Generative Adversarial Residual Pairwise Networks for One Shot Learning

Akshay Mehrotra
akshay.mehrotra@csa.iisc.ernet.in
Indian Institute of Science
Bangalore

Ambedkar Dukkipati
ad@csa.iisc.ernet.in

Abstract

Deep neural networks achieve unprecedented performance levels over many tasks and scale well with large quantities of data, but performance in the low-data regime and tasks like one shot learning still lags behind. While recent work suggests many hypotheses from better optimization to more complicated network structures, in this work we hypothesize that having a learnable and more expressive similarity objective is an essential missing component. Towards overcoming that, we propose a network design inspired by deep residual networks that allows the efficient computation of this more expressive pairwise similarity objective. Further, we argue that regularization is key in learning with small amounts of data, and propose an additional generator network based on the Generative Adversarial Networks where the discriminator is our residual pairwise network. This provides a strong regularizer by leveraging the generated data samples. The proposed model can generate plausible variations of exemplars over unseen classes and outperforms strong discriminative baselines for few shot classification tasks. Notably, our residual pairwise network design outperforms previous state-of-the-art on the challenging mini-Imagenet dataset for one shot learning by getting over 55% accuracy for the 5-way classification task over unseen classes.

1. Introduction

Human intelligence is considered the epitome towards which man-made intelligent systems strive. Two specific abilities that set the human mind apart are its ability to generalize to related but unseen data and its ability to learn from small quantities of data. As machine learning methods have seen tremendous progress in recent years there has been growing focus on measuring the ability of models to generalize to unseen varieties of data and to learn from even very little of it. This is the aim of the one-shot learning problem [20]. Specifically, given a dataset some of whose classes are not used for training, the model is tested for its ability to classify over those unseen classes using a single example for each class. Essentially, the model must learn features that generalize across classes. The one shot learning problem has been studied under various domains like Bayesian learning [6][26] and deep representation learning using distance metrics [18]. Deep networks till recently were felt unsuited for such a problem given the huge number of parameters involved and the possibility of overfitting on a problem with very little data. However recent work [34] [23] has shown that deep models, especially recurrent architectures, can perform very well on the one-shot task.

The focus of our work, however is on two aspects which we believe are essential for a model to do well on the task of one shot learning - inferring an accurate semantic representation in a low dimensional manifold and strong regularization. Convolutional Neural Nets are very effective at both, as is shown by their success on many image classification tasks. We additionally enforce the first criteria by presenting a hypothesis that learning an end-to-end trainable distance measure is better than a fixed distance metric (see figure 1). We do this by implementing a modification of the residual network architecture [12]. Specifically our modification involves using skip residual connections and we refer to the our model as Skip Residual Siamese Network (SRPN). The model takes a pair of images and outputs a single similarity embedding vector. We train this model end-to-end for the similarity matching objective and then use it for few shot classification tasks on the Omniglot and mini-Imagenet datasets.

We propose a solution to the second problem in the form of a novel architecture derived from the Generative Adversarial Networks (GAN) [9]. The field of generative modelling has seen rapid advancement in the past few years. This can majorly be attributed to the development of various frameworks that work well in tandem with deep neural networks. Models have been developed that are able to efficiently approximate data distributions well enough to be of practical utility. An interesting subclass of such models is that of the implicit variety [22] which do not prescribe a fixed parametric form for the learned distribution. These
models are consequently trained using methods of comparison instead of maximizing a fixed log-likelihood function. The de facto framework for implicit models is Generative Adversarial Networks (GANs), which has been successfully used for many learning tasks. While this framework has received great interest, work towards understanding its generalization in the low-data regime and its applicability for tasks such as one shot learning has been limited. Our work attempts to bridge that gap and show that GANs provide effective regularization on unseen data distributions. Specifically, we extend the framework by trying to generate a conditional distribution which can regularize a siamese matching network. The siamese network is itself modified to incorporate a feedback that trains the generator along with the task of similarity matching. Thus, our model can be considered an instance of multi-task learning [2]. We show that the generated data is a strong regularizer for the similarity-matching task and helps in generalization to unseen classes.

