Stochastic Prototype Embeddings

Tyler R. Scott 1 2  Karl Ridgeway 1  Michael C. Mozer 1 3

Abstract
Supervised deep-embedding methods project inputs of a domain to a representational space where same-class instances lie near one another and different-class instances lie far apart. We propose a probabilistic method that treats embeddings as random variables. Based on a state-of-the-art deterministic method, Prototypical Networks (Snell et al., 2017), our approach supposes the existence of a class prototype around which class instances are Gaussian distributed. The prototype posterior is a product distribution over labeled instances, and query instances are classified by marginalizing relative prototype proximity over embedding uncertainty. We describe an efficient sampler for approximate inference that allows us to train the model at roughly the same space and time cost as its deterministic sibling. Incorporating uncertainty improves performance on few-shot learning and gracefully handles label noise and out-of-distribution inputs.

1. Introduction
Supervised deep-embedding methods map instances from an input space to a latent embedding space where same-label pairs are near and different-label pairs are far. The embedding thus captures semantic relationships without discarding inter-class structure. In contrast, consider a standard neural network classifier with a softmax output layer trained with a cross-entropy loss. Although its penultimate layer might be treated as an embedding, the classifier’s training objective attempts to orthogonalize all classes and thereby eliminate any information about inter-class structure.

Embedding methods are popular in the few-shot learning literature (Koch et al., 2015; Vinyals et al., 2016; Snell et al., 2017; Triantafillou et al., 2017; Finn et al., 2017; Edwards et al., 2017; Triantafillou et al., 2017; Finn et al., 2017; Edwards et al., 2017; Triantafillou et al., 2017; Song et al., 2017; Wang et al., 2017; Karaletsos et al., 2016). Quadruplet losses attempt to ensure every within-class pair is closer than every between-class pair, \( \|z_\alpha - z_\alpha'\| < \|z_\alpha'' - z_\beta\| \) (Ustinova & Lempitsky, 2016). Finally, cluster-based losses attempt to use all instances of a class (Snell et al., 2017; Song et al., 2017; Ridgeway & Mozer, 2018; Rippel et al., 2016); for example, Prototypical Networks (PN) compute the mean of a set of instances of a class, \( \bar{z}_\alpha \), and ensure that additional instances of that class, \( z_\alpha \), satisfy a proximity constraint such as \( \|z_\alpha - \bar{z}_\alpha\| < \|z_\alpha - \bar{z}_\beta\| \).

Nearly all methods previously proposed for deep embeddings are deterministic: an instance projects to a single point in the embedding space. Deterministic embeddings fail to capture uncertainty due either to out-of-distribution inputs (e.g., data corruption) or label ambiguity (e.g., overlapping classes). Representing uncertainty is important for many reasons, including robust classification and decision making, informing downstream models, interpreting representations, and detecting out-of-distribution samples. Our proposed method, the Stochastic Prototype Embedding (SPE), is a variant of the PN (Snell et al., 2017), described above. As in the PN, our SPE assumes each class can be characterized by a prototype in the embedding space and an instance is classified based on its proximity to a prototype. In the case of the SPE, the embeddings and prototypes are Gaussian distributions.

\[ \text{Loss} = -\sum_{i=1}^{N} y_i \log(p_i) + \lambda \sum_{i=1}^{N} x_i - \sum_{j=1}^{M} z_j \]

where \( y_i \) is the true label, \( p_i \) is the predicted probability, \( x_i \) is the feature, \( z_j \) is the prototype, and \( \lambda \) is a hyperparameter. The objective attempts to orthogonalize all classes and thereby eliminate any information about inter-class structure.

\[ \text{Loss} = -\sum_{i=1}^{N} y_i \log(p_i) + \lambda \sum_{i=1}^{N} x_i - \sum_{j=1}^{M} z_j \]

where \( y_i \) is the true label, \( p_i \) is the predicted probability, \( x_i \) is the feature, \( z_j \) is the prototype, and \( \lambda \) is a hyperparameter. The objective attempts to orthogonalize all classes and thereby eliminate any information about inter-class structure.
random variables, each class instance is assumed to be a Gaussian perturbation of the prototype, and a query instance is classified by marginalizing out over the embedding uncertainty.

Using a synthetic data set, we demonstrate that the embedding uncertainty is related to both input and label noise. And on a few-shot learning task, we show that the SPE outperforms its state-of-the-art deterministic sibling, the PN.

