Autoencoding Under Normalization Constraints

Sangwoong Yoon 1  Yung-Kyun Noh 2 3  Frank C. Park 1 4

Abstract

Likelihood is a standard estimate for outlier detection. The specific role of the normalization constraint is to ensure that the out-of-distribution (OOD) regime has a small likelihood when samples are learned using maximum likelihood. Because autoencoders do not possess such a process of normalization, they often fail to recognize outliers even when they are obviously OOD. We propose the Normalized Autoencoder (NAE), a normalized probabilistic model constructed from an autoencoder. The probability density of NAE is defined using the reconstruction error of an autoencoder, which is differently defined in the conventional energy-based model. In our model, normalization is enforced by suppressing the reconstruction of negative samples, significantly improving the outlier detection performance. Our experimental results confirm the efficacy of NAE, both in detecting outliers and in generating in-distribution samples.

1. Introduction

An autoencoder (Rumelhart et al., 1986) is a neural network trained to reconstruct samples from a training data distribution. Since in principle the quality of reconstruction is expected to be poor for inputs that deviate significantly from the training data, autoencoders are widely used in outlier detection (Japkowicz et al., 1995), in which an input with a large reconstruction error is classified as out-of-distribution (OOD). Autoencoders for outlier detection have been applied in domains ranging from video surveillance (Zhao et al., 2017) to medical diagnosis (Lu & Xu, 2018).

However, autoencoders have been known to reconstruct outliers consistently across a wide range of experimental settings (Lyudchik, 2016; Tong et al., 2019; Zong et al., 2018; Gong et al., 2019). We name this phenomenon outlier reconstruction. Figure 1 shows examples of some outliers reconstructed by an autoencoder trained with MNIST data; the autoencoder is able to reconstruct a wide range of OOD inputs, including constant black pixels, Omniglot characters, and fragments of MNIST digits. The early works on regularized autoencoders (Vincent et al., 2008; Rifai et al., 2011; Ng et al., 2011) focus for the most part on preventing the autoencoder from turning into the identity mapping that reconstructs every input. Nonetheless, outlier reconstruction can still occur even when the autoencoder is not the identity as shown by the non-identity autoencoder in Figure 1. Not surprisingly, outlier reconstruction is a leading cause of autoencoder’s detection failure.

On the other hand, in a normalized probabilistic model, it is known that maximum likelihood learning suppresses the assignment of probability mass in OOD regions in order to keep the model normalized. Thus, the likelihood is widely used as a predictor for outlier detection (Bishop, 1994). Meanwhile, an autoencoder is not a probabilistic model of the data and does not have a suppression mechanism corresponding to the normalization in other probabilistic models. As a result, the reconstruction of outliers are not inhibited during training of an autoencoder.

This paper formulates an autoencoder as a normalized prob-
abilistic model to introduce a mechanism for preventing outlier reconstruction. In our formulation, which we call the Normalized Autoencoder (NAE), the reconstruction error is re-interpreted as an energy function, i.e., the unnormalized negative log-density, and defines a probabilistic model from an autoencoder. During maximum likelihood learning of NAE, outlier reconstruction is naturally suppressed by enforcing the normalization constraint, and the resulting autoencoder is significantly less prone to reconstruct outliers, as shown in Figure 1.

In each training iteration of NAE, samples generated from the model is used to update the normalization constraint which is implicitly computed as in other energy-based models. Since running a Markov Chain Monte Carlo (MCMC) sampler until convergence every iteration is computationally infeasible, an approximate sampling strategy has to be employed. We observe that training with popular sampling strategies such as Contrastive Divergence (CD; Hinton (2002)) and Persistent CD (PCD; Tieleman (2008)) may often produce poor density estimates. Instead, we propose on-manifold initialization (OMI), a method of initializing an MCMC chain on manifold defined by the decoder of an autoencoder. OMI selects high-model-density initial states by leveraging the assumption that points on the decoder manifold typically have small reconstruction error, i.e. high model density. With OMI, NAE can accurately recover the data density and thus become an effective outlier detector.

Intriguingly, although technically a normalized probabilistic model, the variational autoencoder (VAE; Kingma & Welling (2014)) also reconstructs outliers and assigns a spurious high density to in-distribution data. This is in contrast to NAE, which assigns a zero density to out-of-distribution data.

Our main contributions can be summarized as follows:
- We propose NAE, a novel generative model constructed from an autoencoder;
- We propose OMI, a sampling strategy tailored for NAE;
- We empirically show that NAE is highly effective for outlier detection and can perform other generative tasks.

Section 2 provides brief background on autoencoders and energy-based models. NAE is described in Section 3, and OMI is described in Section 4. Related works are reviewed in Section 5. Section 6 presents experimental results. Section 7 provide discussions and conclude the paper. Our source code and pre-trained models are publicly available online.

Note that the reconstruction error (Eq. (3)) is not a likelihood of a datum, and therefore the minimization of the reconstruction error does not correspond to the maximization of the likelihood. Without modification, an autoencoder per se is not a probabilistic model.

Outlier Detection A datum is an outlier or called OOD if it lies in the ρ-sublevel set of a data density \( \{ x | p(x) \leq \rho \} \) (Steinwart et al., 2005). We particularly focus on \( \rho = 0 \), where an outlier is defined as an input from the outside of the data distribution’s support. Most of the OOD examples which attract the attention of the research community are in fact out-of-support samples. For example, SVHN and CIFAR-10 are out-of-support to each other, as confirmed by a supervised classifier perfectly discriminating the two datasets. Note that the support-based definition provides invariant characterization of outliers, as no invertible transform defined on the data space alters whether a sample is in- or out-of-support. Meanwhile, for \( \rho \neq 0 \), the characterization of outliers are not invariant to the choice of coordinates.
In the autoencoder-based outlier detection (Japkowicz et al., 1995), an input is classified as OOD if its reconstruction error \( l_0(x) \) is greater than a threshold \( \tau \): \( l_0(x) > \tau \). The outlier reconstruction indicates that there exists an input \( x^* \) with \( p(x^*) \leq p(x) \), but \( l_0(x^*) < \tau \). Appendix includes the detailed investigation on outlier reconstruction.

2.2. Energy-based Models

Unlike autoencoders, energy-based models (EBMs) are valid models for a normalized probability distribution. The EBM represents a probability distribution through the unnormalized negative log probability, also called the energy function \( E_\theta(x) \). Here, \( \theta \) denotes the model parameters.

For a continuous input \( x \in \mathcal{X} \subset \mathbb{R}^D \), \( E_\theta(x) \) defines the model density function \( p_\theta(x) \) through Gibbs distribution:

\[
p_\theta(x) = \frac{1}{\Omega_\theta} \exp(-E_\theta(x)/T), \tag{4}
\]

where \( T \in \mathbb{R}^+ \) is called the temperature and is often ignored by setting \( T = 1 \). \( \Omega_\theta \) is the normalization constant and is defined as:

\[
\Omega_\theta = \int_{\mathcal{X}} \exp(-E_\theta(x)/T) \text{d}x < \infty. \tag{5}
\]

The computation of \( \Omega_\theta \) is usually difficult for high-dimensional \( x \). However, maximum likelihood learning can still be performed without the explicit evaluation of \( \Omega_\theta \). The gradient of negative log likelihood of data is given as follows (Younes, 1999):

\[
\mathbb{E}_{x \sim p(x)}[\nabla_\theta \log p_\theta(x)] = \mathbb{E}_{x \sim p(x)}[\nabla_\theta E_\theta(x)/T + \nabla_\theta \log \Omega_\theta] = \mathbb{E}_{x \sim p(x)}[\nabla_\theta E_\theta(x)/T - \mathbb{E}_{x' \sim p_\theta(x)}[\nabla_\theta E_\theta(x')]/T]/T. \tag{6}
\]

\( \nabla_\theta \log \Omega_\theta \) in Eq. (6) is evaluated from the energy gradients of samples \( x' \) generated from the model in Eq. (7). The samples from \( p_\theta(x) \) are often called “negative” samples. The derivation of Eq. (7) is provided in Appendix.

In Eq. (7), the first term decreases the energy of the training data, or “positive” samples, while the second term increases the energy of the generated samples, or “negative” samples. The training converges when \( p_\theta(x) \) becomes identical to \( p(x) \), as the two gradient terms cancel out. In practice, the two expectations in Eq. (7) are approximated with a minibatch of samples during each iteration. Figure 2 visualizes the gradients in Eq. (7).

Langevin Monte Carlo (LMC) The negative samples are generated using MCMC. LMC (Parisi (1981); Grenander & Miller (1994)) is a simple yet effective MCMC method used in recent work on deep EBMs (Du & Mordatch, 2019; Grathwohl et al., 2020; Nijkamp et al., 2019). In LMC, a starting point \( x_0 \) is drawn from a noise distribution \( p_\theta(x) \), typically a Gaussian or uniform distribution. Starting from \( x_0 \), a Markov chain evolves as follows:

\[
x_{t+1} = x_t + \lambda_x \nabla_x \log p_\theta(x_t) + \sigma_x \epsilon_t, \tag{8}
\]

where \( \epsilon_t \sim \mathcal{N}(0, I) \). \( \lambda_x \) and \( \sigma_x \) are the step size and the noise parameters, respectively. A theoretically motivated choice is \( 2\lambda_x = \sigma_x^2 \), but the parameters are often tweaked separately for better performance (Du & Mordatch, 2019; Grathwohl et al., 2020; Nijkamp et al., 2019). As \( \nabla_x \log p_\theta(x) = -\nabla_x E_\theta(x)/T \), tweaking the step size can be seen as adjusting the temperature \( T \).

To ensure the convergence of the chain, either Metropolis-Hastings rejection (Roberts et al., 1996) or annealing of the noise parameter to zero (Welling & Teh, 2011) may be employed, but often omitted in practice.

We discuss specific strategies to evaluate the second term in Eq. (7) in Section 4. For a comprehensive review on various strategies for training an EBM, readers may refer to Song & Kingma (2021).

