EMBEDDING DEEP NETWORKS INTO VISUAL EXPLANATIONS

Anonymous authors
Paper under double-blind review

ABSTRACT

In this paper, we propose a novel explanation module to explain the predictions made by a deep network. Explanation module works by embedding a high-dimensional deep network layer nonlinearly into a low-dimensional explanation space while retaining faithfulness, so that the original deep learning predictions can be constructed from the few concepts extracted by the explanation module. We then visualize such concepts for human to learn about the high-level concepts that deep learning is using to make decisions. We propose an algorithm called Sparse Reconstruction Autoencoder (SRAE) for learning the embedding to the explanation space. SRAE aims to reconstruct part of the original feature space while retaining faithfulness. A visualization system is then introduced for human understanding of features in the explanation space. The proposed method is applied to explain CNN models in image classification tasks, and several novel metrics are introduced to evaluate the performance of explanations quantitatively without human involvement. Experiments show that the proposed approach could generate better explanations of the mechanisms CNN use for making predictions.

1 INTRODUCTION

Deep learning has made significant strides in recent years. It has surpassed human performance in many tasks, such as image classification (Krizhevsky et al., 2012; He et al., 2016), go-playing (Silver et al., 2016), and classification of medical images (Esteva et al., 2017). However, the usage of deep learning in real applications still must overcome a trust barrier. Imagine scenarios with a doctor facing a deep learning prediction: this CT image indicates malignant cancer, or a pilot facing a prediction: make an emergency landing immediately. These predictions may be backed up with a claimed high accuracy on benchmarks, but it is human nature not to trust them unless we are convinced that they are reasonable for each individual case. The lack of trust is worsened because of known cases where adversarial examples can fool deep learning to output wrong answers (Szegedy et al., 2013; Goodfellow et al., 2014). In order to establish trust, human needs to understand how deep learning makes decisions. Such understanding could also help the human to gain additional insights into new problems, potentially improve deep learning algorithms, and improve human-machine collaboration.

People prefer explanations of the form “A is something because of B, C, and D”, e.g. this is a bird because it has feathers, wings and a beak. This type of explanation has two properties. Firstly, it is concise – there are not a hundred different reasons that add up to explain that A is something. Secondly, it relies on B, C, and D, which are high-level concepts as well. Both are often at odds with deep learning predictions, which are combinations of outputs from thousands of neurons in dozens of layers. Approaches have been proposed to visualize each of the filters (Zeiler & Fergus, 2014) and for humans to name them (Bau et al., 2017), but it is difficult for these approaches to obtain a concise representation. On the other hand, many other approaches generate attention maps that backtrack a decision to specific important areas in the original image (Simonyan et al., 2014; Cao et al., 2015; Zhou et al., 2016; Zhang et al., 2016b; Selvaraju et al., 2016b). These are often nice and quite informative, but they work on individual images and do not provide any high-level concept that can be broadly applicable to many images simultaneously, nor can we believe they are complete explanations so that we can trust them.

In this paper, we make an attempt to reconcile these explanation approaches by extracting several high-level concepts from deep networks to aid human understanding. Our model attaches a separate explanation module to a certain layer in the deep network to reduce the network to a few human-
Figure 1: (a) The explanation module is a dimensionality reduction mechanism so that the original prediction \( \hat{y} \) can be reproduced from this low-dimensional space. An explanation module can be attached to any layer in the prediction deep network (DNN). The output of the DNN can be faithfully recovered from this low-dimensional explanation space, which represents high-level features that are interpretable to humans. (b) Two non-localized and highly correlated heat map explanations in the first row; two localized and largely orthogonal heat map explanations in the second row.

understandable concepts, from where one can generate predictions similar to the original deep network (Fig. 1(a)). We focus on making those concepts to have several properties: faithfulness, that the deep learning predictions can be faithfully approximated from those few concepts; locality, that the concepts are relatively spatially localized in images so that human can understand them; as well as orthogonality, that the concepts themselves are as independent from each other as possible.

Our model does not train from ground truth concepts defined by human, but directly infers concepts from the learning network, hence it is difficult to evaluate the explanations quantitatively. We evaluate our approach on a fine-grained bird classification dataset where rich ground truth annotations allow us to define quantitative metrics for the aforementioned properties without active human involvement.

Although the experiments in the paper focus on convolutional neural networks (CNN) applied to images, the explanation framework we develop is general and applicable to other types of deep networks as well. We believe this is one of the first steps towards general explainable deep learning that can advance human knowledge and enhance future collaboration between humans and machines.

