Geometric instability of out of distribution data across autoencoder architecture

Susama Agarwala¹, Benjamin Dees², and Corey Lowman¹

¹Johns Hopkins University Applied Physics Lab
²Johns Hopkins University, Mathematics Department

Abstract—We study the map learned by a family of autoencoders trained on MNIST, and evaluated on ten different data sets created by the random selection of pixel values according to ten different distributions. Specifically, we study the eigenvalues of the Jacobians defined by the weight matrices of the autoencoder at each training and evaluation point. For high enough latent dimension, we find that each autoencoder reconstructs all the evaluation data sets as similar generalized characters, but that this reconstructed generalized character changes across autoencoder. Eigenvalue analysis shows that even when the reconstructed image appears to be an MNIST character for all out of distribution data sets, not all have latent representations that are close to the latent representation of MNIST characters. All told, the eigenvalue analysis demonstrated a great deal of geometric instability of the autoencoder both as a function on out of distribution inputs, and across architectures on the same set of inputs.

The distributions of training, test and validation data is often different than the distribution of the data on which a neural network is deployed. This problem of distribution shift causes neural networks to fail silently, with potentially serious consequences [1], [2]. The research community has tried to address this in many ways with different levels of success. For instance, generative models [3], [4] effectively learn the distributions of the probability distribution of the training data set, but they do not address the fact that one has little control over the deployment data distribution. To address this problem, the research community has come up with a wide family of out-of-distribution detection algorithms [5], [6], [7], [8], with a variety of strengths and weaknesses.

However, to our knowledge, there has not been any concerted effort to understand the geometric properties of the feature map that transforms inputs to a latent representation. While this map is trained on the training, test and validation data distributions, it is a function on a much larger space of possible inputs. In this paper, we consider an autoencoder as a function from input to reconstruction space, such that one can consider its Jacobian matrix at any input point. The eigenvalues and eigenvectors of these Jacobians contain a wealth of information about the geometric properties of the feature map. In [9], the authors studied the geometry of this function on the training data set (MNIST). In this paper, we consider the geometry on points very far out of distribution (specifically, on 10 data sets where pixel brightness is drawn from 10 different distributions).

As autoencoders are supposed to be a method for learning the manifold structure of a data set, they are frequently used as means of out of distribution detection [10], [11]. However, this method of out of distribution detection fails due to the well documented phenomenon of out of distribution reconstruction [3], [12], [13], [14]. We consider the geometric stability of the learned feature map on points so far from the training data set that out of distribution reconstruction is not a worry, and characterize how these geometric properties are different from those on the training set. We believe this line of inquiry will lead to a foundational understanding of what an autoencoder is learning about the geometry of the data manifold as well as the relation to the input space, and lead to a new set of geometric tools for out of distribution detection.

Concretely, we evaluate a family of autoencoders with identical architecture except for the dimension of the latent space for various seeds. Then we evaluate 10 data sets, each with pixel values drawn from a different random distribution on these trained networks. We find that on data sets far out of distribution, at low latent dimension, the reconstruction often appears to be a reconstructed image (under visual inspection) from the training data set. However, the autoencoder will map any given random distribution of pixels to a variety of different training images, and this set will change from seed to seed. Surprisingly, however, the geometric data suggests that even though the reconstruction images appear to be close to the reconstructed images of the training data set, the latent representation of the training data and the out
of distribution data is quite different. Furthermore, we find that for higher latent dimensions, the autoencoder consistently maps each random pixel distribution data set to the same class of generalized character, but that this character is both seed and architecture dependent. We find that the geometries of the learned feature functions cluster by mean value of the pixel distribution. More surprisingly, we learn that for higher latent dimension, the trained autoencoder is not aware of the orientation of the bases of the input space.

I. AUTOENCODERS AND LEARNED GEOMETRY

An autoencoder consists of a pair of neural networks trained in tandem, an encoder that maps points from a high dimensional input space, \( I \), to a lower dimensional latent space \( L \simeq \mathbb{R}^d \), and a decoder that maps the points in the latent space back to a high dimensional reconstruction space (isomorphic to the input space), \( R \simeq \mathbb{R}^N \), with \( d \ll N \). Let \( f_{enc} \) indicate the encoder network, and \( f_{dec} \) the decoder. For any input point \( x \in I \), let \( y = f_{dec} \circ f_{enc}(x) \in R \) be the reconstructed point and \( z = f_{enc}(x) \in L \) the latent representation of said point. By construction, the image of the autoencoder \( f_{dec} \circ f_{enc} : I \rightarrow R \) is at most a \( d \) dimensional subspace of \( R \). For the purposes of this paper, the autoencoders in question are trained to minimize the reconstruction loss, i.e. to minimize the average Euclidean distance between the input and the corresponding reconstruction point.

A. Neural Networks and their Jacobians

In this paper, we think of any neural network as the composition of the functions represented by the weight matrices, bias vectors, and the activation functions in each layer. In other words, if a neural network has an \( N \) dimensional input space and an \( M \) dimensional output, we may represent it as a multi-variable function, \( NN : \mathbb{R}^N \rightarrow \mathbb{R}^M \). The Jacobian matrix of a multi-variable function is the matrix of gradient vectors of each of the components of the function, and is represented as an \( M \times N \) matrix with function valued entries. In general, this Jacobian matrix cannot be represented or computed in function form, however, one can always talk about its the value of the Jacobian matrix at any given input point \( x \), \( J_{NN}(x) \). This matrix represents a linear transformation from the tangent space the input space at \( x \) to the tangent space of the output space at the output point \( y = NN(x) \). One may always study the singular value decomposition of \( J_{NN}(x) \) to find an orthonormal basis of the tangent space \( T_y(\mathbb{R}^N) \) and understand how it transforms in terms of an orthonormal basis of \( T_x(\mathbb{R}^M) \). Note that the Jacobean matrix is only defined where the function is differentiable. In the case of neural networks with ReLU activation functions, as is the case for the autoencoders considered in this paper, the functions are piece wise linear. Therefore, they are not differentiable on a space of measure 0 in \( \mathbb{R}^N \). In other words, the matrix \( J_{NN}(x) \) is not defined with probability 0.

