GENERATIVE CLASS-CONDITIONAL DENOISING AUTOENCODERS

Jan Rudy & Graham Taylor
School of Engineering
University of Guelph
Guelph, Ontario, Canada
{jrudy, gwtaylor}@uoguelph.ca

ABSTRACT

Recent work by [Bengio et al., 2013] proposes a sampling procedure for denoising autoencoders which involves learning the transition operator of a Markov chain. The transition operator is typically unimodal, which limits its capacity to model complex data. In order to perform efficient sampling from conditional distributions, we extend this work, both theoretically and algorithmically, to gated autoencoders (Memisevic, 2013). The proposed model is able to generate convincing class-conditional samples when trained on both the MNIST and TFD datasets.

1 INTRODUCTION

In the field of deep neural networks, purely supervised models trained on massive labeled datasets have garnered much attention over the last few years [Dahl et al., 2010; Deng et al., 2010; Krizhevsky et al., 2012; Goodfellow et al., 2014b; Szegedy et al., 2014]. However, recent work has rekindled interest in generative models of data [Bengio et al., 2013; Bengio & Thibodeau-Laufer, 2013; Kingma & Welling, 2014; Goodfellow et al., 2014a]. The recently proposed sampling procedure for denoising autoencoders [Bengio et al., 2013] and their generalization to Generative Stochastic Networks [Bengio & Thibodeau-Laufer, 2013] presents a novel training procedure which, instead of attempting to maximize the likelihood of the data under the model, amounts to learning a transition operator of a Markov chain [Bengio et al., 2013].

Although these models have shown both theoretically and empirically to have the capacity to model the underlying data generating distribution, the unimodal transition operator learned in [Bengio et al., 2013] and [Bengio & Thibodeau-Laufer, 2013] limits the types of distributions that can be modeled successfully. One way to address this issue is by adopting an alternative generative model such as the Neural Autoregressive Density Estimator (NADE) as the output distribution of the transition operator [Ozair et al., 2013]. In this paper, we propose a simpler approach. When labeled data is available, we can use the label information in order to carve up the landscape of the data distribution.

This work begins by presenting an overview of related work, including a treatment of autoencoders, denoising autoencoders, autoencoders as generative models and gated autoencoders. Next, we propose a class-conditional gated autoencoder along with training and sampling procedures based on the work of [Bengio et al., 2013]. Finally, we present experimental results of our model on two image-based datasets.

2 RELATED WORK

2.1 AUTOENCODERS

An autoencoder is a feed-forward neural network which aims to minimize the reconstruction error of an input data vector via a latent representation. This can be interpreted as the composition of two learned functions, the encoder function $f$ and the decoder function $g$. The encoder function $f$ is a mapping from input space onto the representation space. Formally, given input vector $x \in \mathbb{R}^{n \times x}$,
input weights $W \in \mathbb{R}^{n_H \times n_X}$ and hidden biases $b_h \in \mathbb{R}^{n_H}$,

$$f(x) = s_H(Wx + b)$$

(1)

where $n_H$ is the dimension of the hidden representation and $s_H$ is an activation function. The activation is a non-linear function, often from the sigmoidal family (e.g. the logistic or hyperbolic tangent functions) or a piecewise linear function (e.g. rectified linear). The decoder then projects this representation $h = f(x)$ back onto the input space,

$$\hat{x} = g(h) = s_O(W'h + b')$$

(2)

where $\hat{x}$ is the reconstruction of the input vector, $s_O$ is the output activation function, $W' \in \mathbb{R}^{n_X \times n_H}$ are the output weights and $b' \in \mathbb{R}^{n_X}$ are the output biases. In order to restrict the number of free parameters of the model, the input and output weight matrices are often ‘tied’ such that $W' = W^T$.

The model parameters (i.e. weights and biases) are updated via a gradient-based optimization in order to minimize a loss function $L(x)$ based on reconstruction error. The choice of loss function depends on the data domain. When dimensions of $x$ are real-valued, a typical choice of $L(x)$ is the squared error, i.e. $L(x) = \sum_{i=1}^{n_X} (x_i - \hat{x}_i)^2$. When $x$ is binary, a more appropriate loss function is the cross-entropy loss, i.e. $L(x) = \sum_{i=1}^{n_X} x_i \log \hat{x}_i + (1 - x_i) \log(1 - \hat{x}_i)$.