Our contributions in this paper are as follows:

- We propose a novel explanation module to form a low-dimensional explainable concept space from deep networks. A sparse reconstruction autoencoder approach is proposed to make the explanation module faithful and orthogonal as defined previously.
- We present a visualization paradigm for human understanding of the concept space.
- We propose automatic quantitative metrics to evaluate the performance of an explanation algorithm for faithfulness, locality and orthogonality. Experimental results show that the proposed explanation methods provide insights to how the deep network models work.

2 Model Formulation

2.1 The Explanation Module

Given a deep learning network (DNN) as a prediction module, we propose to learn an extra explanation module (Fig. 1(a)), which can be attached to any intermediate layer of the DNN. The explanation module attempts to learn an embedding that lowers the dimensionality of the intermediate layer of the DNN, and then directly learn a mapping from the embedding space to mimic the output of the original DNN model. We denote the input feature space of the explanation module as \( Z(x; W) \), where \( x \) and \( W \) are the input features and parameters (from multiple layers) of the original DNN model, respectively, and \( Z \) represents the output of a particular intermediate layer of the DNN. The explanation module is used to embed \( Z \) to an explanation space, denoted as \( E_\theta(Z) \), where \( \theta \) represents parameters of the embedding that need to be learned. As a shorthand, we will also refer to the explanation space as an \( x \)-layer, and each dimension in the \( x \)-layer an \( x \)-feature. Note that in the explanation, we do not attempt to change the parameters \( W \) of the original DNN model. The explanation module can in principle be attached to any intermediate layer of the DNN, although the closer to the prediction, the higher level the concepts are and it becomes easier to mimic the prediction of DNN with a low-dimensional embedding.
We claim that low-dimensional embeddings are more effective when they reconstruct the original prediction results \( \hat{y} \). In other words, we would need a low-dimensional feature embedding to be faithful to the DNN. This is generally difficult if the DNN is predicting many concepts simultaneously, such as a multi-class classification. In this paper we propose to obtain faithfulness by explaining 1-dimensional outputs, such as binary classification or one-against-all classifiers. A multi-class explanation can in principle be built up from separate explanations of one-against-all classifiers. For a 1-dimensional prediction \( \hat{y} \), we can definitely assume that the explanation module could remain faithful to the prediction, since a naive case would be to use the 1-dim \( \hat{y} \) as the explanation, which is perfectly faithful but not interpretable. Hence, the low-dimensional embedding \( \mathbf{E} \) can also be thought of as expanding \( \hat{y} \) to several dimensions, therefore enriching the explanations for a single prediction.

In this paper, we focus on attaching explanation modules to fully-connected layers. The concepts generated in these layers are rather high-level, and our conceptual goal is to visualize those concepts and to make humans learn them: human has a quite deep neural network for learning and generalizing perceptual concepts very well. Therefore we would like to show humans examples from a small number of perceptual concepts from the explanation space, so that they can utilize their own perceptual neural network for learning and naming those. Our primary tool for this display is heatmaps (e.g. Fig. 1(b), Fig. 3(a)) highlighting a specific region in the image, similar as those used in attention models in prior work. Our work will provide several different and largely orthogonal concepts, visualized by heatmaps, for improving the understanding of the predictions from a DNN. The two main topics in the explanation module are the embedding algorithm and the visualization of the explanations, which will be discussed in the next three subsections.

2.2 Embedding to the Explanation Space

Explanation space optimization attempts to be faithful to the prediction of the original DNN:

\[
\min_{\theta, \mathbf{v}} \frac{1}{M} \sum_{i=1}^{M} L \left( f \left( \mathbf{E}_{\theta}(\mathbf{Z}^{(i)}); \mathbf{v} \right), \hat{y}_j^{(i)} \right) \tag{1}
\]

where \( \mathbf{Z}^{(i)} = \mathbf{Z}(\mathbf{x}^{(i)}; \mathbf{W}) \) is the output of an intermediate layer in DNN for instance \( \mathbf{x}^{(i)} \); parameter \( \theta \) is used to form the explanation space \( \mathbf{E}_{\theta}(\mathbf{Z}^{(i)}) \); parameter \( \mathbf{v} \) is used to build a predictor \( f(\mathbf{E}; \mathbf{v}) \) from the x-features to mimic \( \hat{y}_j^{(i)} \), e.g. \( f(\mathbf{E}; \mathbf{v}) = \mathbf{v}^\top \mathbf{E} \) would be a simple linear predictor from the explanation space and the one we use in this work; \( \hat{y}_j^{(i)} \) is \( j \)-th output of the original DNN model and the explanation target for instance \( \mathbf{x}^{(i)} \), we usually use the DNN output before the softmax layer to prevent interactions with other predictions; \( M \) is the number of the training examples; \( L \) is a loss function, usually a regression loss such as squared loss or log loss. However, as we argued in Sec. 2.1, this formulation might be almost degenerate if \( \hat{y}_j^{(i)} \) can be used as the explanation variable. Hence, additional terms need to be added to prevent degeneracy and improve interpretability.