1.1. Related Work

Our work is closely related to that on similarity matching using Siamese Networks [1], which was extended for convolutional networks for face verification in [3]. Koch et. al [18] show results using convolutional variants of these networks on the few shot classification tasks for Omniglot. Various formulations for the similarity objective such as contrastive loss [10] and triplet loss [35] and efficient methods to do the same [28] are also closely related.

Other related approaches include those based on Deep Metric Learning such as deep embeddings for triplet loss [13] and better metrics for fine-grained similarity [24], and popular methods like Neighbourhood Component Analysis [15].

The few shot problem specifically has been studied from multiple perspectives, including the similarity-matching [18], optimization [23], metric learning [34], hierarchical graphical models [26] etc. Our work falls in the similarity-matching paradigm i.e. the model learns to classify by individually comparing and contrasting the similarities of the given class data with the test example at hand. To the best of our knowledge, the earliest work on this problem is using Bayesian methods [6][7]. Salakhutdinov et. al [26] proposed an elegant approach using hierarchical bayesian models. Lake et. al [19][20] develop the framework of Bayesian Program Learning that naturally inculcates predicting by learning from small amounts of data. They also developed the Omniglot dataset used in our experiments. Recent work includes methods that try to use deep networks for learning embeddings which are the fed to recurrent networks for calculating embeddings [34]. Vinyals et. al [34] also propose an approach for learning the similarity embedding based on the full context of the input set as opposed to pairwise comparisons used in typical similarity matching settings, including this work. They also modify the training procedure to be similar to the testing protocol for few shot learning. Another recent work [30] also explicitly optimizes the one shot learning objective by essentially training the model for multiclass classification in the one shot setting. In contrast, this work aims to show that deep residual networks are naturally well suited to generalization objectives and even the proper pairwise similarity matching objective can perform the one shot task well. The recent work in [29] proposes a recurrent model that also outputs a pairwise embedding, however their reasoning is towards using attention to selectively infer the next step whereas we are focused on a natural, scalable extension to the CNN for one-shot learning.

Another related area is that of deep generative models for one-shot learning. Edwards et. al [5] propose handling the one shot classification task by learning dataset statistics using the amortized inference of a variational auto-encoder. Another popular framework of Generative Modeling - GANs [9] and their conditional [21] [8] alternatives are the essential components of our Generative Regularizer. Our design of using the generator with a discriminator is inspired by the ImprovedGAN model [27] for semi-supervised learning. Another work which uses generated images for improving one shot learning is [11], although they train their model as a transformer for test time generations using cosine similarity in the training set to generate analogies instead of an adversarial loss.
1.2. Contributions

To summarize, our work proposes a model for similarity matching with two suggested improvements for similarity measures and . The specific contributions are:

- We propose using a trainable distance measure for the task of one shot learning, and our implementation based on the modification of the residual network achieves state-of-the-art on the challenging mini-Imagenet dataset
- We show that generated data acts as a strong regularizer for the task of similarity matching and design a novel network based on the GAN framework that shows improvements for the one shot learning task

2. Preliminaries

2.1. Few Shot Learning

The objective of few shot learning is to measure the ability of a model to learn generalizable features across classes unseen during training. Specifically, the model is trained on labelled training data \((x, y)\) where each example comes from a subset of the total classes \(C_{\text{train}} \subset C\). Then during the testing phase, the model is provided with a single example from each of the chosen classes in \(C_{\text{test}} \subset C - C_{\text{train}}\) from the disjoint testing set. Using these examples only as the support set \(S\), the model must correctly classify another sample chosen from \(C_{\text{test}}\). The number of classes in \(C_{\text{test}}\) (generally 5 or 20) and the number of examples (generally 1 or 5) characterize the problem.

