Abstract

Variational autoencoders (VAE) represent a popular, flexible form of deep generative model that can be stochastically fit to samples from a given random process using an information-theoretic variational bound on the true underlying distribution. Once so-obtained, the model can be putatively used to generate new samples from this distribution, or to provide a low-dimensional latent representation of existing samples. While quite effective in numerous application domains, certain important mechanisms which govern the behavior of the VAE are obfuscated by the intractable integrals and resulting stochastic approximations involved. Moreover, as a highly non-convex model, it remains unclear exactly how minima of the underlying energy relate to original design purposes. We attempt to better quantify these issues by analyzing a series of tractable special cases of increasing complexity. In doing so, we unveil interesting connections with more traditional dimensionality reduction models, as well as an intrinsic yet underappreciated propensity for robustly dismissing outliers when estimating latent manifolds. With respect to the latter, we demonstrate that the VAE can be viewed as the natural evolution of recent robust PCA models, capable of learning nonlinear manifolds obscured by gross corruptions. However, this previously unexplored feature comes with the cost of potential model collapse to a degenerate distribution that may be less suitable as the basis for generating new samples.

1 Introduction

We begin with a dataset \(X = \{x^{(i)}\}_{i=1}^n\) composed of \(n\) iid samples of some random variable \(x \in \mathbb{R}^d\) of interest, with the goal of estimating a tractable approximation for \(p_\theta(x)\), knowledge of which would allow us to generate new samples of \(x\). Moreover we assume that each sample is governed by unobserved latent variables \(z \in \mathbb{R}^\kappa\), such that \(p_\theta(x) = \int p_\theta(x|z)p(z)dz\), where \(\theta\) are the parameters defining the distribution we would like to estimate.

Given that this integral is intractable in all but the simplest cases, variational autoencoders (VAE) represent a powerful means of optimizing with respect to \(\theta\) a tractable upper bound on \(-\log p_\theta(x)\) [16, 21]. Once these parameters are obtained, we can then generate new samples from \(p_\theta(x)\) by first drawing some \(z^{(i)}\) from \(p(z)\), and then a new \(x^{(i)}\) from \(p_\theta(x|z^{(i)})\). The VAE upper bound itself is constructed as

\[
\mathcal{L}(\theta, \phi) = \sum_i \{KL[q_\phi(z|x^{(i)}) || p_\theta(z|x^{(i)})] - \log p_\theta(x^{(i)})\} \geq -\sum_i \log p_\theta(x^{(i)}),
\]

where \(q_\phi(z|x^{(i)})\) defines an arbitrary approximating distribution, parameterized by \(\phi\), and \(KL[]||[]\) denotes the KL divergence between two distributions, which is always a non-negative quantity. For
optimization purposes, it is often convenient to re-express this bound as

$$L(\theta, \phi) \equiv \sum_i \left[ KL \left( q_\phi \left( z|x^{(i)} \right) \| p(z) \right) - E_{q_\phi \left( z|x^{(i)} \right)} \left[ \log p_\theta (x^{(i)} | z) \right] \right].$$  \hspace{1cm} (2)

In these expressions, $q_\phi (z|x)$ can be viewed as an encoder model that defines a conditional distribution over the latent 'code' $z$, while $p_\theta (x|z)$ can be interpreted as a decoder model since, given a code $z$ it quantifies the distribution over $x$.

By far the most common distributional assumptions are that $p(z) = N(z; 0, I)$ and the encoder model satisfies $q_\phi (z|x) = N(z; \mu_z, \Sigma_z)$, where the mean $\mu_z$ and covariance $\Sigma_z$ are some function of model parameters $\phi$ and the random variable $x$. Likewise, for the decoder model we assume $p_\theta (x|z) = N(x; \mu_x, \Sigma_x)$ for continuous data, with means and covariances defined analogously.\footnote{For discrete data, a Bernoulli distribution is sometimes adopted instead.}

For arbitrarily parameterized moments $\mu_z$, $\Sigma_z$, $\mu_x$, and $\Sigma_x$, the KL divergence in (2) computes to

$$2KL[q_\phi (z|x) \| p(z)] \equiv \text{tr} [\Sigma_z] + \| \mu_z \|^2_2 - \log |\Sigma_z| ,$$ \hspace{1cm} (3)

excluding irrelevant constants. However, the remaining integral from the expectation term admits no closed-form solution, making direct optimization over $\theta$ and $\phi$ intractable. Likewise, any detailed analysis of the underlying objective function becomes problematic as well.

At least for practical purposes, one way around this is to replace the troublesome expectation with a Monte Carlo stochastic approximation \cite{16, 21}. More specifically we utilize

$$E_{q_\phi (z|x^{(i)})} \left[ \log p_\theta (x^{(i)} | z) \right] \approx \sum_{i=1}^T \log p_\theta (x^{(i)} | z^{(1:T)})$$ \hspace{1cm} (4)

where $z^{(1:T)}$ are samples drawn from $q_\phi (z|x^{(i)})$. Using a simple reparameterization trick, these samples can be constructed such that gradients with respect to $\mu_z$ and $\Sigma_z$ can be propagated through the righthand side of (4). Therefore, assuming all the required moments $\mu_z$, $\Sigma_z$, $\mu_x$, and $\Sigma_x$ are differentiable with respect to $\phi$ and $\theta$, the entire model can be updated using SGD \cite{2}.

While quite effective in numerous application domains, certain important mechanisms which dictate the behavior of the VAE are obfuscated by the required stochastic approximation and the opaque underlying objective with high-dimensional integrals. Moreover, it remains unclear to what extent minima remain anchored at desirable locations in the non-convex energy landscape. We take a step towards better quantifying such issues via the following contributions:

1. By probing the basic VAE model under a few simplifying assumptions of increasing complexity whereby closed-form integrations are (partially) possible, we unveil a number of interesting connections with more transparent, established generative models, each of which shed light on how the VAE may perform under more challenging conditions. This mirrors the rich tradition of analyzing deep networks under various simplifications such as linear layers or iid random activation patterns \cite{6, 7, 11, 14, 22}.

2. We demonstrate that the canonical form of the VAE, including the Gaussian distributional assumptions described above, harbors an innate agency for robust outlier removal. In fact, when the decoder mean $\mu_x$ is restricted to an affine function of $z$, we prove that the VAE model collapses to a form of robust PCA \cite{4, 5}, a recently celebrated technique for separating data into low-rank (low-dimensional) and sparse outlier components. However, the VAE maintains noteworthy advantages, such as a natural extensibility to handle outlier-robust low-dimensional manifold learning.

3. We expose that a central, albeit underappreciated role of the VAE encoder covariance $\Sigma_z$ is to smooth out undesirable minima in the energy landscape of what would otherwise amount to a traditional deterministic autoencoder (AE) \cite{1}, even if at times it may not alter the globally optimal solution, or contribute to sample diversity when operating as a generative model.

The remainder of this paper is organized as follows. In Section 2 we consider two affine decoder models and connections with past probabilistic PCA-like approaches. Next we examine various partially affine decoder models in Section 3, whereby only the mean $\mu_z$ is affine while $\Sigma_z$ has potentially unlimited complexity. We precisely characterize how minimizers of the VAE cost, although not available in closed form, nonetheless are capable of optimally decomposing data into
low-rank and sparse factors while avoiding bad local optima. This section also discusses extensions as well as interesting behavioral properties of the VAE. Section 4 then considers degeneracies in the full VAE model that can arise even with a trivially simple encoder model and latent representation. Section 5 concludes with experiments that directly corroborate a number of interesting, practically-relevant hypotheses generated by our prior theoretical analysis, suggesting novel usages and potential pitfalls. We provide final conclusions in Section 6.

Notation: We use a superscript \(^{(i)}\) to denote quantities associated with the \(i\)-th sample, which at times may correspond with the columns of a matrix, such as the data \(X\) or related. For a general matrix \(M\), we refer to the \(i\)-th row as \(m_i\) and the \(j\)-th column as \(m_j\). Although technically speaking posterior moments are functions of the parameters \((\theta, \phi)\), the random variables \(x\), and the latent \(z\), i.e., \(\mu_z \equiv \mu_z(z; \theta)\), \(\Sigma_z \equiv \Sigma_z(z; \theta)\), \(\mu_x \equiv \mu_x(x; \phi)\), and \(\Sigma_x \equiv \Sigma_z(x; \phi)\), except in cases where some ambiguity exists regarding the arguments, these dependencies are omitted to avoid undue clutter; likewise for \(\mu^{(i)} \equiv \mu_z(x^{(i)}; \phi)\) and \(\Sigma^{(i)}_z \equiv \Sigma_z(x^{(i)}; \phi)\). Also, with some abuse of notation, we will use \(L\) to denote a number of different VAE-related objective functions and bounds, with varying arguments and context serving as differentiating factors. Finally, the \(\text{diag}[\cdot]\) operator converts vectors to a diagonal matrix, and vice versa as in Matlab.

2 Affine Decoder and Probabilistic PCA

If we assume that \(\Sigma_z\) is fixed at some \(\lambda I\), and force \(\Sigma_z = 0\) (while removing the now undefined \(\log |\Sigma_z|\) term), then it is readily apparent that the resultant VAE model reduces to a traditional AE with squared-error loss function \([1]\), a common practical assumption. To see this, note that if \(\Sigma_z = 0\), then \(\Phi_\theta(z|x^{(i)})\) collapses to \(\delta(\mu_z)\), i.e., a delta function at the posterior mean, and

\[
E_{\Phi_\theta(z|x^{(i)})} \left[ \log p_{\phi}(x^{(i)}|z) \right] = \log p_{\phi}(x^{(i)}|\mu_z^{(i)})
\]

which is just a standard AE with quadratic loss and representation \(\mu_{x_i}(\mu_z|x)\). Moreover, the only remaining (non-constant) regularization from the KL term is \(\sum_m \|\mu_z^{(i)}\|^2\). However, given scaling ambiguities that may arise in the decoder when \(\Sigma_z = 0\), \(\mu_z^{(i)}\) can often be made arbitrarily small, and therefore the effect of this quadratic penalty is infinitesimal. With affine encoder and decoder models, the resulting deterministic network will simply learn principle components like vanilla PCA, a well-known special case of the AE \([3]\).

Therefore to understand the VAE, it is crucial to explore the role of non-trivial selections for the encoder and decoder covariances, that serve as both enlightening and differentiating factors. As a step in this direction, we will explore several VAE reductions that lead to more manageable (yet still representative) objective functions and strong connections to existing probabilistic models. In this section we consider the following simplification:

Lemma 1 Suppose that the decoder moments satisfy \(\mu_z = Wz + b\) and \(\Sigma_z = \lambda I\) for some parameters \(\theta = \{W, b, \lambda\}\) of appropriate dimensions. Furthermore, we assume for the encoder we have \(\mu_z = f(x; \phi)\), \(\Sigma_z = S_zS_z^\top\), and \(S_z = g(x; \phi)\), where \(f\) and \(g\) are any parameterized functional forms that include arbitrary affine transformations for some arrangement of parameters. Under these assumptions, the objective from (2) admits optimal, closed-form solutions for \(\mu_z\) and \(\Sigma_z\) in terms of \(W\), \(b\), and \(\lambda\) such that the resulting VAE cost collapses to

\[
L(W, b, \lambda) = \sum_i \Omega^{(i)}(W, b, \lambda I) + n \log \lambda I + WW^\top,
\]

where

\[
\Omega^{(i)}(W, b, \Psi) = (x^{(i)} - b)^\top \left( \Psi + WW^\top \right)^{-1} (x^{(i)} - b).
\]

Additionally, if we enforce that off-diagonal elements of \(\Sigma_z\) must be equal to zero (i.e., \(\Sigma_z|_{i\neq j} = 0\) for \(i \neq j\)), then (5) further decouples/separates to

\[
L_{sep}(W, b, \lambda) = \sum_i \Omega^{(i)}(W, b, \lambda I) + n \left[ \sum_j \log (\lambda + \|w_j\|^2) + (d-k) \log \lambda \right].
\]