2. The Model

The SPE assumes that the latent representation, \( z \), is a Gaussian conditioned on the input, \( x \):

\[
p(z|x) = \mathcal{N}(z; \mu_x, \sigma^2_x I)
\]

with mean, \( \mu_x \), and variance, \( \sigma^2_x \), computed by a deep neural network, similar to a Variational Autoencoder (Kingma & Welling, 2014). (We discuss the possibility of using a full covariance matrix in Appendix C.) The classification, \( y_i \), in turn is conditioned on \( z \), with \( p(y|x) \) taking the same form as in the original PN (Snell et al., 2017), to be described shortly. Given an input, a class prediction is made by marginalizing over the embedding uncertainty:

\[
p(y|x) = \int_z p(y|z)p(z|x)dz.
\]

We train the SPE using the standard few-shot learning paradigm, consisting of a sequence of episodes, each with \( m \) instances of \( n \) classes. We split the \( m \times n \) instances into \( k \times n \) support examples, defining a set \( S \), and \( (m-k) \times n \) query examples. The support instances for each class \( c \), \( S_c \subset S \), are used to determine the class prototype, \( \nu_c \), and the query instances are evaluated to predict class label (Equation 2).

2.1. Forming class prototypes

In the SPE, each class \( y \) has an associated prototype, \( \nu_y \), in the embedding space, and each instance \( i \) of class \( y \), denoted \( x_i \), projects to an embedding, \( z_i \), in the neighborhood of \( \nu_y \):

\[
\nu_y = z_i + \epsilon, \text{ where } \epsilon \sim \mathcal{N}(0, \sigma^2_y I).
\]

We assume that the prototype is consistent with all support instances, allowing us to express the likelihood of \( \nu_y \) as a product distribution:

\[
p(\nu_y|S_y) = \prod_{i \in S_y} p(\nu_y|x_i)
\]

Because \( p(\nu_y|x_i) \) is Gaussian, the resulting product is too:

\[
\nu_y|S_y \sim \mathcal{N}(\mu_y, \sigma^2_y I) \text{ with } \\
\sigma^2_y = \left( \sum_{i \in S_y} \hat{\sigma}^2_{x_i} \right)^{-1} \text{ and } \mu_y = \sigma^2_y \circ \left( \sum_{i \in S_y} \hat{\sigma}^2_{x_i} \circ \mu_{x_i} \right),
\]

where \( \hat{\sigma}^2_{x_i} = \sigma^2_{x_i} + \sigma^2_y \) and \( \circ \) denotes the Hadamard product. Essentially, the prototype is a confidence-weighted average of the support instances.

2.2. Prediction and approximate inference

We assume a softmax prediction for a query embedding, \( z \):

\[
p(y|z, S) \propto \mathcal{N}(z; \mu_y, \hat{\sigma}^2_y I)
\]

with \( \hat{\sigma}^2_y = \sigma^2_y + \sigma^2_z \) as before, yielding the class posterior for query \( x \):

\[
p(y|x, S) = \int_z \mathcal{N}(z; \mu_x, \sigma^2_x I) \frac{\mathcal{N}(z; \mu_y, \hat{\sigma}^2_y I)}{\sum_c \mathcal{N}(z; \mu_c, \sigma^2_c I)} dz.
\]

The class distribution is equivalent to that produced by the deterministic PN as \( \sigma^2_z \to 0 \) when \( \sigma^2_y = \sigma^2_y' \) for all class pairs \( (y, y') \). However, in the general case, the integral has no closed form solution; thus, we must sample to approximate \( p(y|x, S) \), both for training and evaluation. We employ two samplers, which we refer to as naïve and intersection.

2.2.1. Naïve Sampling

A direct approach to approximating the class posterior is to express Equation 2 as an expectation, \( \mathbb{E}_{z \sim p(z|x)} [p(y|z, S)] \), and to replace the expectation with the average over a set of samples. We utilize the reparameterization trick of Kingma & Welling (2014) to train the model. Although this is the simplest approach, it is sample-inefficient during training, and when the number of samples is reduced, performance is impacted.

