Variational Clustering: Leveraging Variational Autoencoders for Image Clustering

Vignesh Prasad*
Technical University of Darmstadt
Germany
vignesh.prasad@tu-darmstadt.de

Dipanjan Das*
Embedded Systems and Robotics
TCS Research & Innovation, Kolkata, India
TCS Research & Innovation, Kolkata, India
dipanjan.da@tcs.com

Brojeshwar Bhowmick
Embedded Systems and Robotics

Abstract—Recent advances in deep learning have shown their ability to learn strong feature representations for images. The task of image clustering naturally requires good feature representations to capture the distribution of the data and subsequently differentiate data points from one another. Often these two aspects are dealt with independently and thus traditional feature learning alone does not suffice in partitioning the data meaningfully. Variational Autoencoders (VAEs) naturally lend themselves to learning data distributions in a latent space. Since we wish to efficiently discriminate between different clusters in the data, we propose a method based on VAEs where we use a Gaussian Mixture prior to help cluster the images accurately. We jointly learn the parameters of both the prior and the posterior distributions. Our method represents a true Gaussian Mixture VAE. This way, our method simultaneously learns a prior that captures the latent distribution of the images and a posterior to help discriminate well between data points. We also propose a novel reparametrization of the latent space consisting of a mixture of discrete and continuous variables. One key takeaway is that our method generalizes better across different datasets without using any pre-training or learnt models, unlike existing methods, allowing it to be trained from scratch in an end-to-end manner. We verify our efficacy and generalizability experimentally by achieving state-of-the-art results among unsupervised methods on a variety of datasets. To the best of our knowledge, we are the first to pursue image clustering using VAEs in a purely unsupervised manner on real image datasets.

Index Terms—Unsupervised Learning, Clustering, Variational Inference

I. INTRODUCTION

Image Clustering is a fundamental, challenging and widely studied problem in machine learning [3]–[8]. Some classical examples are K-means [9], Gaussian Mixture Models [10] and Spectral clustering [6] which are promising, but require a robust feature representation for good clustering. In recent years, Deep Learning has made huge progress in learning robust feature representations of images. These learned representations help cluster the data more accurately when used with traditional methods like K-means for example [11]. One way to use deep representations, off the shelf, is to extract the feature representation of an image from a pre-trained model and use them directly in any clustering algorithm [12].

The problem with such approaches is that they don’t fully exploit the power of deep neural networks. Song et al. [13] learn a representation to accurately cluster the images in the dataset by integrating K-means into the bottleneck layer of an Autoencoder. This association enables the model to learn a meaningful clustering-oriented representation.

With the motivation to pursue a robust and generalizable methodology in a principled way, we aim to make inferences in a latent space learned specifically for a clustering task. The idea is that it would be easier to group the data in this space, compared to an arbitrary space defined by pre-trained features. Off late, the use of generative methods for clustering has been on the rise as their expressive power helps efficiently capture, represent and recreate sampled data points. As we wish to experiment with data distributions in a latent space that can accurately represent the input data, the paradigm of Variational Autoencoders (VAEs) lends itself directly to the task at hand.

We build on the ideas of GMVAE [1] and VaDE [2] addressing their fallacies while maintaining the underlying motivation of using a Gaussian Mixture Model as the latent space distribution. Instead of deriving the prior from a random variable, as in GMVAE, our prior is deterministic. This is similar to VaDE however, we learn the parameters for the prior and posterior jointly, unlike in VaDE which uses a pre-training phase to initialize the parameters of the prior.

To illustrate the differences between our process, GVMAE [1] and VaDE [2] we visualize the graphical models in Fig. 1. In GMVAE, the Gaussian prior $z_2$ depends on a noise variable $z_1$ & varies for a given cluster, as shown in Fig. 1a. Ours is more intuitive as it depends only on the cluster, as shown in Fig. 1c. Secondly, GMVAE expresses the categorical posterior $q(k|z_1, z_2)$ with the prior $p_\beta(z_2|z_1, k)$ using Bayes’ rule. This applies to VaDE too, along with fixing the GMM prior during pre-training. We learn it during training, giving more flexible learning, the effectiveness of which is seen in the results in Table 1. This can also be seen on a toy dataset, compared to GMVAE, where our method learns a more compact cluster representation as compared to GMVAE, as shown in Fig. 3.

Our method is more principled as we directly learn the cluster assignment probabilities $q(k|z)$ instead of performing a Bayesian classification, as done in both GMVAE and VaDE. Once the cluster predictions $q(k|z)$ become closer to a one-hot vector, it, in turn, minimizes the loss for just a given
and perform K-means on the learnt latent space. Similarly, between positive and negative anchor images from the dataset et al. [15] follow a similar approach by using a triplet loss subsequently performing clustering in the feature space. Nina classical clustering by first learning a feature representation and

Fig. 1: Graphical representation of the inference and generative models used by us and GMVAE [1]. VaDE [2] also has a similar generative model as ours but differ in their inference model. Grey nodes represent data nodes. White ones represent latent nodes, where $z$, $z_1$ and $z_2$ are normally distributed variables are $k$ is a discrete variable. Black nodes represent the network parameters. (Gen - Generative, Inf- Inference)

cluster instead of over all clusters leading to a more effective clustering. This process is shown in Fig. 2.

Along with this, we propose a novel augmentation loss as a mixture of $L2$ distance between the cluster predictions and 2-Wasserstein distance [14] between the predicted posterior distributions. We do so to ensure consistency in the cluster predictions and also in the predicted posterior thereby enforcing a similarity among samples from a given cluster. The idea behind this is to achieve invariance to marginal variations in the data and predict an accurate mapping for both real as well as augmented data. It would be counter-intuitive to map an augmented version of an input to a different distribution.