2.2. Generative Adversarial Networks

Generative Adversarial Networks (GANs) propose a method for learning a continuous-valued generative model without a fixed parametric form for the output. This is done by establishing a generator function that maps from latent to data space and a discriminator function that maps from the data space to a scalar. The discriminator function \(D\) tries to predict the probability of the input being from \(p_{\text{data}}\), and the generator is trained to maximize the error of the discriminator on \(G(z)\). Both the generator and the discriminator are parametrized as deep neural networks. The value function of this min-max formulation can be written as follows:

\[
\min \phi \max \theta \mathcal{V} = \mathbb{E}_{x \sim p_{\text{data}}} \log(D_\theta(x)) + \mathbb{E}_{z \sim G_\phi(z)} \log(1 - (D_\theta(x)))
\]  

(1)

3. Models

3.1. Skip Residual Pairwise Network

Siamese networks in literature have been typically referred to models that have two identical feed-forward paths to generate embeddings for two data-points and the similarity is then computed as a function \(g\) of these two embeddings. While this is a successful paradigm, one can argue that the choice of \(g\) is arbitrary and the model is forced to learn an embedding that works well with a particular choice of \(g\). Such a choice may often be sub-optimal, such as when the embedding itself is an intermediate step in a solving a problem such as similarity matching for one-shot learning.

To circumvent this we propose a pairwise network which is takes as input a pair of data points and is trained end-to-end to optimize a particular objective - in our case the similarity between two data points. Note that this leads to the loss of symmetric property necessary for metrics.

Our network design is presented in figure 2. The initial part of the network focusing on most abstract features is similar to an ordinary residual network. Then, the intermediate embeddings are split for the input pair and are fed through different pathways alternating between a residual skip connection using \(1 \times 1\) convolutions and two \(3 \times 3\) convolutions with Batch Normalization [14] and a non-linearity. The network is designed thus to ensure 2 objectives:

- ensure adequate mixing i.e. allow the intermediate representation of one data point to affect the intermediate representation of the other data point, instead of mixing only at the final layer as in normal siamese networks
- maintain the residual structure which has been successfully trained for very deep networks

The final output of our model is then a single embedding which is fed into a linear classifier to predict the similarity. The whole network is trained end-to-end using the binary cross-entropy loss similar to a normal siamese network.

**Multiplicative Units:** Multiplicative gating units have been shown to be effective in learning with deep models [31]. Multiplicative interactions could improve performance in our case by allowing better mixing of information from the two sources. We followed the formulation used in [16] to replace the second rectified linear unit activation in our block with a three-gated multiplicative unit. However, we found it did have any significant positive effect on the mini-Imagenet experiments while increasing the number of parameters substantially, thus we refrain from using it in our final model.

3.2. Generative Regularizer

We adapt the Generative Adversarial Network to create the second model whose purpose is to provide better regularization for the similarity matching task. The proposed model consists of two networks - a similarity matching discriminator network \(D_\phi(\cdot)\) and a generator network \(G_{\phi}(\cdot)\)
Figure 2. Our proposed model Skip Residual Pairwise Net (SRPN). The network separates the intermediate computations for the inputs \( x \) and the image being compared \( x_t \), which are then passed through separate pathways using the residual connections. The final output is a single similarity vector for the pair where the distance measure is itself learned by the network.

where \( \phi, \theta \) are the parameters of the networks. The objective of the discriminator network is to predict whether an input data point \( x \) belongs to the same class-conditional distribution as another data point \( x_t \). The discriminator is simultaneously trained to classify the generated images as fake. The generator is trained with the objective of being able to generate plausible variations of a given image - i.e. images that belong to the same class conditional distribution as the input image \( x_t \). The structure of our model is depicted in figure 3. The mathematical formulation of the two networks is described below.

**Discriminator Network:** The discriminator network \( D_\phi(x, x_t) \) tries to predict the probability whether the input data point \( x \) belongs to the same class-conditional distribution as \( x_t \), i.e. \( x \sim p_{\text{data}}(x|\text{class}(x_t)) \) where \( \text{class}(x_t) \) is the class of the data point \( x_t \). Thus, the network tries to maximize the probability for \( x \sim p_{\text{data}}(x|\text{class}(x_t)) \) and minimize it for \( x \sim p_{\text{data}}(x|\text{class} \neq \text{class}(x_t)) \) and \( x \sim p_{\text{gen}}(x|G(\tilde{x})) \). We avoid using explicit label vectors for \( \text{class}(x_t) \) chiefly because of 2 reasons: i) we do not want the network to memorize class details but instead only the invariant transformations ii) it would prevent conditioning the generator over classes unseen during training. The network is simultaneously trained to minimize with \( x \) drawn from any other distribution. It thus also acts as the similarity-based classifier where similarity is ascertained from class labels.