3. Normalized Autoencoders

3.1. Definition

We propose Normalized Autoencoder (NAE), a normalized probabilistic model defined from an autoencoder. The probability density of NAE \( p_\theta(x) \) is defined as a Gibbs distribution (Eq. (4)) the energy of which is defined as the reconstruction error of an autoencoder:

\[
E_\theta(x) = l_0(x). \tag{9}
\]

Thus, the model density of NAE is given as

\[
p_\theta(x) = \frac{1}{\Omega_\theta} \exp(-l_0(x)/T), \tag{10}
\]

where \( \Omega_\theta \) is defined as in Eq. (5). Due to the normalization constant, \( p_\theta(x) \) is a properly normalized probability density. As a probabilistic model, NAE is trained to maximize the likelihood of data. The loss function to be minimized is the
negative log-likelihood of data:
\[
E_{x \sim p(x)}[-\log p_\theta(x)] = E_{x \sim p(x)}[l_\theta(x)]/T + \log \Omega_\theta. \tag{11}
\]

The gradient for the negative log-likelihood is evaluated as in conventional EBMs (Eq. (7)).
\[
E_{x \sim p(x)}[-\nabla_\theta \log p_\theta(x)] = E_{x \sim p(x)}[\nabla_\theta l_\theta(x)/T - E_{x' \sim p_\theta(x)}[\nabla_\theta l'(x')]/T. \tag{12}
\]

Therefore, each gradient step decreases the reconstruction error of training data \(x\), while increasing the reconstruction error of negative samples \(x'\) generated from \(p_\theta(x)\).

3.2. Remarks

Normalization as Regularization In NAE, enforcement of normalization can be viewed as a regularizer for the reconstruction loss (1). A typical formulation for a regularized autoencoder is given as \(L = L_{AE} + L_{\text{reg}}\), where \(L_{\text{reg}}\) is a regularizer. By setting the loss function of NAE as \(L = T E_{x \sim p(x)}[-\log p_\theta(x)]\), we have \(L = L_{AE} + T \log \Omega_\theta\).

Therefore, the normalization constant contributes as a regularizer: \(L_{\text{reg}} = T \log \Omega_\theta\).

Suppression of Outlier Reconstruction During the training of NAE, the reconstruction of an outlier is inhibited by enforcing the normalization constraint. Given a successful sampling process, the negative samples should cover all high density regions of \(p_\theta(x)\). A sample from a high density region of \(p_\theta(x)\) has a low \(l_\theta(x)\) by definition (Eq. (9)). Hence, if there exist a reconstructable outlier, which has high \(p_\theta(x)\) due to low \(l_\theta(x)\), it will appear as a negative sample from MCMC. As the gradient update given in Eq. (12) increases the reconstruction error of negative samples, the reconstruction quality of a reconstructable outlier will be degraded. As a result, the reconstruction error of NAE becomes a more informative predictor that discriminates outliers from inliers than that of a conventional autoencoder.

Outlier Detection with Likelihood NAE bridges the two popular outlier detection criteria, namely, the reconstruction error (Japkowicz et al., 1995) and the likelihood (Bishop, 1994). The reconstruction error criterion classifies an input with a large reconstruction error as OOD \(l_\theta(x) > \tau\), whereas the likelihood criterion predicts an input as an outlier if the log-likelihood is smaller than the threshold \(\log p_\theta(x) < \tau'\). These two criteria are equivalent in NAE for appropriately set \(\tau\) and \(\tau'\), as the reconstruction error and the log-likelihood has a linear relationship: \(\log p_\theta(x) = -l_\theta(x) - \log \Omega_\theta\). Note that the two criteria rarely coincide in other models, for example, denoising autoencoders (DAE, Vincent et al. (2008)), VAE (Kingma & Welling, 2014)), and DSEBMs (Zhao et al., 2016), causing confusion on which of the decision rules should be employed for outlier detection.

4. On-Manifold Initialization

The main challenge in the training of NAE through Eq. (12) is that each iteration requires negative sample generation using MCMC, which is computationally expensive. In this section, we first discuss the failure modes of popular approximate sampling strategies for EBMs, namely Contrastive Divergence (CD; Hinton (2002)) and Persistent CD (PCD; Tieleman (2008)). We argue that the method on how the initial state of MCMC is chosen has incurred such failure modes. Then, we propose on-manifold initialization, an approximate sampling strategy effective in training the NAE. On-manifold initialization provides a better initial state for MCMC by leveraging the structure of an autoencoder.

There exist other training methods for EBMs which do not rely on MCMC, for example denoising score matching (Vincent, 2011) or noise contrastive estimation (Gutmann & Hyvärinen, 2010), and they may also be applicable to NAE. We leave application of such methods on NAE as future work.

4.1. Failure Modes of CD and PCD

Failure Mode of CD CD, often called CD-k, draws a negative sample by first initializing a Markov chain of MCMC at a training data point, then proceeding \(k\) steps of MCMC transitions. The strength of CD is that the number of steps \(k\) can be radically smaller, e.g., \(k = 1\), than the usual number

\[\text{Figure 3. Density estimates and negative samples from NAEs trained by various approximate sampling methods. The generated samples (blue dots) are visualized along with the true density, a 2D mixture of 8 Gaussians. The data density is depicted in Figure 5. CD: The learned density has a spurious mode, marked by an arrow. The black crosses denote training data. PCD without restart: The highly correlated samples result in an oscillating density estimate. PCD with restart: Despite the good quality of sampling, the density is poorly estimated. On-manifold: Both density estimation and sample generation are performed well. More details are specified in Section 4.1 and Section 6.2.} \]
of steps required in a convergent MCMC run, significantly reducing the amount of computation.

However, when $k$ is small, CD-$k$ is not able to suppress a spuriously high mode in the model density $p_0(x)$ located far from the data distribution $p(x)$, because negative samples are only generated in the vicinity of training data. Figure 3 shows an instance of a spuriously mode in the model density. Negative samples (blue dots) are close to training data (black crosses) so that they do not reach the density mode in the middle. As a result, the mode is not suppressed. Such a spuriously mode will result in outlier detection failures and, in case of NAE, reconstructed outliers. The possibility of accidentally assigning high density in the unvisited area was acknowledged in the original article (Section 3 of Hinton (2002)). Spurious modes are also observed in DAE, where a corrupted datum is located only in the neighborhood of a training data point (Alain & Bengio, 2014). Increasing $k$ will decrease the chance of have spurious modes, but the computational advantage of CD will be lost when $k$ is large.

**Failure Mode of PCD** An initial state of MCMC in PCD is given as the negative sample generated from MCMC in the previous training iteration. PCD was originally implemented using fully persistent MCMC (Tieleman, 2008). However, without a restart, MCMC chains in a mini-batch may become highly correlated to each other. When $p_0(x)$ is multi-modal, the correlated chains yield degenerate negative samples which only cover a subset of density modes as in Figure 3. The degenerate samples make the density estimate oscillatory, slowing the convergence of the model.

The degeneracy between chains can be mitigated by randomly resetting the initial state to a sample from the noise distribution $p_0(x)$ with a small probability (typically 5%) (Du & Mordatch, 2019; Grathwohl et al., 2020). However, learning with PCD still fails to yield an accurate density estimate (Figure 3). This failure mode can be explained by the study of Nijkamp et al. (2019): When a short MCMC chain initialized from $p_0(x)$ is used in training, an EBM simply learns a flow that maps $p_0(x)$ to $p(x)$, and the energy no longer models the data density. Using a restart drives an EBM to become such a flow, as restarted chains are short and start from $p_0(x)$.

In summary, CD initializes MCMC from the data distribution $p_0(x)$, and PCD initializes MCMC from a noise distribution $p_0(x)$. The convergence of MCMC is independent of its initialization in theory, but the initialization method can be crucial in practice, as shown in Figure 3. When $p_0(x)$, from which we want to sample, deviates significantly from $p_0(x)$ or $p_0(x)$, these initialization methods may lead to a poor density estimate and a suboptimal performance in outlier detection.

![Figure 4. An illustration of the on-manifold initialization. The one-dimensional latent space $Z$ and the two-dimensional input space $X$ are shown. The red star is the on-manifold initialized state. The cross denotes a negative sample obtained at the end of the whole process.](image)

### 4.2. On-manifold Initialization

We propose on-manifold initialization (OMI), a novel MCMC initialization strategy which eventually leads to a significantly better density estimate. We aim to initialize a MCMC chain from a high-density region of $p_0(x)$ instead of $p_0(x)$ or $p(x)$. While finding a high-density region given an energy function is difficult in general, it is possible for NAE’s distribution, since we can exploit the structure of an autoencoder. For a sufficiently well-trained autoencoder, a point with high $p_0(x)$, i.e., a small reconstruction error, will lie near the decoder manifold, which we define as:

$$
\mathcal{M} = \{x|x = f_d(z), z \in Z\}.  \tag{13}
$$

In on-manifold initialization, we initialize MCMC from a point in the decoder manifold $x_0 \in \mathcal{M}$.

Not all points in $\mathcal{M}$ have high $p_0(x)$. To find points with high $p_0(x)$, we run a preliminary MCMC named as latent chain in the latent space $Z$. The latent chain generates a sample from on-manifold density $q_0(z)$ defined from on-manifold energy $H_0(z)$.

$$
q_0(z) = \frac{1}{\Psi_\theta} \exp(-H_0(z)/T_z),  \tag{14}
$$

$$
H_0(z) = E_\theta(f_d(z)),  \tag{15}
$$

where $\Psi_\theta = \int \exp(-H_\theta(z)/T_z)dz$ is the normalization constant and $T_z$ is the temperature. A latent vector $x$ with a small $H_\theta(z)$ will result in a small $E_\theta(x)$ when it is mapped to the input space by $x = f_d(z)$. Thus, $H_\theta(z)$ guides the latent chain to find $z$ which produce $x_0 \in \mathcal{M}$ which has a small energy, i.e., a small reconstruction error.

Similarly to Eq. (8), we use LMC to run the latent chain. An initial state $z_0$ is drawn from a noise distribution defined on the latent space. Then the state propagates as:

$$
z_{t+1} = z_t + \lambda_z \nabla_z \log q_0(z_t) + \sigma_z \epsilon_t,  \tag{16}
$$

where $\lambda_z$ and $\sigma_z$ are the step size and the noise parameters as in Eq. (8). A sample replay buffer (Du & Mordatch, 2019) can be crucial in practice, as shown in Figure 3. When $p_0(x)$, from which we want to sample, deviates significantly from $p_0(x)$ or $p_0(x)$, these initialization methods may lead to a poor density estimate and a suboptimal performance in outlier detection.
5. Related Work

Autoencoders There have been several attempts to formulate a latent probabilistic model from an autoencoder. VAE uses a latent variable model by introducing a prior distribution \( p(z) \). However, the prior may deviate from the actual distribution of data in \( Z \), which may cause problems. GPND (Pidhorskyi et al., 2018) models probability density by factorizing into on- and off-manifold components but still requires a prior distribution. \( \mathcal{M} \)-flow (Brehmer & Cranmer, 2020) only defines a probability density on the decoder manifold and does not assign a likelihood to off-manifold data. DAE models a density by learning the gradient of log-density (Alain & Bengio, 2014).