All proofs are deferred to the appendices. The objective (5) is the same as that used by certain probabilistic PCA models \([23]\), even though the latter is originally derived in a completely different manner. Moreover, it can be shown that any minimum of this objective represents a globally optimal
solution (i.e., no minima with suboptimal objective function value exist). And with \( b \) and \( \lambda \) fixed, the optimal \( W \) will be such that \( \text{span}[W] \) equals the span of the singular vectors of \( X - b1^\top \) associated with singular values greater than \( \sqrt{\lambda} \). So the global optimum produces a principal subspace formed by soft-thresholding the singular values of \( X - b1^\top \), with the rank one offset often used to normalize samples to have zero mean.\(^2\)

In contrast, the alternative cost (7), which arises from the oft-used practical assumption that \( \Sigma_x \) is diagonal, represents a rigorous upper bound to (5), since

\[
\sum_j \log \left( \lambda + \|w_j\|_2^2 \right) + (d - \kappa) \log \lambda \geq \log \left| \lambda I + WW^\top \right|
\]

by virtue of Hadamard’s inequality (see proof of Theorem 1 below), with equality iff \( WW^\top \) is diagonal. Interestingly, all minima of the modified cost nonetheless retain global optimality of the original; however, it can be shown that there will be a combinatorial increase in the actual number of distinct (disconnected) minima:\(^3\)

**Theorem 1** Let \( R \in \mathbb{R}^{n \times k} \) denote an arbitrary rotation matrix and \( P \in \mathbb{R}^{n \times k} \) an arbitrary permutation matrix. Furthermore let \( W^* \) be a minimum of (5) and \( W^{**} \) any minimum of (7) with \( b \) and \( \lambda \) fixed. Then the following three properties hold:

1. \( \mathcal{L}(W^*, b, \lambda) = \mathcal{L}(W^* R, b, \lambda) = \mathcal{L}_{\text{sep}}(W^{**}, b, \lambda) \)
   \[ = \mathcal{L}(WW^*, b, \lambda) = \mathcal{L}_{\text{sep}}(W^{**} P, b, \lambda). \]  
   \[ (9) \]

2. For any \( W^{**} \) (\( W^{**} \))\(^T\) with distinct nonzero eigenvalues, there will exist at least \( \kappa! \) distinct (disconnected) minima of (7) located at some \( UAP \), where \( U \Lambda^2 U^\top \) represents the SVD of \( W^{**} \) \((W^{**})^\top \) and \( r = \text{rank}[W^{**}] \).

3. \( W^{**} \) will have at most \( r \) nonzero columns, while \( W^* \) can have any number in \( \{r, \ldots, \kappa\} \).

Although this result applies to relatively simplistic affine decoders, it nonetheless highlights a couple interesting principles. First, the diagonalization of \( \Sigma_x \) collapses the space of globally minimizing solutions to a subset of the original. While the consequences of this may be muted with the fully affine decoder model where any of these solutions are equally good, we surmise that with more sophisticated parameterizations this partitioning of the energy landscape to distinct basins-of-attraction could potentially introduce suboptimal local extrema.

But there is a second, potentially-advantageous counter-affect as well. Specifically, even if \( W \) is overparameterized, meaning that \( \kappa \) is unnecessarily large, there exists an inherent mechanism to prune superfluous columns to zero. Regardless, we have shown that both variants of the affine decoder model lead to reasonable probabilistic PCA-like objectives regardless of how overparameterized \( \mu_z \) and \( \Sigma_x \) happen to be.

### 3 Partially Affine Decoder and Robust PCA

Thus far we have considered tight limitations on the complexity allowable in the functional forms of both \( \mu_z \) and \( \Sigma_x \), while \( \mu_z \) and \( \Sigma_x \) were free-range variables granted arbitrary flexibility. We now turn our gaze to the case where \( \Sigma_x \) can be any parameterized, diagonal matrix\(^4\) while \( \mu_z \) remains restricted. Although this administers considerable capacity to the model at the potential risk of overfitting, we will soon see that the VAE is nonetheless able to self-regularize in a very precise sense: Global minimizers of the VAE objective will ultimately correspond with optimal solutions to

\[
\min_{L, S} n \cdot \text{rank}[L] + \|S\|_0, \quad \text{s.t. } X = L + S, \quad (10)
\]

\(^2\)While we omit details here, optimal solutions for both \( b \) and \( \lambda \) can be analyzed as well.

\(^3\)By disconnected we mean that, to traverse from one minimum to another, we must ascend the objective function at some point along the way.

\(^4\)A full covariance over \( x \) is infeasible given the high dimension, and can lead to undesirable degeneracies anyway.

---

4
where \( \| \cdot \|_0 \) denotes the \( \ell_0 \) norm, or a count of the number of nonzero elements in a vector or matrix. This problem represents the canonical form of robust principal component analysis (RPCA) \([4, 5]\), decomposing a data matrix \( X \) into low-rank principal factors \( L = UV \) and a sparse outlier component \( S \). In fact, if we were to replace the \( \ell_0 \) penalty with an \( \ell_2 \) norm, we would exactly recover one formulation of vanilla PCA, where by replacing the weighting factor \( n \) with different arbitrary scalars, the optimal solution will simply reflect principal subspaces of varying dimensions. That the complex, probabilistic VAE model shares any kinship with \((10)\) is seemingly quite remarkable.

Before elucidating this relationship, we require one additional technical caveat. Specifically, since \( \log 0 \) and \( \frac{1}{0} \) are both undefined, and yet we will soon require an alliance with degenerate (or nearly so) covariance matrices that mimic the behavior of sparse and low-rank factors through log-det and inverse terms, we must place the mildest of restrictions on the minimal allowable singular values of \( \Sigma_x \) and \( \Sigma_z \). For this purpose we define \( S_{\alpha}^m \) as the set of \( m \times m \) covariance matrices with singular values all greater than or equal to \( \alpha \), and likewise \( S_{\alpha}^m \) as the subset of \( S_{\alpha}^m \) containing only diagonal matrices. We also define \( \text{supp}_\alpha(x) = \{ i : |x_i| > \alpha \} \), noting that per this definition, \( \text{supp}_\alpha(x) = \text{supp}(x) \), meaning we recover the standard definition of support: the set of indices associated with nonzero elements.

Given the affine assumption from above, and the mild restriction \( \Sigma_x \in \tilde{S}_\alpha^d \) and \( \Sigma_z \in \tilde{S}_\alpha^c \) for some small \( \alpha > 0 \), the resulting constrained VAE minimization problem can be expressed as

\[
\min_{\theta, \phi} \mathcal{L}(W, b = 0, \Sigma_x \in \tilde{S}_\alpha^d, \mu_z, \Sigma_z \in \tilde{S}_\alpha^c),
\]

where now \( \theta \) includes \( W \) as well as all the parameters embedded in \( \Sigma_x \), while \( \mu_z \) and \( \Sigma_z \) are parameterized as in Lemma 1. We have also set \( b = 0 \) merely for ease of presentation as its role is minor. We then have the following:

**Theorem 2** Suppose that \( X = \{x^{(i)}\}_{i=1}^n \) admits a feasible decomposition \( X = UV + S \) that uniquely\(^3\) optimizes \((10)\). Then for some \( \alpha \) sufficiently small, and all \( \alpha \in [0, \alpha] \), any global minimum \( \{W, \Sigma_x, \mu_z, \Sigma_z\} \) of \((11)\) will be such that

\[
\text{span}[\tilde{W}] = \text{span}[U] \quad \text{and} \quad \text{supp}_\alpha \left( \text{diag} \left( \Sigma_x \left( \mu_z \left[ x^{(i)} \right] \right) \right) \right) = \text{supp}[s^{(i)}]
\]

for all \( i \) provided that the latent representation satisfies \( \kappa \geq \text{rank}[U] \).

Several important remarks are warranted here regarding this result:

- Given \( \tilde{W}, \Sigma_x, \) and \( \mu_z \) as described, we can directly recover the generating low-rank \( L \) and sparse \( S \) by solving a simple linear system. Therefore if we can globally optimize the VAE objective, we can recover the correct latent representation.

- The requirements \( \Sigma_x \in \tilde{S}_\alpha^d \) and \( \Sigma_z \in \tilde{S}_\alpha^c \) do not portend the need for specialized tuning or brittleness of the result; these are merely technical conditions for dealing with degenerate covariances that occur near optimal solutions. While it might seem natural that \( \Sigma_z \) has diagonal elements pushed to zero in regions where near perfect data fit is possible, less intuitively, global optima of \((11)\) can be achieved with an arbitrarily small \( \Sigma_z \), e.g., \( \Sigma_z = \alpha I \) (see proof construction). Perhaps counterintuitively, this implies that in areas surrounding a global optimum, the VAE objective can resemble that of a regular AE. As we will discuss more below, desirable smoothing effects of integration over \( \Sigma_z \) occur elsewhere in the energy landscape while preserving extrema anchored at the correct latent representation.

- Even if \( \kappa \) is large, meaning \( \tilde{W} \) is possibly complete, the VAE will not overfit in the sense that there exists an inherent regulatory effect pushing \( \text{span}[\tilde{W}] \) towards \( \text{span}[U] \).

- If the globally optimal solution to \((10)\) is not unique (this is different from uniqueness regarding the VAE objective), then a low-rank-plus-sparse model may not be the most reasonable, parsimonious representation of the data to begin with, and exact recovery of \( L \) and \( S \) will not be

\(^3\)Obviously only \( L \) and \( S \) will be unique; the actual decomposition of \( L \) into \( U \) and \( V \) is indeterminate up to an inconsequential invertible transform.

\(^4\)Although somewhat cumbersome in print, the expression \( \hat{\Sigma}_x \left( \hat{\mu}_z \left[ x^{(i)} \right] \right) \) refers to \( \Sigma_x \) evaluated at \( \hat{\mu}_z \), where the latter is evaluated at \( x^{(i)} \), the \( i \)-th sample.
possible by any algorithm without further assumptions. More concretely, an arbitrary data point \( x(i) \in \mathbb{R}^d \) requires \( d \) degrees-of-freedom to represent; however, if the data succinctly adheres to the RPCA model, then for properly chosen \( U, V, \) and \( S \), we can have \( x(i) = Uv(i) + s(i) \), where \( \|v(i)\|_0 + \|s(i)\|_0 < d \). Arbitrary data in general position will never admit such a unique decomposition, and we should only expect such structure in data well-represented by our VAE model, or the original RPCA predecessor from (10).

- A number of celebrated results have stipulated conditions [4, 5] whereby global solutions of the convex relaxation into nuclear and \( \ell_1 \) norm components given by

\[
\min_{L, S} \sqrt{\nu} \cdot \text{rank}(L) + \|S\|_1, \quad \text{s.t.} \quad X = L + S,
\]

will equal global solutions of (10). While elegant in theory, and practically relevant given that (10) is discontinuous, non-convex, and difficult to optimize, the required conditions for this equivalence to hold place strong restrictions on the allowable structure in \( L \) and support pattern in \( S \). In practice these conditions can never be verified and are unlikely to hold, so an alternative modeling approach such as the VAE, which can be viewed as a smoothed version of (10) when an affine decoder mean is used (more on this later), remains attractive. Additionally, there is no clear way to modify (13) to handle nonlinear manifolds, which is obviously the bread and butter of the VAE.

We emphasize that these conclusions are not the product of an overly contrived situation, given that a

\[
\Sigma \]

will be produced. In the large-

\[
\text{regime then, global VAE and global AE solutions do in fact deviate,}
\]

which emerges when \( \Sigma_x \) is forced to zero, behaves under analogous conditions to Theorem 2.

**Corollary 1** Under the same conditions as Theorem 2, if we remove the \( \log \| \Sigma_x \| \) term and assume \( \Sigma_x = 0 \) elsewhere, then (11) admits a closed-form solution for \( \Sigma_x \) in terms of \( W \) and \( \mu_z \) such that minimizers of the VAE cost are minimizers of

\[
\mathcal{L}(W, \mu_z) = \sum_i \| x(i) - W \mu_z \left( x(i) \right) \|_0 \quad \text{in the limit } \alpha \to 0.
\]

From this result we immediately observe that minimization of (14) is just a constrained version of (10), exactly equivalent to solving

\[
\min_{L, S} \| S \|_0, \quad \text{s.t.} \quad X = L + S, \quad \text{rank}(L) = \kappa.
\]

This expression immediately exposes one weakness of the AE; namely, if \( \kappa \) is too large, there is no longer any operation in place to prune away unnecessary dimensions, and the trivial solution \( L = X \) will be produced. In the large-\( \kappa \) regime then, global VAE and global AE solutions do in fact deviate, ultimately because of the removal of the \( \log \| \Sigma_x \| \) term in the latter.