### 2.2 Denoising Autoencoders

When the dimension of the hidden representation $n_H$ is smaller than the dimension of the data space $n_X$, the learning procedure encourages the model to learn the underlying structure of the data. The data representation can exploit structure in order to compress the data to fewer dimensions than the original space. As such, each dimension of the representation space is interpretable as a useful feature of the data. For example, when trained on images of handwritten digits these features are interpretable as strokes.

However, when $n_H \geq n_X$, the autoencoder can achieve perfect reconstruction without learning useful features in the data by simply learning the identity function. In this so-called “overcomplete” setup, regularization is essential. Among the various kinds of regularized autoencoders, the denoising autoencoder (DAE) \cite{Vincent2008} is among the most popular and well-understood. Instead of reconstructing the data from the actual input vector $x$, the DAE attempts to reconstruct the original input from an encoding of a corrupted version, $f(\tilde{x})$. This effectively prohibits the model from learning a trivial solution while learning robust features of the data.

The corruption procedure is defined as a sample from the conditional distribution $\tilde{x} \sim C(\tilde{x}|x)$. Here, $\tilde{x}$ is a noisy version of $x$ where the type of noise is defined by the distribution $C(\tilde{x}|x)$. Typical choices of noise are

1. Gaussian noise - adding $\epsilon_i \sim N(0, \sigma)$ to each dimension.
2. Masking noise - setting $x_i = 0$ with probability $\rho$.
3. Salt-and-pepper noise - similar to masking noise, but corrupting $x_i$ with probability $\rho$ and each corrupted dimension is set to $x_i = 0$ or $x_i = 1$ with probability 0.5.

Apart from preventing the model to learn a trivial representation of the input by acting as a form or regularization, the DAE can be interpreted as a means of learning the manifold of the underlying data generating distribution \cite{Vincent2008}. Under the assumption that the data lies along a low dimensional manifold in the input space, the corruption procedure is a means of moving the training data away from this manifold. In order to successfully denoise the corrupted input, the model must learn to project the corrupted input back onto the manifold. Under this interpretation the hidden representation can be interpreted as a coordinate system of manifolds \cite{Vincent2008}.

### 2.3 Denoising Autoencoders as Generative Models

Although DAEs are useful as a means of pre-training discriminative models, especially when stacked to form deep models \cite{Vincent2010}, recent work by \cite{Bengio2013} has shown that DAEs
and their variants locally characterize the data generating density. This provides an important link between DAEs and probabilistic generative models.

We define observed data \( x \) such that \( x \sim P(x) \) where \( P(x) \) is the true data distribution and we define \( C(\tilde{x} | x) \) as the conditional distribution of the corruption process. When such models are trained using a loss function that can be interpreted as log-likelihood, by predicting \( x \) given \( \tilde{x} \), the model is learning the conditional distribution \( P_\theta(x | \tilde{x}) \) (where \( \theta \) represents the parameters of the model).

In order to generate samples from the model, one simply forms a Markov chain which alternately samples from learned distribution and the corruption distribution (Bengio et al., 2013). Where \( x_t \) is the state of the Markov chain at time \( t \), then \( x_t \sim P_\theta(x | \tilde{x}_{t-1}) \) and \( \tilde{x}_t \sim C(x | \tilde{x}_t) \). In other words, samples can be generated by alternating between the corruption process and the denoising function learned by the autoencoder.

Notice that this is not a true Gibbs sampling procedure, as \((x_t, \tilde{x}_{t-1})\) may not share the same asymptotic distribution as \((x_t, \tilde{x}_t)\). Regardless, theoretical results indicate that under some conditions elaborated on in Sec. 3 the asymptotic distribution of the generated samples converges to the data-generating distribution (Bengio et al., 2013).