In the special case of \( N = M \), as is the case for autoencoders, one may also consider the eigenvalues and eigenvectors of the Jacobian matrix, which quantifies the directions and amounts in which the map \( J_{NN}(x) \) dilates or contracts the tangent space \( T_x(\mathbb{R}^N) \). This is fundamentally different from a singular value decomposition of \( J_{NN}(x) \) as it identifies a common basis for the two tangent spaces, \( T_x(\mathbb{R}^N) \) and \( T_y(\mathbb{R}^N) \), given by the eigenvectors. In other words, the eigenvalues gives insight into the local deformations of the input space as the function learned by the autoencoder maps it to the reconstruction space.

The Jacobian matrix of the autoencoder is computed by \( J_I := D(f_{dec} \circ f_{enc})(x) = Df_{dec}(z) \cdot Df_{enc}(x) \). See Appendix A for details. For any matrix square matrix \( A \), let \( \hat{A} \) be the vector of norm decreasing eigenvalues of \( A \). Note that the image of the autoencoder in the reconstruction space is at most \( d \) dimensional, for \( L = \mathbb{R}^d \). Therefore, for any point \( x \in I \), the vector \( \hat{X}_{J_L(x)} \) will have at most \( d \) non-zero entries, each indicating the amount of stretching or warping that the corresponding eigenspace of the data point (as a subspace of \( T_x(I) \) undergoes. In particular, the eigenspace of 0 corresponds to the kernel of \( J_I(x) \). Geometrically, these are the directions of the input space that are collapsed to the origin in the image of the autoencoder.

Calculating the eigenvalues of \( J_I(x) \) is computationally expensive, as algorithms for calculating eigenvalues of an \( n \times n \) matrix are \( O(n^3) \). Therefore, it is easier to calculate the eigenvalues of the Jacobian of a related function, \( J_L := D(f_{enc} \circ f_{dec})(x) = Df_{enc}(y) \cdot f_{dec}(z) \) which represents the deformations of the latent space under the action of the autoencoder composed in the opposite order. In general, there is no reason to expect that these two Jacobians should have any similarity in their eigenvalues. However, in [9], the authors show that when the the reconstruction error is 0, the eigenvalues of \( J_L \) are similar to the eigenvalues of \( J_I \).

**Theorem 1.1.** If \( f_{dec} \circ f_{enc}(x) = x \), then for \( z = f_{enc}(x) \), the \( d \) nonzero eigenvalues of \( J_I(x) \) are the same as the eigenvalues of \( J_L(z) \).
Theorem I.2. The same reconstruction point. M large kernel. That is, many out of distribution points will dimension than the latent space, \( z \) in the image of the data manifold in latent space. Then \( f(x) \) function restricted to the data manifold, \( f \in \mathcal{I} \), consists of learning a diffeomorphism \( \phi_U \) with an embedding into the latent space: \( \pi: \mathbb{R}^d \rightarrow \mathbb{R}^d \). If the latent space has greater dimension than the data manifold, \( \delta > d \), then \( f(\mathcal{M}) \) is the composition of \( \phi_U \) with an embedding into the latent space: \( \pi: \mathbb{R}^d \rightarrow \mathbb{R}^d \). The function \( f_{\text{dec}}(\mathcal{L}) \) is the inversion of this function. The commutative diagram for this interaction is shown in display (1).

B. Probing the data manifold structure

The Jacobians \( J_L(x) \) and \( J_L(z) \) give insight into how well an autoencoder is learning the data manifold underlying the training data.

The data manifold conjecture simply states that, for any given data set of related objects \( \mathcal{D} \), the data actually lies noisily around some low (\( \delta \)) dimensional manifold \( \mathcal{M} \subset \mathcal{L} \). If a neural network learns a good representation of the data, then it learns the structure of \( \mathcal{M} \). In topological terms, learning the structure of \( \mathcal{M} \) consists of learning a diffeomorphism \( \phi_U \) of some low dimension \( \delta \) dimensional manifold \( \mathcal{M} \) to \( \mathcal{L} \). Ideally, if \( \delta > d \), then the learned function restricted to the data manifold, \( f_{\text{enc}}(\mathcal{M}) \) is the composition of \( \phi_U \) with a projection onto the latent space: \( \pi: \mathbb{R}^d \rightarrow \mathbb{R}^d \). If the latent space has greater dimension than the data manifold (\( \delta \leq d \)) then \( f_{\text{enc}}(\mathcal{M}) \) is the composition of \( \phi_U \) with an embedding into the latent space: \( \pi: \mathbb{R}^d \rightarrow \mathbb{R}^d \). The function \( f_{\text{dec}}(\mathcal{L}) \) is the inversion of this function. The commutative diagram for this interaction is shown in display (1).

The function \( f_{\text{enc}} \) is not just defined on the points near \( \mathcal{M} \), but on all of \( \mathcal{I} \). Little is understood about the geometry of the neural network \( f_{\text{enc}} \) on points far away from the data manifold. Let \( \mathcal{M} \subset \mathcal{L} \) be the image of \( \mathcal{M} \) under \( f_{\text{enc}} \). Since the input space has much greater dimension than the latent space, \( N \gg d \), \( f_{\text{enc}} \) has a large kernel. That is, many out of distribution points will map onto \( \mathcal{M} \). Then \( f_{\text{dec}} \) maps all these points to the same reconstruction point.

**Theorem 1.2.** Let \( x \in \mathcal{I} \) be an input point with latent representation, \( z' = f_{\text{enc}}(x) \), is close to a point \( z \in \mathcal{M} \) in the image of the data manifold in latent space. Then

\[
||\tilde{J}_L(z') - \tilde{J}_L(z)||^2 \leq ||J_L(z') - J_L(z)||^2 = (O(||z' - z||^2))^2.
\]

Therefore, the distance between the eigenvalue vectors of \( J_L(z') \) and \( J_L(z) \) gives a lower bound on the Frobenius norm of difference of the Jacobian matrices. Namely, even if an out of distribution point is reconstructed to an element of \( f_{\text{dec}} \circ f_{\text{enc}}(\mathcal{M}) \subset \mathcal{R} \), the eigenvalues of \( J_L(z') \) gives information about its latent representation.