Therefore, our novelty is in modelling a GMM prior whose parameters are learnt during training, which is more flexible than fixed distributions like in other methods. This is too rigid a constraint mainly in complex datasets (CIFAR/STL). Due to our principled & effective modelling, coupled with our novel incorporation of an augmentation loss, our accuracy is significantly better than others and is very coherent on similar datasets. We perform well even in a cross-dataset transfer.

The main contributions of this paper are:

- A novel unsupervised image clustering algorithm by combining VAEs with a true Gaussian Mixture prior learnt without any pre-training in an end-to-end manner.
- More principled latent space priors that subsequently lead to a simpler inference model.
- A novel augmentation loss making our method robust and leading to strong intra-cluster relations.

In contrast to other methods, our method performs consistently well over all datasets using only raw pixel inputs, showcasing the generalization capability of our method. To the best of our knowledge, we are the first to do so using VAEs in a purely unsupervised manner, especially on real image datasets.

II. RELATED WORKS

Tian et al. [12] explore the use of deep methods in classical clustering by first learning a feature representation and subsequently performing clustering in the feature space. Nina et al. [15] follow a similar approach by using a triplet loss between positive and negative anchor images from the dataset and perform K-means on the learnt latent space. Similarly, Das et al. [16] propose a novel method for selecting images for calculating a triplet loss, which however depends on the quality of the pre-training. Yang et al. [17] follow a similar approach for learning a latent space but follow a graph-based spectral clustering approach with the learnt representation.

Song et al. [13] take a step further by integrating K-means into the bottleneck of an Autoencoder. This enables the model to learn meaningful clustering-oriented representations. Deep Embedded Clustering (DEC) [18] builds on a similar idea by minimizing the KL Divergence between cluster assignment probabilities and an auxiliary target distribution derived from the current predictions. However, this causes the auxiliary distribution to change as the predictions do during training.

Deep Adaptive Clustering (DAC) [19] uses a pairwise classification approach to distinguish between image pairs. It learns features that correspond directly to predicted class labels and achieve reasonable accuracy. Similarly, Ji et al. [20] propose a method that tries to preserve pair-wise semantic mutual information in the data. Deep Embedded Regularized Clustering (DEPICT) [21] uses a convolutional autoencoder to jointly learn representations and cluster predictions by constraining clusters to have similar no. of samples. Their performance deteriorates when data is not distributed well across clusters. To this end, RDEC [22] uses adversarial training to improve performance on imbalanced datasets. Along similar lines, Joint Unsupervised Learning (JULE) [7] learns representations and cluster assignments simultaneously using agglomerative clustering. Though it gets good results, their method is computationally intensive and has a heavy memory usage [23]. Sarfaraz et al. [24] also develop an agglomerative clustering method but with lower overheads in computing distances by partitioning the data points more efficiently.

Haeussler et al. [25] attempt to enforce intra-class similarity with associative constraints between images and their augmented versions to ensure similarity in predictions. However, the robustness and generalization capability of their method are questionable since they show vastly differing results on CIFAR10 [26] and STL-10 [27], both of which are real-world datasets having 9 same classes out of 10.

Information-Maximizing Self-Augmented Training (IM-SAT) [28] learn a probabilistic classifier using Regularized In-
formation Maximization (RIM) [29]. For feature-rich datasets (CIFAR10 and CIFAR100 [26]), they use ResNet [30] features as input. Thus, it is difficult to properly gauge their performance as results without pre-trained models are unavailable.

Coming to Deep Generative methods, ClusterGAN [31] is a Generative Adversarial framework for unsupervised clustering using a discrete-continuous mixed approach for clustering. Ghasedi et al. [32] build on this idea by introducing a self-paced learning algorithm that helps guide the learning, similar to a curriculum learning framework, to get better results. Variational Deep Embedding (VaDE) [2] and Gaussian Mixture VAEs (GMVAE) [1] use VAEs with GMMs simultaneously to model the inference process. Yang et al. propose DGG [33] along similar lines with the additional constraint of minimizing the graph distances between embeddings of data points.

Both ClusterGAN and VaDE require pre-training to initialize cluster centroids, and DGG requires pre-training to initialize the graph embeddings. Their success relies on the success of the initial pre-training. In this context, GMVAE learns the prior and posterior parameters jointly. However, their prior representation seems counter-intuitive as they use a sample from a normal distribution to generate the parameters (mean and variance) of the prior for each of the clusters. This implies that the prior for each class is dependent on a random variable rather than the class itself and hence would vary each time one would want to sample a latent for a class.

III. VARIATIONAL AUTOENCODERS

Variational Autoencoders (VAEs) [34], [35] are an application of Autoencoders for performing Variational Bayesian Inference over a set of data points. The main idea of Variational Inference is to learn a distribution in a latent space that can accurately capture the true distribution of the dataset. In particular, we wish to represent the joint probability \( p(x, z) \) for points in dataset \( x \) and their latent space representations \( z \). This joint probability can be written as \( p(x, z) = p(x|z)p(z) \) where \( p(z) \) is a prior distribution from where latent variables are drawn and \( p(x|z) \) is the conditional likelihood of a data point \( x \) conditioned on the drawn latent variable \( z \). The goal of variational inference is to infer the latent distribution from observed samples i.e. to accurately calculate \( p(z|x) \).