We claim that low-dimensional embeddings are more effective when they reconstruct the original high-dimensional feature space better. If the original DNN features are localized, then one can hope the low-dimensional explanation features are also localized, since aggregating different localities in the same dimension is also not helpful for reconstructing each of them. Thus, adding reconstruction loss \( L \left( \mathbf{E}_{\theta}^{-1}(\mathbf{E}_{\theta}(\mathbf{Z}^{(i)})); \mathbf{Z}^{(i)} \right) \) to optimization (1) will prevent degeneracy and improve locality. Here \( \mathbf{E}_{\theta}^{-1} \) is a mapping that maps from the explanation space \( \mathbf{E} \) back to \( \mathbf{Z} \); \( \theta \) is the parameter for this mapping. However, when the weight of the reconstruction loss is large in the optimization, features irrelevant to the predict target may also be reconstructed.

To avoid this, we propose to enhance the objective by adding a sparsity term which reconstructs some dimensions of the original features \( \mathbf{Z} \), but not all of them. By attempting to reconstruct some dimensions of \( \mathbf{Z} \) with only a few embeddings, and to mimic the original predictions \( \hat{y} \) with the same embeddings, the maximal amount of diverse information that are relevant to \( \hat{y} \) in \( \mathbf{Z} \) needs to be packed in the low-dimensional space. Packing redundant information in correlated dimensions would be harmful for reconstruction, and reconstructing irrelevant features would harm the ability to recover \( \hat{y} \). By introducing a sparse penalty in the reconstruction loss, we obtain:

\[
\min_{\theta, \theta, \mathbf{v}} \frac{1}{M} \sum_{i=1}^{M} L \left( f \left( \mathbf{E}_{\theta}(\mathbf{Z}^{(i)}); \mathbf{v} \right), \hat{y}_j^{(i)} \right) + \beta \text{Sparsity}(\mathbf{Q}); \quad Q_k = \frac{1}{M} \sum_{i=1}^{M} L \left( \mathbf{E}_{\theta}^{-1}(\mathbf{E}_{\theta}(\mathbf{Z}^{(i)}))_k; \mathbf{Z}_k^{(i)} \right) \tag{2}
\]
where $Q_k$, $Z_k^{(i)}$, and $E_{\theta}^{-1}(E_{\theta}(Z^{(i)}))_k$ are the $k$-th dimension of $Q$, $Z^{(i)}$, and $E_{\theta}^{-1}(E_{\theta}(Z^{(i)}))$, respectively and $\beta$ is the parameter for the sparsity term. In the optimization, $Q_k$ measures the capability of reconstructing the $k$-th dimension in the space of $Z$. The sparsity term will be detailed in Sec. 2.3. With this term, optimization (2) achieves faithfulness, locality, orthogonality, and little irrelevant information for the explanation space.

### 2.3 Dimensionality Reduction Method

In general, any dimensionality reduction method can be used to obtain the explanation space $E_{\theta}(Z)$. Here we propose a novel network called Sparse Reconstruction Autoencoder (SRAE), which handles the objective as defined in (2). SRAE is also a neural network, hence can seamlessly combine with the visualization paradigm in the next subsection, this facilitates better understanding of black-box DNN models to both experts and non-specialists.

![Illustration of the SRAE used for the explanation module.](image)

*Figure 2: Illustration of the SRAE used for the explanation module. Both the prediction and a sparse reconstruction are generated from the explanation space; (b) The log penalty function $\log(1 + q \cdot x^2)$ when $q = 1$; (c) The log penalty function $\log(1 + q \cdot x^2)$ when $q = 10$.***
2.4 Visualizing the Explanation Space

The goal in the visualization of low-dimensional explanation features is to bridge the communication gap between human and machine, and enable human to name concepts learned by the explanation module and be able to construct sentences with those named concepts. For this paper though, we only focus on visualizing the concepts. We utilize ExcitationBP (Zhang et al., 2016b) to compute the contrastive marginal winning probability (c-MWP) from each neuron in x-layer to the pixels in the original image, then generate the heat maps using c-MWP normalized on each neuron for each image. A prototype interactive visualization system is introduced for human understanding of neurons in the explanation space, which contains two types of visualizations (Fig. 3(a) and Fig. 3(b)). The first type shows the heatmap for different neurons and their prediction weights in a single image (Fig. 3(a)), and the second type shows a single neuron across many images for human to name this particular neuron (Figure 3(b)) and vote for whether to trust this neuron in the final classifier.