C. In distribution eigenvalue behavior

Let \( \mathcal{D}_{\text{train}} \) be the training data set, and \( \mathcal{M}_{\text{train}} \) the corresponding \( \delta_{\text{train}} \) dimensional data manifold. Minimizing the reconstruction error ensures the the autoencoder is a good zeroth order model for a sample of points in and around \( \mathcal{M}_{\text{train}} \). Studying the eigenvalues of the Jacobian \( J_L(x) \) gives information about how well the autoencoder performs as a first order approximation of data manifold, locally around \( x \). For instance, suppose \( d \leq \delta_{\text{train}} \). If the top \( d \) eigenvalues of \( J_L(x) \) are one, then the auto-encoder has projected exactly onto the manifold \( \mathcal{M}_{\text{train}} \) at each input point \( x \). If the arguments of the eigenvalues of \( J_L(x) \) are 0, then there is little rotation locally in passing from each input to reconstruction point. If the product of the top \( d \) eigenvalues of \( J_L(x) \) remain at 1 for all \( d \).

D. Out of distribution eigenvalue behavior

Let \( \mathcal{D} \) be a fundamentally different data set than \( \mathcal{D}_{\text{train}} \). For \( x \in \mathcal{D} \), one cannot use the norms of the eigenvalues of \( J_L(x) \) alone to understand whether or not \( f_{\text{enc}} \) is projecting \( T_x(\mathcal{I}) \) onto the tangent space of point on \( \mathcal{M}_{\text{train}} \). To see why, consider the points on the inside and outside of a \( d \) dimensional unit sphere, \( S^d \). Consider the points that lie on the rays emanating from the origin through \( S^d \) in \( \mathbb{R}^N \). For points lying close to the origin, any projection onto the surface of the sphere will have the properties that a small perturbation in the domain will result in a large perturbation on the sphere. I.e. the eigenvalues will be large. For projections of the points on the rays on the outside of the sphere, however, a large perturbation in the domain will correspond to a small perturbation on the surface. I.e. the eigenvalues will be small.

Furthermore, the average size of the argument of the eigenvalues and the sign of the product of the eigenvalues \( J_L(x) \) has structure if the function \( f_{\text{enc}}(x) \) factors through a projection onto \( \mathcal{M}_{\text{train}} \).

**Theorem 1.3.** Let \( x \in \mathcal{D} \) be far away from the data manifold \( \mathcal{M}_{\text{train}} \). If the function \( f_{\text{enc}}(x) \) factors through a
parallel transport onto $M_{D_{\text{train}}}$, the sign of the product of the non-zero eigenvalues will be positive (the Jacobian does not reverse orientation from $T_x I$ to $T_y R$), and the arguments of the eigenvalues will be zero (the Jacobian does induce a rotation from $T_x I$ to $T_y R$).

Finally, it is worth noting that an autoencoder trained on $M_{D_{\text{train}}}$ will not capture information on the geometry of $M_D$. For instance, there is no reason for an autoencoder $f_{\text{dec}} \circ f_{\text{enc}}$ that has learned the geometry of $M_{D_{\text{train}}}$ (as outlined in Section I-C) will have captured any information about the geometry of a distant evaluation manifold $M_D$. For instance, the appearance of zero eigenvalues after latent dimension $d$ in the Jacobean $J_T(x)$, for $x \in D$ should not indicate that $M_D$ has dimension $d$. Rather, it indicates that the trained autoencoder is keeping track of fewer than $d$ of the dimensions of the input space near $x$.

E. Observed behavior

In this paper, we observe that for an $x \in M_{D_{\text{train}}}$, the autoencoder displays several properties one would expect if the map $f_{\text{dec}} \circ f_{\text{enc}}(x)$ induced a projection onto $T_y M_{D_{\text{train}}}$. Namely, the norm of the eigenvalues are, on average, less than one, but remain relatively close to it for both $J_T(x)$ and $J_L(z)$. Furthermore, as the latent dimension increases, the distribution of eigenvalues develop increasingly long left tails on a log scale, see Figure 2. That is, the proportion of eigenvalues with small norms increases, though not as quickly as one would expect for a projection. Furthermore, the arguments of the eigenvalues are small, as are the proportion of points with locally orientation reversing behavior. This is consistent with work studying autoencoders as an iterative system, where the output of a trained autoencoder is evaluated again by the same autoencoder, where one finds that the outcome is not the same, but does converge [18]. Furthermore, this behavior is consistent across autoencoder architecture.

However, this behavior is not observed for data sets that are far out of distribution. For instance, we note that, for $J_L$, the arithmetic mean of the eigenvalues of the out of distribution points is frequently quite different from the arithmetic mean of the eigenvalues of the in distribution points (Figure 2), indicating that Frobenius norms of the two matrices are large (by Theorem 2), even when, visually, the reconstruction image appears to be in $M_{D_{\text{train}}}$. In other words, even when the reconstructed image appears to be in the reconstruction of the training manifold, the latent representation of the out of domain point can be quite different from the latent representations of the training data.

Furthermore, when the latent dimension is large, about half of the out of distribution data points show orientation reversing behavior by $J_T(x)$ and the eigenvalues have a larger range of arguments than in the training data, indicating that the map $f_{\text{enc}}$ does not factor through a parallel transport onto $M_{D_{\text{train}}}$. Since approximately 50% of the points display orientation reversing data, the autoencoder has not learned anything about the orientation of the tangent space, $T_x I$, far out of distribution.

II. Experiment

For this paper, we trained nineteen autoencoders on the MNIST data set, each with different latent dimensions, but otherwise identical architectures. We then evaluated these nineteen neural networks on 10 different out of distribution data sets, each consisting of 70,000 draws from different random distributions on the pixel values. Henceforth, we refer to the full MNIST data set as $D_{\text{train}}$, even though the training was done on the standard 60,000 training points of the 70,000 point sample.

We observe several notable empirical results. First, at low latent dimension, the autoencoders reconstructs the out of domain data as MNIST images, though inconsistently. As the latent dimension increases, the autoencoders stop reconstructing the data sets at MNIST images, but rather reconstruct them as generalized characters. It is interesting to note, however, that while the autoencoder seems to have learned some general features of written characters from the MNIST data set, there is no consistency of the reconstructions across either architectures or seeds, indicating the instability of network performance on out of domain data.

As further evidence of the instability of the autoencoders, we note variation in the arithmetic and geometric means of the eigenvalues, and that the standard deviation of the log normal of the eigenvalues is, in general greater for the out of distribution data than for the training data (see Figure 3). We consider the log normal of the eigenvalues rather than just the eigenvalues themselves in order to capture the expectation that as latent dimension increases past the intrinsic dimension of $M_{D_{\text{train}}}$, while one expects the emergence of more zero (or very small in norm) eigenvalues, which we do not observe. The increased variation within each autoencoder indicates a lack of consistency of the eigenvalues of $J_T(x)$ on each out of domain point $x$. The increased variation across
autoencoders is further evidence of the instability of network performance on out of domain data.