But there is also a more important, yet subtle, advantage of the VAE over both (15) and the original unconstrained RPCA model from (10). For both RPCA constructions, any feasible support pattern, even the trivial ones associated with non-interesting decompositions satisfying \( \|v(i)\|_0 + \|s(i)\|_0 \geq d \) for some \( i \), will necessarily represent a local minimum, since there is an infinite gradient to overcome to move from a zero-valued element of \( S \) to a nonzero one.

Unlike these deterministic approaches, the behavior of the VAE reflects a form of differential smoothing that rids the model of many of these pitfalls while retaining desirable minima that satisfy (12).

\footnote{A more rudimentary form of this smoothing has been observed in much simpler empirical Bayesian models derived using Fenchel duality [24].}
dependent on other variables and a constant scale factor of $-\log \alpha$, then a lower bound on the VAE objective associated with each sample index $i$ behaves like

$$\text{rank}[W] + \text{supp}_a \left( \text{diag} \left[ \Sigma_x \left( \mu_x \left( x^{(i)} \right) \right) \right] \right),$$

(16)

but crucially, this behavior lasts only as long as (16) is strictly less than $d$ and $\Sigma_z$ is forced to be small or degenerate. In contrast, when the value is at or above $d$, (16) no longer reflects the energy function, which becomes relatively flat because of smoothing via $\Sigma_z$, avoiding the pitfalls described above.

To situate things in the narrative of (10), the VAE can be viewed (at least to first order approximation) as minimizing the alternative objective function

$$\sum_i \text{rank} \left[ LL^\top + \text{diag} \left( s^{(i)} \right)^2 \right] \geq n \cdot \text{rank} \left[ L \right] + \| S \|_0,$$

(17)

or a smooth surrogate thereof, over the constraint set $X = L + S$. The advantages of this upper bound are substantial: As long as a unique solution exists to the RPCA problem, the globally optimal solution with $\| v^{(i)} \|_0 + \| s^{(i)} \|_0 < d$ for all $i$ will be unchanged; however, any feasible solution with $\| v^{(i)} \|_0 + \| s^{(i)} \|_0 \geq d$ will have a constant cost via the expression on the left of the inequality, truncating the many erratic peaks that will necessarily occur with the energy on the right-hand side.

In fact, away from the strongly attractive basins of optimal VAE solutions, the KL term from (2) is likely to push $\Sigma_z$ more towards

$$\arg \min_{\Sigma_z > 0} \mathbb{E}_q \left[ q_\phi \left( z|x \right) \| p(z) \right] \equiv \arg \min_{\Sigma_z > 0} \text{tr} \left[ \Sigma_z \right] - \log |\Sigma_z| = I.$$

(18)

Experiments presented in Section 5 confirm that this is indeed the case. And once $\Sigma_z$ moves away from zero, it will generally contribute a strong smoothing effect via the expectation in (2). However, there exists an important previously unobserved caveat here: If the decoder mean function is excessively complex, it can potentially squash all effects from $\Sigma_z$, leading to undesirable degenerate solutions with no function value as described next.

### 4 Degeneracies Arising from a Flexible Decoder Mean

In this section we consider the case where $\mu_z$ is finally released from its affine captivity to join with posterior colleagues in the wild. That simultaneously granting $\mu_z$, $\Sigma_z$, $\mu_x$, and $\Sigma_z$ unlimited freedom leads to overfitting may not come as a surprise; however, it turns out that even if the latter three are severely constrained, overfitting will not be avoided when $\mu_z$ is over-parameterized. This is because, at least at a high level, the regulatory effect of $\Sigma_z$ can be squashed in these situations leading to the following:

**Theorem 3** Suppose $\kappa = 1$ (i.e., a latent dimension of only one), $\Sigma_x = \lambda_x (a \text{ scalar})$, $\mu_x = a^\top x$ for some fixed vector $a$, $\Sigma_x = \lambda_x I$, and $\mu_z$ is an arbitrary piecewise linear function with $n$ segments. Then the VAE objective is unbounded from below at a trivial solution $\{ \lambda_x, a, \lambda_z, \mu_z \}$ such that the resulting posterior mean $\hat{\mu}_z(z; \theta)$ will satisfy $\hat{\mu}_z(z; \theta) \in \{ x^{(i)} \}_{i=1}^n$ with probability one for any $z$.

In this special case, $\Sigma_x$, $\Sigma_z$, and $\mu_z$ are all simple affine functions and the latent dimension is minimal, and yet an essentially useless, degenerate solution can arbitrarily optimize the VAE objective. This occurs because the VAE has limited power to coral certain types of heavily over-parameterized decoder mean functions, even when all other degrees of freedom are constrained, and in this regime the VAE essentially has no advantage whatsoever over a traditional autoencoder (its natural self-regulatory agency may sometimes break down). In contrast, as we saw in a previous section, there is no problem taming the influences of an unlimited latent representation (meaning $\kappa$ is large, e.g., even $\kappa > n$) and its huge, attendant parameterized mean function, provided the latter is affine, as in $\mu_z = W z + b$.

Indeed then, the issue is clearly not the degree of over-parameterization in $\mu_z$ per se, but the actual structures in place. And the key problem is that, at least in some situations, the model can completely override the regulatory mechanism of the KL term, pushing the latent variances towards zero. For example, in the context of Theorem 3, the piecewise linear structure of $\mu_z$ allows the decoder to
act much like a vector quantization process, pushing \( z \) towards training samples \( x^{(i)} \). And because this will lead to perfect reconstruction error if the correct sample index \( i \) is found for a particular \( z^{(i)}, \Sigma_{x} = \lambda_{i} I \approx 0 \) serves as a reasonable characterization of posterior uncertainty, pushing \( p(x^{(i)}|z^{(i)}) \rightarrow \delta(x^{(i)}) \) provided that \( z^{(i)} \approx \mu_{x}(x^{(i)}, a) = a^{T}x^{(i)} \), or \( \Sigma_{x} = \lambda_{i} \) is not too large. This in turn leads to a useless, degenerate solution, either for the purposes of generating representative samples, or for outlier removal as we have described herein.

Of course an analogous issue exists with generative adversarial networks (GAN) as well, a popular competing deep generative model composed of a generator network analogous to the VAE decoder, and a discriminator network that replaces the VAE encoder in a loose sense [12]. If the generator network merely learns a segmentation of \( z \)-space such that all points in the \( i \)-th partition map to \( x^{(i)} \), the discriminator will be helpless to avert this degenerate situation even in principle. But there is an asymmetry when it comes to the GAN discriminator network and the VAE encoder: Over-parameterization of the former can be problematic (e.g., it can easily out-wit an affine or other proportionally simple generator), but the latter not so, at least in the sense that a highly flexible VAE encoder need not bully a simple decoder into trivial solutions as we have shown in previous sections.

5 Experiments

Theoretical analysis of simplified cases can be viewed as a powerful vehicle for generating accessible hypotheses that describe likely behavior in more complex, practical situations. In this section we empirically evaluate three concrete hypotheses that directly emanate from our previous analyses. Each of these have wide-ranging consequences in terms of how VAE models should be applied and interpreted in practice:

(i) When the decoder mean function is allowed to be nonlinear, the VAE should behave like a nonlinear extension of RPCA, but with natural regularization mechanisms in place that help to avoid local minima and/or overfitting to outliers. It is therefore likely to outperform either RPCA algorithms or an AE on diverse manifold recovery/outlier discovery problems unrelated to the generative modeling tasks for which the VAE was originally designed.

(ii) If the VAE latent representation \( z \) is larger than needed (meaning its dimension \( \kappa \) is higher than the underlying data manifold dimension), we have proven that unnecessary columns of \( W \) in a certain affine decoder mean model \( \mu_{x} = Wz + b \) will automatically be pruned as desired. Analogously, in the arbitrary nonlinear case we would then expect that columns of the weight matrix from the first layer of the decoder mean function should be pushed to zero, again effectively pruning away the impact of any superfluous elements of \( z \).

(iii) Although originally promoted as a probabilistic generative model, when granted sufficient capacity in both \( \mu_{x}(\mu_{x}[x]) \) and \( \Sigma_{x} \) to model inliers and outliers respectively, the VAE should have a tendency to push elements of the encoder covariance \( \Sigma_{z} \) to exactly zero, overriding the KL regularizer that would otherwise push these values towards one. In doing so, the VAE’s value as a true (or non-degenerate) generative model is undermined; however, its utility as a nonlinear outlier removal tool is dramatically enhanced per Hypothesis (i) above.

5.1 Hypothesis (i) Evaluation

If our theory is generally applicable, then a VAE with suitable parameterization should be able to significantly outperform an analogous deterministic AE (i.e., the VAE with \( \Sigma_{x} = 0 \)) on the task of recovering data points drawn from a low-dimensional nonlinear manifold, but corrupted with gross outliers. We demonstrate this VAE capability here for the first time across an array of manifold dimensions and corruption percentages, recreating a nonlinear version of what are commonly termed phase transition plots in the RPCA literature [4, 8, 15, 24]. These plots evaluate the reconstruction quality of competing algorithms for every pairing of subspace dimension and outlier ratio, creating a heat map that differentiates success and failure regions.

Of course explicit knowledge of the ground-truth low-dimensional manifold is required to accomplish this. With linear subspaces it is trivial to generate appropriate synthetic data by simply creating two low-rank random matrices \( U \in \mathbb{R}^{d \times \kappa} \) and \( V \in \mathbb{R}^{n \times \kappa} \), a sparse outlier matrix \( S \), and then computing \( X = L + S \) with \( L = UV \). Algorithms are presented with \( X \) and attempt to reconstruct \( L \). We generalize this process to the nonlinear regime in the following way.
Data Generation: First we draw \( n \) low-dimensional samples \( z^{(i)} \in \mathbb{R}^\kappa \) from \( \mathcal{N}(z; 0, I) \) and pass them through a 3-layer network with ReLU activations [19]. The layer sizes are 1000, 2000, and \( d \) respectively, each created using the initialization procedure from [13]. The \( d \)-dimensional output is denoted as \( l^{(1)} \), the collection of which form a matrix \( L \), with columns effectively lying on a \( \kappa \)-dimensional manifold. This network can be viewed as a ground-truth decoder, projecting \( z^{(i)} \) to clean samples \( l^{(i)} \).

But we must also ensure that there exists a ground-truth encoder that can correctly invert the decoder (otherwise we cannot be sure that our VAE structure is even an appropriate model, unlike the linear RPCA case where this is trivially satisfied). We learn this inverse mapping by training something like an inverted autoencoder. Basically, the decoder described above now acts as an encoder, to which we append a new \( \kappa \)-dimensional manifold. This network can be viewed as a ground-truth decoder, projecting \( z^{(i)} \) to clean samples \( l^{(i)} \).

We could train the entire system end-to-end to accomplish this, which should be easy since \( \kappa \ll d \); however, we found that although \( z^{(i)} = z^{(i)} \) is obviously not difficult to achieve, the corresponding learned samples \( l^{(i)} \) are pushed to very near a low-rank matrix when assembled into \( L \). This would imply that non-linear manifold learning is not actually required. To circumvent this issue, we instead held the initial \( \kappa-1000-2000-d \) structure fixed, which ensures that the rank of \( L \) cannot be altered, and only train the second half using a standard \( \ell_2 \) loss. In doing so we are able to obtain an \( L \) matrix, extracted from the middle layer, that is both (i) not well-represented by a low-rank approximation, and (ii) does lies on a known low-dimensional non-linear manifold. And the learned decoder from this process implicitly becomes the ground-truth encoder underlying the data structure.

Once \( L \) has been created in this manner, we then generate noisy samples \( X \) by randomly corrupting \( 100 \cdot \nu \% \) of the entries, replacing the original value with samples from a standardized Gaussian distribution. The resulting data matrix is fed to a VAE formed from the inverted \( d-2000-1000-1000-2000-d \) structure to form the encoder and decoder mean functions, but randomly initialized so as not to copy the ground-truth template. The encoder covariance shares the first two layers, and also has an exponential layer appended at the output to produce only positive values, consistent with the design in [16]. We choose \( d = 100 \), and vary the manifold dimension from \( \kappa = 2, 4, \ldots, 20 \) while the outlier ratio ranges as \( \nu = 0.05, 0.10, \ldots, 0.50 \). In each case we measure the normalized MSE recovering the true \( L \).