3 Related Work

The explanation for high accuracy but black-box models has become a significant need in many real applications. In the medical domain, several approaches were proposed to utilize interpretable models to explain the predictions for individual patients in a concise way (Caruana et al., 2015; Letham et al., 2015; Ustun & Rudin, 2016). In Natural Language Processing, Kulesza et al. (2015) propose an interactive system which builds a cycle of explanations from the learning system to the user, and then back to the system. In computer vision, methods have been introduced to explain the predictions either by associating the images with captions/descriptions (Kiros et al., 2014; Kong et al., 2014; Lin et al., 2014; Karpathy & Fei-Fei, 2015; Hendricks et al., 2016), visualizing individual convolutional filters in the network (Zeiler & Fergus, 2014; Bau et al., 2017) or heatmaps that indicate important regions in the original images (Simonyan et al., 2014; Cao et al., 2015; Zhou et al., 2016; Zhang et al., 2016b; Selvaraju et al., 2016a). Park et al. (2016) and Selvaraju et al. (2016a) propose to explain via visual question answering which utilized both natural language descriptions and heatmaps. Ribeiro et al. (2016) propose an explanation technique which tries to explain single prediction of general models, and select several representative predictions to provide a global view of the model.

Image captioning approaches (Kiros et al., 2014; Kong et al., 2014; Lin et al., 2014; Karpathy & Fei-Fei, 2015; Hendricks et al., 2016) need to be trained on human-generated sentences, hence they would not work in any domain where human is not an expert in. Our approach does not require any natural language descriptions. Visualizing individual neurons/filters were important for human intuition about CNNs (Zhou et al., 2015; Zeiler & Fergus, 2014; Jain et al., 2016). Recently, Bau et al. (2017) went to great lengths in visualizing thousands of neurons and asking human to name each of them. However, it is difficult for such efforts to provide a concise yet complete representation. Agrawal et al. (2014) analyzed the number of filters required to generate good performance on the PASCAL VOC dataset and the conclusion is that each class would need at least dozens of filters. We adopt the heatmap approach in (Zhang et al., 2016b), but visualize explanation features instead of
directly visualizing classification results. With this approach we can generate high-level concepts that are broadly applicable to multiple images in the same category.

Recently, there has been a focus of detecting parts using deep neural networks without part annotations, usually in fine-grained classification. Simon & Rodner (2015b) and Xiao et al. (2015) use combinations of convolutional filters to generate part proposals that improves prediction performance. Gkioxari et al. (2015) and Zhang et al. (2016a;c) use various approaches to detect parts. Our focus is different in that we focus on explaining a trained deep model instead of trying to enhance it, and the explanation may not necessarily be parts that can be expressed in terms of bounding boxes as in those approaches. Gonzalez-Garcia et al. (2016) conducted comprehensive experiments on whether semantic parts naturally emerge from convolutional filters. They explored combinations of filters using a genetic algorithm but only combine an average of 5 filters, hence did not have the dramatic dimensionality reduction effect as in our work. Independent from our work, recently Zhao et al. (2017) train a hybrid CNN-LSTM model featuring diversified attention models jointly and generate diverse attention maps similar to ours in the middle of the network, but it cannot be utilized to explain an already-trained DNN because of the joint training that is needed, and there was no attempt in quantitatively evaluating the explanations.

Model compression for deep learning was proposed in (Ba & Caruana, 2014), where a shallow model is used to mimic the output of a deep network. Most model compression work since then were used for speeding up testing (Chen et al., 2015; Rastegari et al., 2016). Che et al. (2016) learn a decision tree on top of deep network results in an attempt for an interpretable model, however their framework cannot discover new features as they were only utilizing categorical predictions with known categories (that were trained on) as the basis for interpretation.

4 Experiments

4.1 Evaluation Metrics

The most challenging part in the experiments is to find objective metrics to evaluate the performance of the explanation module, since the explanation of images is a relatively subjective matter. Evaluating explanations objectively without a human study is important, because simple parameter variations can easily generate thousands of different explanations, vastly outpacing the speed of human studies. In this paper we make an attempt to define some quantitative metrics. We utilize the CUB-200-2011 dataset (Wah et al., 2011) in the experiments. This is a task for fine-grained bird classification into 200 categories. This dataset is chosen because in addition to category labels and bounding boxes surrounding each object, it also has part labels denoted as one pixel per part (Fig. 3(a)) for each object as additional ground truth. One can argue that the majority of bird classifications are based on specific, discriminative parts of the bird, which can be confirmed from encyclopedias and expert annotations (Reed et al., 2016). In order to measure locality, we propose a metric which associates neurons in the x-layer with various parts of one category in the image, and measures how well they associate with these parts. Note that this metric is by no means perfect and would struggle at features that do not represent a single part, it merely reflects our current best efforts in quantitatively measuring different explanations.