MemAE (Gong et al., 2019) is a rare example that directly tackles the outlier reconstruction problem. MemAE employs a memory module that memorizes training data to prevent outlier reconstruction, but in this case, the reconstruction error for an inlier can be large because the model’s generalization ability is also limited.

Design of Energy Functions Specifying the class of \( E_D(x) \) not only has computational consequences but alters the inductive bias that an EBM encodes. Feed-forward convolutional networks are used in Xie et al. (2016), Du & Mordatch (2019) and Grathwohl et al. (2020) and are shown to effectively model the distribution of images. The energy can also be modeled in an auto-regressive manner (Nash & Durkan, 2019; Meng et al., 2020). Auto-regressive energy functions are very flexible and thus are capable of modeling high-frequency patterns in data. VAEBM (Xiao et al., 2021) combines VAE and a feed-forward EBM to model complicated data distribution.

The reconstruction error of an autoencoder is used as a conventional autoencoder by minimizing the reconstruction error following Eq. (2), before the main training. By providing a good initialization for network weights and the decoder manifold, pre-training greatly reduces the number of NAE training iterations (Eq. (12)) required until convergence. Pre-training is not always necessary: In our experiments, we observe that NAE can be trained successfully without pre-training for synthetic data. However, pre-training was essential to obtain decent results for larger scale data, such as MNIST and CIFAR-10.

Latent Space Structure Two configurations for the latent space are used in experiments: the unbounded real space \( \mathbb{R}^{D_z} \) and the surface of a hypersphere \( \mathbb{S}^{D_z-1} \). When \( Z = \mathbb{R}^{D_z} \), a linear layer is used as the output of an encoder. \( q_0(z) \) is set as \( \mathcal{N}(0, I) \). The squared norm of the latent vectors are added to the loss function as a regularizer so that \( z \)'s concentrate near the origin (Ghosh et al., 2020).

For the hyperspherical space \( Z = \mathbb{S}^{D_z-1} \) (Davidson et al., 2018; Xu & Durrett, 2018; Zhao et al., 2019), the output of an encoder is projected to the surface of a unit ball through the division by its norm: \( z \leftarrow z/||z|| \). In Langevin dynamics, a sample is projected to \( \mathbb{S}^{D_z-1} \) at the end of each step. \( q_0(z) \) is set to a uniform distribution on \( \mathbb{S}^{D_z-1} \).

The hyperspherical latent space has a few advantages over \( \mathbb{R}^{D_z} \). First, it is impossible to draw uniformly random samples, because \( \mathbb{R}^{D_z} \) is not compact. Second, for large \( D_z \), it is difficult to draw samples near the origin, because of its exponentially decreasing volume. However, we believe more works needs to be done to completely understand the effect of hyperspherical geometry on the latent representation.

Regularizing Negative Sample Energy As introduced in Du & Mordatch (2019), we regularize the energy of negative samples to prevent its divergence. We add the average squared energy of negative samples in a mini-batch to the loss function: \( L = L_{\text{NAE}} + \alpha \sum_{i=1}^{D_z} E(x_i^e)/2 \) for the batch size \( B \) and the hyperparameter \( \alpha \). We set \( \alpha = 1 \).
Table 1. MNIST hold-out class detection AUC scores. The values in parentheses denote the standard error of mean after 10 training runs.

| HOLD-OUT: | 0    | 1    | 2    | 3    | 4    | 5    | 6    | 7    | 8    | 9    | AVG  |
|----------|------|------|------|------|------|------|------|------|------|------|------|
| NAE-OMI  | 0.989 | 0.910 | 0.992 | 0.949 | 0.949 | 0.978 | 0.938 | 0.975 | 0.929 | 0.934 | 0.955 |
| NAE-CD   | 0.799 | 0.899 | 0.787 | 0.769 | 0.656 | 0.806 | 0.874 | 0.537 | 0.876 | 0.500 | 0.679 |
| NAE-PCD  | 0.744 | 0.112 | 0.872 | 0.816 | 0.690 | 0.813 | 0.872 | 0.509 | 0.902 | 0.544 | 0.682 |
| AE       | 0.819 | 0.131 | 0.843 | 0.734 | 0.661 | 0.755 | 0.844 | 0.542 | 0.902 | 0.537 | 0.677 |
| DAE      | 0.769 | 0.124 | 0.872 | 0.935 | 0.884 | 0.793 | 0.865 | 0.533 | 0.910 | 0.625 | 0.731 |
| VAE(R)   | 0.958 | 0.391 | 0.978 | 0.910 | 0.860 | 0.939 | 0.916 | 0.774 | 0.946 | 0.721 | 0.839 |
| VAE(L)   | 0.967 | 0.326 | 0.976 | 0.906 | 0.798 | 0.927 | 0.928 | 0.751 | 0.935 | 0.614 | 0.813 |
| WAE      | 0.817 | 0.145 | 0.975 | 0.950 | 0.751 | 0.942 | 0.853 | 0.912 | 0.907 | 0.799 | 0.805 |
| GLOW     | 0.803 | 0.014 | 0.624 | 0.625 | 0.364 | 0.561 | 0.583 | 0.532 | 0.721 | 0.426 | 0.505 |
| PXCNN++  | 0.757 | 0.030 | 0.663 | 0.483 | 0.506 | 0.642 | 0.506 | 0.307 | 0.810 | 0.497 | 0.545 |
| IGEBM    | 0.926 | 0.401 | 0.642 | 0.644 | 0.664 | 0.752 | 0.851 | 0.572 | 0.747 | 0.522 | 0.672 |
| DAGMM    | 0.386 | 0.304 | 0.407 | 0.435 | 0.444 | 0.429 | 0.446 | 0.349 | 0.609 | 0.420 | 0.423 |

6.2. 2D Density Estimation

We demonstrate the density estimation capability of NAE with a two-dimensional mixture of 8 Gaussians. First, we benchmark negative sample generation strategies for NAE, including CD, PCD with and without restart, and on-manifold initialization. The results are shown in Figure 3 and discussed in Section 4.1 in detail.

Second, we compare NAE trained with the on-manifold initialization to a conventional autoencoder and VAE (Figure 5). An autoencoder assigns high densities on regions between Gaussian modes, meaning that an autoencoder gives a small reconstruction error from a points from the region. For the overcomplete case ($D_x = 3 > D_z$), an autoencoder almost becomes the identity map, and its reconstruction error is not an informative predictor for an outlier. VAE and NAE learn a non-identity function under the overcomplete setting, showing the effectiveness of their regularizers.

In the experiments, the identical network architecture is used, and the temperature is optimized by gradient descent. In on-manifold initialization, temperature values are shared by the main MCMC and the latent chain. When performing MCMC in $X$, Metropolis-Hastings rejection is applied to ensure the detailed balance but is not applied in the latent chain. For visualization, the normalization constants for an autoencoder and NAE are computed by numerically integrating over the domain, $[-4, 4]^2$.

6.3. Outlier Detection

Experimental Setting We empirically demonstrate the effectiveness of NAE as an outlier detector. In outlier detection tasks, an outlier detector is trained only using inlier data and then asked to discriminate outliers from inliers during test phase. Given an input, a detector is assumed to produce a scalar decision function which indicates the outlierness of the input. We measure the detection performance in AUC, i.e., the area under the receiver operating characteristic curve. Following the protocol of Ren et al. (2019) and Hendrycks et al. (2019), we use an OOD dataset different from the datasets used in test phase to tune model hyperparameters. Additional details on model implementation and datasets can be found in the supplementary material.

The identical networks architectures are used for all autoencoder-based methods. The reconstruction error is used as the decision function, except for VAE. For deep generative models, PixelCNN++ (PXCNN++, Salimans et al. (2017)), Glow (Kingma & Dhariwal, 2018) and a feed-forward EBM (IGEBM, Du & Mordatch (2019)), we use the negative log-likelihood (i.e., the energy) as the decision function. For VAE, we show two results from using the reconstruction error ($R$) or the negative log-likelihood ($L$) as decision functions.

MNIST Hold-Out Class Detection One class from MNIST is set as the outlier class and the rest as the inlier class. Then, the procedure is repeated for all ten classes in MNIST. ConstantGray dataset is used for model selection.

This problem is not as easy as it seems, as confirmed in the very low performance of various algorithms in Table 1. When a class is held out from MNIST, the remaining 9 classes may contain a set of visual features sufficient to reconstruct the hold-out class, i.e., the outlier reconstruction occurs. The outlier reconstruction is particularly severe for the digit 1, 4, 7 and 9, possibly because their shape can be reconstructed from the recombination of other digits. For example, overlapping 4 and 7 produces a shape similar to 9. Interestingly, most of the other baseline algorithms also show poor performance when 1, 4, 7 or 9 are held out as the outlier. NAE shows the highest AUC score for all classes and effectively suppresses the reconstruction of the outlier class (Figure 6).

We also compare CD and PCD along with OMI in training NAES. Using CD and PCD show poor outlier detection performance, although given the identical set of MCMC parameters.

Out-of-Distribution Detection The samples from different datasets are used as the outlier class. We test two inlier datasets, CIFAR-10 or ImageNet $32 \times 32$ (ImageNet32).
Autoencoding Under Normalization Constraints

Table 2. OOD detection performance in AUC.

| In: CIFAR-10 ConstantGray FMNIST SVHN CelebA Noise | NAE | .963 | .819 | .920 | .887 | 1.0 |
| | AE | .006 | .650 | .175 | .655 | 1.0 |
| | DAE | .001 | .671 | .175 | .669 | 1.0 |
| | VAE(R) | .002 | .700 | .191 | .662 | 1.0 |
| | VAE(L) | .002 | .767 | .185 | .684 | 1.0 |
| | WAE | .000 | .649 | .168 | .652 | 1.0 |
| | GLOW | .384 | .222 | .260 | .419 | 1.0 |
| | PXCNN++ | .000 | .013 | .074 | .639 | 1.0 |
| | IGEBM | .192 | .216 | .371 | .477 | 1.0 |

| In: ImageNet32 ConstantGray FMNIST SVHN CelebA Noise | NAE | .966 | .994 | .985 | .949 | 1.0 |
| | AE | .005 | .915 | .102 | .325 | 1.0 |
| | DAE | .069 | .991 | .102 | .426 | 1.0 |
| | VAE(R) | .030 | .936 | .132 | .501 | 1.0 |
| | VAE(L) | .028 | .950 | .132 | .545 | 1.0 |
| | WAE | .069 | .991 | .081 | .364 | 1.0 |
| | GLOW | .413 | .856 | .169 | .479 | 1.0 |
| | PXCNN++ | .000 | .004 | .027 | .238 | 1.0 |

Figure 6. Reconstruction examples in MNIST hold-out class detection. Data and their reconstructions are shown for four difficult hold-out settings (1, 4, 7 and 9). Digit 2 is shown as an inlier example. The bottom two rows depict the reconstructions from four autoencoders (AE) and four NAEs trained on each setting. AEs reconstruct the outlier class well, while NAEs selectively reconstruct only inliers.