Results: We compare the VAE against the corresponding AE, and include the ground-truth manifold within the parameterization of the cascaded encoder/decoder mean networks \( \mu_\mu(x) \) for all models. Therefore perfect reconstruction is theoretically possible by either approach provided that outlier contributions can be mitigated. Note that once \( \Sigma_x = 0 \) for the AE, at every sample \( \Sigma_x \) can be solved for in closed form as

\[
\Sigma_x^{[j]} = \left( x_j^{[j]} - \mu_{x_j}^{[j]} \right)^2 \quad \text{for} \quad j = 1, \ldots, d \text{ assuming sufficient capacity}
\]
5.2 Hypothesis (ii) Evaluation

**MNIST Results:** We train analogous AE and VAE models with nonlinear decoder mean networks on the MNIST dataset of handwritten digit images \[17\] as \( \kappa \) is varied. We use all \( n = 70000 \) samples, each of size \( 28 \times 28 \). The encoder is a 4-layer ReLU network \((d-1000-500-250-\kappa)\), where \( d = 28 \times 28 = 784 \). We draw values of \( \kappa \) from \( \{3, 5, 8, 10, 15, 20, 25, 30, 35, 40\} \). Also, \( \mu_z \) and \( \Sigma_z \) share the first three hidden layers, but have separate output layers, similar to \[16\]. The decoder is a 4-layer network which simply reverses the encoder structure.

The first layer of the decoder mean network can be expressed as \( h_1 = W_1^\top z + b_1 \) (before the nonlinearity), which in isolation is equivalent to the affine decoder mean model. A nonzero column in \( W_1 \) implies that the corresponding dimension in \( z \) is actually useless for any subsequent representation. Therefore, we can estimate the intrinsic dimension of the latent code by counting the number of nonzero columns in \( W_1 \). Of course in practice, it is unlikely that a column of \( W_1 \) converges all the way to exactly 0 via SGD. So we define a simple threshold by \( \text{thr} = 0.01 \times \max_{\kappa} ||w_j||_2 \). If \( ||w_j||_2 < \text{thr} \), we regard it as a zero column.

Figure 2 displays the number of nonzero columns produced by each model averaged across 10 trials. We observe that when \( \kappa > 15 \), the number of nonzero columns plateaus for the VAE consistent with Hypothesis (ii). In contrast, with the AE model the number is always equal to \( \kappa \) since there is no agency for self-regularization. Of course in this situation, we do not have access to ground truth for determining what the optimal manifold dimension should be. For this type of evaluation we turn to synthetic data.

**Synthesized Data Results:** Our data generation process is as follows. We randomly sample \( z \) from a 20-dimensional normal Gaussian distribution, which means that the ground-truth manifold dimension per Corollary 1. We then plug this value into the AE cost, effectively optimizing \( \Sigma_z^{(i)} \) out of the model making it entirely deterministic. For direct comparison, we apply the same procedure to the VAE. As an additional baseline, we also apply the convex RPCA formulation from 13 to the same corrupted data.

Results are shown in Figure 1, where the VAE outperforms both RPCA and AE by a wide margin. Perhaps most notably, the VAE outperforms the regular AE, supporting our theory that the smoothing effect of integrating over \( \Sigma_z \) has immense practical value in avoiding bad minimizing solutions through its unique form of differential regularization. Even though by design both network structures are equivalent in terms of their predictive capacity, only the VAE is able to capitalize on the regularizing effect of \( \Sigma_z \) to actually reach a good solution in challenging conditions. In contrast, we found that in many cases the AE had a lower MSE with respect to the noisy matrix \( X \) than the clean \( L \), a sign that it was stuck at a useless extrema which overfit the data. This confirms Hypothesis (i) and suggests that VAEs are a viable candidate for replacing existing RPCA algorithms \[4, 8, 15, 24\] in regimes where a single linear subspace is an inadequate signal representation.
Table 1: Number of nonzero columns in the VAE decoder mean first-layer weights \(W_1\) with different encoder and decoder depths on the synthesized dataset. The correct dimension is 20, and provided that the VAE model is sufficiently complex, the correct estimate is obtained. For an analogous AE, the number is 30 in all cases.

| \(N_e\) | \(N_d = 0\) | \(N_d = 1\) | \(N_d = 2\) | \(N_d = 3\) |
|---|---|---|---|---|
| 0  | 30.0 | 21.1 | 21.0 | 20.0 |
| 1  | 30.0 | 21.0 | 20.0 | 20.0 |
| 2  | 30.0 | 21.0 | 20.0 | 20.0 |
| 3  | 30.0 | 20.4 | 20.0 | 20.0 |

is 20. To create \(x\) we pass \(z\) through a neural network via the structure \(z(20)\rightarrow200\rightarrow200\rightarrow x(400)\). Since our VAE model should not know the ground-truth manifold dimension in advance, we set the dimension of the unknown latent representation to be \(\kappa = 30\). We try different encoder and decoder depths and apply the VAE using the network structure \(x(400)\rightarrow E_1(200)\rightarrow E_{N_e}(200)\rightarrow z(30)\rightarrow D_1(200)\rightarrow \cdots D_{N_d}(200)\rightarrow x(400)\) for both mean and covariance networks, where \(N_e\) is the number of hidden layers in the encoder, and \(N_d\) is the corresponding number for the decoder.

If the VAE has the ability to find the true underlying manifold dimension, then the number of nonzero columns in the decoder mean network first-layer weights should be 20. Table 1 reports these numbers (after applying the same thresholding rule as before), where we have run 10 trials for every setting and averaged the results. When there is no hidden layer in the decoder, which implies that the decoder is affine, all the columns are nonzero, since the network is overly-simplistic and all degrees of freedom are being utilized. However, once we increase the depth, especially of the decoder, the number of nonzero columns tends to become 20, which is the correct ground-truth manifold dimension, directly supporting Hypothesis (ii). In contrast, for the corresponding AE model, the number of nonzero columns is always 30 regardless of the network size.

### 5.3 Hypothesis (iii) Evaluation

We create histograms of all diagonal elements of \(\{\Sigma_z^{(i)}\}_{i=1}^n\) as noise ratios and manifold dimensions vary under the same conditions described in Section 5.1. The results are plotted in Figure 3, where we observe that on easier problems, meaning smaller outlier ratios and/or lower manifold dimension, the diagonal elements of \(\Sigma_z^{(i)}\) are forced towards zero. For this to happen, \(\mu_z(\mu_z(x))\) must accurately fit the inlier positions while \(\Sigma_z\) must reflect the outlier support where needed. This situation allows the data fit term to overpower the KL regularizer that would otherwise prevent \(\Sigma_z^{(i)}\) from ever being rank-deficient in the region surrounding a global optima of the VAE energy function. In contrast, for harder problems (i.e., higher outlier ratio and/or manifold dimension), tightly fitting the data becomes difficult and the KL regularizer pushes \(\Sigma_z^{(i)}\) diagonal values more towards one given the influence of (18) in affecting global solutions.

Consistent with our theory, these results then imply a rather curious behavior of the VAE: If \(\mu_z(\mu_z(x))\) is suitably parameterized to model inlier samples, and \(\Sigma_z\) is sufficiently complex to model outlier locations, then \(\Sigma_z\) will be pushed towards zero possibly compromising the VAE model’s ability to act as a non-degenerate generative model. It may still capture manifold structure, but when attempting to generate new samples they may not be distributed on or around the manifold in the same way as the training set. However, we can nonetheless enjoy perfect recovery of original clean training data samples. In contrast, if \(\mu_z(\mu_z(x))\) and/or \(\Sigma_z\) are inadequate, or alternatively, we provide a lower bound for allowable values of \(\Sigma_z\), then such degeneracies are avoided at the expense of exact recovery of \(L\) from \(X\).

### 6 Discussion

Although originally developed as a viable deep generative model or tractable bound on the data likelihood, in this work we have revealed certain behaviors of the VAE that are not obvious from first inspection. For example, in addition to its putative role in driving diversity into the learned generative process, the latent covariance \(\Sigma_z\) also serves as an important smoothing mechanism that
Figure 3: Histograms of $\{\Sigma_i^{(i)}\}_1^n$ diagonal elements as noise ratios and manifold dimensions are varying for the corrupted manifold recovery experiment corresponding with Figure 1. The three columns represent noise ratios of 0.0, 0.25, and 0.50 from left to right. The four rows represent manifold dimensions of $\kappa \in \{2, 8, 14, 20\}$ from top to bottom. When the noise ratio and the manifold dimension are both very low (easy case), almost all the $\Sigma_i^{(i)}$ diagonal elements become very close to 0, which means the network has nearly perfectly fit the inliers and rejected the outliers, consistent with theory. As the noise ratio and manifold dimension increase (harder case), some elements of $\Sigma_i^{(i)}$ gradually drift away from 0 and becomes very close to 1; in this regime the VAE has not perfectly modeled all of the data, and the KL penalty pushes these covariances towards the value minimizing the KL term. Note that on the top row, there exists a large spike at zero that is difficult to visualize. Also, as we move from top to bottom, the number of elements in the histograms ($n \times \kappa$) increases proportional to the increase in the dimensionality of the latent $z$.

Appendix A — Additional MNIST Dataset Experiment

Here we examine practical denoising of MNIST data corrupted with outliers using a VAE model. Outliers are added to MNIST handwritten digit data [17] by randomly replacing from 5% to 50% of the pixels with a value uniformly sampled from [0, 255] to create $X$. The encoder is the same as in Section 5.2, i.e., a 4-layer ReLU network (d-1000-500-250-$\kappa$), where we choose $\kappa = 30$ for the dimension of $z$. We train a VAE using both $\tau = 1$ and $\tau = 5$ latent samples $\{z^{(i)}\}_{t=1}^\tau$ for each $x^{(i)}$, observing that the latter, which more closely approximates the posterior, should perform significantly better.

We compare the VAE against convex RPCA on the task of recovering the original, uncorrupted digits. Note that RPCA is commonly used for unsupervised cleaning of this type of data [9], and MNIST is known to have significant low-rank structure [18] as shown in Figure 4(a). Regardless, we observe in Figure 4(b) that the VAE performs significantly better in terms of normalized MSE by capturing additional manifold details that deviate from a purely low-rank representation. Furthermore, we hypothesize that using extra latent samples (the $\tau = 5$ case) may work better on outlier removal tasks given the strong need for accurate smoothing of the VAE objective as described previously.
Appendix B — Proof of Lemma 1