Given image $I_m$, for each neuron $n$ in the x-layer and each pixel $(i, j)$ in $I_m$, we denote $S_{i,j}^{n,m} \triangleq P(\text{Pixel}_{ij}^{m} | \text{Neuron}_n) = \frac{C_{i,j}^{n,m}}{\sum_{(i,j) \in I_m} C_{i,j}^{n,m}}$, where $C_{i,j}^{n,m}$ is the c-MWP generated by ExcitationBP for pixel $(i, j)$ in $I_m$ with neuron $n$ in x-layer, $(i, j)$ is the coordinate of the pixel. For the CUB dataset, since the given part label ($p = 1, ..., 15$) of each image is just one pixel in the middle of the part, and there is no extra information about the shape and the size of the part regions, we utilize the Voronoi diagram to partition the bounding box into 15 regions where the nearest neighbor part annotation in each region would be the same (Fig. 3(a)). Then we compute the probability $S_{p}^{m} \triangleq P(\text{Part}_{p}^{m} | \text{Neuron}_n) = \sum_{(i,j) \in I_m} P(\text{Part}_{p}^{m} | \text{Pixel}_{ij}^{m}) P(\text{Pixel}_{ij}^{m} | \text{Neuron}_n)$ using Algorithm 1 in the Appendix. The Voronoi diagram is used instead of a segmentation, because firstly we do not have segmentation ground truth and do not wish to include additional errors from an arbitrary segmentation algorithm, and secondly because some of the heatmap activations fall slightly outside the object and we still want to capture those. For all the c-MWP outside of the ground truth bounding box, we introduce a 16-th part called context, which indicates that the x-feature is using the context to classify rather than the object features.
Next, we propose several metrics to evaluate the performance of the explanation module. For each x-feature $n$ we have a histogram $S_p$, whose element is $S_p^{m,n} = \frac{1}{|m|} \sum_{m} S^{n,m}$. The Locality for each x-feature is defined as the entropy: $H_n = -\sum_{p} \left( \frac{S_p^{n,n}}{\sum_{p} S_p^{n,n}} \cdot \log \left( \frac{S_p^{n,n}}{\sum_{p} S_p^{n,n}} \right) \right)$. Locality is roughly measuring the log of the number of parts captured by each x-feature. If the x-feature falls perfectly in one part, locality will be 0. Note that there are many small parts hence often x-features will fall on more than one of them just because the blur in the attention map. For the whole explanation module, we have: (1) Faithfulness: We introduce a regression metric and a classification metric for faithfulness. (a) $F_{reg} = \frac{1}{|m|} \sum_{m} L(\hat{y}^{(m)} - \bar{y}^{(m)}) = \frac{1}{|m|} \sum_{m} |\hat{y}^{(m)} - \bar{y}^{(m)}|$, the mean absolute loss between $\hat{y}^{(m)}$ and its approximation $\bar{y}^{(m)}$; (b) We replace $\hat{y}^{(m)}$ with $\bar{y}^{(m)}$ in the original multi-class prediction vector $\hat{y}^{(m)}$ before softmax and check whether the classification result changes. We denote $c_r$ as the number of examples whose classification results remain the same, then $F_{cls} = \frac{c_r}{|m|}$. (2) Orthogonality: In order to measure whether different attention maps fall on the same region, we directly treat attention maps of different x-features as different vectors and compute their covariance matrix. We denote $C$ as the covariance matrix among x-features aggregated over the dataset. Then $P = \text{diag}(C)^{-1/2} \text{Cdiag}(C)^{-1/2}$ is the matrix of correlation coefficients. The orthogonality between neurons in the x-layer is defined as: (a) $O_1 = ||P||_F - \sqrt{n}$, where $|| \cdot ||_F$ is the Frobenius norm for matrix; (b) $O_2 = -\log \det (P)$, where logdet is the logarithm of determinant of a matrix. Both $O_1$ and $O_2$ obtain the optimum at 0, when $P$ is a unit matrix.