Finally, in spite of the instability or reconstructions across architectures, certain patterns still emerge. Namely, the arithmetic and geometric means of the eigenvalues cluster according to the means of the distributions from which they are drawn. In other words, while the autoencoders do not geometrically encode much data about out of distribution points, they do learn information about the mean pixel values.

A. Data and architecture

For this paper, we trained nineteen unregularized autoencoders on the MNIST data set on two seeds. While we are aware that there are many regularization processes that will improve the accuracy and/or generalization abilities of our autoencoder, we intentionally work with unregularized networks as these have the easiest to interpret geometric properties. Each autoencoder has four identical layers in the encoder and decoder differing only by the dimension of the latent dimension: the encoder half consists of layers mapping between spaces of dimension (784, 128, 64, 32, d), and the decoder half consists of layers between dimensions (d, 32, 64, 128, 784), with d ∈ {2, . . . , 19}.

The MNIST images are 28x28 arrays flattened to a vector for input. Thus the input and reconstruction spaces are \( \mathcal{I} = [0, 1]^{784} = \mathcal{R} \). Furthermore, the decoder has a final tanh function to renormalize the output to a vector with values in the interval [0, 1]. The activation function for all layers is ReLU, making the autoencoder represent a piece wise linear function, and trained for 300 epochs, with seeds 0 and 1.

After training, we evaluate 10 different samples of 70,000 datapoints drawn from 10 different out of distribution data sets, each defined by a random distribution on \( \mathcal{I} \), with different means: truncated normal between 0 and 1, (mean 0.5), uniform over \([0, 1]\) (mean 0.5), 4 Bernoulli distributions with means 0.13, 0.25, 0.5, 0.75, and 0.87, and three Beta distributions one with \( \alpha = .8, \beta = 5, \) mean .14, another with \( \alpha = .5, \beta = .5, \) mean .5, and the final with \( \alpha = 5, \beta = .8, \) mean = .86. We refer to the data sets as \( \mathcal{D}_{\text{norm}}, \mathcal{D}_{\text{unif}}, \mathcal{D}_p \) for the 4 Bernoulli distributions (where \( p \in \{.13, .25, .5, .74, .87\} \)) and \( \mathcal{D}_{\alpha, \beta} \) for the three Beta distributions (where \( (\alpha, \beta) \in \{(8, 5), (.5, .5), (5, 8)\} \)).

We note that the mean value for the MNIST data set is .13, with most of the the values being 0 (black), and a small percentage being near 1 (white). While the location of the bright pixels is clearly important for the classifier, we chose \( \mathcal{D}_{.13} \) and \( \mathcal{D}_{.8,5} \) to mimic this behavior. The data sets \( \mathcal{D}_{.87} \) and \( \mathcal{D}_{.5,8} \) are chosen to reverse this behavior. All other distributions are chosen to interpolate between these two extremes.

B. Geometry of out of distribution data

As we draw the out of distribution data from well-defined distributions, we may characterize this data in terms of several data manifolds. Most simply, we may consider each data set as being noisily distributed around a 0 dimensional manifold, the point where each pixel has the mean brightness. In this manner, we have 10 different 0 dimensional data manifolds, indicated as above as \( M_{\text{D}_p}, M_{\alpha, \beta}, M_{\text{norm}} \) and \( M_{\text{unif}} \). Note that given the similarities of the means, from this perspective, the manifolds \( M_{\text{D}_13} \) and \( M_{\text{D}_{.8,5}} \) are close; \( M_{\text{norm}}, M_{\text{unif}} \) and \( M_{\text{D}_{.8,5}} \) are the same; and \( M_{\text{D}_{.87}} \) and \( M_{\text{D}_{.5,8}} \) are close together. However, the corresponding data sets are different, as the sampling around the point corresponding to the manifold is different in each case.

We may also consider these points to be lying on a larger data manifold parameterized by the properties of the distributions. Allowing \( p \) to vary from 0 to 1, we obtain a 1 dimensional data manifold \( M_{\text{Bernoulli}} \), where each \( \mathcal{D}_p \) is a sample of points distributed noisily (according to the appropriate Bernoulli distribution) about the point \( p \in M_{\text{Bernoulli}} \). Similarly, there is a two dimensional \( M_{\text{Beta}} \) parametrized by \( 0 < \alpha, \beta \) where each \( \mathcal{D}_{\alpha, \beta} \) is a sample of points distributed noisily according to the appropriate Beta distribution. Finally, \( \mathcal{D}_{\text{norm}} \) and \( \mathcal{D}_{\text{unif}} \) come from tow points on the two dimensional manifold \( M_{\text{norm}} \), parametrized by \( \mu \) and \( \sigma \) with data is distributed around it according to the truncated normal distribution with mean \( 0 < \mu < 1 \) and \( 0 < \sigma < \infty \); \( \mathcal{D}_{\text{norm}} \) samples around the point \( \mu = .5, \sigma = 1 \) and \( \mathcal{D}_{\text{unif}} \) around \( \mu = .5, \sigma = \infty \).

Note that, as discussed in Section 1-D, the eigenvalues of the \( J_{\mathcal{I}}(x) \) do not capture the intrinsic dimension of the out of distribution data. Namely, one does not observe the emergence of 0 (or small normed) eigenvalues at low latent dimension, as one would expect if the autoencoder had learned the intrinsic dimension (see Figure 3).

C. Reconstruction images

Looking at these 10 data sets, evaluated on the 19 different autoencoders, we find that for each autoencoder
with large enough latent dimension, the reconstructed images can qualitatively be placed into two groups, those with mean less than .5, and those with means at least .5 (see Tables I and II). Examining the behavior of the eigenvalues, we get a finer granularity of three mean based clusters: those with mean less than .5, those with mean .5 and those with mean greater than .5 (see Figure 2). Because of this behavior, in the tables and figures below, we only present the data from a low mean, or dark, data set, \( D_{13} \), the data from a moderate meaned data set \( D_{\text{norm}} \) and the data from a high meaned, or bright, data set, \( D_{5.8} \).