Under the stated assumptions, the VAE cost can be simplified as

\[ \mathcal{L}(\theta, \phi) = \sum_i \left\{ \mathbb{E}_{q_\phi(z|x^{(i)})} \left[ \frac{1}{\lambda} \left\| x^{(i)} - Wz - b \right\|_2^2 + d \log \lambda \right] + \text{tr} \left[ \Sigma_z^{(i)} \right] - \log \left| \Sigma_z^{(i)} \right| + \left\| \mu_z^{(i)} \right\|^2_2 \right\} \]

\begin{align*}
&= \sum_i \left\{ \frac{1}{\lambda} \left\| x^{(i)} - W\mu_z^{(i)} - b \right\|_2^2 + \frac{1}{\lambda} \text{tr} \left[ \Sigma_z^{(i)} W^T W \right] + d \log \lambda \\
&\quad + \text{tr} \left[ \Sigma_z^{(i)} \right] - \log \left| \Sigma_z^{(i)} \right| + \left\| \mu_z^{(i)} \right\|^2_2 \right\}, \\
&\quad (19)
\end{align*}

where \( \mu_z^{(i)} \triangleq \mu_z(x^{(i)}; \phi) \) and \( \Sigma_z^{(i)} \triangleq \Sigma_z(x^{(i)}; \phi) \). Given that

\[ \log |AA^T| = \arg \inf_{\Gamma \succ 0} \text{tr} \left[ AA^T \Gamma^{-1} \right] + \log |\Gamma|, \quad (20) \]

when optimization is carried out over positive definite matrices \( \Gamma \), minimization of (19) with respect to \( \Sigma_z^{(i)} \) leads to the revised objective

\begin{align*}
\mathcal{L}(\theta, \phi) \equiv \sum_i \left\{ \frac{1}{\lambda} \left\| x^{(i)} - W\mu_z^{(i)} - b \right\|_2^2 + \log \left| \frac{1}{\lambda} W^T W + I \right| + d \log \lambda + \left\| \mu_z^{(i)} \right\|^2_2 \right\}, \\
= \sum_i \left\{ \frac{1}{\lambda} \left\| x^{(i)} - W\mu_z^{(i)} - b \right\|_2^2 + \log \left| \frac{1}{\lambda} W^T W + \lambda I \right| + \left\| \mu_z^{(i)} \right\|^2_2 \right\}, \\
&\quad (21)
\end{align*}

ignoring constant terms. This expression only requires that \( \Sigma_z^{(i)} = \left[ \frac{1}{\lambda} W^T W + I \right]^{-1} \), or a constant parameterization, independent of \( x^{(i)} \). Similarly we can optimize over \( \mu_z^{(i)} \) in terms of the other variables. This is just a ridge regression problem, with optimal solution

\[ \mu_z^{(i)} = W^T \left( \lambda I + WW^T \right)^{-1} (x^{(i)} - b), \quad (22) \]

or a simple linear function of \( x^{(i)} \). Hence as long as the parameterization of both \( \mu_z^{(i)} \) and \( \Sigma_z^{(i)} \) allows for arbitrary affine functions as stipulated in the lemma statement, these optimal solutions are
feasible. Plugging (22) into (21) and applying some basic linear algebra, we arrive at
\[
L(\theta, \phi) \equiv \sum_i \left( x^{(i)} - b \right)^\top \left( \sum_i \left( x^{(i)} - b \right) + n \log |WW^\top + \lambda I| \right). \tag{23}
\]

Finally, in the event that we enforce that \( \Sigma^{(i)} \) be diagonal, (21) must be modified via
\[
\Sigma^{(i)} = \left[ \frac{1}{d} \text{diag} \left( \text{diag} \left( \lambda \right) \right) \right]^{-1} = \sum_j \log \left( \lambda + \| \bar{w} \cdot j \|_2^2 \right) - \kappa \log \lambda, \tag{24}
\]
where the \text{diag}[\cdot] operator converts vectors to diagonal matrices, and a matrix to a vector formed from its diagonal (just as in the Matlab computing environment), leading to the stated result.

### Appendix C — Proof of Theorem 1

First, for part 1 on the theorem, given that \( WRR^\top W^\top = WPP^\top W^\top = WW^\top \) for any rotation \( R \) and permutation \( P \), then obviously if \( W^* \) is a minimum of (5), \( W^* R \) and \( W^* P \) must also be. Likewise, since \( \sum_j \log (\lambda + \|w_j\|_2^2) \) is invariant to the order of the summation, then if \( W^{**} \) is a minimum of (7), \( W^{**} P \) must be as well.

We also have that
\[
L_{sep}(W^{**}, b, \lambda) = \sum_i \Omega^{(i)}(W^{**}, b, \lambda I) + n \left[ \sum_j \log \left( \lambda + \|w^*_j\|_2^2 \right) + (d - \kappa) \log \lambda \right]
\]
where the second inequality follows from the fact that \( W^* \) is an optimal solution to (5). The first inequality stems from Hadamard’s inequality \([10]\) applied to
\[
\frac{1}{n} (W^{**})^\top W^{**} + I = M^\top M
\]
for some square matrix \( M \) of appropriate dimension. This results in
\[
\log \left[ \frac{1}{n} (W^{**})^\top W^{**} + I \right] = 2 \log |M| \leq 2 \log \left( \prod_j \|m_i\|_2 \right) = \log \left( \prod_j (1 + \frac{1}{\lambda} \|w^*_j\|_2^2 \right),
\]
with equality iff \( M^\top M \) is diagonal. We can further manipulate the log-det term in (25) via
\[
n \log \left| \lambda I + W^* R (W^* R)^\top \right| = \log \left[ \frac{1}{n} (W^* R)^\top W^* R + I \right] + d \log \lambda
\]
\[
= \log \left[ \frac{1}{n} U \Lambda V^\top R \right] U \Lambda V^\top R + I \right] + d \log \lambda
\]
\[
= \log \left[ \frac{1}{n} R^\top V \Lambda^2 V^\top R + I \right] + d \log \lambda,
\]
where \( U \Lambda V^\top \) is the SVD of \( W^* \). Now if we choose \( R = V \) and define \( W \triangleq WW^\top \), then \( \Lambda_{jj} = \|w_j\|_2^2 \) and this expression further reduces via
\[
\log \left[ \frac{1}{n} R^\top V \Lambda^2 V^\top R + I \right] + d \log \lambda = \sum_j \log \left( \lambda + \frac{1}{\lambda} \Lambda_{jj} \right) + d \log \lambda
\]
\[
= \sum_j \log \left( \lambda + \|w_j\|_2^2 \right) + (d - \kappa) \log \lambda. \tag{28}
\]
Of course we cannot have
\[
\sum_i \Omega^{(i)}(W^{**}, b, \lambda I) \geq \sum_i \log (\lambda + \|w^{**}_j\|_2^2) + (d - \kappa) \log \lambda
\]
otherwise \(W^{**}\) would not be a minimum of \((7)\). Therefore, \(W\) must also be a minimum of \((7)\), from which the remaining parts of \((9)\) immediately follows.

We next confront the arrangement of disconnected minima for part 2 of the theorem. It is not difficult to show that \((5)\), and by virtue of the analysis above \((7)\), will be uniquely minimized by \(U\) and \(A\) arising from the SVD of either \(W^{**}\) or equivalently \(W^{**}\). Let \(W^{**} = UAV^\top\) via such a decomposition. So any partitioning into disconnected minimizers must come at the hands of \(V\), which only influences the \(\sum_j \log (\lambda + \|w^{**}_j\|_2^2)\) term in \((7)\).

At stated above, if \(W^{**}\) is a minimum, then \(W^{**}P\) must also be a minimum. Assume for the moment that \(W^{**}\) is full column rank. There will obviously be \(r!\) unique permutations of its columns, with \(r = \text{rank}(W^{**})\). Moreover, any transition from some permutation \(P\) to another \(P'\) will necessarily involve some non-permutation-matrix rotation \(V\). Given our assumption of distinct eigenvalues, this will ensure that
\[
\frac{1}{2}(W^{**})^\top W^{**} + I = \frac{1}{2}V\Lambda^2V^\top + I
\]
is non-diagonal. While this will not increase \((5)\), it must increase \((7)\) when diagonalized by Hadamard’s inequality. Therefore every permutation will reflect a distinct, disconnected minimizer. If \(W^{**}\) also has \(\kappa - r\) zero-valued columns, then the resulting number of unique permutations increases to \(\frac{\kappa!}{(\kappa - r)!}\) by standard rules of combinatorics.

Finally, part 3 of the theorem follows directly from part 2: Given that any minimizer of \((7)\) must be of the form \(UAP\), then there cannot be more than \(r\) nonzero columns. In contrast, for \((5)\) we may apply any arbitrary rotation to \(W^*\), and hence all columns can be nonzero even if the rank is smaller than \(\kappa\).

### Appendix D – Proof of Theorem 2

The basic high-level strategy here is as follows: We first present a candidate solution that satisfies \((12)\) and carefully quantify the achievable objective function value for \(\alpha \in (0, \alpha]\), and \(\alpha\) small. We then analyze a lower bound on the VAE cost and demonstrate that no solution can do significantly better, namely, any solution that can match the performance of our original proposal must necessarily also satisfy \((12)\). Given that this is a lower bound, this implies that no other solution can both minimize the VAE objective and not satisfy \((12)\). We now proceed to the details.

Define \(\mu^{(i)}_z \triangleq \mu_z(x^{(i)}; \phi)\) and \(\Sigma^{(i)}_z \triangleq \Sigma_z(x^{(i)}; \phi).\) We first note that if \(z = \mu^{(i)}_z + S^{(i)}_z \epsilon,\) with \(S^{(i)}_z\) satisfying \(\Sigma^{(i)}_z = S^{(i)}_z (S^{(i)}_z)^\top,\) and \(\epsilon \sim p(\epsilon) = \mathcal{N}(\epsilon; 0, I),\) then \(z \sim q_\phi(z|x^{(i)}).\) With this reparameterization and
\[
\mu^{(i)}_z \triangleq \text{diag}([\Sigma^{(i)}_z]) \triangleq \nu(\mu^{(i)}_z + S^{(i)}_z \epsilon; \theta)
\]
for some function \(\nu\)
\[
S^{(i)}_z \triangleq f(x^{(i)}; \phi)
\]
for some function \(f,\)
\[
\mu^{(i)}_z \triangleq g(x^{(i)}; \phi)
\]
for some function \(g,\)
the equivalent VAE objective becomes
\[
\mathcal{L}(\theta, \phi) = \sum_i \mathbb{E}_{p(\epsilon)} \left[ (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon)^\top \left(\Sigma^{(i)}_z\right)^{-1} (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon) \right] + \mathbb{E}_{p(\epsilon)} \left[ \log \left| \Sigma^{(i)}_z \right| \right] + \text{tr} \left[ \Sigma^{(i)}_z \right] - \log \left| \Sigma^{(i)}_z \right| + \|\mu^{(i)}_z\|_2^2
\]
\[
= \sum_i \mathbb{E}_{p(\epsilon)} \left[ (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon)^\top \left(\Sigma^{(i)}_z\right)^{-1} (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon) \right] + \mathbb{E}_{p(\epsilon)} \left[ \log \left| \Sigma^{(i)}_z \right| \right] + \text{tr} \left[ \Sigma^{(i)}_z \right] - \log \left| \Sigma^{(i)}_z \right| + \|\mu^{(i)}_z\|_2^2
\]
\[
= \sum_i \mathbb{E}_{p(\epsilon)} \left[ (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon)^\top \left(\Sigma^{(i)}_z\right)^{-1} (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon) \right] + \mathbb{E}_{p(\epsilon)} \left[ \log \left| \Sigma^{(i)}_z \right| \right] + \text{tr} \left[ \Sigma^{(i)}_z \right] - \log \left| \Sigma^{(i)}_z \right| + \|\mu^{(i)}_z\|_2^2
\]
\[
= \sum_i \mathbb{E}_{p(\epsilon)} \left[ (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon)^\top \left(\Sigma^{(i)}_z\right)^{-1} (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon) \right] + \mathbb{E}_{p(\epsilon)} \left[ \log \left| \Sigma^{(i)}_z \right| \right] + \text{tr} \left[ \Sigma^{(i)}_z \right] - \log \left| \Sigma^{(i)}_z \right| + \|\mu^{(i)}_z\|_2^2
\]
\[
= \sum_i \mathbb{E}_{p(\epsilon)} \left[ (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon)^\top \left(\Sigma^{(i)}_z\right)^{-1} (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon) \right] + \mathbb{E}_{p(\epsilon)} \left[ \log \left| \Sigma^{(i)}_z \right| \right] + \text{tr} \left[ \Sigma^{(i)}_z \right] - \log \left| \Sigma^{(i)}_z \right| + \|\mu^{(i)}_z\|_2^2
\]
\[
= \sum_i \mathbb{E}_{p(\epsilon)} \left[ (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon)^\top \left(\Sigma^{(i)}_z\right)^{-1} (x^{(i)} - W\mu^{(i)}_z - W S^{(i)}_z \epsilon) \right] + \mathbb{E}_{p(\epsilon)} \left[ \log \left| \Sigma^{(i)}_z \right| \right] + \text{tr} \left[ \Sigma^{(i)}_z \right] - \log \left| \Sigma^{(i)}_z \right| + \|\mu^{(i)}_z\|_2^2
\]
when \( b = 0 \) as stipulated. For now assume that \( \kappa \), the dimension of the latent \( z \), satisfies \( \kappa = \text{rank}[U] \) (later we will relax this assumption).