4.2 Experiment Settings and Results

The fine-tuned VGG19 model (Simon & Rodner, 2015a) for CUB-200-2011 birds is used as the prediction DNN to be explained. The explanation module is a 3-middle-layer SRAE with 800–100–$n$ hidden units in each layer, where $n$ represents the number of x-features. We trained an explanation module on a random 30 of the 200 bird categories. For each category, we utilized 50 positive examples and 8,000 negative examples as the training data; the remaining positive examples (8–10) and 2,000 negative examples as the testing data. In the training process, we enhance the weights of the positive examples to avoid imbalance. $n$ is set to 5, as our experiments showed that more x-features do not improve performance and create x-features which have 0 weight in $v_i E_i$, indicating that one one-against-all classifier of one bird does not depend on many high-level visual features. We compared the proposed SRAE with a fully-connected neural network (NN), a conventional stacked autoencoder (SAE), a feature selection model (Lasso) on $Z$, as well as directly performing ExcitationBP on the classification output $\hat{y}$ (ExcitationBP). The baseline neural network methods (NN and SAE) can also perform a faithful dimensionality reduction, and are the most closely related to our approach. Lasso represents a simple approach which can also perform feature selection. All the learning-based approaches (SRAE, NN, SAE, and Lasso) were tuned to the optimal parameters by cross-validation on the training set.

In Table 1(a), we summarize the results for different explanation embedding approaches with different parameters. Results show that we can achieve excellent faithfulness to the predictions when using SRAE, NN, and SAE. The $F_{reg}$ in both training and testing are less than 0.2. Since $\hat{y}$ before softmax usually has a range in $[0, 50]$ and especially large in the positive examples, we consider the regression loss to be small. The classification faithfulness $F_{cls}$ is even better, as only $1 - 2$ examples out of all the categories we tested have switched labels after replacing the original $\hat{y}$ with the approximation from the x-features. We also summarize the faithfulness for Lasso using different parameters in Table 2(a), where $\alpha$ is the parameter that multiplies the $L_1$ term in Lasso, $N_{num_x}$ is the average number of the selected features for 30 categories. From Table 1(a) and Table 2(a) we observe that the faithfulness for Lasso are all very bad with different parameters, indicating that it is almost impossible for the feature selection method to select few X-features form Z directly to make the prediction faithful.

In terms of orthogonality and locality, our algorithm showed significant improvements over NN, SAE, and Lasso ($\alpha = 2.5$ in Table 1(a)). Besides, the locality of the x-features improves significantly over the ones from ExcitationBP, indicating that we are capable of separating information that come from different parts. The average locality of the x-features generated by SRAE are almost matching the average locality of features in Z. This means we are close to the limit of part separation on this layer: many of the features on the Z layer already represent multiple parts. In future work we plan to conduct more experiments explaining earlier convolutional layers to see whether the locality could be further lowered while preserving faithfulness.
Table 1: (a) The average faithfulness, orthogonality, and locality for different approaches in 30 categories selected randomly. The column $Z$ represents the average locality computed over all the dimensions of $Z$, the 4096-dimensional first fully-connected layer of the deep network. This is obtained by separately running ExcitationBP on each dimension of $Z$ and evaluating the resulting heatmaps. (b) A preliminary human study comparing SRAE with Lasso.

<table>
<thead>
<tr>
<th>Method</th>
<th>SRAE</th>
<th>NN</th>
<th>SAE</th>
<th>Lasso</th>
<th>$Z$ ExcitationBP</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F_{reg}$ Training</td>
<td>0.0831</td>
<td>0.0657</td>
<td>0.0987</td>
<td>3.8039</td>
<td>—</td>
</tr>
<tr>
<td>Testing</td>
<td>0.1539</td>
<td>0.1170</td>
<td>0.1928</td>
<td>3.7028</td>
<td>—</td>
</tr>
<tr>
<td>$F_{cls}$ Training</td>
<td>99.99%</td>
<td>99.99%</td>
<td>99.99%</td>
<td>71.82%</td>
<td>—</td>
</tr>
<tr>
<td>Test</td>
<td>99.99%</td>
<td>99.99%</td>
<td>99.99%</td>
<td>68.33%</td>
<td>—</td>
</tr>
<tr>
<td>O1 Positive</td>
<td>0.6141</td>
<td>0.8851</td>
<td>0.7161</td>
<td>1.1407</td>
<td>—</td>
</tr>
<tr>
<td>O2 Positive</td>
<td>2.0790</td>
<td>3.6483</td>
<td>2.7710</td>
<td>2.8632</td>
<td>—</td>
</tr>
</tbody>
</table>

Table 2: (a) The average faithfulness for Lasso with different $\alpha$; (b) The average classification accuracy for images masked by our method and ExcitationBP so that only highlighted areas are shown to the classifier.