Visually, there are two things to note. First, for a given autoencoder with a large enough latent dimension, the reconstructed image appears be a generalized character, not a one from the MNIST data set. For lower latent dimensions, the reconstructed images appear uniformly to be a character from the MNIST data set. For very low latent dimensions, the 10 distributions are reconstructed as elements of the MNIST data set, but not uniformly. Visual similarity of the reconstruction images for each autoencoder implies that one may think of the image of all these data manifolds as lying in a subspace of \( \mathcal{R} \), \( M_{\text{dist},d} \), where \( d = \dim(L) \). That is, for \( f_{\text{enc},d} \) and \( f_{\text{dec},d} \) the autoencoder with \( d \) dimensional latent space, we write

\[
f_{\text{dec},d} \circ f_{\text{enc},d} : M_{\mathcal{D}}, \rightarrow M_{\text{dist},d}
\]

for \( M_{\mathcal{D}} \), corresponding to the Bernoulli, Beta or truncated normal distribution manifolds. It is striking to note that the manifold \( M_{\text{dist},d} \) is a function of \( d \), i.e. different for each architecture. Furthermore, it appears to be different for each seed.

We posit that some of this observed behavior is due to the fact that at very low latent dimensions, there are not enough degrees of freedom in the latent space for the autoencoder to have learned enough features to be able to do anything but noisily assign out of distribution objects similarly. As the degrees of freedom increase, the autoencoders seem to first be able to identify the out of distribution elements as similar. However, these systems do not have the potential to reconstruct images as anything other than those that are in distribution. Eventually, for high enough \( d \), the autoencoder has enough degrees of freedom to be able to reconstruct the out of distribution image as a different out of distribution image. How it does it, however, is my no means consistent across systems.

Next, we study the behavior of the eigenvalues of \( J_{\mathcal{I}}(x) \) and \( J_{\mathcal{L}}(z) \). By Theorem 1, if the reconstruction error is small, we expect the vectors \( \vec{\lambda}_{\mathcal{I}}(x) - \vec{\lambda}_{\mathcal{L}}(z) \) to be small. When the reconstruction error is large, we expect to see no such pattern. This is borne out in Figure 1.

For the in distribution data, the arithmetic and geometric means of the eigenvalues are near 1, with a slow decline as the latent dimension increases (see Figure 2). The similarity of scale between the arithmetic and geometric means indicates that eigenvalues do not contain extreme outliers at any latent dimension. As discussed in Section 3C, this indicates that the autoencoder is learning a function that is close to a projection onto the data manifold. At high latent dimension, the autoencoder is not learning to ignore certain dimensions of the data (as evidenced by the failure of 0 eigenvalues to appear in significant quantities, see 3), but the decrease in mean eigenvalue indicates that the autoencoder has learned to contract certain dimensions. The fact that, at higher latent dimension, the autoencoder retains some information about all dimensions of the latent space (rather than collapsing them altogether) is consistent with the fact that at higher latent dimension, the out of domain data is reconstructed as generalized characters. In other words, this is exactly the behavior one would expect if the autoencoder is learning (and therefore reconstructing) more than just the MNIST digits.

For the out of distribution data the arithmetic and geometric means for both \( J_{\mathcal{I}} \) and \( J_{\mathcal{L}} \) are far less constant than those of the in distribution data. This architecture...
dependent variation of the eigenvalues of the autoencoder is evidence of the geometric instability of the autoencoder on out of distribution data. However, for large enough latent dimension, there are three distinct clusters of eigenvalues of $J_L$: the three darkest distributions (those with the lowest mean pixel value) have the highest average eigenvalue, followed by the distributions with a mean of .5, and the three with the highest mean pixel value have the lowest mean eigenvalue.

Inspite of the apparent learning, most of the eigenvalue information points to a low level of geometric stability on out of domain data. At low latent dimension, when the reconstructed images appear to lie in $M_{D_{train}}$, for all out of distribution data sets, the mean eigenvalues of $J_L$ for many out of distribution data sets are not close to the mean eigenvalue for the training data. By Theorem I.2, the squared distance between the vectors of eigenvalues $\|\hat{\lambda}_{J_L}(z) - \hat{\lambda}_{J_L}(z')\|^2$ is a lower bound for the distance squared between the latent representation $z,z' \in \mathcal{L}$. A large difference in means (as observed in Figure 1) implies that the latent representations of the points in certain data sets are, on average, far away from the latent representations of the points in the training data, even though the reconstructed images are similar.

Figure 3 shows the distribution of eigenvalues in the training data, representative bright, moderate and dark data sets. Note that for each of the out of distribution data set, the variance of the distribution of logarithms of the norms of the eigenvalues in any given latent dimension, as well as the medians of the same across latent dimension is much greater than the same variance for the in distribution data (see Figure 4). This again points to the geometric instability of the autoencoder far from the training manifold.

Finally, we note that, by Theorem 1.3, autoencoder does not map points in $\mathcal{I}$ far from the training manifold onto $M_{D_{train}}$ via an orientation preserving, non-rotating map (such as a parallel transport in $\mathcal{I}$ in the Euclidean metric). Notably, on the training data, the distribution of arguments of the eigenvalues is small (see Figure 5) as is the proportion of points for which the orientation is reversed (see Figure 6). However, for the out of distribution data, the arguments for $J_L(x)$ can be any angle for the bright data sets. The range of possible angles decreases with range, but even for the dark data sets, is consistently larger than for the training data. Similarly, for the all but the darkest data sets, at high enough latent dimension, the matrices $J_L(x)$ reverse the orientation of $T_x(\mathcal{I})$ approximately half the time. Given the general instability across architectures of other
Fig. 5: The proportion of points for which the product of the top $d$ eigenvalues of $J_I(x)$ (left) or $J_L(z)$ (right) is negative, indicating that orientation of coordinate system has been flipped. There are very few of these points for $D_{train}$, while for the out of distribution data, the proportions are near half for $J_I(x)$.

Fig. 6: The box plots for $|\text{Arg}(\lambda_{J_I(x)})|$ (blue) and $|\text{Arg}(\lambda_{J_L(z)})|$ (red). Note these arguments cover a significantly wider range for the out of distribution data sets than the training data.

geometric properties on out of distribution data, the consistency of this coin flip on the orientation of the tangent space is remarkable.