Using Bayes theorem, we can write this posterior distribution as:

\[
q(z\mid x) = \frac{p(x, z)}{p(x)} = \frac{p(x|z)p(z)}{p(x)}
\]

By Jensen’s inequality [36], the KL Divergence is always non-negative. Hence, the expectation in Eq. 3 acts as a lower bound for the evidence log-likelihood, and is hence called the Evidence Lower Bound (ELBO), given in Eq. 4.

\[
ELBO = \mathbb{E}_{q,p} \log \frac{p(x, z)}{q_\theta(z|\mathbf{x})}
\]

This allows us to write Eq. 3 as:

\[
\mathbb{E}_{q,p} \log p(x) = \mathbb{E}_{q,p} KL(q_\theta(z|x)||p(z|x)) + ELBO
\]

Therefore, minimizing the KL Divergence and hence, maximizing the log-likelihood of the evidence can be done by maximizing the ELBO. Since deep networks have strong representational abilities, Autoencoders have shown to perform well in approximating the distributions, leading to the birth of Variational Autoencoders (VAEs). Further information on Variational Inference and VAEs can be found in [35].

IV. PROPOSED APPROACH

VAEs traditionally model the prior as a single multivariate Gaussian. Since our objective is to cluster the data accurately, we use a Gaussian mixture prior for the latent space representation such that each Gaussian represents a cluster in the data. We aim to learn these Gaussians and an effective representation of the probability models, thereby learning the distribution a given data point belongs to, which corresponds to learning the clustering of the data.

An overview of our approach is shown in Fig. 2. Given a set of input images, we first predict their cluster probabilities. For each cluster, we infer a posterior latent distribution given the input and generate an independent prior distribution as well. We sample a latent from the posterior of each class from which we generate image samples which are used in computing the ELBO, along with the prior and the cluster probabilities.

A. Generative Process

We first select a cluster \( k \), from a categorical distribution characterized by \( \pi \), we draw a sample \( z \) from the latent distribution \( p(z|k) \) of that cluster parameterized by a neural network \( \beta \), to generate the conditional distribution \( p(x|z) \), which is parameterized by another neural network \( \theta \). In mathematical terms, our generative model can be seen as

\[
p_{\beta,\theta}(\mathbf{x}, \mathbf{z}, k) = p_\theta(\mathbf{x}|\mathbf{z})p_\beta(\mathbf{z}|k)p(k)
\]

\[
p(k) = \text{Cat}(\pi)
\]

\[
p_\beta(\mathbf{z}|k) = N(\mathbf{z}|\mu_\beta(\mathbf{e}_k), diag(\sigma^2_\beta(\mathbf{e}_k)))
\]

\[
p_\theta(\mathbf{x}|\mathbf{z}) = N(\mathbf{x}|\mu_\theta(\mathbf{z}), diag(\sigma^2_\theta(\mathbf{z})) \text{ or } B(\mathbf{x}|\mu_\theta(\mathbf{z}))
\]

where \( \pi = \frac{1}{K} \) is the categorical probability, \( \mathbf{e}_k \) is a one-hot vector with a 1 at the \( k_{th} \) position, \( N(\cdot) \) refers to a Normal distribution & \( B(\cdot) \) refers to a Bernoulli distribution. \( \mu_\beta, \sigma^2_\beta, \mu_\theta, \sigma^2_\theta \) are the means & variances, characterized by deep networks with parameters \( \beta \) & \( \theta \) respectively.

Our process differs from GMVAE [1] & VaDE [2] in the following ways. In GMVAE, a neural network samples a standard normal distribution as an input (\( \mathbf{z}_1 \) in Fig. 1a) &
generates a mean & variance for each cluster \((z_2)\). Therefore, the latent distribution for any given cluster depends on a normally distributed variable & not just on the cluster it represents. Out of these, the \(k^{th}\) mean & variance is selected from which they sample their latent.

In VaDE, the process is similar to ours however, they first train a stacked autoencoder with the input data & then learn a GMM over the predicted latent representations from the encoder’s bottleneck. This learnt GMM is used as the prior a GMM over the predicted latent representations from the encoder’s bottleneck. This learnt GMM is used as the prior from which the latent variables are sampled. The performance of VaDE depends on how well the pre-training & GMM initialization go, which would lead to a bad performance in case the initial learning doesn’t properly converge.

B. Inference Model

We perform variational inference by maximizing the Evidence Lower Bound (ELBO), which in turn leads to maximizing the log-likelihood of the evidence \(\log p(x)\). With a slight abuse of notation, the ELBO can be written as:

\[
ELBO = \mathbb{E}_{q_{\omega,p}} \log \frac{p_{\beta,\theta}(x, z, k)}{q_{\omega,\psi}(z, k|x)} \quad (10)
\]

where \(\mathbb{E}_{q_{\omega,p}}\) is the expectation with respect to \(q_{\omega,\psi}(z, k|x)\)\(p_{\beta,\theta}(x, z, k)\). Here, \(q_{\omega,\psi}(z, k|x)\) is the approximate posterior of the inference model, which we factorize as:

\[
q_{\omega,\psi}(z, k|x) = q_{\omega}(k|x)q_{\psi}(z|x, k) \quad (11)
\]

such that \(\sum_{k=1}^{K} q_{\omega}(k|x) = 1\) and \(q_{\psi}(z|x, k) \sim \mathcal{N}(z|\mu_{\psi}(x, e_k), diag(\sigma_{\psi}^2(x, e_k)))\) where \(\mu_{\psi}, \sigma_{\psi}^2\) refer to the mean and variance of the posterior parameterized by a deep network \(\psi\).