Zero-padded 32×32 MNIST images are used for model selection. Results are shown in Table 2.

It is known that constant images and SVHN images are particularly difficult outliers for generative models trained on a set of images with rich visual features (Nalisnick et al., 2019; Serrà et al., 2020). However, NAE detect such difficult outliers successfully. All models are able to discriminate noise outliers, indicating that their poor performance is not from the failure of training.

6.4. Sample Generation

Samples are generated from NAE using MCMC with OMI. Figure 7 shows the samples from NAEs trained on MNIST and on CelebA 64×64. The random initial states of the latent chain (z₀) map to unrecognizable images. After the latent chain, OMI produces somewhat realistic images. MCMC on X refines the OMI images. Although quantitative image (in Appendix) quality metric for samples generated from NAE is not on a par with that of generative models which specialize in sampling, but the generated samples are indeed visually sensible.

Figure 7. Sampling with NAEs trained on MNIST and CelebA 64×64. (z₀) The random initialization of the latent chain. We visualize fₙ(z₀). (OMI) Images after OMI. (Samples) Samples obtained after MCMC starting from OMI. OMI images and Samples corresponds to the red start and the green cross in Figure 4, respectively.

7. Discussion and Conclusion

Comparison to Other EBMs NAE uses Gibbs distribution to define a density function as in other EBMs (Eq. 4). The main difference between NAE and other EBMs is the choice of an energy function. However, this difference results in significant theoretical and practical consequences. First, we naturally incorporate the manifold hypothesis, i.e. the assumption that high-dimensional data lie on a low-dimensional manifold, into a model. Second, the energy function of NAE can be pre-trained as a conventional autoencoder. Third, more effective sampling can be performed by using OMI, leading to a more accurate density estimate.

Likelihood-based Outlier Detection and Inductive Bias The likelihood is considered as a poor decision function for outlier detection, after the failures of likelihood-based deep generative models such as VAE, PixelCNN++, and Glow (Nalisnick et al., 2019; Hendrycks et al., 2019). Those generative models fail to detect obvious outlier images which typically have low complexity. However, we believe that the failures should not be attributed to the use of the likelihood. There are likelihood-based models, particularly EBMs (Du & Mordatch, 2019; Grathwohl et al., 2020), including NAE, that show better outlier detection performance than VAE, PixelCNN++, and Glow. Instead, inductive bias of a generative model is likely to be responsible for the failure of detecting low-complexity outliers. It is reported that the likelihoods of the failed models are negatively correlated to the complexity of images (Serrà et al., 2020). Meanwhile,
the reconstruction of low-complexity images are explicitly suppressed in NAE training, as the simple images tend to lie on the decoder manifold.

OMI in Early Stage of Training Sampling with OMI generates samples with high model density $p_θ(x)$ even in the early stage of training. In fact, the early stage is where the advantage of OMI over CD is salient, because $p_θ(x)$ differs from $p(x)$ significantly. Figure 8 visualizes samples generated via CD and OMI from a randomly initialized NAE and shows that CD fails to draw samples from $p_θ(x)$.

OMI draws high-model-density proposals because it is designed to exploit the assumption that well-reconstructed points lie on the decoder manifold. We find that this assumption holds well for all experimental settings used in the paper.

Analytic Solution for Linear Case Linear NAEs reduce to Gaussian distributions. Consider $f_ε(x) = Wx$ and $f_d(z) = W^Tz$ with $W \in \mathbb{R}^{D_x \times D_x}$. Given the squared $L^2$ distance reconstruction error, the density of NAE is written as:

$$p_θ(x) = \exp(-x^T \Sigma^{-1} x / 2) / \Omega_θ, \quad (17)$$

where $\Sigma^{-1} = 2(I - W^T W)^2 / T$. When the determinant of $I - W^T W$ is non-zero, $p_θ(x)$ becomes a well-defined Gaussian. Under certain conditions (see Appendix), the maximum likelihood estimate of $\Sigma$ becomes the empirical covariance of data, as in a usual Gaussian distribution.

It is interesting to note that a linear VAE also reduces into a Gaussian, as it is equivalent to probabilistic PCA (Kingma & Welling, 2014). On the other hand, a linear autoencoder is equivalent to PCA (Bourlard & Kamp, 1988), which is not a generative model.

Conclusion We have introduced a novel interpretation of the reconstruction error as an energy function. Our interpretation leads to a novel class of probabilistic autoencoders, which shows impressive OOD detection performance and bridges EBMs and autoencoders.

Acknowledgements

S. Yoon and F.C. Park were supported in part by the SNU Artificial Intelligence Institute (AIIS), NRF Grant 2016R1A5A1938472 (SRRC), the SNU BK21+ Program in Mechanical Engineering, and SNU-IAMD. Y.-K. Noh was partly supported by NRF/MSIT (No. 2018R1A5A7059549, 2021M3E5D2A01019545), IITP/MSIT Artificial Intelligence Graduate School Program for Hanyang University (2020-0-01373), and Hanyang University (HY-2019).

References

Akçay, S., Atapour-Abarghouei, A., and Breckon, T. P. Ganomaly: Semi-supervised anomaly detection via adversarial training. In Asian conference on computer vision, pp. 622–637. Springer, 2018.

Alain, G. and Bengio, Y. What regularized auto-encoders learn from the data-generating distribution. The Journal of Machine Learning Research, 15(1):3563–3593, 2014.

Bergmann, P., Löwe, S., Fauser, M., Sattlegger, D., and Steger, C. Improving unsupervised defect segmentation by applying structural similarity to autoencoders. arXiv preprint arXiv:1807.02011, 2018.

Bishop, C. M. Novelty detection and neural network validation. IEE Proceedings-Vision, Image and Signal processing, 141(4):217–222, 1994.

Bourlard, H. and Kamp, Y. Auto-association by multilayer perceptrons and singular value decomposition. Biological cybernetics, 59(4-5):291–294, 1988.

Brehmer, J. and Cranmer, K. Flows for simultaneous manifold learning and density estimation. arXiv preprint arXiv:2003.13913, 2020.

Davidson, T. R., Falorsi, L., De Cao, N., Kipf, T., and Tomczak, J. M. Hyperspherical variational auto-encoders. In 34th Conference on Uncertainty in Artificial Intelligence 2018, UAI 2018, pp. 856–865. Association For Uncertainty in Artificial Intelligence (AUAI), 2018.

Du, Y. and Mordatch, I. Implicit generation and modeling with energy based models. In Wallach, H., Larochelle, H., Beygelzimer, A., d Alche-Buc, F., Fox, E., and Garnett, R. (eds.), Advances in Neural Information Processing Systems 32, pp. 3608–3618. Curran Associates, Inc., 2019.
Autoencoding Under Normalization Constraints

Ghosh, P., Sajjadi, M. S. M., Vergari, A., Black, M., and Scholkopf, B. From variational to deterministic autoencoders. In *International Conference on Learning Representations*, 2020. URL https://openreview.net/forum?id=S1g7tpEYDS.

Gong, D., Liu, L., Le, V., Saha, B., Mansour, M. R., Venkatesh, S., and Hengel, A. v. d. Memorizing normality to detect anomaly: Memory-augmented deep autoencoder for unsupervised anomaly detection. In *IEEE International Conference on Computer Vision (ICCV)*, 2019.

Grathwohl, W., Chen, R. T., Bettencourt, J., Sutskever, I., and Duvenaud, D. Ffjord: Free-form continuous dynamics for scalable reversible generative models. *arXiv preprint arXiv:1810.01367*, 2018.

Grathwohl, W., Wang, K.-C., Jacobsen, J.-H., Duvenaud, D., Norouzi, M., and Swersky, K. Your classifier is secretly an energy based model and you should treat it like one. In *International Conference on Learning Representations*, 2020. URL https://openreview.net/forum?id=Hkxzx0NtDB.

Grenander, U. and Miller, M. I. Representations of knowledge in complex systems. *Journal of the Royal Statistical Society: Series B (Methodological)*, 56(4):549–581, 1994.

Gutmann, M. and Hyvärinen, A. Noise-contrastive estimation: A new estimation principle for unnormalized statistical models. In *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics*, pp. 297–304, 2010.

Hendrycks, D., Mazeika, M., and Dietterich, T. Deep anomaly detection with outlier exposure. In *International Conference on Learning Representations*, 2019. URL https://openreview.net/forum?id=HyxXz0RcY7.

Heusel, M., Ramsauer, H., Unterthiner, T., Nessler, B., and Hochreiter, S. Gans trained by a two time-scale update rule converge to a local nash equilibrium. *arXiv preprint arXiv:1706.08500*, 2017.

Hinton, G. E. Training products of experts by minimizing contrastive divergence. *Neural computation*, 14(8):1771–1800, 2002.

Japkowicz, N., Myers, C., Gluck, M., et al. A novelty detection approach to classification. In *Proceedings of the International Joint Conference on Artificial Intelligence*, volume 1, pp. 518–523, 1995.

Keysers, D., Schärli, N., Scales, N., Buismman, H., Furrer, D., Kashubin, S., Momchev, N., Sinopalinikov, D., Stafniak, L., Tihon, T., et al. Measuring compositional generalization: A comprehensive method on realistic data. *arXiv preprint arXiv:1912.09713*, 2019.

Kingma, D. P. and Ba, J. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*, 2014.

Kingma, D. P. and Dhariwal, P. Glow: Generative flow with invertible 1x1 convolutions. In *Advances in Neural Information Processing Systems*, pp. 10215–10224, 2018.

Kingma, D. P. and Welling, M. Auto-encoding variational bayes. *International Conference on Learning Representations (ICLR)*, 2014.

Lan, C. L. and Dinh, L. Perfect density models cannot guarantee anomaly detection. *arXiv preprint arXiv:2012.03808*, 2020.

Lu, Y. and Xu, P. Anomaly detection for skin disease images using variational autoencoder. *arXiv preprint arXiv:1807.01349*, 2018.

Lyudchik, O. Outlier detection using autoencoders. Technical report, 2016.

Meng, C., Yu, L., Song, Y., Song, J., and Ermon, S. Autoregressive score matching. *arXiv preprint arXiv:2010.12810*, 2020.

Mikolov, T., Sutskever, I., Chen, K., Corrado, G. S., and Dean, J. Distributed representations of words and phrases and their compositionality. In *Advances in neural information processing systems*, pp. 3111–3119, 2013.