III. COMPARISON WITH RELATED WORK

The machine learning community is not a stranger to the differential geometry literature. There is a large body of work on learning metric functions on the latent spaces for (variational) autoencoders and to determine the reconstruction loss [19], [20], [21], [22], [23]. Others propose building the reconstruction error out of the Mahalanobis distance function [14] to better detect out of distribution inputs. These, and other efforts, aim to use differential geometry tools to improve the performance of neural networks. Our work differs from these in that we are not interested in performance enhancing methodologies, but in understanding the geometry feature map so that we may explain how the feature map perceives and interacts with out of domain data.

We note that Contraction Autoencoders (CAEs) use the Frobenius norm of the Jacobian of the encoder map to regularize the loss function [24]. CAEs and their higher order counterparts [25] are better at capturing smoother, more accurate and lower dimensional representations of the data manifold. As mentioned above, we explicitly avoid regularization techniques in the autoencoders trained for this paper in order to better understand the geometry of the learned functions. Furthermore, the Jacobian matrices used in these cases were of the encoder maps only, while our work focuses on the Jacobian matrix for the two networks combined.

IV. CONCLUSION

In this paper, we study the learned geometry of a family of trained autoencoders, on input points far away from the data set on which the system was trained. Instead of studying the performance outputs of the autoencoders (which we expect to be poor) we look at the geometric features of the autoencoder, viewed as a function from input to reconstruction space. In doing so, we make the following observations. From the point of view of the reconstructed images, at low latent dimension the data sets of randomly distributed pixel values are all mapped to images that appear to come from the training data set. However, which class of training image is reconstructed is not consistent neither within random data set, nor across random data sets, nor across seeds. At higher latent dimensions, the reconstructed images across all data sets in a given architecture and seed appear to be a generalized characters. However, this character is not consistent across architecture or seed.

From a geometric perspective, we show that while, for lower latent dimension, the reconstructed images appear to be the same as those in the training data, the latent representations of the training and out of distribution points are quite different. Furthermore, we find evidence that geometries of the learned functions (as measured by the eigenvalues of $J_I(x)$) cluster according to the mean value of the pixel distribution. Finally, and possibly most surprisingly, we observe that for higher latent dimension, the trained autoencoder is not aware of the orientation of the bases of the input space.

We contend that studying the geometry of the trained autoencoder will give insight into how the network is processing both in and out of distribution data, and will play a key role in explaining the phenomenon of out of distribution reconstruction.
APPENDIX

COMPUTING THE JACOBIANS

Explicitly, for the autoencoder structure used in this paper we may write \( f_{\text{enc}} \) as a composition of the weight matrices and activation functions at each layer. That is,

\[
f_{\text{enc}} = f_{\text{enc},4} \circ f_{\text{enc},3} \circ f_{\text{enc},2} \circ f_{\text{enc},1}
\]

\[
f_{\text{dec}} = f_{\text{dec},4} \circ f_{\text{dec},3} \circ f_{\text{dec},2} \circ f_{\text{dec},1}
\]

where

\[
f_{\text{enc},i}(x) = \begin{cases}
\text{ReLU}_{128}(A_{128 \times 784}x + b_{128}) & i = 1 \\
\text{ReLU}_{64}(A_{64 \times 128}x + b_{64}) & i = 2 \\
\text{ReLU}_{32}(A_{32 \times 64}x + b_{32}) & i = 3 \\
A_{d \times m}x + b_d & i = 4,
\end{cases}
\]

\[
f_{\text{dec},i}(x) = \begin{cases}
\text{ReLU}_{32}(A_{32 \times 128}x + b_{32}) & i = 1 \\
\text{ReLU}_{64}(A_{64 \times 32}x + b_{64}) & i = 2 \\
\text{ReLU}_{128}(A_{128 \times 64}x + b_{128}) & i = 3 \\
\tanh_{784}(A_{784 \times 128}x + b_{784}) & i = 4,
\end{cases}
\]

Here, each \( A_{n \times m} \) is a real \( n \times m \) matrix, \( b_m \) is a \( m \) dimensional column vector, and \( \text{ReLU}_m : \mathbb{R}^m \rightarrow \mathbb{R}^m \) is the vector valued function that is \( \text{ReLU} \) in each component (similarly for \( \tanh_m \)).

The Jacobians for the autoencoders \( J_\mathcal{L}(x) \) and \( J_\mathcal{L}(z) \) are computed locally by repeated application of the chain rule through both the encoder and decoder layers. Note that the derivative of a layer is applied to the output from the last layer:

\[
F = F_n \circ \cdots \circ F_1, \text{ then } \partial F = \prod \partial F_i |_{F_{i-1} \circ \cdots \circ F_1(x)}.
\]

Explicitly the derivative of a affine transformation is the associated matrix

\[
\frac{\partial(Ax + b)}{\partial x} = A.
\]

Recall that the ReLU function is, component wise the piece wise linear function

\[
\text{ReLU}(x) = \begin{cases}
0 & x < 0 \\
x & x \geq 0
\end{cases}.
\]

The derivative of the ReLU function applied to an \( N \) dimensional vector is the Heaviside function embedded along the diagonals of an \( N \times N \):

\[
\frac{\partial \text{ReLU}(x)}{\partial x} = H(x) = \begin{cases}
1, & x \geq 0 \\
0, & x < 0.
\end{cases}
\]

and the derivative of the \( \tanh \) function applied to an \( N \) dimensional vector is the derivative embedded along the diagonals of an \( N \times N \) dimensional matrix is

\[
\frac{\partial \tanh(x)}{\partial x} = 1 - \tanh^2(x)
\]

Note that in the autoencoder, the ReLU and the \( \tanh \) are applied component wise to the outputs of the previous layer. Thus the corresponding term in the Jacobian calculation is a matrix with the functions \( H(x) \) or \( \tanh(x) \) along the diagonals.

As a particular example, we can compute that the derivative of \( f_{\text{enc},1} \) is

\[
\partial f_{\text{enc},1}(x) = H(A_{128 \times 784}x + b)\|_{128} A_{128 \times 784}
\]

and the other derivatives can be computed similarly, as can the derivatives of compositions (using the chain rule).

GEOMETRIC RESULTS

Proof of Theorem I.1

Proof. This is a result of the chain rule.