<table>
<thead>
<tr>
<th>Method</th>
<th>Original</th>
<th>Mask by X features</th>
<th>Mask by ExcitationBP</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F_{reg}$ Training</td>
<td>3.80</td>
<td>3.06</td>
<td>3.86</td>
</tr>
<tr>
<td>Testing</td>
<td>3.70</td>
<td>2.99</td>
<td>3.84</td>
</tr>
</tbody>
</table>

Table 2: (a) The average faithfulness for Lasso with different $\alpha$; (b) The average classification accuracy for images masked by our method and ExcitationBP so that only highlighted areas are shown to the classifier.

In Table 1(b), we show the results from a preliminary human study to compare the performance of SRAE and Lasso. Given the visualization heatmaps for each x-feature, each participant needs to choose which parts (including 15 parts of birds and the context) each heatmap represents. Then, one can use the same quantitative metrics to determine whether the heatmaps from 1 x-feature represent the same part in different images. 8 persons participate in the human study, including 4 experts and 4 non-experts in computer science. We compared SRAE with Lasso in 5 randomly selected categories with 2,810 heatmaps in total. The number of the x-features is 5. We observe that the orthogonality and locality of SRAE are smaller than those of Lasso (the approach with the best locality among competitors), indicating that our method performs better in explaining the deep networks from human subjective judgments.

We also show some qualitative examples from different categories in Fig. 4. Fig. 4(a) shows the most important x-feature in several categories, where we can see that they fit our intuitions on the discriminative features of the birds. Fig. 4(b) compares x-features with directly running ExcitationBP on $\hat{y}$. One can see x-features nicely separate different discriminative aspects of the bird while ExcitationBP sometimes focuses only on one part and miss others, and sometimes produces a heatmap that incorporates many parts simultaneously. Also, each x-feature seems distinct enough as a concept. Hence we believe they indeed provide more explanation on the decisions made by CNN algorithms. More qualitative results are shown in the Appendix.

To further examine whether the proposed algorithm offers a complete explanation of the decision made by the CNN, we attempted to try to classify just using the regions that are presented in the heatmaps, similar to (Gonzalez-Garcia et al., 2016). First, images are masked so that pixels that have < 5% of the highest response in the heatmap are painted as black; then an inpainting algorithm is applied to recover the masked images; finally we utilize the prediction CNN to classify the recovered images and test the classification accuracy. In Table 2(b), one can see that ExcitationBP fails in more cases whereas the 5 heatmaps from x-features result in substantially increased classification accuracy. More experimental results are shown in the Appendix.
5 Conclusion

In this paper we propose an explanation module, that can be attached to any layer in a deep network to compress the layer into several concepts that can approximate a 1-dimensional prediction output from the network. A sparse reconstruction autoencoder (SRAE) is proposed to avoid degeneracy and improve orthogonality. We also proposed automatic evaluation metrics to evaluate the explanations on a fine-grained bird classification dataset. Quantitative and qualitative results show that the network can indeed extract high-level concepts from a CNN that make sense to human. We view this work as one of the first steps toward understanding deep learning and have many future plans to it, including performing more experiments on different kinds of data, including those without ground truth, and extending it to explain other types of neural networks, such as recurrent networks and convolutional-recurrent ones.

References


under review as a conference paper at ICLR 2018


6 APPENDIX

For the CUB-200-2011 dataset, the given part label of each image is just one pixel in the middle of the part. For the p-th part label of image \( I_m \), we denote \((i_p,j_p)\) as its pixel location. The pixel level probability is defined as \( S_{p,m}^{n,m} = P(\text{Pixel}_{i_p,j_p}^m | \text{Neuron}_n) \). Figure 5(a) shows the probability \( S_{p,m}^{n,m} \) for each neuron \((n = 1, \ldots, 9)\) at the pixel locations of the part labels \((p = 1, \ldots, 15)\) for the example image shown in Figure 3(a). From Figure 5(a) we observe that the probability \( S_{p,m}^{n,m} \) is reasonable when capturing small parts like eye and beak, but is not on larger parts like wing and tail, for the part label is just one pixel in the middle of the wing or tail, while the x-features mainly focus on the edges (Fig. 3(a) shows an example). Thus, we utilize the Voronoi diagram to partition the bounding box into 15 regions in which the nearest neighbor part annotation in each region would be the same. However, the larger parts such as wing and tail always obtain a much higher scores than the smaller parts such as eye and beak do; and there are also many background pixels far from the center contained in the Voronoi diagram. To solve these issues, we introduce the inverse distance as a factor when computing the Voronoi-based probability \( S_{p,m}^{n,m} \) in Algorithm 1, trying to keep the balance between the large part region and the small part region. Figure 5(b) shows the probability \( S_{p,m}^{n,m} \) for each neuron and each part label for the same example image in Figure 3(a). From Figure 5(b) one can also see evidence that the probabilities on wing, tail, and belly of some neurons are higher, indicating the metric based on the Voronoi diagram enhances the evaluation on these larger parts.