Miyato, T., Kataoka, T., Koyama, M., and Yoshida, Y. Spectral normalization for generative adversarial networks. *arXiv preprint arXiv:1802.05957*, 2018.

Nalisnick, E., Matsukawa, A., Teh, Y. W., Gorur, D., and Lakshminarayanan, B. Do deep generative models know what they don’t know? In *International Conference on Learning Representations*, 2019. URL https://openreview.net/forum?id=H1xwNhCcYm.

Nash, C. and Durkan, C. Autoregressive energy machines. In *International Conference on Machine Learning*, pp. 1735–1744. PMLR, 2019.

Ng, A. et al. Sparse autoencoder. *CS294A Lecture notes*, 2011.

Nijkamp, E., Hill, M., Zhu, S.-C., and Wu, Y. N. Learning non-convergent non-persistent short-run mcmc toward energy-based model. In Wallach, H., Larochelle, H., Beygelzimer, A., d’Alché-Buc, F., Fox, E., and Garnett, R. (eds.), *Advances in Neural Information Processing Systems*.
Oord, A. v. d., Kalchbrenner, N., and Kavukcuoglu, K. Pixel recurrent neural networks. *arXiv preprint arXiv:1601.06759*, 2016.

Oord, A. v. d., Vinyals, O., and Kavukcuoglu, K. Neural discrete representation learning. *arXiv preprint arXiv:1711.00937*, 2017.

Parisi, G. Correlation functions and computer simulations. *Nuclear Physics B*, 180(3):378–384, 1981.

Pichhorskyi, S., Almohsen, R., and Doretto, G. Generative probabilistic novelty detection with adversarial autoencoders. In *Advances in neural information processing systems*, pp. 6822–6833, 2018.

Ren, J., Liu, P. J., Fertig, E., Snoek, J., Poplin, R., Depristo, M., Dillon, J., and Lakshminarayanan, B. Likelihood ratios for out-of-distribution detection. In *Advances in Neural Information Processing Systems*, pp. 14680–14691, 2019.

Rifai, S., Vincent, P., Muller, X., Glorot, X., and Bengio, Y. Contractive auto-encoders: explicit invariance during feature extraction. In *Proceedings of the 28th International Conference on International Conference on Machine Learning*, pp. 833–840, 2011.

Roberts, G. O., Tweedie, R. L., et al. Exponential convergence of langevin distributions and their discrete approximations. *Bernoulli*, 2(4):341–363, 1996.

Rumelhart, D. E., Hinton, G. E., and Williams, R. J. *Learning Internal Representations by Error Propagation*, pp. 318–362. MIT Press, Cambridge, MA, USA, 1986. ISBN 026268053X.

Salimans, T., Karpathy, A., Chen, X., and Kingma, D. P. Pixelcnn++: Improving the pixelcnn with discretized logistic mixture likelihood and other modifications. *arXiv preprint arXiv:1701.05517*, 2017.

Serrà, J., Álvarez, D., Gómez, V., Slizovskaia, O., Núñez, J. F., and Luque, J. Input complexity and out-of-distribution detection with likelihood-based generative models. In *International Conference on Learning Representations*, 2020. URL https://openreview.net/forum?id=SyxIWpVYvr.

Song, Y. and Ermon, S. Improved techniques for training score-based generative models. *arXiv preprint arXiv:2006.09011*, 2020.

Song, Y. and Kingma, D. P. How to train your energy-based models. *arXiv preprint arXiv:2101.03288*, 2021.

Steinwart, I., Hush, D., and Scovel, C. A classification framework for anomaly detection. *Journal of Machine Learning Research*, 6(Feb):211–232, 2005.

Tieleman, T. Training restricted boltzmann machines using approximations to the likelihood gradient. In *Proceedings of the 25th international conference on Machine learning*, pp. 1064–1071, 2008.

Tong, A., Yousefzadeh, R., Wolf, G., and Krishnaswamy, S. Fixing bias in reconstruction-based anomaly detection with lipschitz discriminators. *arXiv preprint arXiv:1905.10710*, 2019.

Vincent, P. A connection between score matching and denoising autoencoders. *Neural computation*, 23(7):1661–1674, 2011.

Vincent, P., Larochelle, H., Bengio, Y., and Manzagol, P.-A. Extracting and composing robust features with denoising autoencoders. In *Proceedings of the 25th international conference on Machine learning*, pp. 1096–1103, 2008.

Wang, Z., Bovik, A. C., Sheikh, H. R., and Simoncelli, E. P. Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, 13(4):600–612, 2004.

Welling, M. and Teh, Y. W. Bayesian learning via stochastic gradient langevin dynamics. In *Proceedings of the 28th international conference on machine learning (ICML-11)*, pp. 681–688, 2011.

Wu, Y. and He, K. Group normalization. In *Proceedings of the European conference on computer vision (ECCV)*, pp. 3–19, 2018.

Xiao, Z., Yan, Q., and Amit, Y. Likelihood regret: An out-of-distribution detection score for variational auto-encoder. In Larochelle, H., Ranzato, M., Hadsell, R., Balcan, M. F., and Lin, H. (eds.), *Advances in Neural Information Processing Systems*, volume 33, pp. 20685–20696. Curran Associates, Inc., 2020. URL https://proceedings.neurips.cc/paper/2020/file/eddea82ad2755b24c4e168c5fc2ebd40-Paper.pdf.

Xiao, Z., Kreis, K., Kautz, J., and Vahdat, A. *{VAEBM}: A symbiosis between variational autoencoders and energy-based models*. In *International Conference on Learning Representations*, 2021. URL https://openreview.net/forum?id=5m3SEczOV8L.
Xie, J., Lu, Y., Zhu, S.-C., and Wu, Y. A theory of generative convnet. In *International Conference on Machine Learning*, pp. 2635–2644. PMLR, 2016.

Xu, J. and Durrett, G. Spherical latent spaces for stable variational autoencoders. In *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing*, pp. 4503–4513, 2018.

Younes, L. On the convergence of markovian stochastic algorithms with rapidly decreasing ergodicity rates. *Stochastics: An International Journal of Probability and Stochastic Processes*, 65(3-4):177–228, 1999.

Zhao, D., Zhu, J., and Zhang, B. Latent variables on spheres for autoencoders in high dimensions. *arXiv*, pp. arXiv–1912, 2019.

Zhao, J., Mathieu, M., and LeCun, Y. Energy-based generative adversarial network. *arXiv preprint arXiv:1609.03126*, 2016.

Zhao, Y., Deng, B., Shen, C., Liu, Y., Lu, H., and Hua, X.-S. Spatio-temporal autoencoder for video anomaly detection. In *Proceedings of the 25th ACM international conference on Multimedia*, pp. 1933–1941, 2017.

Zong, B., Song, Q., Min, M. R., Cheng, W., Lumezanu, C., Cho, D., and Chen, H. Deep autoencoding gaussian mixture model for unsupervised anomaly detection. In *International Conference on Learning Representations*, 2018. URL https://openreview.net/forum?id=BJJLHbb0-.
The Appendix is organized as follows: Section A provides mathematical derivations, Section B contains extended experimental results, Section C addresses additional topics for discussions, and experimental details are provided in Section D.

A. Derivations

A.1. Derivation for Log-Likelihood Gradient in EBM

Here, we present the derivation for the gradient of log-likelihood in Eq. (7).

\[ \nabla \theta \log p_\theta(x) \]

\[ = - \nabla \theta E(x)/T - \nabla \theta \log \Omega_\theta \]

\[ = - \nabla \theta E(x)/T - \nabla \theta \log \Omega_\theta / \Omega_\theta \]

\[ = - \nabla \theta E(x)/T - 1 / \Omega_\theta \int \exp(-E_\theta(x')/T)dx' \]

\[ = - \nabla \theta E(x)/T - 1 / \Omega_\theta \int \nabla \theta \exp(-E_\theta(x')/T)dx' \]

\[ = - \nabla \theta E(x)/T \]

\[ + \int 1 / \Omega_\theta \exp(-E_\theta(x')/T)\nabla \theta E_\theta(x')/Tdx' \]

\[ = - \nabla \theta E(x)/T + \mathbb{E}_{x' \sim p_\theta(x')} [\nabla \theta E(x')/T]. \]

Taking the expectation over the data density \( p(x) \),

\[ \mathbb{E}_{x \sim p(x)} [\nabla \theta \log p_\theta(x)] \]

\[ = - \mathbb{E}_{x \sim p(x)} [\nabla \theta E(x)/T] \]

\[ + \mathbb{E}_{x \sim p(x)} [\mathbb{E}_{x' \sim p_\theta(x')} [\nabla \theta E_\theta(x')/T]] \]

\[ = - \mathbb{E}_{x \sim p(x)} [\nabla \theta E(x)/T] + \mathbb{E}_{x' \sim p_\theta(x')} [\nabla \theta E_\theta(x')/T]. \]

Thus, we obtain Eq. (7) of the main manuscript.

A.2. Analytic Solution for Linear Case

We provide a more detailed derivation for linear NAE. When a linear overcomplete autoencoder is used, NAE reduces into a Gaussian distribution. Consider a linear deterministic encoder \( f_\theta(x) = Wx \) and a decoder \( f_\mu(z) = W^Tz \), where \( W \in \mathbb{R}^{D_x \times D_x} \). For the squared \( L^2 \) distance reconstruction error,

\[ l(x) = \|x - W^T W x\|^2 \]

\[ = x^T (I - W^T W)^2 x, \]

and therefore the density of NAE can be written as:

\[ p_\theta(x) = \frac{1}{\Omega_\theta} \exp(-x^T \Sigma^{-1} x/2), \]

where \( \Sigma^{-1} = 2(I - W^T W)^2/T \).

Eq. (20) is a Gaussian distribution with zero mean and \( \Sigma \) covariance. For this Gaussian to be well-defined, the normalization constant should be finite \( \Omega_\theta < \infty \). To the covariance positive definitive, we need that the determinant of \( (I - W^T W) \) is non-zero, i.e., no eigenvalue of \( W^T W \) should be one. This means that the autoencoder should not be the identity along any of orthogonal bases.

As an interesting special case, consider \( W = 0 \). This zero-autoencoder is uninformative, since all inputs are mapped to the origin, but it still defines a valid probability distribution. In fact, \( p_\theta(x) \) becomes a standard normal distribution.