For our purpose we found that having the discriminator separate outputs for \( p_{\text{data}}(x|\text{class} \neq \text{class}(x_t)) \) and \( p_{\theta}(x|\tilde{x}_t) \) leads to better performance. This is consistent with the work of [27] for semi-supervised learning. Hence we formulate our discriminator to minimize the following loss:

\[
L_{\text{dis}} = -\mathbb{E}_{(x, x_t, y) \sim p_{\text{data}}} \log(p_{\phi}(y|x, x_t)) - \mathbb{E}_{x \sim p_{\theta}} \log(1 - p_{\phi}(y = 0,1|x, x_t)) \quad (2)
\]

where \( y = 1 \) is the label associated with the tuple \( (x, x_t) \), \( x \sim p_{\text{data}}(x|\text{class}(x_t)) \) and \( y = 0 \) is associated with \( x \sim p_{\text{data}}(x|\text{class} \neq \text{class}(x_t)) \).

**Generator Network:** The generator in our proposed model is a parametric function \( G_\theta(.) \) that maps from the data space to another point in the same space, i.e. acts as an auto-encoder. To prevent the generator from simply copying the input we enforce regularization by corrupting the input data point \( x_t \) by some stochastic process. The corrupted input data point \( \tilde{x}_t \) is then down-scaled by passing through a series of convolutions followed by up-scaling using a series of transposed convolutions. Essentially our generator behaves as a denoising autoencoder [33] but instead of a reconstruction loss it is trained with an adversarial loss. The generator is trained to minimize the following objective:

\[
\mathcal{L}_{\text{gen}} = -\mathbb{E}_{x \sim p_{\text{data}}, \tilde{x} \sim \mathcal{C}(\tilde{x}|x)} \log(p_{\phi}(y = 1|G_\theta(\tilde{x}), x_t))
\]

(3)

4. Experiments

We perform experiments to validate the proposed models for few shot learning over two datasets - Omniglot and mini-Imagenet. All our models are implemented using the Lasagne library [4] for Theano [32].

4.1. Omniglot

Omniglot was introduced in [20] for the express purpose of measuring one shot learning performance of models. It consists of 1623 classes of characters with 20 binary images per class. Results on the dataset have been reported using two different configurations in literature - a within alphabet setting of [20] and the more recent across alphabet setting of [34]. In this paper we follow [34] to have consistent results with other recent works.
Figure 3. An indicative figure of the proposed Generative Regularizer model. The Discriminator \( D_\phi \) takes two samples \( x, x_t \) and outputs a probability distribution over the 3 indicated output classes. The conditioning sample \( x_t \) is spatially transformed and fed to the discriminator. The other data point \( x \) comes from either the Generator which takes as input the corrupted conditioning data point \( x_t \) or from real data samples. Since the labels are known, the real data point \( x \) is chosen with equal probability from the same class as \( x_t \), or a different one.

Figure 4. One-shot generation results over unseen classes. The first row is of the samples from the test set used to condition the generator.

The dataset is divided into two parts - the first 1200 classes are used for training and validation, while the remaining are test classes for the few shot tasks. For this dataset we follow the training protocol (algorithm 1) with num tests = 200 and runs per test = 20.

We tested both our proposed improvements, Skip Residual Pairwise Networks (SRPN) and Generative Regularizer (GR) on this dataset.

We train two architectures for the convolutional siamese network: i) Siam-I: a smaller one with 5 convolutional layers and a final global pooling layer ii) Siam-II: a larger network with 5 residual blocks followed by global pooling. We follow the Wide Residual Networks design with k=2 [36]. We modify Siam-II for the design of our SRPN model. While the depth of Siam-I and Siam-II is different, both have a similar number of trainable parameters. We also use these convolutional siamese networks as baselines for our proposed models.