2.2.2. Intersection Sampling

In Equation 6, the product of Gaussian densities in the numerator can be rewritten:

\[
\mathcal{N}(z; \mu_x, \sigma^2_x I) \mathcal{N}(z; \mu_y, \sigma^2_y I) = \\
\mathcal{N}(z; \mu_{xy}, \sigma^2_{xy} I) \mathcal{N}(\mu_x; \mu_y, (\sigma^2_x + \sigma^2_y I)),
\]

where

\[
\sigma^2_{xy} = \sigma^2_x + \sigma^2_y - 1 \text{ and } \\
\mu_{xy} = \sigma^2_{xy} \circ \mu_x + \sigma^2_y \circ \mu_y.
\]

Substituting Equation 7 into Equation 6,

\[
p(y|x, S) = \mathcal{N}(\mu_x; \mu_y, (\sigma^2_x + \sigma^2_y I)) \times \\
\mathbb{E}_{z \sim \mathcal{N}(\mu_{xy}, \sigma^2_{xy} I)} \left[ \sum_c \mathcal{N}(z; \mu_c, \sigma^2_c I) \right]^{-1}
\]

Approximating the expectation with samples from \( \mathcal{N}(\mu_{xy}, \sigma^2_{xy} I) \), we obtain a sampler that focuses on the
3.1. Synthetic color-orientation data set

Using a synthetic image data set, we demonstrate that the SPE can capture the generative structure of a domain and provide sensible estimates of uncertainty. The data set consists of \(64 \times 64\) pixel images with a well-defined class structure. The four classes in our domain are distinguished by orientation, color, or both (Figure 1). Class-conditional generative parameters—orientation and color—are sampled from an isotropic Gaussian distribution. Class overlap on color and orientation dimensions is symmetric. We tuned the variance such that there would be significant overlap between classes in order to elicit embeddings with increased uncertainty in overlapping regions. Full details of the synthetic data set can be found in Appendix A.2.

We trained a two-dimensional, intersection-sampling SPE on samples from this domain, using two instances per class to form prototypes. Classification accuracy of held-out samples is approximately 86%. Accounting for class overlap, a Bayes optimal classifier has an accuracy of approximately 87%. For visualization, we selected 25 examples by interpolating between the class means. The examples and their embeddings are shown in the left and right panels of Figure 2. The network has captured the structure of the domain by disentangling the two factors of variation. To identify the input array and the embedding space, the input array must be mirrored along the horizontal axis. The embedding variance encodes label ambiguity. Instances half way between two classes on one dimension have maximal variance along that dimension. Label ambiguity is one type of uncertainty. An equally important source of uncertainty comes from noisy or out-of-distribution (OOD) inputs. We examined OOD inputs generated in two different ways. In the left panel of Figure 3, we show the consequence of adding pixel hue noise to the four class centroids. Only one of these centroids is shown along the abscissa, but all four are used to make the graph, with many samples per noise level. The grey and black bars in the graph indicate variance on the vertical and horizontal dimensions of the embedding space, respectively. As pixel hue noise increases, uncertainty in the color grows but uncertainty in the orientation does not.

In the right panel of Figure 3, we show the consequence of shortening the length of the legs of the shape. Shortening the legs removes cues that can be used both for determining both color and orientation. As a result, the uncertainty grows on both dimensions.

3.2. Omniglot

The Omniglot data set contains images of labeled, handwritten characters from diverse alphabets. Omniglot is one of the standard data sets for comparing methods in the few-shot learning literature. The data set contains 1623 unique characters, each with 20 instances. Following Snell et al. (2017),
we augment the original classes with all 90° rotations, resulting in 6492 total classes, and we use the same train, validation, and test splits. Each grayscale image is resized from 32 × 32 to 28 × 28. We trained and evaluated deterministic Prototypical Networks, naïve-sampling SPEs, and intersection-sampling SPEs. Each is trained episodically, where a training episode contains 60 randomly sampled classes and 5 query instances per class, and test episodes contain 15 query instances per class.

We first compare the effectiveness of using naïve and intersection samplers during SPE training of Omniglot. We vary both the sampler and the number of samples drawn per training query, denoted by s. We evaluate in a 1-shot 20-class setting, where shot refers to the number of support examples used to compute a prototype, and class refers to the number of candidate test classes per episode. Figure 4 shows test classification accuracy as the number of samples drawn per training trial (s) increases. As we previously claimed, the intersection-sampling SPE is much more sample-efficient and systematically outperforms the naïve-sampling SPE. Furthermore, the intersection-sampling SPE is more robust and less susceptible to poor initialization or uninformative samples.