Our inference model is more straightforward than GMVAE [1] since they calculate their categorical posterior based on their latent’s prior which, as mentioned towards the ending of Sec. IV-A, depends on a sample from a standard normal distribution. This implies that the probability of a given category being assigned to a fixed category is stochastic in nature, which ideally shouldn’t be the case. A latent variable is a representation of a sample data point. Therefore, the categorical posterior that depends on the latent, it should directly be inferred from the sampled data point itself. Our method directly predicts the categorical posterior \(q_{\omega}(k|x)\) directly from the sampled data point \(x\).

C. Evidence Lower Bound

Eq. 10 can be factorized using Eq. 6 & 11 as:

\[
ELBO = \mathbb{E}_{q_{\omega,p}} \log \frac{p_{\theta}(x|z)p_{\beta}(z|k)p(k)}{q_{\omega}(k|x)q_{\psi}(z|x, k)} \quad (12)
\]

Since \(\log p(k)\) is a constant, we drop it from Eq. 12 for ease of notation. Eq. 12 can then be re-written as:

\[
ELBO = \mathbb{E}_{q_{\omega,p}} \log p_{\theta}(x|z) - \mathbb{E}_{q_{\omega}(k|x)p_{\beta}(z|k)} \log q_{\omega}(k|x) - \mathbb{E}_{q_{\omega}(k|x)p_{\beta}(z|k)} \mathbb{E}_{z \sim q_{\psi}(z|x, k)} \log p_{\theta}(x|z) \quad (13)
\]

In Eq. 13, the first term \(\mathbb{E}_{q_{\omega,p}} \log p_{\theta}(x|z)\) is the likelihood of a sampled data point \(x\) w.r.t. the generated distribution. It is similar to ensuring a proper reconstruction of the sampled input. It is further written as 

\[
\frac{1}{N} \sum_{i=1}^{N} \sum_{k=1}^{K} q_{\omega}(k|x_i) \mathbb{E}_{z \sim q_{\psi}(z|x, k_i)} \log p_{\theta}(x_i|z) \]

where \(N\) is the batch size. This expansion allows us to circumvent the issue of having to sample from a discrete distribution which in
due to their Gaussian form, given by the latter allows us to give a higher weight to the predicted similarity in the predictions, we minimize the Wasserstein distance \[14\] between the posteriors.

Different augmenteds used are given in Sec. V-A.

predictions of the original images to guide the predictions of a larger number of samples. Secondly, it allows us to use of this is two-fold. Firstly, it allows the network to learn from augmented images along with the original images. The advantage turn would involve a discrete reparametrization. This expansion leaves us with having to sample a continuous latent \( z \) for each cluster \( k \), which can easily be reparametrized for each \( k \). The second term \( \mathbb{E}_{q_k(k|\mathbf{x})} \{ KL(q_k(\mathbf{x}|k)||p_\beta(z|k)) \} \) is the expected entropy of the posterior distribution of \( k \) w.r.t. the sampled data point \( \mathbf{x} \), written as \( \frac{1}{N} \sum_{i=1}^{N} \sum_{k=1}^{K} q_k(k|\mathbf{x}_i) \log q_k(k|\mathbf{x}_i) \).

The third and final term is the \( z \) KL term \( \mathbb{E}_{q_k(k|\mathbf{x})} \{ KL(q_k(\mathbf{x}|k)||p_\beta(z|k)) \} \), which refers to the Kullback-Leibler Divergence of the prior w.r.t. the posterior distribution of \( z \). Since they are both Gaussians, the KL Divergence has a closed form solution.

One interesting point to note in the formulation is the anti-clustering nature of the ELBO, caused by the maximization of the entropy of \( q_k(k|\mathbf{x}) \). This regularization forces the information stored in \( q_k(k|\mathbf{x}) \) to be distributed among the clusters, rather than learning a one-hot prediction for the cluster labels. This is however mitigated by the reconstruction term, which would force the data to belong to a particular cluster. One advantage of this entropy maximization is that it prevents the trivial solution where all inputs are mapped to a single cluster, also known as “mode collapse” which is a common problem associated with VAEs. In their implementation, we found that the scale of the reconstruction term is exponentially larger than the KL term on real image data. Hence, to ensure numerical stability, we multiply the reconstruction term in Eq. 13 with a scale-factor, \( \lambda_{\text{recons}} \).

D. Augmentation Loss

To make our model robust to input variations, we add augmented images along with the original images. The advantage of this is two-fold. Firstly, it allows the network to learn from a larger number of samples. Secondly, it allows us to use predictions of the original images to guide the predictions of the augmented images, resulting in a form of self-supervision. Different augmenteds used are given in Sec. V-A.