Since \( f_{\text{dec}} \circ f_{\text{dec}}(x) = x \), let \( w \) be an eigenvector of \( J_\mathcal{L}(x) \) with eigenvalue \( \lambda \). Then

\[
\partial f_{\text{dec}|z} \circ \partial f_{\text{enc}|z}(w) = \lambda w,
\]

where \( z = f_{\text{enc}}(x) \) as above. If \( v = \partial f_{\text{enc}|z}(w) \) then

\[
\partial f_{\text{enc}|z} \circ \partial f_{\text{dec}|z}(v) = \partial f_{\text{enc}|z} \circ \partial f_{\text{dec}} \circ \partial f_{\text{enc}|z}(w) = \partial f_{\text{enc}|z}(\lambda w) = \lambda(v).
\]

Topological interpretation of an autoencoder

Display (1) shows how an autoencoder learns from a dataset \( \mathcal{D} \). The actual data set \( \mathcal{D} \) lies on and around \( M_\mathcal{D} \). We say that it is distributed noisily around \( M_\mathcal{D} \), however, we make no statements about the properties (such as
higher moments or homoskedasticity) of this distribution. The autoencoder is supposed to approximate \( M_D \) using piecewise linear maps, and reconstruct this piecewise linear approximation in \( \mathcal{R} \). This learning process is shown in the bottom row. If an autoencoder has correctly learned the manifold structure of \( M_D \), then the composition on the bottom row, restricted to the manifold is the identity:

\[
f_{\text{dec}} \circ f_{\text{dec}}(M_D) = I.
\]

Note, this identity should hold everywhere on \( M_D \), specifically, we do not expect it to hold on the \( \mathcal{D} \), which are, with high probability, not on the manifold. In other words, for a point \( x \) on \( M_D \), the Jacobian matrix \( J_I(x) \) should be the identity on the tangent space of \( M_D \), \( T_x(M_D) \subset T_x(I) \) and the normal space, \( T^\bot_x(M_D) \subset T_x(I) \), should be its kernel.

If the autoencoder learns the manifold \( M_D \), then it has learned an atlas on \( M_D \). Any \( \delta \) dimensional manifold is defined by a set of open sets \( U_i \) such that their union gives the manifold \( \bigcup U_i = M_D \), and a set of diffeomorphisms \( \phi_i : U_i \rightarrow \mathbb{R}^d \). Each pair \( (U_i, \phi_i) \) is called a chart on \( M_D \). The set of charts is called an atlas. If an autoencoder learns the structure of \( M_D \), it has learned a chart on \( M_D \), call it \( \phi(U) \). The open set \( U \) is an open set that contains all the points on the manifold, as well as the projection of the data points off the manifold onto it. The image \( \phi(U) \) is in \( \mathbb{R}^d \). If \( d \geq \delta \), this is embedded into the latent space (the map \( \pi \) in display \([1]\)). If \( d < \delta \) then the map \( \pi \) is a projection of \( \phi(U) \) onto \( \mathbb{R}^d \).

In actuality, the map \( \pi \) is never a projection, or an embedding. The autoencoder learns to fit the data as best it can with the \( d \) degrees of freedom that is given. Therefore, when \( d < \delta \), the autoencoder minimizes its loss function, not by projecting onto a lower dimensional space as it would do if it had learnt the manifold structure, but by finding a \( d \) dimensional submanifold of \( M_D \) that better fits the data. Similarly, when \( d > \delta \), the autoencoder minimizes its loss function by using the extra dimensions to fit the data. In doing so, it has learned a manifold that is too large, and allows for phenomenon such as out of domain reconstructions and reconstruction to generalized characters, as seen in this paper.

**Proof of Theorem 1.2**

**Proof.** Recall that the Frobenius norm of an \( n \times n \) matrix, \( A \), can be written

\[
\|A\|_F^2 = \sum_{i=1}^{\min(m,n)} \sigma_i(A)^2
\]

where \( \sigma_i(A) \) denotes the \( i \)th singular value of \( A \) (in decreasing order).

Weyl’s majorization theorem gives, for any \( p > 0 \) and any \( 1 \leq k \leq n \) that

\[
\sum_{i=1}^{k} |\lambda_i|^p \leq \sum_{i=1}^{k} \sigma_i^p.
\]

The first inequality comes from setting \( p = 2 \).

The equality is a result of Taylor’s theorem. \( \square \)

**Proof of Theorem 1.3**

**Proof.** Display \([3]\) gives the commutative diagram if \( f_{\text{enc}}(x) \) factors through a projection onto \( M_{D_{\text{train}}} \):

\[
\begin{array}{ccc}
\mathcal{I} & \xrightarrow{f_{\text{enc}}} & \mathcal{L} \\
\pi & \downarrow & \downarrow f_{\text{dec}} \\
M_{D_{\text{train}}} & \xrightarrow{f_{\text{enc}}} & \mathcal{R}
\end{array}
\]

where \( \pi \) denotes a paralell transport of \( x \) onto the data manifold. Note that for \( x' \in M_{D_{\text{train}}} \), \( J_I(x') \) has eigenvalues of 1 or 0. Therefore, the sign of the products of the non-zero eigenvalues will be 1. Similarly, the arguments of the eigenvalues of \( J_I(x') \) are 0. Furthermore, as geodesics in Euclidean space are straight lines, any parallel transport of \( x \) to \( x' \), will not introduce rotation (including orientation reversal) of the of the basis of \( T_x\mathcal{I} \). Therefore, the composition \( f_{\text{enc}} : \mathcal{I} \rightarrow \mathcal{L} \) will not introduce rotation or orientation reversing behavior. \( \square \)
ADDIONAL FIGURES