Table 1 presents results for simulations with Omniglot comparing the deterministic PN to the intersection-sampling SPE. For both 2- and 64-dimension embeddings, the SPE either matches or outperforms the PN, a state-of-the-art algorithm in few-shot learning. In the 64D embedding, both methods are close to ceiling. In the 2D embedding, the SPE particularly shines in the 1-shot tests, perhaps because, relative to the 5-shot tests, performance is further from ceiling. However, another possibility is that the role of uncertainty is greater when only one instance is used to form the prototype. When 5 instances are used, the uncertainty shrinks significantly, causing the SPE to behave more like its deterministic sibling. To emphasize, the improved performance of the SPE does not incur much of a computational cost in training. And by providing an estimate of uncertainty associated with embedded instances, the SPE offers the possibility of detecting OOD samples and informing downstream systems that operate on the embedding.

4. Conclusion

We propose a Stochastic Prototype Embedding (SPE) and demonstrate its effectiveness in representing uncertainty related to both input and label noise on a synthetic data set. Furthermore, we show that the SPE consistently outperforms its deterministic sibling, the Prototypical Network (PN), at approximately the same space and time cost.
References


A. Network Architectures and Hyperparameters

A.1. Omniglot

For all Omniglot experiments, the network consisted of four convolutional blocks. The first three blocks had a convolutional layer with 64 filters, a $3 \times 3$ kernel, zero-padding of length 1, and a stride of 1, followed by a batch normalization layer, ReLU activation, and $2 \times 2$ max-pooling. The fourth and final block had a convolutional layer with $2d$ filters, a $3 \times 3$ kernel, zero-padding of length 1, and a stride of 1, followed by $2 \times 2$ max-pooling, where $d$ represents the dimensionality of the embedding space. The flattened output of the network is a vector of length $2d$, where the first $d$ elements were considered the mean of the Gaussian distribution and the remaining $d$ elements were the diagonal covariance entries. The weights were initialized using He initialization and the biases with the following uniform distribution:

$$U(-\frac{1}{\sqrt{\text{fan in}}}, \frac{1}{\sqrt{\text{fan in}}})$$

All Omniglot models were trained with an initial learning rate of 0.0001 which was cut in half every 50 epochs. The models were stopped early using a patience parameter when performance on the validation set no longer increased.

A.2. Synthetic data

The images in the synthetic data set are $64 \times 64$ pixels in size. For orientation, we chose class centers at $90^\circ$ and $180^\circ$, with a standard deviation of $30^\circ$. For color, we manipulated the hue and kept value and saturation constant. Like orientation, hue is a circular quantity. If hue ranges from 0 to 360 degrees, we chose color class centers and standard deviation in the same way as orientation. Additionally, we add noise to a minority (15%) of the images used to train the model. For these, we add Gaussian noise to the hue of each pixel inside the shape. The standard deviation of the hue noise was chosen uniformly between $18^\circ$ and $54^\circ$. We also added noise to the leg lengths of the L shapes. The leg length was chosen uniformly between 10% and 98% of its original length. See Figure 3 for some examples.

The network followed an architecture similar to the one we used for Omniglot, except that we added two additional blocks of convolution, batch normalization, ReLU, and max-pooling because the images are larger. We used 2 instances per class to form prototypes and 8 samples per query instance during training. We used a learning rate of 0.0001 and the models were stopped early using a patience parameter when performance on the validation set no longer increased.

B. Simulation Details

For all SPE models, 

$$\sigma^2_c = \text{softplus}(\epsilon),$$

where $\epsilon$ is a trainable parameter. We initialize $\epsilon$ using the following prescription:

$$\epsilon = |S|\epsilon_0^{2/d},$$

where $|S|$ is the number of support examples per episode during training and $d$ is the dimensionality of the embedding. We chose this prescription for two reasons: (1) as the number of support examples increases, the variance of the prototype distribution approaches zero, so scaling linearly by $|S|$ tends to provide a stronger training signal early on, and (2) the amount of noise in the projection of an embedding should scale with the dimensionality of the embedding space as to maintain unit-volume. All models used $\epsilon_0 = 0.01$.

It should also be noted that there is no constraint for $\sigma^2_x > 0$, since $\sigma^2_x$ is a direct output of a deep network. To ensure a positive value, $\sigma^2_x \leftarrow \text{softplus}(\sigma^2_x)$.

C. SPE Variants

We assumed only diagonal covariance matrices in this work. Switching to a full covariance matrix would require matrix inversion, which is ordinarily infeasible, but because one purpose of deep embeddings is visualization, there may be interesting cases involving 2D embeddings where the cost of inversion is trivial.