Let \( \mathbf{x} \) be an input image and \( \hat{\mathbf{x}} \), its augmented image. Intuitively, both should belong to the same cluster and posterior distribution. This enforces a strong constraint on the posterior predicted for \( \hat{\mathbf{x}} \) by providing a form of supervision. Therefore, to ensure similarity in the predictions, we minimize the \( L2 \) distance between the predicted clusters and the expectation of the Wasserstein distance \[14\] between the posteriors.

\[
\mathcal{L}_{\text{aug}} = \sum_{k=1}^{K} ||q_k(k|\mathbf{x}) - q_k(k|\hat{\mathbf{x}})||^2_2 + \mathbb{E}_{q_k(k|\mathbf{x})} [\mathcal{W}_2(q_k(\mathbf{z}|\mathbf{x}, k), q_k(\hat{\mathbf{z}}|\hat{\mathbf{x}}, k))] \tag{14}
\]

where \( \mathcal{W}_2 \) is the 2-Wasserstein distance. The expectation in the latter allows us to give a higher weight to the predicted cluster and a lower weight for clusters that are not associated with the given image. This has a closed form solution \[37\], due to their Gaussian form, given by

\[
\mathcal{W}_2(q_\psi(\mathbf{z}|x,k), q_\psi(\hat{\mathbf{z}}|\hat{x},k)) = ||\mu_\psi(\mathbf{x}, e_k) - \mu_\psi(\hat{\mathbf{x}}, e_k)||^2_2 + \text{trace}(C_1 + C_2 - 2(C_2^\frac{1}{2} C_1 C_2^\frac{1}{2})) \tag{15}
\]

the trace in Eq. 15 can be simplified as:

\[
C_1 + C_2 - 2(C_2^\frac{1}{2} C_1 C_2^\frac{1}{2})^2 = \text{diag}(\sigma_\psi^2(\mathbf{x}, e_k)) + \text{diag}(\sigma_\psi^2(\hat{\mathbf{x}}, e_k) - 2\sigma_\psi(\mathbf{x}, e_k)\sigma_\psi(\hat{\mathbf{x}}, e_k))
\]

\[
= \text{diag}(\sigma_\psi^2(\mathbf{x}, e_k)) + \sigma_\psi^2(\mathbf{x}, e_k) - 2\sigma_\psi(\mathbf{x}, e_k)\sigma_\psi(\hat{\mathbf{x}}, e_k)
\]

\[
= \text{diag}(\sigma_\psi(\mathbf{x}, e_k) - \sigma_\psi(\hat{\mathbf{x}}, e_k))^2 \tag{16}
\]

Substituting Eq. 16 in Eq. 15, we get

\[
\mathcal{W}_2(q_\psi(\mathbf{z}|x,k), q_\psi(\hat{\mathbf{z}}|\hat{x},k)) = ||\mu_\psi(\mathbf{x}, e_k) - \mu_\psi(\hat{\mathbf{x}}, e_k)||^2_2 + \text{trace}(\sigma_\psi(\mathbf{x}, e_k) - \sigma_\psi(\hat{\mathbf{x}}, e_k)^2))
\]

\[
= ||\mu_\psi(\mathbf{x}, e_k) - \mu_\psi(\hat{\mathbf{x}}, e_k)||^2_2 + ||\sigma_\psi(\mathbf{x}, e_k) - \sigma_\psi(\hat{\mathbf{x}}, e_k)||^2_2 \tag{17}
\]

To prevent the augmentation from driving the initial learning phases, we anneal the effect of this loss so as to bring about its significance once a suitable amount of learning has progressed by modifying its weight \( \lambda_{\text{aug}} \). Our final loss can be written as

\[
\mathcal{L} = -\text{ELBO} + \lambda_{\text{aug}}\mathcal{L}_{\text{aug}} \tag{18}
\]

V. EXPERIMENTAL DETAILS

Details about the datasets used are given in Sec. V-A and about the network architecture in the appendix in Sec. V-B. We implement the system using Tensorflow \[38\] using Adam \[39\] as our optimizer with \( \beta_1 = 0.9, \beta_2 = 0.999 \) and the learning rate as \( 10^{-3} \) for MNIST & Fashion-MNIST and \( 10^{-4} \) for the rest. The value of \( \lambda_{\text{aug}} \) is 0.01 for the first 40 epochs, followed by 0.5 till 80 epochs and 1 thereafter.

We use a batch-size of 100 for MNIST and Fashion-MNIST and 30 for the others. The value of the scale-factor for the reconstruction term, \( \lambda_{\text{recons}} \), is kept at 0.5 for 40 epochs after which we keep it as 0.1 for CIFAR10 and STL-10.

A. Datasets

- **Toy Data** used in the GMVAE paper, which is a 2D dataset consisting of 10000 points from the arcs of 5 circles. No augmentation is used for this.
- **MNIST** \[41\] consists of 70000 black and white images of handwritten digits of size 28x28 split into 60000 training images and 10000 testing images. We use random rotations between 3° to -3° for the augmentation.
- **Fashion MNIST** \[42\] consists of grayscale images of fashion items like sandals, T-shirts, handbag etc. It has the same size and split as MNIST but a greater complexity, making it more challenging. We add random brightness variations within a delta factor of 0.2 followed by an image binarization by checking if the pixel value is greater than a uniform random value.
- **STL-10** \[27\] consists of 13000 labelled and 100000 unlabelled colour images of real word objects from
### Table I: Clustering accuracy (%). * - Use pre-trained features as input. † - Results reported using source code. ‡ - Results reported in [40]. We put a "-" where results are unavailable. For our results, we use $k=10$ except when specified. The methods above the red line, although unsupervised, use pre-trained features as input which itself boosts their performance by a big margin. Our main comparison is with unsupervised methods, shown below the red line. (Best viewed in colour)