To ensure consistency with other published results, we rescale the images to 28x28 pixels, and augment the training data with random rotations (by ±45 degrees and/or translations (6 pixels) in both X and Y axis. The training is done using mini-batch gradient descent with Adam [17] updates and batch size of 128. The initial learning rate is set to \( 8 \times 10^{-4} \) and \( \beta_1 = 0.5 \) for GR experiments. L2 regularization is used with all models except those with GR. We maintain a validation set of 60 classes from training for early stopping. Results are reported in table 1

4.2. Mini-Imagenet

Mini-Imagenet was introduced recently in [34] as a more challenging dataset for one shot learning tasks. The dataset consists of 100 classes of natural images from the Imagenet
total-correct-pred = 0;
for num-tests do
    sample support set $S$ by randomly picking $N$ classes and 1 example for each of those classes;
    for runs-per-test do
        sample a test case $x_t$ from one of the classes in $S$;
        if predict($S, x_t$) == class($x_t$) then
            total-correct-pred += 1
        end
    end
end
return (total-correct-pred / (num-tests*runs-per-test))

Algorithm 1: Testing protocol for $N$-way one shot learning

Figure 5. Actual data samples from some of the test classes for the Mini-Imagenet Dataset. Each column shows two images from the same class. Given the huge inter-class variation in these natural images, the problem of recognizing the class by comparing it to a single image of each of the other classes is challenging.

dataset [25] with 600 RGB images per class, rescaled to 84x84 pixels. Since the standard splits for the dataset were not released, researchers have reported results by randomly selecting 100 classes from the Imagenet dataset [23],[30]. We follow a similar practice here.

The dataset is divided into two parts - the first 80 classes are used for training and validation, while the remaining are test classes for the few shot tasks. For this dataset we follow the training protocol (algorithm 1) with num-tests = 100 and runs-per-test = 100.

We tested both our proposed improvements, Skip Residual Pairwise Networks (SRPN) and Generative Regularizer (GR) separately on this dataset. However we found that Generative Regularization (GR) did not yield any benefits for these very deep models as the generator itself was not able to learn well. We believe it is due to the unstable nature of GAN training. Hence we only report results on Skip Residual Pairwise Networks (SRPN) for this task.

Since network depth has been shown to be essential for good performance on Imagenet, we restrict ourselves to the Wide Resnet model [36] with network depth of 40 and $k=2$. We train a siamese network using this model as our baseline and we modify it for the design of our SRPN model to ensure the results are comparable.

To ensure consistency with other published results, we rescale the images to 84x84 pixels. No data augmentation or pre-processing of any kind is done. The training is done using mini-batch gradient descent with Adam [17] updates and batch size of 64. Both models are trained for 100000 updates. The initial learning rate is set to $5 \times 10^{-4}$, and is annealed linearly to $1 \times 10^{-4}$. L2 regularization is used for both models with initial value of $5 \times 10^{-7}$ increased to $1 \times 10^{-6}$ after 60000 updates. Results are reported in table 2.

| Model                      | 1 shot | 5 shot |
|----------------------------|--------|--------|
| Baseline (Siam-I)         | 88.4   |        |
| Baseline (Siam-II)        | 92.0   |        |
| GR + Siam-I               | 93.6   |        |
| GR + Siam-II              | 91.2   |        |
| SRPN                      | 94.8   |        |

Table 1. Accuracy (%) for the 20-way one shot learning experiment on the Omniglot dataset.

| Model                      | 1 shot | 5 shot |
|----------------------------|--------|--------|
| Pixel Distance [34]        | 26.7   | 25.5   |
| Matching Nets w/ Finetuning [34] | 93.5   | 91.8   |
| Neural Statistician [5]    | 93.1   |        |
| Conv ARC [29]              | 97.5   |        |
| Prototypical Networks [30] | 96.0   |        |
| Baseline (Wide Resnet depth=40) | 50.7   | 55.0   |
| SRPN                       | 55.2   | 69.6   |

Table 2. Accuracy (%) for the 5-way few shot learning experiments on the mini-Imagenet dataset. Note that all models have reported results using a random 100 class subset of the Imagenet dataset.