### D.1 A Candidate Solution

Here we consider a candidate solution that, by design, satisfies (12). For the encoder parameters we choose

\[
\hat{\mu}_z^{(i)} = \pi^{(i)}, \quad \Sigma_z^{(i)} = \alpha I.
\]  

(33)

where \( \alpha \) is a non-negative scalar and \( \pi^{(i)} \) is defined in conjunction with a matrix \( \Psi \) such that

\[
\text{supp}_\alpha \left[ \mathbf{x}^{(i)} - \Psi \pi^{(i)} \right] = \text{supp} \left[ s^{(i)} \right]
\]

\[
\text{span} \left[ U \right] = \text{span} \left[ \Psi \right].
\]

(34)

All quantities in (33) can be readily computed via \( \mathbf{X} \) applied to an encoder module provided that \( \kappa = \text{dim}[\mathbf{z}] = \text{rank}[U] \) as stipulated, and sufficient representational complexity for \( \mu_z \) and \( \Sigma_z \). Additionally, for the encoder we only need to define the posterior moments at specific points \( x^{(i)} \), hence the indexing via \( i \) in (33).

In contrast, for the decoder we consider the solution defined over any \( z \) given by

\[
\hat{\mathbf{w}} = \Psi
\]

\[
\hat{\mu}_z \approx \hat{\mathbf{w}} z
\]

\[
\text{diag} \left[ \hat{\Sigma}_z \right] \approx \Lambda^{(h_x(z))}, \tag{35}
\]

where \( \Lambda^{(i)} \in \mathbb{R}^{d \times d} \) is a diagonal matrix with

\[
\Lambda^{(i)}_{jj} = \begin{cases} \alpha, & \text{if } s^{(i)} = 0, \\ 1, & \text{otherwise}, \forall j. \end{cases}
\]

(36)

and \( h_x : \mathbb{R}^\kappa \to \{1, \ldots, n\} \) is a function satisfying

\[
h_x(z) \triangleq \arg \min_{i \in \{1, \ldots, n\}} \| z - \pi^{(i)} \|_2. \tag{37}
\]

Again, given sufficient capacity, this function can always be learned by the decoder such that (35) is computable for any \( z \). Given these definitions, then the index-specific moments \( \hat{\mu}_z^{(i)} \) and \( \hat{\Sigma}_z^{(i)} \) are of course reduced to functions of \( \epsilon \) given by

\[
\hat{\mu}_z^{(i)} = \hat{\mu}_z (\hat{\mu}_z^{(i)} + \hat{\Sigma}_z^{(i)} \epsilon; \theta)
\]

\[
\hat{\Sigma}_z^{(i)} = \hat{\Sigma}_z (\hat{\mu}_z^{(i)} + \hat{\Sigma}_z^{(i)} \epsilon; \theta) \tag{38}
\]

We next analyze the behavior of (32) at this specially parameterized solution as \( \alpha \) becomes small, in which case by design all covariances will be feasible by design. For this purpose, we first consider the integration across all cases where \( \Sigma_x^{(i)} \) does not reflect the correct support, meaning \( \epsilon \notin S^{(i)} \), where

\[
S^{(i)} \triangleq \left\{ \epsilon : \left[ \Sigma_x^{(i)} \right]_{jj} = \alpha \iff s^{(i)} = 0, \forall j \right\}. \tag{39}
\]

With this segmentation in mind, the VAE objection naturally partitions as

\[
\mathcal{L}(\theta, \phi) = \sum_i \left\{ \mathcal{L}^{(i)}(\theta, \phi; \epsilon \notin S^{(i)}) + \mathcal{L}^{(i)}(\theta, \phi; \epsilon \in S^{(i)}) \right\} \tag{40}
\]

where \( \mathcal{L}^{(i)}(\theta, \phi; \epsilon \notin S^{(i)}) \) denotes the cost for the \( i \)-th sample when integrated across those samples not in \( S^{(i)} \), and \( \mathcal{L}^{(i)}(\theta, \phi; \epsilon \in S^{(i)}) \) is the associated complement.

\*The extension to arbitrary \( b \) is trivial but clutters the presentation.
D.2 Evaluation of $L(i)(\theta, \phi; \epsilon \notin S(i))$

First we define

$$\rho = \min_{i,j \in \{1, \ldots, n\}, i \neq j} \frac{1}{2} \|\pi(i) - \pi(j)\|_2^2,$$  \hspace{1cm} (41)$$

which is just half the minimum distance between any two distinct coefficient expansions. If any $z$ is within this distance of $\pi(i)$, it will necessarily be quantized to this value per our previous definitions. Therefore if $\|S_z(i)\|_2 < \rho$, we are guaranteed that the correct generating support pattern will be mapped to $\hat{\Sigma}_z(i)$, and so it follows that

$$P\left(\epsilon \notin S(i)\right) \leq P\left(\|\hat{S}_z(i)\|_2 > \rho\right) = P\left(\|\sqrt{\alpha}\|_2 > \rho\right) \hspace{1cm} (42)$$

at our candidate solution. We also make use of the quantity

$$\eta \triangleq \max_{i \in \{1, \ldots, n\}} \|x(i) - \Psi\pi(i)\|_2^2, \hspace{1cm} (43)$$

which represents the maximum data-fitting error. Then for the $i$-th sample we have

$$L(i)(\theta, \phi; \epsilon \notin S(i)) = \int_{\epsilon \notin S(i)} \left[ (x(i) - \tilde{W}\hat{\mu}_z(i) - \tilde{W}\tilde{S}_z(i)\epsilon) ^\top (\hat{\Sigma}_z(i))^{-1} (x(i) - \tilde{W}\hat{\mu}_z(i) - \tilde{W}\tilde{S}_z(i)\epsilon) + \log \hat{\Sigma}_z(i) + \frac{1}{2} \log \|\mu_z(i)\|_2^2 \right] p(\epsilon) d\epsilon \hspace{1cm} (44)$$

where the second inequality comes from setting $\hat{\Sigma}_z(i) = \alpha I$ (its smallest possible value) in the inverse term and $\hat{\Sigma}_z(i) = I$ (its largest value) in the log-det term. Next, given that

$$\|x(i) - \Psi\pi(i)\|_2^2 \leq \eta \hspace{1cm} (45)$$

it follows that the bound from (44) can be further reduced via

$$L(i)(\theta, \phi; \epsilon \notin S(i)) \leq \int_{\|\sqrt{\alpha}\|_2 > \rho} \left[ \frac{1}{\alpha} \eta + \kappa \alpha - \kappa \log \alpha + \|\pi(i)\|_2^2 \right] p(\epsilon) d\epsilon \hspace{1cm} (46)$$

where the second inequality holds based on the vector version of Chebyshev’s inequality, which ensures that

$$\int_{\|\sqrt{\alpha}\|_2 > \rho} p(\epsilon) d\epsilon = P(\|\sqrt{\alpha}\|_2 > \rho) \leq \frac{\eta}{\rho^2}. \hspace{1cm} (47)$$

Clearly then, as $\alpha$ becomes small, we have established that

$$L(i)(\theta, \phi; \epsilon \notin S(i)) \rightarrow O(1). \hspace{1cm} (48)$$
D.3 Evaluation of $\mathcal{L}(\theta, \phi; \epsilon \in S(i))$

In analyzing $\mathcal{L}(\theta, \phi; \epsilon \in S(i))$, we note that

$$
\int_{\epsilon \in S(i)} (x(i) - \hat{W} \hat{\mu}(i) z - \ldots) \, d\epsilon = 0
$$
on $L(\theta, \phi)$ and show that essentially any candidate solution violating the theorem conditions will be worse than (53).

$$\int (x(i) - \Psi \pi(i) - \sqrt{\alpha} \Psi \epsilon) \, d\epsilon
$$

$$\leq \int (x(i) - \Psi \pi(i)) \, d\epsilon + \text{tr} \left[ \Psi^\top \Psi \right]
$$

$$\leq \eta + \text{tr} \left[ \Psi^\top \Psi \right]
$$

$$= \Theta(1)
$$
given the alignment of $\Lambda(i)$ with zero-valued elements in $x(i) - \Psi \pi(i)$. Furthermore, the remaining terms in $\mathcal{L}(\theta, \phi; \epsilon \in S(i))$ are independent of $\epsilon$ giving

$$\int_{\epsilon \in S(i)} \left[ \log \left| \Sigma_z(i) \right| + \text{tr} \left[ \Sigma_z(i) \right] - \log \left| \Sigma_z(i) \right| + \| \hat{\mu}_z(i) \|^2 \right] \, d\epsilon
$$

$$= \left[ \log \left| \Lambda(i) \right| + \kappa \alpha - \kappa \log \alpha + \| \pi(i) \|^2 \right] \int_{\|\sqrt{\alpha} \epsilon\| < \rho} \, d\epsilon
$$

$$= \left[ (r(i) - \kappa) \log \alpha + \kappa \alpha + \| \pi(i) \|^2 \right] \int_{\|\sqrt{\epsilon}\| < \rho} \, d\epsilon
$$

$$= \left[ (r(i) - \kappa) \log \alpha \right] \int_{\|\sqrt{\epsilon}\| < \rho} \, d\epsilon + O(\alpha) + O(1),
$$

where

$$r(i) \triangleq \left\{ j : \Lambda(i)_{jj} = \alpha \right\} = d - \| s(i) \|_0.
$$

Therefore, since $\int_{\|\sqrt{\epsilon}\| < \rho} \, d\epsilon \rightarrow 1$ as $\alpha$ becomes small, we may conclude that

$$\mathcal{L}(\theta, \phi; \epsilon \in S(i)) \rightarrow \left( d - \kappa - \| s(i) \|_0 \right) \log \alpha + O(1),
$$

D.4 Compilation of Candidate Solution Cost

After combining (48) and (52) across all $i$ we find that

$$\mathcal{L}(\theta, \phi) \rightarrow \sum_i \left( d - \kappa - \| s(i) \|_0 \right) \log \alpha + O(1)
$$

for any $\alpha \in (0, \alpha]$ as $\alpha$ becomes small. If $d > \kappa + \| s(i) \|_0$, then this expression will tend towards minus infinity, indicative of an objective value that is unbounded from below, certainly a fertile region for candidate minimizers. Note that per the theorem statement, $L = UV$ and $S$ must represent a unique feasible solution to

$$\min_{L, S} d \cdot \text{rank}[L] + \| S \|_0 \quad \text{s.t.} \quad X = L + S.
$$

Given that each column $x(i)$ has $d$ degrees of freedom, then with $U$ fixed there will be an infinite number of feasible solutions $x(i) = Uv(i) + s(i)$ such that $\text{dim}[v(i)] + \| s(i) \|_0 = \kappa + \| s(i) \|_0 > d$ and a combinatorial number such that $k + \| s(i) \|_0 = d$. Therefore for uniqueness we require that $k + \| s(i) \|_0 < d$, so it follows that indeed $\mathcal{L}(\theta, \phi)$ will be unbounded from below as $\alpha$ and therefore $\alpha$ becomes small, with cost given by (53) as a candidate solution satisfying the conditions of the theorem.

Of course it still remains possible that some other candidate solution could exist that violates one of these conditions and yet still achieves (53) or an even lower cost. We tackle this issue next. For this purpose our basic strategy will be to examine a lower bound on $\mathcal{L}(\theta, \phi)$ and show that essentially any candidate solution violating the theorem conditions will be worse than (53).
D.5 Evaluation of Other Candidate Solutions

To begin, we first observe that if granted the flexibility to optimize \( \Sigma^{(i)} \) independently over all values of \( \epsilon \) inside the integral for computing \( \mathcal{L}(\theta, \phi) \), we immediately obtain a rigorous lower bound. For this purpose we must effectively solve decoupled problems of the form

\[
\inf_{\gamma > \alpha} \frac{c}{\gamma} + \log \gamma,
\]

(55)

to which the optimal solution is just

\[
\gamma^* = \xi(\alpha) \triangleq [c - \alpha]_+ + \alpha,
\]

(56)

where the operator \([ \cdot ]_+\) retains only the positive part of its argument, setting negative values to zero. Plugging this solution back into (55), we find that

\[
\inf_{\gamma > \alpha} \frac{c}{\gamma} + \log \gamma = \log \xi(\alpha) + O(1).
\]

(57)

In the context of our bound, this leads to

\[
\mathcal{L}(\theta, \phi) \geq \sum_i \left\{ \mathbb{E}_{\rho(\epsilon)} \left[ \sum_j \log \xi_\alpha \left( \left[ x_j^{(i)} - w_j \mu_j^{(i)} - w_j S_z^{(i)} \right]^2 \right) \right] + \right. \]

\[
\left. \text{tr} \left[ \Sigma_z^{(i)} \right] - \log \left| \Sigma_z^{(i)} \right| + \| \mu_z^{(i)} \|^2 + O(1) \right].
\]

(58)

From this expression, it is clear that the lowest objective value we could ever hope to obtain cannot involve arbitrarily large values of \( \Sigma_z^{(i)} \) and \( \mu_z^{(i)} \) since the respective trace and quadratic terms grow faster than log-det terms. Likewise \( \mu_z^{(i)} \) cannot be unbounded for analogous reasons. Therefore, optimal solutions to (58) that will be unbounded from below must involve the first term becoming small, at least over a range of \( \epsilon \) values with significant probability measure. Although the required integral admits no closed-form solution, we can simplify things further using refinements of the above bound.