<table>
<thead>
<tr>
<th>Method</th>
<th>Remarks</th>
<th>MNIST</th>
<th>Fashion-MNIST</th>
<th>STL-10</th>
<th>CIFAR10</th>
<th>CIFAR100</th>
<th>FRGCv2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k$-means on pixels</td>
<td>-</td>
<td>53.49</td>
<td>47†</td>
<td>22.0</td>
<td>20.4</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IMSAT [28]</td>
<td>use ResNet [30]</td>
<td>98.4</td>
<td>94.1*</td>
<td>45.6*</td>
<td>27.5*</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>VaDE [2]</td>
<td></td>
<td>94.46</td>
<td>57.8†</td>
<td>84.5*</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Sarfaraz et al. [24]</td>
<td>Generative, use ResNet [30]</td>
<td>91.89</td>
<td>-</td>
<td>95.24*</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>DDG [33]</td>
<td></td>
<td>97.58</td>
<td>-</td>
<td>90.59*</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Das et al. [16]</td>
<td>Unsupervised, Pre-training</td>
<td>98.93</td>
<td>-</td>
<td>44.19</td>
<td>25.4</td>
<td>47.28</td>
<td></td>
</tr>
<tr>
<td>Yang et al. [17]</td>
<td></td>
<td>98</td>
<td>66.2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Nima et al. [15]</td>
<td></td>
<td>96.8</td>
<td>70.98</td>
<td>-</td>
<td>30.9</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>JULE [7]</td>
<td></td>
<td>96.1</td>
<td>56.3†</td>
<td>-</td>
<td>-</td>
<td>46</td>
<td></td>
</tr>
<tr>
<td>DEC [18]</td>
<td></td>
<td>84.3</td>
<td>61.8†</td>
<td>35.9</td>
<td>14.3*</td>
<td>37.8</td>
<td></td>
</tr>
<tr>
<td>DEPICT [21]</td>
<td></td>
<td>96.3</td>
<td>39.2†</td>
<td>-</td>
<td>-</td>
<td>47</td>
<td></td>
</tr>
<tr>
<td>RDEC [22]</td>
<td>Purely Unsupervised</td>
<td>98.41</td>
<td>-</td>
<td>21.27</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>DEC-DA [40]</td>
<td></td>
<td>98.6</td>
<td>58.6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Haeusser et al. [25]</td>
<td></td>
<td>98.7</td>
<td>38.9</td>
<td>26.7</td>
<td>-</td>
<td>43.7</td>
<td></td>
</tr>
<tr>
<td>GMVAE [1]</td>
<td></td>
<td>96.92</td>
<td>59.56†</td>
<td>25.36†</td>
<td>24.74†</td>
<td>10.10‡</td>
<td>21.24†</td>
</tr>
<tr>
<td>ClusterGAN [31]</td>
<td></td>
<td>95</td>
<td>63</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Ghasedi et al. [32]</td>
<td></td>
<td>96.4</td>
<td>-</td>
<td>42.3</td>
<td>41.2</td>
<td>-</td>
<td>47.6</td>
</tr>
<tr>
<td>Ours</td>
<td>Generative, Purely Unsupervised</td>
<td>98.2</td>
<td>71.72</td>
<td>43.9</td>
<td>44.5</td>
<td>25.6</td>
<td>56.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>95.4 ($k = 8$)</td>
<td></td>
<td></td>
<td></td>
<td>($k = 100$)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>98.4 ($k = 20$)</td>
<td></td>
<td></td>
<td></td>
<td>($k = 20$)</td>
<td></td>
</tr>
</tbody>
</table>

TABLE I: Clustering accuracy (%). * - Use pre-trained features as input. † - Results reported using source code. ‡ - Results reported in [40]. We put a "-" where results are unavailable. For our results, we use $k=10$ except when specified. The methods above the red line, although unsupervised, use pre-trained features as input which itself boosts their performance by a big margin. Our main comparison is with unsupervised methods, shown below the red line. (Best viewed in colour)

- CIFAR10 and CIFAR100 [26] are diverse datasets of real world images. 9 classes in CIFAR10 are similar to STL-10. Achieving good clustering accuracy on them in an unsupervised manner is truly challenging. They consist of 50000 training and 10000 testing images each with 10 classes in CIFAR10 and 100 in CIFAR100. We use the same augmentations as in STL-10.

- FRGCv2 consists of 2462 images having 20 face samples. It’s a subset of the larger FRGC dataset. We use the subset provided by the authors of [7], which is what other methods report their results on as well.

### B. Network Architecture

The network architectures for the prior and posterior networks are given in Tables IIa and IIb respectively. The $z$ prior consists of fully connected networks as there aren’t any images involved. The convolutional part of the posterior networks for CIFAR10, STL-10, CIFAR100 entail complex representations which are thereby, captured better by weight-sharing.

### VI. RESULTS

#### A. Clustering Results

Firstly, to see the representation capability of our method, we show the latent space learnt by our method & GMVAE on the synthetic dataset given in their paper. As seen in Fig. 3, our clusters are tightly packed individually & more spread overall compared to GMVAE. Good latent space separation is key for clustering as it can partition the data in a better way.

Furthermore, to see how well the clusters are separated in the latent space, we visualize the means of the posterior and the prior using t-SNE [43]. The posterior representation of a subset of testing images can be seen in Fig. 4. For the prior, we randomly generate 500 samples from each cluster, to see how well the prior has been learnt. This can be seen in Fig. 5. Evidently, we can see a clear separation between clusters from the beginning itself (11 epochs), which gets refined as the iterations go on. This not only shows the discriminatory nature of the learnt representations, but also the speed with which it becomes a characteristic of the latent space.

For evaluating our method, we use the unsupervised clustering accuracy (ACC) [18], which can be given as

$$ACC = \max_{m \in M} \frac{\sum_{i=1}^{N} I(l_i = m(c_i))}{N} \quad (19)$$

where $N$ is the total no. of images, $l_i$ and $c_i$ are the label and cluster for the $i^{th}$ image respectively and $M$ is the set of possible one-to-one mappings between clusters and labels.