Although the above procedure does produce convincing samples, it will also generate spurious examples that lie far from any training data. This is because the training procedure does not sufficiently explore the input space. Under the manifold interpretation described above, the corruption procedure defines a region around each example that is explored during training, the size of which is determined by the amount of the corruption (e.g. \( \sigma \) in the case of Gaussian noise and \( \rho \) for masking or salt and pepper noise). This can leave much of the input space unexplored, allowing the model to place non-insignificant amounts of probability mass (i.e. spurious modes) in regions of the space that lie far from any training example.

One solution involves using large or increasing amounts of noise during training, however this results in a naive search of the space. A more efficient procedure called “walkback training” is described in (Bengio et al., 2013) and bears resemblance to contrastive divergence training of restricted Boltzmann machines. Instead of defining the loss as the reconstruction cost of a single step of corruption and reconstruction chain, walkback training defines a series of \( k \) reconstructions via a random walk originating at the training example. Each reconstruction is corrupted and subsequently reconstructed, where the final cost is defined as the sum of the reconstruction costs of each intermediate reconstruction. Since the training procedure mimics that of the sampling procedure, walkback training is a means of seeking out these spurious modes and redistributing their probability mass back towards the manifold.

### 2.4 GATED AUTOENCODERS

Gated autoencoders (GAEs), also called Relational autoencoders, are an extension of the autoencoder framework which learn relations on input-output pairs \( x \in \mathbb{R}^{n_x} \) given \( y \in \mathbb{R}^{n_y} \) (Memisevic, 2013). Instead of defining a fixed weight matrix \( W \in \mathbb{R}^{n_H \times n_x \times n_y} \), the GAE learns a function \( w(y) \) where the model weights are modulated by the value of the conditioning variable \( y \).

The naive implementation involves constructing a weight tensor \( W \in \mathbb{R}^{n_H \times n_x \times n_y \times n_x} \) and defining

\[
w_{ij}(y) = \sum_{k=1}^{n_y} W_{ijk} y_k
\]

where the subscripts indicate indexing. Under this model, the encoder in Equation 1 becomes

\[
\mathbf{h} = f(x, y) = s_H(w(y)x + \mathbf{b})
\]

However, this requires storing and learning \((n_X \times n_Y \times n_H)\) model parameters. In practice, this is infeasible for all but the smallest problems as the number of weights is cubic in the number of units (assuming \( n_X, n_Y \), and \( n_H \) are roughly equal). However, we can restrict the interactions between \( x, y, \) and \( h \) by first projecting each onto factors \( F^X, F^Y, F^H \in \mathbb{R}^{n_F} \) and allowing only element-wise interaction between the factors. Instead of a quadratic number of weights needed in the naive method above, the factored model is parameterized via three weight matrices: \( W^X \in \)
The hidden representation under the factored model is defined as
\[
  h = f(x, y) = s_H \left( (W^H)^T (W^X x \otimes W^Y y) + b^H \right) \tag{5}
\]
where \( \otimes \) denotes elementwise multiplication and \( b^H \in \mathbb{R}^{n_H} \) is the hidden bias. Notice that the encoder is a function over both \( x \) and \( y \). Similarly, the decoder function will also be over two input variables, the choice of which being dependant on which of \( x \) and \( y \) are to be reconstructed. When learning a conditional model, one of the input variables will be held fixed. For example, the reconstruction of \( x \) given \( y \) is defined as
\[
  \hat{x} = g(h, y) = s_O \left( (W^X)^T (W^H h \otimes W^Y y) + b^X \right) \tag{6}
\]
where \( b^H \in \mathbb{R}^{n_X} \) is the output bias and \( s_O \) is the output activation function. Equations (5) and (6) describe a symmetric model where the encoder and decoder share the same set of weight matrices. However, this is not a hard requirement and various regimes of tied vs untied weights for gated models have been explored by Alain & Olivier (2013).

Like the traditional autoencoder, the GAE is typically trained with a denoising criterion where the noise is applied to both \( x \) and \( y \) inputs. Yet where a traditional autoencoder learns features of the input, a GAE can learn relationships between its two inputs. For example, when trained on pairs of images where one is a translated version of the other, the filters learned by the input factors resemble phase-shifted Fourier components (Memisevic, 2013).