For this purpose consider any possible candidate solution \( \hat{W} = \Psi \) and \( \hat{\mu}_z^{(i)} = \pi^{(i)} \) (not necessarily one that coincides with \( U \) and the optimal subspace), and define

\[
\Delta^{(i)}(\Psi, \pi) \triangleq \sup_{\alpha} \left[ x^{(i)} - \Psi \pi \right],
\]

(59)

Without loss of generality we also specify that

\[
S_z^{(i)} \triangleq \Xi_d^{(i)} D_z^{(i)},
\]

(60)

where \( \Xi_\cdot \in \mathbb{R}^{d \times \kappa} \) has orthonormal columns and \( D_z^{(i)} \) is a diagonal matrix with

\[
\left[ D_z^{(i)} \right]_{kk} = \xi_\sqrt{\pi} \left( \sigma_k^{(i)} \right),
\]

(61)

and \( \sigma^{(i)} = [\sigma_1^{(i)}, \ldots, \sigma_\kappa^{(i)}]^{\top} \in \mathbb{R}_+^{\kappa} \) is an arbitrary non-negative vector. Any general \( \Sigma_z^{(i)} = S_z^{(i)} \left( S_z^{(i)} \right)^{\top} \), with singular values bounded by \( \alpha \), is expressible via this format. We then reexpress

---

\( \text{Note that this is never possible in practice, even with an infinite capacity network for computing } \Sigma_z^{(i)}, \text{ since it would require a unique network for each data sample; however, it nonetheless serves as a useful analysis tool.} \)
(58) as
\[
L(\theta, \phi) \geq \sum_i \left[ \mathbb{E}_p(\epsilon) \left[ \sum_{j \in \Delta^{(i)}} \log \xi_{\alpha} \left( \left[ x_j^{(i)} - \psi_j^{(i)} - \psi_j^{(i)} \mathbf{D}^{(i)} \epsilon \right]^2 \right) \right] + \mathbb{E}_p(\epsilon) \left[ \sum_{j \notin \Delta^{(i)}} \log \xi_{\alpha} \left( \left[ \psi_j^{(i)} \mathbf{D}^{(i)} \epsilon \right]^2 \right) \right] + \text{tr} \left[ \mathbf{E}^{(i)} \left( \mathbf{D}^{(i)} \right)^2 \left( \mathbf{E}^{(i)} \right)^\top \right] - \log \left| \mathbf{E}^{(i)} \left( \mathbf{D}^{(i)} \right)^2 \left( \mathbf{E}^{(i)} \right)^\top \right| + \| \pi^{(i)} \|_2^2 \right] + O(1),
\]
(62)
\[
= \sum_i \left[ \mathbb{E}_p(\epsilon) \left[ \sum_{j \in \Delta^{(i)}} \log \xi_{\alpha} \left( \left[ x_j^{(i)} - \psi_j^{(i)} - \sum_k \bar{\psi}_{jk}^{(i)} \cdot \xi \sqrt{\sigma_k^{(i)}} \left( \sigma_k^{(i)} \right) \cdot \epsilon_k \right]^2 \right) \right] + \sum_k \xi_{\alpha} \left[ \left( \sigma_k^{(i)} \right)^2 \right] + \| \pi^{(i)} \|_2^2 \right] + O(1),
\]
(63)
where \( \bar{\psi}_{jk}^{(i)} \) is the \( k \)-th element of the vector \( \psi_j^{(i)} \). We can now analyze any given point \( \{ \mathbf{Y}, \pi^{(i)}, \mathbf{E}^{(i)}, \sigma^{(i)} \} \) as \( \alpha \) becomes small. The first term can be shown to be \( \Theta(1) \) with all other variables fixed, leading to the revised bound
\[
L(\theta, \phi) \geq \sum_i \left[ \mathbb{E}_p(\epsilon) \left[ \sum_{j \notin \Delta^{(i)}} \log \xi_{\alpha} \left( \left[ \sum_k \bar{\psi}_{jk}^{(i)} \cdot \xi \sqrt{\sigma_k^{(i)}} \left( \sigma_k^{(i)} \right) \cdot \epsilon_k \right]^2 \right) \right] - \sum_k \log \xi_{\alpha} \left[ \left( \sigma_k^{(i)} \right)^2 \right] \right] + \Theta(1),
\]
(64)
where the terms \( \sum_k \xi_{\alpha} \left[ \left( \sigma_k^{(i)} \right)^2 \right] \) and \( \| \pi^{(i)} \|_2^2 \) have also been absorbed into \( \Theta(1) \).

Given that
\[
\mathbb{E}_p(\epsilon) \left[ \log \xi_{\alpha} \left( \left| a^\top \epsilon \right|^2 \right) \right] = \log \xi_{\alpha} \left[ \max_k (a_k)^2 \right] + O(1) \geq \log \alpha + O(1)
\]
(65)
for any vector \( \alpha \), we have the new bound
\[
L(\theta, \phi) \geq \sum_i \left[ \mathbb{E}_p(\epsilon) \left[ \sum_{j \notin \Delta^{(i)}} \log \xi_{\alpha} \left( \left[ \sum_k \bar{\psi}_{jk}^{(i)} \cdot \xi \sqrt{\sigma_k^{(i)}} \left( \sigma_k^{(i)} \right) \cdot \epsilon_k \right]^2 \right) \right] - \sum_k \log \xi_{\alpha} \left[ \left( \sigma_k^{(i)} \right)^2 \right] \right] + \Theta(1).
\]
(66)
If then we choose \( \sigma_k^{(i)} = 0 \) for all \( i = 1, \ldots, n \) and \( k = 1, \ldots, \kappa \), then
\[
\max_k \left[ \bar{\psi}_{jk}^{(i)} \cdot \xi \sqrt{\sigma_k^{(i)}} \left( \sigma_k^{(i)} \right) \right]^2 = \log \alpha + \Theta(1)
\]
(67)
and we obtain the lower bound
\[
L(\theta, \phi) \geq \sum_i \left[ \left( d - \kappa - \left| \Delta^{(i)} \left( \mathbf{Y}, \pi^{(i)} \right) \right| \right) \right] \log \alpha + \Theta(1).
\]
(68)
\footnote{This is ultimately because \( \int_{c_1 + x > c_2} \log |c_1 + x| \mathcal{N}(x; 0, 1) dx < c_2 \int_{c_1 + x > c_2} \log |c_1 + x| dx = \Theta(1) \) for any \( c_1 \) and \( c_2 \) sufficiently large.}
Additionally, if any set $\Delta_\alpha^{(i)}(\Psi, \pi^{(i)})$ exists such that
\[
\sum_i \left( d - \kappa - \left| \Delta_\alpha^{(i)}(\Psi, \pi^{(i)}) \right| \right) \leq \sum_i \left( d - \kappa - \|s^{(i)}\|_0 \right),
\] (69)
then $s^{(i)}$ cannot be part of the unique, feasible solution to (10), i.e., we could use the support pattern from each $\Delta_\alpha^{(i)}(\Psi, \pi^{(i)})$ to find a different feasible solution with equal or lower value of $n \cdot \text{rank}[L] + \|S\|_0$, which would violate either the uniqueness or optimality of the original solution. Therefore, we have established that with $\sigma_k^{(i)} = O(\alpha)$ for all $i$ and $k$, the resulting bound on $\mathcal{L}(\Theta, \phi)$ is essentially no better than (53), or the same bound we had before from our feasible trial solution. Moreover, the resulting $W = \Psi$ that maximizes this bound, as well as the implicit
\[
\hat{\Sigma}_\alpha^{(i)}(\mu_\alpha, \Psi) = \text{diag} \left[ \alpha_1^{\top} \tau \times 1, 1^{\top} (\kappa - \tau) \times 1 \right]
\] (70)
will necessarily satisfy (12). We then only need consider whether other choices for $\sigma_k^{(i)}$ can do better.

Let $\hat{\Psi}^{(i)}$ denote the the rows of $\Psi^{(i)}$ associated with row indices $j \notin \Delta_\alpha^{(i)}(\Psi, \pi^{(i)})$, meaning the indices at which we assume no sparse corruption term exists. Additionally, define $B^{(i)} = \hat{\Psi}^{(i)} \Xi^{(i)}$. This implies that
\[
\sum_{j \notin \Delta_\alpha^{(i)}(\Psi, \pi^{(i)})} \log \xi_\alpha \left( \max_k \left[ \hat{\gamma}^{(i)}_{j,k} \cdot \xi_\pi \left( \sigma_k^{(i)} \right) \right]^2 \right) - \sum_k \log \xi_\alpha \left( \sigma_k^{(i)} \right)^2
\] (71)
\[
= \sum_j \log \xi_\alpha \left( \max_k \left[ B^{(i)}_{j,k} \cdot \xi_\pi \left( \sigma_k^{(i)} \right) \right]^2 \right) - \sum_k \log \xi_\alpha \left( \left( \sigma_k^{(i)} \right)^2 \right).
\]

Contrary to our prior assumption $\sigma = 0$, now consider any solution with $\|\sigma\|_0 = \beta > 0$. For the time being, we also assume that $B^{(i)}$ is full column rank. These conditions imply that
\[
\sum_j \log \xi_\alpha \left( \max_k \left[ B^{(i)}_{j,k} \cdot \xi_\pi \left( \sigma_k^{(i)} \right) \right]^2 \right) \geq \left( d - \beta - \left| \Delta_\alpha^{(i)}(\Psi, \pi^{(i)}) \right| \right) \log \alpha + \Theta(1)(72)
\]
since at least $\beta$ elements of the summation over $j$ must now be order $\Theta(1)$. By assumption we also have $\sum_k \log \xi_\alpha \left( \left( \sigma_k^{(i)} \right)^2 \right) = (\kappa - \beta) \log \alpha + \Theta(1)$. Combining with (72), we see that such a solution is equivalent or worse than (68). So the former is the best we can do at any value of $(\Psi, \pi^{(i)}, \Xi^{(i)}, \sigma^{(i)})_{i=1}^n$, provided that $B^{(i)}$ is full rank, and obtaining the optimal value of $\Delta_\alpha^{(i)}(\Psi, \pi^{(i)})$ implies that (12) holds.

However, if $B^{(i)}$ is not full rank it would indeed entail that (71) could be reduced further, since a nonzero element of $\sigma^{(i)}$ would not increase the first summation, while it would reduce the second. But if such a solution were to exist, it would violate the uniqueness assumption of the theorem statement. To see this, note that rank$[B^{(i)}] = \text{rank}[\hat{\Psi}^{(i)}]$ since $\Xi^{(i)}$ is orthogonal, so if the former is not full column rank, neither is the latter. And if $\hat{\Psi}^{(i)}$ is not full column rank, there will exist multiple solutions such that $\|x^{(i)} - \Psi \pi^{(i)}\|_0 = \|s^{(i)}\|_0$ or equivalently $\|x^{(i)} - Uv^{(i)}\|_0 = \|s^{(i)}\|_0$ in direct violation of the uniqueness clause.

Therefore to conclude, a lower bound on the VAE cost is in fact the same order as that obtainable by our original trial solution. If this lower bound is not achieved, we cannot be at a minimizing solution, and any solution achieving this bound must satisfy (12).