Our accuracy can be seen in Table I. It is important to note that we only lag behind methods which use pre-trained ResNet [30] features as input, which itself is an extremely informative representation, giving them a large advantage as it has already covered thousands of samples of the classes present in STL-10 and CIFAR10 in a supervised manner. In comparison with Das et al. [16] who use a lot of epochs for pre-training, we perform better especially on more complex datasets like Fashion-MNIST, STL-10, CIFAR10 and CIFAR100.

Our main comparison is with unsupervised methods, shown below the red line in Table I. Our performance significantly exceeds them in all the complex real world datasets achieving state-of-the-art results among unsupervised methods. Our performance exceeds that of generative methods [31], [32] on all
| Dataset         | Type of Layer | \( p_\theta(z|k) \) | \( p_\theta(x|z) \) |
|-----------------|---------------|----------------------|--------------------|
| Toy Data        | Input         | Input \( \mathbf{x} \) [batch, K] | Input \( \mathbf{x} \) [batch, K] |
| Hidden          | FCN 120, No activation | FCN 120, No activation | FCN 120, No activation |
| Output          | \( \mu_1, \sigma_2^2 \), FCN 32, softplus activation | \( \mu_1, \sigma_2^2 \), FCN 32, softplus activation | \( \mu_1, \sigma_2^2 \), FCN 32, softplus activation |

<table>
<thead>
<tr>
<th>MNIST Fashion Mnist</th>
<th>Hidden</th>
<th>FCN 64, No activation</th>
<th>FCN 64, No activation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CIFAR10 STL-10 CIFAR100</th>
<th>Hidden</th>
<th>FCN 64, No activation</th>
<th>FCN 64, No activation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>( \mu_3, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_3, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_3, \sigma_2^2 ), FCN 32, softplus activation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FRGCv2</th>
<th>Hidden</th>
<th>FCN 64, No activation</th>
<th>FCN 64, No activation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>( \mu_4, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_4, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_4, \sigma_2^2 ), FCN 32, softplus activation</td>
</tr>
</tbody>
</table>

(a) Network architecture for the prior probabilities \( p_\theta(z|k) \) & \( p_\theta(x|z) \).

| Dataset         | Type of Layer | \( q_\phi(z|x) \) | \( q_\phi(x|z) \) |
|-----------------|---------------|------------------|------------------|
| Toy Data        | Input         | Input \( \mathbf{x} \) [batch, 2] | Input \( \mathbf{x} \) [batch, 2], \( \mathbf{e}_k \) [batch, K] |
| Hidden          | FCN 120, No activation | FCN 10, No activation | FCN 10, No activation |
| Output          | \( \mu_2, \sigma_2^2 \), FCN 32, softplus activation | \( \mu_2, \sigma_2^2 \), FCN 32, softplus activation | \( \mu_2, \sigma_2^2 \), FCN 32, softplus activation |

<table>
<thead>
<tr>
<th>MNIST Fashion Mnist</th>
<th>Hidden</th>
<th>FCN 64, No activation</th>
<th>FCN 64, No activation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CIFAR10 STL-10 CIFAR100</th>
<th>Hidden</th>
<th>FCN 128, Dropout 0.8</th>
<th>FCN 128, Dropout 0.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FRGCv2</th>
<th>Hidden</th>
<th>FCN 64, No activation</th>
<th>FCN 64, No activation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
<td>( \mu_2, \sigma_2^2 ), FCN 32, softplus activation</td>
</tr>
</tbody>
</table>

(b) Network architecture for the prior probabilities \( p_\psi(z|k) \) & \( p_\psi(x|z) \).

**TABLE II: Network architectures for (a) posterior probabilities and (b) prior probabilities.** All the Conv and UpConv layers have a stride of 2 with padding as 'same' unless specified otherwise. For MNIST and Fashion MNIST, all layers have ReLU activations unless specified. For others, all layers have leaky ReLU activations unless specified. \( K \) - number of clusters (Toy Data - 5, MNIST, Fashion MNIST, STL-10, CIFAR10 - 10, FRGCv2 - 20, CIFAR100 - 100)
datasets, showing that the inference power of VAEs is greater than GANs for clustering, where a strong representation of the data distribution is important. We perform better than GMVAE [1] and VaDE [2] on all datasets showing the effectiveness of our approach to using a Gaussian Mixture latent space.

B. STL-CIFAR Transfer Learning

CIFAR10 and STL-10 are inherently similar, having 9 same classes out of 10 and has some scope for transfer learning. To show such a capability of our method, we test the model trained on CIFAR10 using STL-10 and vice-versa on these common classes. The results of this are shown in Table III.

<table>
<thead>
<tr>
<th>Trained on</th>
<th>Tested on</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>STL-10</td>
<td>CIFAR10</td>
<td>38.8</td>
</tr>
<tr>
<td>CIFAR10</td>
<td>STL-10</td>
<td>41.03</td>
</tr>
</tbody>
</table>

TABLE III: Transfer learning between CIFAR10 and STL-10

C. Imbalanced Clusters

To study our performance on imbalanced data, we follow the imbalanced sampling mechanism as in DEC [18] for MNIST. We define which is the probability of retaining samples of class 0 is defined as a minimum retention rate $r_{min}$, for class 9 the retention probability is 1 and for other classes, it varies linearly from $r_{min}$ to 1. The ratio of the sizes of the largest and smallest clusters is $1/r_{min}$. We perform significantly better than other methods as shown in Table IV.