Now, we consider the overcomplete setting, where \( D_x \geq D_z \), and look for the maximum likelihood parameter estimate. When \( D_x \geq D_z \), the matrix \( (I - W^T W) \) spans all positive semidefinite matrices. Given a zero-centered dataset \( D = \{x_i\}_{i=1}^N \), \( \Sigma \) that maximizes the likelihood of data is the empirical covariance \( \Sigma_{\text{ML}} = \sum_{i=1}^N x_i x_i^\top / N \). Therefore, NAE trained to maximum the likelihood of data is identical to a Gaussian distribution fitted via maximum likelihood.

Recall that a conventional linear autoencoder becomes the identity when \( D_x \geq D_z \).

B. Extended Experimental Results

In this section, we provide additional experimental results.

B.1. MNIST Hold-Out Class Detection

Table 3 augments Table 1 by providing results from VQVAE (Oord et al., 2017) and Ganomaly (Akcay et al., 2018).

We could not experiment with MemAE (Gong et al., 2019) as the training code was not provided by the authors. Instead, we experiment with VQVAE, since it has a similar inductive bias that the only finite number of discrete latent representation can be used.

For Ganomaly, we report two versions of results. Ganomaly(Repro) indicates our re-implementation that shares the network architectures with other autoencoders.
Table 3. MNIST hold-out class detection AUC scores. The values in parentheses denote the standard error of mean after 10 training runs. The values below the horizontal divider line are the newly appended values.

| HOLD-OUT: | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | AVG |
|-----------|----|----|----|----|----|----|----|----|----|----|-----|
| NAE-OMI   | **.989** (.002) | **.919** (.013) | **.992** (.001) | **.949** (.004) | **.949** (.005) | **.978** (.003) | **.938** (.004) | **.975** (.024) | **.929** (.004) | **.934** (.005) | **.955** |
| NAE-CD    | .799 | .098 | .878 | .769 | .656 | .806 | .874 | .537 | .876 | .500 | .679 |
| NAE-PCD   | .745 | .114 | .879 | .754 | .690 | .813 | .872 | .509 | .902 | .544 | .682 |
| AE        | .819 | .131 | .843 | .734 | .661 | .755 | .844 | .542 | .902 | .537 | .677 |
| DAE       | .769 | .124 | .872 | .935 | .884 | .793 | .865 | .533 | .910 | .625 | .731 |
| VAE(R)    | .954 | .391 | .978 | .910 | .860 | .939 | .916 | .774 | .946 | .721 | .839 |
| VAE(L)    | .967 | .326 | .976 | .906 | .798 | .927 | .928 | .751 | .935 | .614 | .813 |
| WAE       | .817 | .145 | .975 | **.950** | .751 | .942 | .853 | .912 | .907 | .799 | .805 |
| GLOW      | .803 | .014 | .624 | .625 | .364 | .561 | .583 | .326 | .721 | .426 | .505 |
| PXCNN++   | .757 | .030 | .663 | .663 | .483 | .642 | .596 | .307 | .810 | .497 | .545 |
| IEGBM     | .926 | .401 | .642 | .644 | .664 | .752 | .851 | .572 | .747 | .522 | .672 |
| DAGMM     | .386 | .304 | .407 | .435 | .444 | .429 | .446 | .349 | .609 | .420 | .423 |
| VQVAE     | .937 | .272 | .915 | .807 | .673 | .807 | .892 | .643 | .816 | .596 | .736 |
| Ganomaly(Repro) | .418 | .676 | .479 | .750 | .591 | .615 | .480 | .546 | .551 | .427 | .553 |
| Ganomaly(Pub) | .740 | .142 | .873 | .699 | .695 | .725 | .787 | .502 | .840 | .508 | .651 |

Table 4. OOD detection performance for MNIST as the in-distribution dataset. AUC scores are shown. Half indicates HalfMNIST dataset, and Chimera indicates ChimeraMNIST dataset.

| CONSTANTGRAY | HALF | CHIMERA | OMNIGLOT | NOISE |
|--------------|------|---------|----------|-------|
| NAE          | **1.00** | **.999** | **.992** | **.995** | 1.00 |
| AE           | .934  | .523    | .761    | .885  | 1.00 |
| PXCNN        | .982  | .154    | .334    | .665  | 1.00 |
| GLOW         | **1.00** | .948    | .445    | .653  | 1.00 |
| IEGBM        | **1.00** | .986    | .948    | .946  | 1.00 |

B.2. Out-of-Distribution Detection

We repeat OOD detection experiment in Section 6.3 with MNIST as the in-distribution dataset. The results are present in Table 4.

We use images from Constant Gray, HalfMNIST, ChimeraMNIST, Omniglot, FashionMNIST and Noise dataset for OOD inputs. The whole MNIST training set without holding out is used to train models. As shown in Figure 1, an autoencoder shows limited performance due to outlier reconstruction. Note that the blank image used in Figure 1 is an instance of ConstantGray dataset. However, NAE successfully detects all the specified OOD inputs. We omit FashionMNIST results from Table 4, because all models detects FashionMNIST inputs with AUC very close to 1.0.

B.3. Sample Generation

Visualization of Negative Samples We collect negative samples used in training NAE on MNIST and visualize them in Figure 9. Additionally, OMI samples generated from the latent chain are also visualized.

Samples obtained right after pre-training (“Iter:0” in the figure) does not visually close to digits. Since sampling procedure tends to generates images with high $p_\theta(x)$, i.e., $\log l_\theta(x)$, these samples may have lower reconstruction error than in-distribution MNIST digits. As training proceeds, the samples become more visually similar to digits in MNIST.

Figure 9. Samples collected from NAE during training. Initial states given by OMI and final states after MCMC on $X$ are shown. Each column corresponds to a training iteration of NAE. Iter 0 is right after the autoencoder pre-training. NAE is trained on MNIST excluding the digit 9.

Quantitative Result for Sample Quality We generate 50,000 samples from NAE trained on CelebA $64 \times 64$ and compute FID score (Heusel et al., 2017). We also visualize
Table 5. FID score of 50,000 images generated from a model trained on CelebA $64 \times 64$. A low FID score indicates that the generated images have similar statistics to the real images in Inception network’s feature space.

| Model               | FID  |
|---------------------|------|
| NAE                 | 94.00|
| From Ghosh et al. (2020) |
| AE                  | 127.85|
| AE-L2               | 346.29|
| VAE                 | 48.12 |
| RAE-GP              | 116.30|
| RAE-L2              | 51.13 |
| RAE-SN              | 44.74 |
| From Song & Ermon (2020) |
| NCSN (w/ denoising) | 26.89 |
| NCSNv2 (w/ denoising)| 10.23 |

some of images generated by NAE in Figure 10. While FID score of NAE was not as low as ones from models specialized in generation, such as NCSN (Song & Ermon, 2020), FID score of NAE resides in a ballpark of what is achievable by autoencoder-based methods. We believe that tuning network architecture and sampling procedure will result in enhanced samples.

C. Additional Discussion

C.1. Parameter Sensitivity Study

To demonstrate the contribution of learning techniques and components used in NAE, we alter or ablate components in NAE and observe how it behaves differently. As a model scenario, we consider a setting where digit 0-8 in MNIST are the inlier class and MNIST 9 is the outlier class. To run multiple experiments, we shorten the number of NAE epochs to 20 for these experiments.

The Effect of Pre-training We alter the number of training epochs in pre-training and observe how AUC of detection changes. The results are shown in Table 6. Training as NAE is beneficial for the outlier detection, since AUC scores always increase after NAE training. The gain from the pre-training starts to saturate after a certain number (50 in Table 6) of epochs, and the resulting performance remains within a certain range. Therefore, significant performance boost can be obtained with the limited amount of pre-training.

The Effect of Sampling Parameters We mainly investigate the effect of three components: latent LMC chain, sample replay buffer, and spherical latent space. Table 7 shows different configurations experimented and their anomaly detection performance in AUC. Experiment No.1 represents the original NAE configuration used in the experiments in the main manuscript.

Figure 10. More samples from NAE trained on CelebA $64 \times 64$. While most of the samples are visually sensible, a few generation failures can be spotted. Improving the sample generation process will be able to eliminate such non-realistic images.
Table 6. The effect of pre-training as a conventional autoencoder. We vary the number of pre-training epochs and observe AUC scores before and after NAE training. Note that “AUC Before NAE” indicates the outlier detection performance as a conventional autoencoder.

| PRE-TRAINING EPOCHS | AUC BEFORE NAE | AUC AFTER NAE |
|---------------------|----------------|---------------|
| 0                   | .486           | .552          |
| 10                  | .581           | .754          |
| 50                  | .539           | .945          |
| 100                 | .532           | .937          |
| 150                 | .548           | .914          |
| 200                 | .537           | .919          |

Table 7. Experiments with sampling parameters.

| No. | Latent chain length | Using sample replay buffer | Using spherical latent space | AUC  |
|-----|---------------------|-----------------------------|-----------------------------|------|
| 1   | 10                  | Yes                         | Yes                         | .957 |
| 2   | 0                   | No                          | Yes                         | .839 |
| 3   | 50                  | Yes                         | Yes                         | .944 |
| 4   | 10                  | No                          | Yes                         | .936 |
| 5   | 50                  | No                          | Yes                         | .952 |
| 6   | 10                  | Yes                         | No                          | .662 |

- The use of latent chain is substantially beneficial, as shown from the comparison between No.1 and No.2.
- A longer latent chain is needed for a better result. Comparing No.2, No.4, and No.5, the performance increases monotonically with the chain length. Note that longer chain length requires proportionally longer time in training.
- The sample replay buffer helps to reduce the length of the latent chain required in training. We see that with the sample replay buffer, the latent chain with 10 steps (No.1) can achieve performance comparable to that of 50 latent chain steps (No.5). In other words, using sample replay buffer may reduce the training time up to five times without the loss of performance.
- The gain from a longer latent chain saturates. Especially when a sample replay buffer is used, a chain longer than a certain threshold does not improve the performance (No.1 & No.3).
- The use of spherical latent space is essential in achieving a good performance.

The Effect of $D_z$. One of the most critical hyperparameter in autoencoders is the size of the latent space. We vary $D_z$ from 2 to 256 and observe how the performance of detecting digit 9 varies accordingly. The result is shown in Table 8.

The performance of an autoencoder is very sensitive to the choice of $D_z$, achieving good performance only in the vicinity of $D_z = 8$. Meanwhile, NAE achieves better performance than NAE in a wider range of $D_z$, from 16 to 128. Therefore, NAE is more robust to the choice of $D_z$ than an autoencoder.