5. Discussion

We discuss some observations about our two suggested models - the Skip Residual Pairwise Network (SRPN) and the Generative Regularizer (GR). First, we notice that not only does the SRPN achieve higher accuracy than the equivalent Residual Siamese Network but its convergence is much faster and the mean network weight is noticeably smaller. (see figure 6,7) In our opinion, this happens because the SRPN is not forced to learn an embedding that
works well with a fixed distance metric, instead it is able to adapt to the distance measure that best minimizes the total loss. This allows the network to find a manifold which reduces the similarity loss as well as the regularization penalty, effectively leading to better generalization performance. We also note that while the SRPN is not explicitly trained to learn a symmetric embedding the model does this automatically as can be seen by the diminishing difference between the embeddings (pre-final layer) in figure 8.

Also interesting to note is that for the mini-Imagenet task our siamese residual net baseline outperforms the previous state-of-the-art, which reinforces the importance of depth in complicated image recognition tasks but is also an indicator that deep convolutional models with millions of parameters can be successful in learning from features that generalize well to unseen data distributions and thus do well in the one shot learning setup.

Our experiments with the Generative Regularizer (GR) give a mixed-bag of results - the regularization is much more effective than L2 regularization as shown by the results on Omniglot with Siam-I model reaffirming the results in semi-supervised learning with such methods [27]. However, training the generator-discriminator framework is challenging due to its sensitivity to hyperparameters, often leading to poorly trained generator that impedes training as seen with very deep models as discriminators. We believe that advances in the GAN training methodology could be applied here directly and that a properly trained GR+SRPN network would outperform one with L2-regularization.

As an aside, we also tried training the GR model without providing conditioning information, ie. mapping from Gaussian noise to the image space. We observed that the generator inevitably collapsed to a single point, but was still able to regularize the siamese network. This indicates that there are multiple failure modes of the generator and that good generation is not essential for regularization. We will continue to experiment in this direction.

6. Conclusion

To summarize, we identified fixed distance measures and weak regularization as major challenges to similarity matching and its extension to one shot learning and presented a network design for each of the problems. Our Skip Residual Pairwise Network outperforms an equivalent Residual Siamese Network and achieves state of the art performance on the mini-Imagenet one shot classification dataset. Our Generative Regularizer shows promising results and outperforms L2-regularization on the Omniglot dataset. Future work would focus on integrating the two networks presented here by tapping into advancements in the training of Generative Adversarial models.

References

[1] J. Bromley, J. W. Bentz, L. Bottou, I. Guyon, Y. LeCun, C. Moore, E. Säckinger, and R. Shah. Signature verification using a "siamese" time delay neural network. IJPRAI, 7(4):669–688, 1993.
[2] R. Caruana. Multitask learning. In Learning to learn, pages 95–133. Springer, 1998.
[3] S. Chopra, R. Hadsell, and Y. LeCun. Learning a similarity metric discriminatively, with application to face verification. In Computer Vision and Pattern Recognition, 2005.
A. Manzagol. Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion. Journal of Machine Learning Research, 11(Dec):3371–3408, 2010. 4

F. Schroff, D. Kalenichenko, and J. Philbin. Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 815–823, 2015. 2

P. Shyam, S. Gupta, and A. Dukkipati. Attentive recurrent comparators. arXiv preprint arXiv:1703.00767, 2017. 2, 6

J. Snell, K. Swersky, and R. Zemel. Prototypical networks for few-shot learning. arXiv preprint arXiv:1703.05175, 2017. 2, 6

R. K. Srivastava, K. Greff, and J. Schmidhuber. Highway networks. arXiv preprint arXiv:1505.00387, 2015. 3

Theano Development Team. Theano: A Python framework for fast computation of mathematical expressions. arXiv e-prints, abs/1605.02688, May 2016. 4

P. Vincent, H. Larochelle, I. Lajoie, Y. Bengio, and P.-A. Manzagol. Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion. Journal of Machine Learning Research, 11(Dec):3371–3408, 2010. 4

O. Vinyals, C. Blundell, T. Lillicrap, D. Wierstra, et al. Matching networks for one shot learning. In Advances in Neural Information Processing Systems, pages 3630–3638, 2016. 1, 2, 4, 5, 6

K. Q. Weinberger and L. K. Saul. Distance metric learning for large margin nearest neighbor classification. Journal of Machine Learning Research, 10(Feb):207–244, 2009. 2

S. Zagoruyko and N. Komodakis. Wide residual networks. arXiv preprint arXiv:1605.07146, 2016. 5, 6