The loss function is defined in much the same way as the classical autoencoder described above, using squared error on real-valued inputs and cross entropy loss where the input values are binary. As all operations are differentiable, the model can be trained via stochastic gradient descent while making use of any optimization techniques (e.g. momentum, adaptive learning rates, RMSprop, etc.) that have been developed for neural network training.

### 3 Gated Autoencoders as Class-Conditional Generative Models

The sampling procedure proposed by Bengio et al. (2013) for classical denoising autoencoders can also be applied to a GAE. Here, we define the true data distribution as the conditional distribution
\( P(\mathbf{x}|\mathbf{y}) \). Here \( \mathbf{x} \in \mathbb{R}^n \) is an input data point and \( \mathbf{y} \in \mathbb{R}^m \) is the associated class label in a ‘one-hot’ encoding. Although GAE training typically applies noise to both \( \mathbf{x} \) and \( \mathbf{y} \), we will examine the case where the corruption procedure is applied to \( \mathbf{x} \) only. Thus, the corruption distribution is the same as in the DAE framework, namely the noise procedure draws samples from \( C(\tilde{\mathbf{x}}|\mathbf{x}) \). By choosing a loss function which is interpretable as log-likelihood, the GAE learns the conditional distribution \( P_\theta(\mathbf{x}|	ilde{\mathbf{x}}, \mathbf{y}) \)

Like the sampling procedure for DAEs, the Markov chain formed by alternating samples from \( \mathbf{x}_t \sim P_\theta(\mathbf{x}|	ilde{\mathbf{x}}_{t-1}, \mathbf{y}) \) and \( \tilde{\mathbf{x}}_t \sim C(\tilde{\mathbf{x}}|\mathbf{x}) \) will generate samples from the true distribution \( P(\mathbf{x}|\mathbf{y}) \). During training, we can also apply a class-conditional version of the walkback training algorithm to seek out and squash any spurious modes of our model.

Bengio et al. (2013) provide a proof of the following theorem:

**Theorem 1.** If \( P_\theta(\mathbf{x}|	ilde{\mathbf{x}}) \) is a consistent estimator of the true conditional distribution \( P(\mathbf{x}|\tilde{\mathbf{x}}) \) and \( T_n \) defines an ergodic Markov chain, then as the number of examples \( n \to \infty \), the asymptotic distribution \( \pi_n(\mathbf{x}) \) of the generated samples converges to the data-generating distribution \( P(\mathbf{x}) \).

For the conditional case of GAE the same arguments hold, where each of the following substitutions are made: \( P_\theta(\mathbf{x}|	ilde{\mathbf{x}}) \) with \( P_\theta(\mathbf{x}|	ilde{\mathbf{x}}, \mathbf{y}) \), \( P(\mathbf{x}|	ilde{\mathbf{x}}) \) with \( P(\mathbf{x}|	ilde{\mathbf{x}}, \mathbf{y}) \) and \( P(\mathbf{x}) \) with \( P(\mathbf{x}|\mathbf{y}) \). The arguments for consistency and ergoticity can also be made in the same manner as those in (Bengio et al., 2013).

Geometrically, this model can be seen as learning a conditional manifold of the data. Like the DAE, the model learns to correct the noisy input by pushing it back towards the data manifold. However, the model makes use of the class labels in order to learn a separate manifold for each class label. The \( F^Y \) factors, via their multiplicative interactions, scale the features learned by the \( F^X \) factors depending on the class. It is akin to learning a DAE for each class, yet the gated model can make use of cross-class structure by sharing weights between each of the class-specific models.

When training on images of hand written digits, for example, the ‘tail’ of a 4, 7, or 9 may all make use of the same feature learned by one of the \( F^X \) factors. As such, the \( F^Y \) factor for these classes would have a relatively large value for this shared feature. However, this tail feature may not be useful for reconstruction of a 3, 8 or 6. For these classes, the \( F^Y \) values that correspond to the tail feature can learn to down-weight the importance of this tail feature. Under this interpretation, the \( F^Y \) factors are a means of weighting each of the \( F^X \) factors dependent on the conditioning class label.