<table>
<thead>
<tr>
<th>Method</th>
<th>$r_{min}$</th>
<th>0.1</th>
<th>0.3</th>
<th>0.5</th>
<th>0.7</th>
<th>0.9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k$-means</td>
<td></td>
<td>47.14</td>
<td>49.93</td>
<td>53.65</td>
<td>54.16</td>
<td>54.39</td>
</tr>
<tr>
<td>AE+$k$-means</td>
<td></td>
<td>66.82</td>
<td>74.91</td>
<td>77.93</td>
<td>80.04</td>
<td>81.31</td>
</tr>
<tr>
<td>DEC</td>
<td></td>
<td>70.10</td>
<td>80.92</td>
<td>82.68</td>
<td>84.69</td>
<td>85.41</td>
</tr>
<tr>
<td>Ours</td>
<td></td>
<td>89.6</td>
<td>90.3</td>
<td>96.1</td>
<td>96.9</td>
<td>97.1</td>
</tr>
</tbody>
</table>

TABLE IV: Clustering accuracy (%) for MNIST with imbalanced clusters using different min. retention rates $r_{min}$.

D. Generated Samples

In order to see the effectiveness of our latent space representation, we generate images to see if captures the underlying data distribution in a meaningful manner. Since our approach is inherently a generative one, it should be able to extrapolate samples from the latent space, as is the case with any generative approaches. The ability to generate high quality samples is the true test for any generative approach.
As it can be seen in Fig. 6, our learned model is able to generate realistic samples from each cluster. Moreover, one more important inference that can be drawn is that our method learns to distinguish properly between classes since it is able to generate distinct samples from each of the clusters. This shows that our generative approach works well not only in distinguishing between different clusters but also in being able to generate realistic samples given latent data.

![Fig. 6: Images generated from each learned cluster.](a) MNIST  (b) Fashion MNIST)

**E. Latent Space Interpolation**

To see how well the learning has progressed, we visualize how variations in the latent space correspond to variations in generated samples. We perform 2 types of interpolations, one in the continuous space and one in the categorical space. Though is a discrete variable, we vary it continuously to see how data generation for unknown inputs looks like. In our model, we have two sets of variables on which the output of the generative model depends on. The first is the categorical distribution for , followed by a Gaussian distribution corresponding to the th cluster, for obtaining . We generate samples by interpolating in both these spaces to see how the generated samples are, giving us further insight into the extent to which each of these variables influence the generation process.

1) Interpolation: We choose two clusters and and sample latents and from their respective Gaussians. We calculate our interpolated latent as by varying from 0 to 1, from which we generate our output.

As shown in Fig. 7a, smooth variations in the latent space generate smooth transitions in the image space. This shows that our distributions in the latent space capture the data distribution accurately. This is an important result showing the ability of our method to accurately capture changes in the latent space and reflect them in the input space.

2) -Interpolation: We choose two clusters and and linearly interpolate between their one-hot vector representations and . We generate , by varying from 0 to 1. From , we generate the parameters of the prior for sampling from which we generate our output.

From Fig. 7b, it can be said that our method is able to extrapolate data not just from continuous variations in the latent space but more importantly from continuous variations in a discrete space. The main takeaway is that we train our model using only one-hot vectors, our method is able to generate meaningful images representing the interpolated vector . This result shows that our model is able to learn a truly effective representation for each cluster, where the data distribution is preserved not just in the latent space (z) but in the categorical space (k) as well. The -interpolation is not as smooth as the -interpolation mainly because the former is a discrete space whereas the latter is a smooth continuous one.

**F. Ablation study**

We perform an ablation study to understand the effect of different parts of our loss where we compare the following:

- A vanilla implementation of our proposed VAE.
- Adding a scale factor to the reconstruction term.
- Adding just the L2 loss for the cluster predictions.
- Adding just the V2 loss for the predicted posteriors.
- The final proposed loss function.

The results for this study are given in Table V. As it can be seen, our vanilla method itself performs decently. Adding just the scale-factor for STL-10 helps improve the accuracy. Just adding the L2 loss increases the accuracy by a small margin, while adding the V2 loss increases it by a larger margin. This shows that enforcing a consistent latent space representation helps make the learning more robust. Finally, we get the best performance by combining all our additions together.

**VII. Conclusion and Future Works**

We propose an image clustering method using VAEs with a GMM prior where each component represents a cluster. The prior is learned jointly with the posterior, which in turn learns a strong latent representation that leads to accurate clustering, as shown in extensive experiments. Our method doesn’t require any pre-training and can be trained from scratch in an end-to-end manner. We show results on a variety of datasets ranging from simple handwritten digits to complex real-world datasets.
objects, achieving state-of-the-art clustering accuracy among purely unsupervised methods. To the best of our knowledge, we are the first to achieve such significant results on real world datasets in a purely unsupervised manner. Moreover, we achieve comparable accuracy between similar datasets (CIFAR10/STL-10) in a transfer learning scenario. With the rise in the popularity of GANs, one way to move forward could be to replace the generator network in a GAN with our VAE model, thereby leading to a hybrid VAE-GAN model, that can has the strong latent representational powers of a VAE and the realistic generative powers of a GAN. Furthermore, adding explicit inference constraints on the GAN prior, somewhat as an increment along the lines of ClusterGAN [31], could be another way to approach the VAE-GAN hybrid architecture.

REFERENCES