REFERENCES

[1] T. Romm, “Amazon’s facial-recognition tool misidentified 28 lawmakers as people arrested for a crime, study finds,” Washington Post, July 26, 2018.
[2] B. Wilson, J. Hoffman, and J. Morgenstern, “Predictive inequity in object detection,” arXiv preprint arXiv:1902.11097, 2019.
[3] E. Nalisnick, A. Matsukawa, Y. W. Teh, D. Gorur, and B. Lakshminarayanan, “Do deep generative models know what they don’t know?” arXiv preprint arXiv:1810.09136, 2018.
[4] J. D. Havtorn, J. Frelsen, S. Hauberg, and L. Maaløe, “Hierarchical vaes know what they don’t know,” arXiv preprint arXiv:2102.08248, 2021.
[5] D. Hendrycks and K. Gimpel, “A baseline for detecting misclassified and out-of-distribution examples in neural networks,” arXiv preprint arXiv:1610.02136, 2016.
[6] S. Liang, Y. Li, and R. Srikant, “Enhancing the reliability of out-of-distribution image detection in neural networks,” arXiv preprint arXiv:1706.02690, 2017.
[7] T. DeVries and G. W. Taylor, “Learning confidence for out-of-distribution detection in neural networks,” arXiv preprint arXiv:1802.04865, 2018.
[8] D. Krueger, E. Caballero, J.-H. Jacobsen, A. Zhang, J. Binas, D. Zhang, R. Le Priol, and A. Courville, “Out-of-distribution generalization via risk extrapolation (rex),” in International Conference on Machine Learning. PMLR, 2021, pp. 5815–5826.
[9] S. Agarwal, B. Dees, A. S. Gearheart, and C. Lowman, “Geometry and generalization: Eigenvalues as predictors of where a network will fail to generalize,” arXiv:2107.06386.
[10] Y. Zhao, B. Deng, C. Shen, Y. Liu, H. Lu, and X.-S. Hua, “Spatio-temporal autoencoder for video anomaly detection,” in Proceedings of the 25th ACM International Conference on Multimedia, ser. MM ’17. New York, NY, USA: Association for Computing Machinery, 2017, p. 1933–1941. [Online]. Available: https://doi.org/10.1145/3123266.3123451
[11] S. Liang, Y. Li, and R. Srikant, “Enhancing the reliability of out-of-distribution image detection in neural networks,” in International Conference on Learning Representations, 2018. [Online]. Available: https://openreview.net/forum?id=H1VGkIrRZ
[12] S. Yoon, Y.-K. Noh, and F. C. Park, “Autoencoding under normalization constraints,” arXiv preprint arXiv:2105.05735, 2021.
[13] Z. Xiao, Q. Yan, and Y. Amit, “Likelihood regret: An out-of-distribution detection score for variational auto-encoder,” arXiv preprint arXiv:2003.02977, 2020.
[14] T. Denouden, R. Salay, K. Czarnecki, V. Abdelzad, B. Phan, and S. Vernekar, “Improving reconstruction autoencoder out-of-distribution detection with mahalanobis distance,” arXiv preprint arXiv:1812.02765, 2018.
[15] B. Parlett, “The qr algorithm,” Computing in Science Engineering, vol. 2, no. 1, pp. 38–42, 2000.
[16] Y. Bengio, A. Courville, and P. Vincent, “Representation learning: A review and new perspectives,” IEEE transactions on pattern analysis and machine intelligence, vol. 35, no. 8, pp. 1798–1828, 2013.
[17] G. Alain and Y. Bengio, “What regularized auto-encoders learn from the data-generating distribution,” The Journal of Machine Learning Research, vol. 15, no. 1, pp. 3563–3593, 2014.
[18] A. Radhakrishnan, M. Belkin, and C. Uhler, “Downsampling leads to image memorization in convolutional autoencoders,” CoRR, vol. abs/1810.10333, 2018. [Online]. Available: [http://arxiv.org/abs/1810.10333]
[19] G. Arvanitidis, L. K. Hansen, and S. Hauberg, “Latent space oddity: on the curvature of deep generative models,” arXiv preprint arXiv:1710.11379, 2017.
[20] G. Arvanitidis, S. Hauberg, and B. Schölkopf, “Geometrically enriched latent spaces,” arXiv preprint arXiv:2008.00565, 2020.
[21] D. Eklund and S. Hauberg, “Expected path length on random manifolds,” arXiv preprint arXiv:1908.07377, 2019.
[22] S. Hauberg, “Only bayes should learn a manifold (on the estimation of differential geometric structure from data),” arXiv preprint arXiv:1806.04994, 2018.
[23] A. Tosi, S. Hauberg, A. Vellido, and N. D. Lawrence, “Metrics for probabilistic geometries,” arXiv preprint arXiv:1411.7432, 2014.
[24] S. Rifai, P. Vincent, X. Muller, X. Glorot, and Y. Bengio, “Contractive auto-encoders: Explicit invariance during feature extraction,” in Icml, 2011.
[25] S. Rifai, G. Mesnil, P. Vincent, X. Muller, Y. Bengio, Y. Dauphin, and X. Glorot, “Higher order contractive auto-encoder,” in Joint European conference on machine learning and knowledge discovery in databases. Springer, 2011, pp. 645–660.
TABLE I: Reconstructions of a bright distribution ($D_{5.8}$), and moderate meaned distribution ($D_{\text{normal}}$) and a dark distribution ($D_{1.3}$) for seed 0. Note that by latent dimension 12, all of the reconstructioned images look like the same generalized (non-MNIST) character. For low latent dimension, there is variation in the reconstructed images, which all look like MNIST characters. For moderate latent dimensions, the variations between classes has disappeared, but the reconstructions still look like MNIST characters.
| d  | Bright ($D_{5.8}$) | Moderate ($D_{\text{normal}}$) | Dark ($D_{13}$) |
|----|------------------|-----------------------------|--------------|
| 2  | 44445545        | 890656764                | 111167199   |
| 3  | aaaaaga6        | 222222222                | 977177777   |
| 4  | 555555555      | 5955856758              | 171011111   |
| 5  | 2222222222     | 2222222222               | 171011111   |
| 6  | 2222222222     | 2222222222               | 171011111   |
| 7  | 2222222222     | 2222222222               | 171011111   |
| 8  | 2222222222     | 2222222222               | 171011111   |
| 9  | 2222222222     | 2222222222               | 171011111   |
| 10 | 2222222222     | 2222222222               | 171011111   |
| 11 | 2222222222     | 2222222222               | 171011111   |
| 12 | 2222222222     | 2222222222               | 171011111   |
| 13 | 2222222222     | 2222222222               | 171011111   |
| 14 | 2222222222     | 2222222222               | 171011111   |
| 15 | 2222222222     | 2222222222               | 171011111   |
| 16 | 2222222222     | 2222222222               | 171011111   |
| 17 | 2222222222     | 2222222222               | 171011111   |
| 18 | 2222222222     | 2222222222               | 171011111   |
| 19 | 2222222222     | 2222222222               | 171011111   |
| 20 | 2222222222     | 2222222222               | 171011111   |

TABLE II: Reconstructions of a bright distribution ($D_{5.8}$), and moderate meaned distribution ($D_{\text{normal}}$) and a dark distribution ($D_{13}$) for seed 1. Note that for high latent dimension, all of the reconstructioned images look like the same genearlized (non-MNIST) character, but that these characters are different from those in seed 0 (shown in Figure 1).