Table 8. The effect of the latent dimensionality $D_z$. The best performance from an autoencoder is underlined, and the performance of NAE better than the best performance of an autoencoder is marked as bold.

| $D_z$ | AE AUC | NAE AUC |
|-------|--------|---------|
| 2     | .626   | .591    |
| 4     | .748   | .550    |
| 8     | .825   | .723    |
| 16    | .614   | .911    |
| 32    | .525   | .926    |
| 64    | .506   | .884    |
| 128   | .546   | .830    |
| 256   | .556   | .732    |

C.2. Computational Properties of NAE

The inference step of NAE is as fast as that of a conventional autoencoder, requiring no more than a single forward pass. The Langevin Monte Carlo (LMC) is the most time consuming procedure in NAE training and sampling. A single draw of sample involves dozens of LMC transition steps, and each transition step requires multiple backward passes one of which is comparable to a single training step for an autoencoder. However, the number of transition step required is less than 100 per step, and it is feasible to run it on a modern hardware. Thanks to availability of the pre-training, NAE becomes a decent sampler as well as an outlier detector even after a few epochs, while the performance tends to gradually increase for a few dozens of epochs. A single epoch of NAE training on MNIST with Conv28 network takes 10 minutes using a single Tesla V100 GPU. A single epoch of NAE training on CIFAR-10 with Conv32 network takes 500 seconds.

C.3. Outlier Reconstruction

The outlier reconstruction is a phenomenon that an autoencoder unexpectedly succeeds in reconstructing an input even though it is located outside of the training distribution. In this section, we provide illustrative examples that show that outlier reconstruction is a consequence from the inductive biases of an autoencoder.

Multi-modal data When the training data distribution consists of multiple clusters, the outliers from the region between the clusters are likely to be reconstructed. Figure 11 depicts 2D synthetic data generated from a mixture of two disconnected uniform distributions and their reconstruction from autoencoders with one-dimensional latent space. The outliers (red crosses) from the middle of two clusters show reconstruction errors (the length of thin black lines) smaller
than some inliers (blue dots). (Tong et al., 2019) noted this type of outlier reconstruction and mentioned that outliers “close to the mean” of data or “in the convex hull” of data are likely to be reconstructed.

This phenomenon arises from the inductive bias of an autoencoder that its encoder and decoder are smooth mappings. The extreme case of this inductive bias can be found in linear principal component analysis (PCA). PCA, a linear counterpart of an autoencoder (Bourlard & Kamp, 1988), would reconstruct any outliers which reside on the principal axis. Note that this phenomenon is consistent with the objective function of an autoencoder and PCA, as the objective does not penalize the reconstruction of outliers.

Compositionality When there is a compositional structure in data, we can still observe a reconstructed outlier even if it lies outside of the convex hull of training data. The data are compositional if each datum can be broken down into smaller reusable components; For example, MNIST can be considered highly compositional, since a digit image can be decomposed into smaller sub-patterns, such as straight lines and curves. An outlier can be successfully reconstructed when composed of a subset of components existing in the training data.

HalfMNIST and ChimeraMNIST datasets (See Section D.1) are constructed to demonstrate the effect of compositionality in outlier reconstruction. Although these images are not in the convex hull of MNIST digits, they share components found in MNIST. As shown in Figure 1, an autoencoder trained on MNIST have no problem reconstructing them and achieves poor AUC scores in classifying HalfMNIST and ChimeraMNIST from MNIST (See Table 4).

It seems that an autoencoder learns to reconstruct each part of an image separately but is not able to judge whether the combination of the parts is valid as a whole. This compositional way of processing facilitates generalization of a model (Keysers et al., 2019), but the generalization of reconstruction in OOD inputs is not desirable for an autoencoder-based outlier detector.

D. Experimental Detail

Here, we present details on our experiments, including datasets, network architectures, and details regarding implementing NAE and baselines. A sample code is provided in the supplementary material. We will make the whole experiment codebase public.

D.1. Datasets

Here, we present the details on the datasets used in the experiments.

2D Synthetic Dataset We use a two-dimensional mixture of 8 Gaussians initially used in (Grathwohl et al., 2018). The means of 8 Gaussians are $[2\sqrt{2}, 0]^T$, $[0, 2\sqrt{2}]^T$, $[-2\sqrt{2}, 0]^T$, $[0, -2\sqrt{2}]^T$, $[2, 2]^T$, $[-2, 2]^T$, $[2, -2]^T$, $[-2, -2]^T$. All Gaussians are isotropic and have a covari-
ance matrix of $\frac{1}{2}I$.

**Image Dataset** Table 9 summarizes image datasets used in our experiment. Pixel values are de-quantized by adding uniform noise $u \sim U(0, 1)$ and then normalized to interval $[0, 1]$. For MNIST, FashionMNIST, SVHN, and CIFAR-10, we use the predefined test splits as the test sets and randomly select 10% from the train splits as validation set.

We use the non-background Omniglot dataset only during the test phase. Omniglot images are inverted in order to produce black background.

For CelebA, we used the official train-validation-test split. Each image in CelebA is center-cropped in $140 \times 140$ and then resized into $32 \times 32$ or $64 \times 64$ depending on the experiment. When MNIST and FashionMNIST are needed to be fed to a network trained on $32 \times 32$ images, an input is resized into $32 \times 32$. The training set of ImageNet32 (Oord et al., 2016) is the randomly selected 80% from the original train split, and the rest 20% are used as the validation set. We use the original validation split as the test set in our experiment.

ConstantGray dataset is a synthetic dataset with images all pixels of which have the same gray-scale value. An image in ConstantGray dataset is a $1 \times 28 \times 28$ or $3 \times 32 \times 32$ array filled with a single number drawn from the interval $[0, 1]$. As shown in our experiment, most of existing autoencoders tend to reconstruct an image from ConstantGray with significantly low reconstruction error. Similarly, generative models tend to assign a very high likelihood to an image from ConstantGray. A similar observation is provided in Serrà et al. (2020).

Noise dataset is created by randomly generating each pixel value from interval $[0, 1]$. Noise dataset is very difficult to reconstruct exactly. Classifying Noise dataset can be a sanity check for an outlier detection that it can detect very obvious outliers.

Two additional datasets synthesized from MNIST are used. HalfMNIST dataset is created by randomly replacing the upper or the lower half of an MNIST test image with zero pixels. An image in ChimeraMNIST dataset is constructed by randomly joining the upper and the lower part of two MNIST test images from different classes. We add six zero pixels in the middle as a padding. HalfMNIST and ChimeraMNIST images are clearly OOD from MNIST but partially shares local visual features.

**D.2. Network Architecture**

Several network architectures are used throughout the experiments, and the architectures are summarized in Table 10. We name the architectures as FCRes2, Conv28, Conv32, Conv32Big, and Conv64. The numbers indicate the dimensionality of an input or a spatial dimension of an input image. All networks do not have batch normalization, as batch normalization violates the assumption in EBM that the energy is a deterministic function of an input. Conv32 and Conv64 architectures are similar to ones used in Ghosh et al. (2020). The encoder of Conv32Big is the energy function used in Du & Mordatch (2019), and the decoder of Conv32big is the generator used in Miyato et al. (2018).

FCRes2 is used in 2D density estimation. Conv28 is used in the experiments with MNIST dataset. Conv32 is used in the experiments with CIFAR-10 dataset, and Conv32Big is used in the experiments with ImageNet 32×32 dataset. Conv64 is used in the experiments with CelebA 64×64.

We use the following notations to denote operations in networks.

- Conv2d(in, out, kernel, stride, padding): A 2D convolutional operation with bias.
- ConvT2d(in, out, kernel, stride, padding): A 2D transposed convolutional operation with bias.
- ReLU: A rectified linear unit activation function. $y = \max\{0, x\}$.
- LReLU: A leaky ReLU function with the negative slope of 0.2.
- Sigmoid: A sigmoid activation function. $y = \frac{1}{1 + \exp(-x)}$.
- MaxPool(kernel_size): A max-pooling operator with the window of kernel_size×kernel_size and the stride of kernel_size.
- Bilinear(scale_factor): A bilinear upscaling operation that upsamples an input array into an scale_factor times larger array.
- Nearest(scale_factor): A nearest upscaling operation which upsamples an input array into an scale_factor times larger array.
- FC(in, out): A fully-connected layer performing a linear mapping with a bias.
- FCRes(in, hidden, out): A residual block composed of two fully-connected layers.
  $F_1 = FC(in, hidden)$
  $F_2 = FC(hidden, out)$
  $y = x + F_2(ReLU(F_1(ReLU(x))))$
  for an input $x$ and an output $y$.
- Res(in, hidden, out): A convolutional residual block composed of two Conv2d layers. For an input $x$ and an
output $y$,

\[
F_1 = \text{Conv2d}(\text{in}, \text{hidden}, 3, 1, 1) \\
F_2 = \text{Conv2d}(\text{hidden}, \text{out}, 3, 1, 1) \\
y = x + F_2(\text{LReLU}(F_1(\text{LReLU}(x))))
\]

- **ResUp**(in, hidden, out, scale): A residual block with upsampling.

\[
F_1 = \text{Conv2d}(\text{in}, \text{hidden}, 3, 1, 1) \\
F_2 = \text{Conv2d}(\text{hidden}, \text{out}, 3, 1, 1) \\
U = \text{Nearest}(\text{scale}) \\
y = U(x) + F_2(\text{ReLU}(F_1(U(\text{ReLU}(x)))))
\]

- **ResAtt**(in, hidden, out): A residual attention block which has two residual blocks $R_1 = \text{Res}(\text{in}, \text{hidden}, \text{out})$ and $R_2 = \text{Res}(\text{in}, \text{hidden}, \text{out})$ and operates as $y = x + R_1(x) \odot \text{Sigmoid}(R_2(x))$, where $\odot$ denotes an element-wise product.

### D.3. NAE Implementation

The procedure for generating a negative sample in NAE is described in Algorithm 1.

#### Sampling Parameters and Techniques

The most important hyperparameter in NAE is the parameters related to MCMC sampling. Detailed MCMC parameters can be found in Table 11.

Note that the step size parameters and the noise parameters in 2D setting follows the theoretically motivated relationship $2\lambda = \sigma^2$. For the rest of the cases, $2\lambda \neq \sigma^2$, meaning that the effective temperatures are implicitly fixed to values different from 1. In all experiments, we set $T = T_z$, i.e., the temperature of the latent chain is tied to the temperature of NAE. In 2D dataset experiments, the temperature is tuned with gradient descent. For faster convergence, in updating $T$, we use a learning rate 100 times larger than that used to update the model parameters.

Following Du & Mordatch (2019), we clip the gradient $\nabla_x \log E_\theta(x)$ is clipped at 0.01.

We use the sample replay buffer with the buffer size of 10,000 and the replay ratio of 95% as described in Du & Mordatch (2019). A starting point of a latent chain is drawn from the noise distribution $q_0(z)$ with the probability of 5% or randomly drawn from the replay buffer with the probability of 95%.