D.6 Generalization to Case where $\kappa > \text{rank}[U]$

Finally, we briefly consider the case where $\kappa > \text{rank}[U] \triangleq \tau$, meaning that $W$ contains redundant columns that are unnecessary in producing an optimal solution to (??). The candidate solution described in Section D.1 can be expanded via $W = [\Psi, \begin{bmatrix} 0_{d \times (\kappa - \tau)} \end{bmatrix}]$, $\mu_\alpha^{(i)} = \begin{bmatrix} (\pi^{(i)})^\top, \begin{bmatrix} 0_{1 \times (\kappa - \tau)} \end{bmatrix}^\top \end{bmatrix}$, and $\hat{\Sigma}_\alpha^{(i)} = \text{diag} \left[ \alpha_1^\top \begin{bmatrix} \tau \times 1 \end{bmatrix}, \begin{bmatrix} 1^\top \end{bmatrix} \right]_{(\kappa - \tau) \times 1}$ such that the same objective function value is obtained.
Now consider the general case where $\kappa \geq \text{rank}[^{\hat{W}}] > \tau$. If we review the lower bound described in Section D.5, with this general $W$ replacing $\Psi$, it can be shown that $\hat{\Sigma}_z^{(i)}$ will be forced to have additional diagonal elements lowered to $\alpha$, increasing the achievable objective by at least $-\log \alpha$ per sample. The details are not especially enlightening and we omit them here for brevity. Consequently, at any minimizer we must have $\text{rank}[^{\hat{W}}] = \tau$.

**Appendix E – Proof of Corollary 1**

Under the stated conditions, the partially-affine VAE cost simplifies to the function

$$
\mathcal{L}(W, \Sigma_x, \mu_z) = \sum_i \left\{ \left( x^{(i)} - W \mu_z^{(i)} \right)^T \Sigma_x^{-1} \left( x^{(i)} - W \mu_z^{(i)} \right) + \log \left| \Sigma_x \right| + \beta \left\| \mu_z^{(i)} \right\|^2 \right\}
$$

$$
= \sum_i \left\{ \left( x^{(i)} - W \beta^{-1} \beta \mu_z^{(i)} \right)^T \Sigma_x^{-1} \left( x^{(i)} - W \beta^{-1} \beta \mu_z^{(i)} \right) + \log \left| \Sigma_x \right| + \beta \left\| \mu_z^{(i)} \right\|^2 \right\},
$$

(73)

where $\beta > 0$ is an arbitrary scaler, $\Sigma_x^{(i)} \triangleq \Sigma_x \left( \mu_z^{(i)}; \theta \right)$, and $\mu_x^{(i)} \triangleq \mu_z(x^{(i)}; \phi)$. Taking the limit as $\beta \to 0^+$, we can minimize (73) while ignoring the $\beta^2 \| \mu_z^{(i)} \|^2$ regularization factor. Consequently, we can without loss of generality consider minimization of

$$
\mathcal{L}(W, \Sigma_x, \mu_z) \equiv \sum_i \left\{ \left( x^{(i)} - W \mu_z^{(i)} \right)^T \Sigma_x^{-1} \left( x^{(i)} - W \mu_z^{(i)} \right) + \log \left| \Sigma_x \right| \right\},
$$

(74)

ignoring any explicit reparameterization by $\beta$ for convenience. If we optimize over $\Sigma_x^{(i)}$ in the feasible region $\mathcal{S}_d$ and plug in the resulting value, then (74) reduces to the new cost

$$
\mathcal{L}(W, \mu_z) \equiv \sum_{i,j} \log \xi_{\alpha} \left( \left\| x^{(j)} - w, \mu_z^{(i)} \right\|^2 \right),
$$

(75)

an immaterial constant notwithstanding. Given that $\lim_{x \to 0} \frac{1}{x} (|x| - 1) = \log |x|$, and $\lim_{n \to 0} \sum_j x^p = \|x\|_p$, then up to an irrelevant scaling factor and additive constant, the stated result follows.

**Appendix F – Proof of Theorem 3**

Based on the stated conditions, the VAE objective simplifies to

$$
\mathcal{L}(\theta, \phi) = \sum_i \left\{ \mathbb{E}_{q(z|x^{(i)})} \left[ \frac{1}{x} \left\| x^{(i)} - \mu_z(z; \theta) \right\|^2 \right] + d \log \lambda_x + \lambda_z - \log \lambda_x + \left( a^T x^{(i)} \right)^2 \right\}.
$$

(76)

Now choose some $\tilde{a}$ such that $\tilde{\mu}_z^{(i)} = \tilde{a}^T x^{(i)}$ has a unique value for every sample $x^{(i)}$ (here we assume that each sample is unique, although this assumption can be relaxed). We then define the function $h : \mathbb{R} \to \{1, \ldots, n\}$ as

$$
h(z) \triangleq \arg \min_{i \in \{1, \ldots, n\}} \| z - \tilde{\mu}_z^{(i)} \|_2.
$$

(77)

and the piecewise linear decoder mean function

$$
\mu_z(z; \theta) = x^{(h(z))}.
$$

(78)

Given these definitions, (76) becomes

$$
\mathcal{L}(\theta, \phi) = \sum_i \left\{ \mathbb{E}_{q(z|x^{(i)})} \left[ \frac{1}{x} \left\| x^{(i)} - x^{(h(z))} \right\|^2 \right] + d \log \lambda_x + \lambda_z - \log \lambda_x + \left( \tilde{\mu}_z^{(i)} \right)^2 \right\}
$$

$$
= \sum_i \left\{ \mathbb{E}_{p(z)} \left[ \frac{1}{x} \left\| x^{(i)} - x^{(h(\tilde{\mu}_z^{(i)} + \sqrt{\lambda_x}))} \right\|^2 \right] + d \log \lambda_x + \lambda_z - \log \lambda_x + \left( \tilde{\mu}_z^{(i)} \right)^2 \right\}.
$$

(79)
Now define the set
\[ S(i) \triangleq \left\{ \epsilon : h \left( \hat{\mu}(i) + \sqrt{\lambda z} \epsilon \right) = i \right\}, \tag{80} \]
which represents the set of \( \epsilon \) that quantize to the correct index. We then have
\[
E_p(\epsilon) \left[ \frac{1}{\lambda z} \left\| x(i) - x(h\hat{\mu}^{(i)} + \sqrt{\lambda z} \epsilon) \right\|^2 \right] \\
= \int_{\epsilon \in S(i)} \left[ \frac{1}{\lambda z} \left\| x(i) - x(h\hat{\mu}^{(i)} + \sqrt{\lambda z} \epsilon) \right\|^2 \right] p(\epsilon) d\epsilon + \int_{\epsilon \notin S(i)} \left[ \frac{1}{\lambda z} \left\| x(i) - x(h\hat{\mu}^{(i)} + \sqrt{\lambda z} \epsilon) \right\|^2 \right] p(\epsilon) d\epsilon \\
\leq \int_{\epsilon \notin S(i)} \frac{n}{\lambda z} p(\epsilon) d\epsilon \\
= \frac{n}{\lambda z} P \left( \epsilon \notin S(i) \right), \tag{81} \]
where
\[ \eta \triangleq \max_{i,j \in \{1, \ldots, n\}, i \neq j} \left\| x(i) - x(j) \right\|_2^2, \tag{82} \]
the maximal possible quantization error. Now we also define
\[ \rho \triangleq \max_{i,j \in \{1, \ldots, n\}, i \neq j} \frac{1}{2} \left\| \hat{\mu}_z^{(i)} - \hat{\mu}_z^{(j)} \right\|_2^2, \tag{83} \]
which is half the minimum distance between any two \( \hat{\mu}_z^{(i)} \) and \( \hat{\mu}_z^{(j)} \), with \( i \neq j \). Then
\[ P \left( \epsilon \notin S(i) \right) \leq P \left( \sqrt{\lambda z} \epsilon > \rho \right) \leq \frac{\lambda_z}{\rho^2} \tag{84} \]
by Chebyshev’s inequality as was used in proving Theorem 2. This implies that (79) can be bounded via
\[
\mathcal{L}(\theta, \phi) \leq \sum_i \left\{ \frac{n}{\lambda z} P \left( \epsilon \notin S(i) \right) + d \log \lambda_z + \lambda_z - \log \lambda_z + \left( \hat{\mu}_z^{(i)} \right)^2 \right\} \\
= \sum_i \left\{ \frac{n}{\rho^2} + (d - 1) \log \alpha + \alpha + \left( \hat{\mu}_z^{(i)} \right)^2 \right\} \tag{85} \]
assuming we are at the trial solution \( \hat{\lambda}_z = \hat{\lambda}_z = \lambda z = \alpha \). As we allow \( \alpha \to 0 \), this expression is unbounded from below, and as an upper bound on the VAE objective, the theorem follows. Incidentally, it should also be possible to prove that for \( \alpha \) sufficiently small, no other solution can do appreciably better in terms of the dominate \((d - 1) \log \alpha\) factor, but we will reserve this for a future extended journal article.

References

[1] Y. Bengio. Learning deep architectures for ai. In Foundations and Trends in Machine Learning, 2009.

[2] L. Bottou. Large-scale machine learning with stochastic gradient descent. In International Conference on Computational Statistics, page 177–187, 2010.

[3] H. Bourlard and Y. Kamp. Auto-association by multilayer perceptrons and singular value decomposition. In Biological Cybernetics, 1988.

[4] E. Candès, X. Li, Y. Ma, and J. Wright. Robust principal component analysis? J. ACM, 58(2), May 2011.
[5] V. Chandrasekaran, S. Sanghavi, P.A. Parrilo, and A.S. Willsky. Rank-sparsity incoherence for matrix decomposition. *SIAM J. Optimization*, 21(3), June 2011.

[6] A. Choromanska, M. Henaff, M. Mathieu, G. Ben Arous, and Y. LeCun. The loss surfaces of multilayer networks. In *International Conference on Artificial Intelligence and Statistics*, page 192–204, 2015.

[7] A. Choromanska, Y. LeCun, and G. Ben Arous. Open problem: The landscape of the loss surfaces of multilayer networks. In *Conference on Learning Theory*, page 1756–1760, 2015.

[8] X. Ding, L. He, and L. Carin. Bayesian robust principal component analysis. *IEEE Trans. Image Processing*, 20(12), Dec. 2011.

[9] E. Elhamifar and R. Vidal. Sparse subspace clustering: Algorithm, theory, and applications. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 35(11), 2013.

[10] D.J.H. Garling. *A Journey into Linear Analysis*. Cambridge University Press, 2007.

[11] I. Goodfellow, Y. Bengio, and A. Courville. *Deep Learning*. MIT Press, 2016.

[12] I.J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio. Generative adversarial networks. In *arXiv:1406.2661*, 2014.

[13] K. He, X. Zhang, S. Ren, and J. Sun. Delving deep into rectifiers: Surpassing human-level performance on imagenet classification. In *IEEE International Conference on Computer Vision*, 2015.

[14] K. Kawaguchi. Deep learning without poor local minima. In *Advances in Neural Information Processing Systems 29*, pages 586–594, 2016.

[15] T.H. Oh and H. Kim, Y.W. Tai, J.C. Bazin, and I.S. Kweon. Partial sum minimization of singular values in RPCA for low-level vision. In *International Conference on Computer Vision*, 2013.

[16] D. Kingma and M. Welling. Auto-encoding variational bayes. In *International Conference on Learning Representations*, 2014.

[17] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11):2278–2324, Nov. 1998.

[18] C. Lu, J. Feng, Z. Lin, and S. Yan. Correlation adaptive subspace segmentation by trace lasso. In *IEEE International Conference on Computer Vision*, 2013.

[19] V. Nair and G.E. Hinton. Rectified linear units improve restricted Boltzmann machines. In *International conference on Machine Learning*, 2010.

[20] S. Rao, R. Tron, R. Vidal, and Y. Ma. Motion segmentation in the presence of outlying, incomplete, or corrupted trajectories. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 32(10), 2010.

[21] D.J. Rezende, S. Mohamed, and D. Wierstra. Stochastic backpropagation and approximate inference in deep generative models. In *International Conference on Machine Learning*, 2014.

[22] A.M. Saxe, J.L. McClelland, and S. Ganguli. Exact solutions to the nonlinear dynamics of learning in deep linear neural networks. In *International Conference on Learning Representations*, 2014.

[23] M. Tipping and C. Bishop. Probabilistic principal component analysis. *J. Royal Statistical Society, Series B*, 61(3):611–622, 1999.

[24] D. Wipf. Non-convex rank minimization via an empirical Bayesian approach. In *Uncertainty in Artificial Intelligence*, 2012.