**Algorithm 1:** The metric based on Voronoi diagram

\begin{verbatim}
foreach Neuron n of X layer in image I_m do
  foreach Part p with its Voronoi graph G_p do
    foreach Pixel (i, j) ∈ G_p do
      Compute the distance between (i, j) and part label (i_p, j_p): \( d_{ijp} = ((i - i_p)^2 + (j - j_p)^2)^{\frac{1}{2}} \)
      Normalize the distance \( d_{ijp} \) into [0, 1], obtain the normalized distance \( \bar{d}_{ijp} \)
    foreach Pixel (i, j) ∉ G_p do
      \( \bar{d}_{ijp} = 1 \)
      \( P(\text{Part}_p^m | \text{Pixel}_{i,j}^m) = 1 - \bar{d}_{ijp} \)
    Compute the probability \( S_{p,m}^{n,m} = P(\text{Part}_p^m | \text{Neuron}_n) = \sum_{(i,j)\in I_m} P(\text{Part}_p^m | \text{Pixel}_{i,j}^m) P(\text{Pixel}_{i,j}^m | \text{Neuron}_n) = \sum_{(i,j)\in I_m} (1 - \bar{d}_{ijp}) S_{i,j}^{n,m} \).
\end{verbatim}

Table 3 shows more results for the mask, inpainting, and classification task. In Table 3, images are masked so that pixels that have \(< \gamma \) of the highest response in the heatmap are painted as black; then an inpainting algorithm is applied to recover the masked images; finally we utilize the prediction CNN to classify the recovered images and test the classification accuracy.

Figure 6 shows the most important x-feature for several categories. The weight above the feature is \( v_i E_i \), the product of the weight of the x-feature in the approximation of \( \hat{y} \) timed by the activation of the x-feature.

Figure 7 shows some examples to illustrate the degeneration issue. Our propose method SRAE can avoid degeneration, and make the prediction model explainable.

Figure 8 compares x-features with directly running ExcitationBP on \( \hat{y} \). One can see x-features nicely separate different discriminative aspects of the bird while ExcitationBP sometimes focus only on one part and miss others, and sometimes produces a heatmap that incorporates many parts simultaneously. Also, each x-feature seems like a distinct visual feature that makes sense at least to the authors.

![Figure 5](attachment:image.png)  
**Figure 5:** (a) Pixel-level probability \( S_{p,m}^{n,m} \), (b) Voronoi-based probability \( S_{p,m}^{n,m} \) for the example image in Figure 3(a).
Table 3: The average classification accuracy on images masked by our method and ExcitationBP, respectively. Here results with different thresholds $\gamma$ are reported. With larger $\gamma$, less image region is shown to the classifier hence classification becomes more difficult.

<table>
<thead>
<tr>
<th>Method</th>
<th>Original Image</th>
<th>Mask by x-features</th>
<th>Mask by ExcitationBP</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\gamma = 1%$</td>
<td>0.8798</td>
<td>0.8972</td>
<td>0.7921</td>
</tr>
<tr>
<td>$\gamma = 5%$</td>
<td>0.8798</td>
<td>0.8428</td>
<td>0.6742</td>
</tr>
<tr>
<td>$\gamma = 10%$</td>
<td>0.8798</td>
<td>0.7771</td>
<td>0.5481</td>
</tr>
<tr>
<td>$\gamma = 30%$</td>
<td>0.8798</td>
<td>0.4097</td>
<td>0.1832</td>
</tr>
</tbody>
</table>

Figure 6: The most important x-feature for several categories. The weight above the feature is $v_i E_i$, the product of the weight of the x-feature in the approximation of $\hat{y}$ timed by the activation of the x-feature.

Figure 7: (a) Good examples learned by SRAE, the number of the x-feature is 3, where the 3 neurons are orthogonal to each other; (b) Degenerated examples learned by NN, the number of the x-feature is 3, where the first two neurons are very similar, and there is only one positive neuron; (c) Another degenerated example learned by NN, the number of the x-feature is 9. Most of the neurons are very similar, and there are only two positive neurons.
Figure 8: ExcitationBP on the predictions and on the x-features.