### 4 Experiments

We demonstrate the generative properties of the class-conditional GAE model on two datasets: binarized MNIST (LeCun & Cortes, 1998) and the Toronto Face Database (TFD) (Susskind et al., 2010). The MNIST database of handwritten digits consists of 60,000 training examples and 10,000 test examples. Pixel intensities of each \( 28 \times 28 \) image have been scaled to \([0, 1]\) and thresholded at 0.5, such that each pixel takes on a binary value from \([0, 1]\). For the MNIST dataset, a GAE was trained with 1024 factors and 512 hidden units. The hidden units used a rectified linear (ReLU) activation function, while the visible activation was the logistic (i.e. sigmoid) function. Using a cross entropy loss, the model was trained for 200 epochs via mini-batch gradient descent with a batch size of 100. The initial learning rate of 0.25 was decreased multiplicatively at each epoch by a factor of 0.9995. For optimization, the model was trained using Nesterov’s accelerated gradient (Sutskever et al., 2013) with a parameter of 0.9. Salt and pepper noise was applied during training where each pixel has a 0.5 probability of corruption. Training followed the walkback training procedure, with the training loss averaged over 5 reconstructions from the Markov chain starting at the training example.

Figure 2 shows 250 consecutive samples generated while conditioning on each class label. Note that the ‘samples’ depicted show the expected value of each pixel for each step of the Markov chain defined by the sampling procedure. Each chain was initialized to a vector of zeros and at each step, the image was corrupted with 0.5 salt-and-pepper noise. The model begins to generate convincing samples after only a few steps of the chain. Also notice that the chain exhibits mixing between modes in the data distribution. For example, the samples from the ‘2’ class contains both twos with
Figure 2: Consecutive samples generated by the Markov chain learned by the class-conditional GAE model trained on binarized MNIST.

a loop and a cusp. Finally, notice that the samples contain very few spurious examples – i.e. most samples resemble recognizable digits.

The TFD consists of 4,178 expression-labeled images of human faces. Each image is 48 \times 48 pixels with 256 integer value levels of gray intensity. The intensity values were linearly scaled to the range [0, 1]. Unlike the MNIST experiment, the intensity values were not binarized.

A GAE with 512 factors and 1024 ReLU hidden units and sigmoid outputs was trained on squared-error loss for 500 epochs. Again, we used mini-batch gradient descent, however, a mini-batch size of 50 was used with a learning rate of 1.0 annealed by a factor of 0.995 at each epoch. Training followed 5 walkback steps with a Nesterov momentum of 0.9. The model was trained and sampled using salt-and-pepper noise with probability of 0.5.

When training on MNIST, each walkback reconstruction was then sampled using the sigmoid activation as the probabilities of a factorized Bernoulli distribution. Since the TFD faces were not binarized, the sigmoid activations were used instead. Figure [3] shows 150 consecutive samples for each class label, each starting at the zero vector.
Figure 3: Consecutive samples generated by the Markov chain learned by the class-conditional GAE model trained on TFD images. From left to right, top to bottom, the classes are: anger, disgust, fear, happiness, sadness, surprise, neutral.

Notice that there is less variation in the TFD samples than those from the MNIST model. This is likely due to the relative small size of the TFD training set (4,178 TFD training cases vs. 60,000 MNIST training cases). The TFD dataset also provides 112,234 unlabeled examples and it may be possible to pretrain the $F^X$ factor weights on this unlabeled data. However, these experiments are beyond the scope of the current analysis.
5 CONCLUSION

The class-conditional GAE can be interpreted as a generative model in much the same ways as the DAE. In fact, the GAE is akin to learning a separate DAE model for each class, but with significant weight sharing between the models. In this light, the gating acts as a means of modulating the model’s weights depending on the class label. As such, the theoretical and practical consideration that have been applied to DAE’s as generative models can also be applied to gated models. Future work will apply these techniques to richer conditional distributions, such as the task of image tagging as explored by Mirza & Osindero (2014).

REFERENCES


