td>
<td>(3@5, 1, 1)</td>
</tr>
<tr>
<td>Fashion-10</td>
<td>(128@5, 1, 1)</td>
<td>(64@4, 2, 2)</td>
<td>(32@4, 2, 2)</td>
<td>(16@5, 1, 1)</td>
<td>(1@5, 1, 1)</td>
</tr>
</tbody>
</table>