The choice of a noise distribution $q_0(z)$ is dependent on the configuration of the latent space. For $\mathbb{R}^{D_x}$, $q_0(z)$ is a standard normal distribution. For $S_{D_x-1}$, a uniform distribution is used. Samples from a uniform distribution on $S_{D_x-1}$ is generated by first draw samples from a standard normal distribution in $\mathbb{R}^{D_x}$, then project them onto $S_{D_x-1}$ by dividing with its norm.

$\sigma_{\epsilon}$ annealing in Table 11 indicates that during MCMC in $X$, we let the standard deviation of $\epsilon_{\epsilon}$ decay as the visible chain proceeds: $\text{std}(\epsilon_{\epsilon}) = 0.05/(1 + \text{step})$ for step $= 0, \cdots, s$ with $s$ as the number of steps in $X$. This contributes to obtaining finer samples.

For generating new samples, a longer latent chain is used instead of a sample replay buffer. In our experiments, we let a latent chain be 8 times longer than the chain used in training.

#### Learning of NAE

NAE is trained using Adam optimizer (Kingma & Ba, 2014) with the learning rate of $1 \times 10^{-5}$ for 50 epochs. When using the reconstruction error as the energy function, we divide the reconstruction error by the probability of 95%. This keeps the energy in a reasonable scale and facilitates hyperparameter setting.

Autoencoder pre-training is not used in 2D experiments but is conducted for 100 epochs for MNIST and 120 epochs for CIFAR-10.

The encoders and the decoders in NAE are regularized as follows:

- **FCRes2**: No regularization;

### Table 9. Summary of dataset statistics.

| Dataset                  | Original Shape | Training | Validation | Test  |
|--------------------------|----------------|----------|------------|-------|
| Constant (Synthetic)     | -              | -        | 4,000      | 4,000 |
| MNIST                    | $1 \times 28 \times 28$ | 54,000    | 6,000      | 10,000 |
| FashionMNIST             | $1 \times 28 \times 28$ | 54,000    | 6,000      | 10,000 |
| Omniglot                 | $1 \times 28 \times 28$ | -        | -          | 13,180 |
| SVHN                     | $3 \times 32 \times 32$ | 65,930    | 7,327      | 20,632 |
| CIFAR-10                 | $3 \times 32 \times 32$ | 45,000    | 5,000      | 10,000 |
| CelebA                   | $3 \times 178 \times 218$ | 162,079   | 20,260     | 20,260 |
| ImageNet32               | $3 \times 32 \times 32$ | 1,024,919 | 256,229    | 49,999 |
| Noise (Synthetic)        | $3 \times 32 \times 32$ | -        | 4,000      | 4,000 |
| HalfMNIST (Synthetic)    | $1 \times 28 \times 28$ | -        | -          | 10,000 |
| ChimeraMNIST (Synthetic) | $1 \times 28 \times 28$ | -        | -          | 10,000 |
**Table 10. Network architectures for autoencoders.**

| Encoder | Conv28 ($D_{\kappa}=1\times28\times28$) | Conv32 ($D_{\kappa}=3\times32\times32$) |
|---------|----------------------------------------|--------------------------------------|
| FC(2, 256)- | Conv2d(3, 128, 3, 1, 1)-ReLU- | Conv2d(3, 32, 4, 1, 0)-ReLU- |
| FCRes(256, 128)- | Conv2d(64, 128, 3, 1, 1)-ReLU- | Conv2d(64, 64, 4, 2, 0)-ReLU- |
| FCRes(256, 128)- | Conv2d(256, 256, 128, 3, 1, 0)-ReLU- | Conv2d(256, 256, 128, 4, 2, 0)-ReLU- |
| FCRes(256, 128)- | FC(1024, $D_{\kappa}$) | Conv2d(1024, $D_{\kappa}$) |
| Conv2d(3, 32, 4, 2)-ReLU- | | |
| Conv2d(128, 32, 4, 2)-ReLU- | | |
| Conv2d(256, 32, 4, 2)-ReLU- | | |
| Conv2d(512, 64, 4, 2)-ReLU- | | |
| Conv2d(1024, 16, 4, 2)-ReLU- | | |

| Decoder | Conv32Big ($D_{\kappa}=3\times32\times32$) | Conv64 ($D_{\kappa}=3\times64\times64$) |
|---------|----------------------------------------|--------------------------------------|
| FC(256, 2) | Conv2d(128, 32, 4, 1)-ReLU- | Conv2d(128, 3, 3, 1, 0)-Sigmoid |
| Conv2d(128, 64, 4, 2)-ReLU- | Conv2d(128, 64, 4, 2)-ReLU- |
| Conv2d(256, 64, 4, 2)-ReLU- | Conv2d(256, 64, 4, 2)-ReLU- |
| Conv2d(128, 32, 4, 2)-ReLU- | Conv2d(128, 32, 4, 2)-ReLU- |
| Conv2d(256, 32, 4, 2)-ReLU- | Conv2d(256, 32, 4, 2)-ReLU- |
| Conv2d(128, 24, 4, 2)-ReLU- | Conv2d(128, 24, 4, 2)-ReLU- |
| Conv2d(256, 16, 4, 2)-ReLU- | Conv2d(256, 16, 4, 2)-ReLU- |

- Conv28: L2 norm of the encoder’s weights with the coefficient 0.0001;
- Conv32: L2 norm of the encoder’s weights with the coefficient 0.0001;
- Conv32Big: Spectral normalization (Miyato et al., 2018) (encoder) and group normalization (Wu & He, 2018) with 8 groups (decoder);
- Conv64: group normalization with 8 groups (encoder & decoder).

**D.4. Baseline Implementation**

In all autoencoder-based methods, i.e., NAE, AE, DAE, WAE, VAE, DAGMM, VQVAE and Ganomaly, we ensure that they all use the same network architecture.

The optimal $D_{\kappa}$ is searched among {2, 4, 8, 16, 32, 64, 128, 256}. The best parameter is selected according to AUC of classifying a separate OOD dataset, as described in the main manuscript.

PixelCNN++ (Salimans et al., 2017) is implemented based on an open-source code base\(^3\). We use set parameters as

\[
nr\_resnet=5 \text{ and } nr\_filters=80. \quad \text{Input values are scales to } [-1, 1] \text{ only when running PixelCNN++}.\]

Glow (Kingma & Dhariwal, 2018) is also implemented based on the open-source repository\(^4\). We set $K = 12$, $L = 1$, $\text{hidden\_channels} = 64$.

We failed to obtain sensible result using GPND (Pidhorskyi et al., 2018)\(^5\).

DAGMM (Zong et al., 2018) is implemented based on the public repository\(^6\). We failed to train it on CIFAR-10 such that it produces AUC of 1.0 for Noise dataset, and therefore we exclude the result from the Table 2 of the main manuscript.

WAE-MMD is implemented. We use median heuristic to determine the kernel parameter of RBF kernel. Regularization coefficient is searched between 0.001 and 0.1

For DAE, we use Gaussian noise with standard deviation of

\[
\text{pixel-cnn-pp} \quad \text{https://github.com/pclucas14/}
\]

\[
\text{glow-pytorch} \quad \text{https://github.com/chaiyujin/glownn}
\]

\[
\text{GPND} \quad \text{https://github.com/podgorskiy/GPND}
\]

\[
\text{dagmm} \quad \text{https://github.com/danieltan07/dagmm}
\]
Table 11. Sampling parameters for NAE. See Section D.3 for description.

|                      | 2D      | MNIST   | CIFAR-10 | CELEBA |
|----------------------|---------|---------|----------|--------|
| LATENT SPACE         | $\mathbb{R}^{D_x}$ | $\mathbb{R}^{D_x-1}$ | $\mathbb{R}^{D_x-1}$ | $\mathbb{R}^{D_x-1}$ |
| STEP SIZE $\lambda_z$ | 0.005   | 0.2     | 1        | 1      |
| NOISE $\sigma_z$    | 0.1     | 0.05    | 0.02     | 0.02   |
| LATENT CHAIN LENGTH $\tau_z$ | 10      | 10      | 20       | 20     |
| REPLAY BUFFER FOR LATENT CHAIN | O      | O     | O        | O      |
| STEP SIZE $\lambda_x$ | 0.005   | 10     | 10       | 10     |
| NOISE $\sigma_x$    | 0.1     | 0.05    | 0.02     | 0.02   |
| MAIN CHAIN LENGTH $\tau_x$ | 30     | 50     | 40       | 40     |
| $\sigma_x$ ANNEALING | X      | O      | O        | O      |
| GRADIENT CLIPPING IN $\mathcal{X}$ | X     | O      | O        | O      |
| TEMPERATURE $T = T_z$ | 0.5, TRAINABLE | 1, FIXED | 1, FIXED | 1, FIXED |
| MH REJECTION         | O       | X      | X        | X      |

Algorithm 1 Negative sample generation using OMI

**Input:** Sample replay buffer $B$, noise distribution $q_0(z)$, latent energy $H_\theta(z)$, NAE energy $E_\theta(z)$, decoder $f_d(z)$

- Latent chain parameters $\sigma_z$, $\lambda_z$, $\tau_z$
- Main chain parameters $\sigma_x$, $\lambda_x$, $\tau_x$

// Initialization
Draw $u$ from $Uniform(0, 1)$.

if $u < 0.95$ then
  Draw $z_0$ from $B$
else
  Draw $z_0$ from $q_0(z)$
end if

// Latent chain
for $t = 0$ to $\tau_z$ do
  $z_t = -\lambda_z \nabla H_\theta(z_{t-1}) + \sigma_z \epsilon$, $\epsilon \sim \mathcal{N}(0_z, I_z)$
  // Project $z_t$ to $\mathbb{S}^{D_z-1}$ if needed
end for
Append $z_{\tau_z}$ to $B$

$x_0 = f_d(z_{\tau_z})$ // On-manifold initialization

// Main chain
for $t = 0$ to $\tau_x$ do
  $x_t = -\lambda_x \nabla E_\theta(x_{t-1}) + \sigma_x \epsilon$, $\epsilon \sim \mathcal{N}(0_x, I_x)$
  // Metropolis-Hastings rejection step if needed
  // Anneal $\sigma_x$ if needed
end for

return $x_{\tau_x}$ // Negative sample

0.3.

We implement VQVAE based on the PyTorch version\(^7\). In the reproduction of Ganomaly, we use the official implementation from the authors\(^8\).

---

\(^7\)https://github.com/ritheshkumar95/pytorch-vqvae

\(^8\)https://github.com/samet-akcay/ganomaly