Neural Simpletrons – Learning in the Limit of Few Labels with Directed Generative Networks

Dennis Forster
Machine Learning Group
University of Oldenburg
26129 Oldenburg, Germany
FIAS, Goethe-University
60438 Frankfurt, Germany
dennis.forster@uol.de

Abdul-Saboor Sheikh
Zalando Research
11501 Berlin, Germany
Cluster of Excellence H4a
University of Oldenburg
26129 Oldenburg, Germany
sheikh.abdulsaboor@gmail.com

Jörg Lücke
Machine Learning Group
Cluster of Excellence H4a &
RC Neurosensory Sciences
University of Oldenburg
26129 Oldenburg, Germany
joerg.luecke@uol.de

Abstract

We investigate the task of classifier training for data sets with limited labels using a neural network derived from a hierarchical normalized Poisson mixture model. With the single objective of likelihood optimization, both labeled and unlabeled data are naturally incorporated into learning. Using standard benchmarks for non-negative data, such as text document representations (20 Newsgroups), MNIST and NIST SD19, we study the classification performance when only very few labels are used for training and parameter tuning. In different settings, the network’s performance is compared to standard and recently suggested semi-supervised classifiers. While other recent approaches are more competitive for many labels or fully labeled data sets, we find that the here studied network can be applied to limits of few labels where no other system has been reported to operate so far.

1 Introduction

Large data sets, e.g., in the form of digital texts, images or sounds, become increasingly ubiquitous. However, acquisition of fully labeled data becomes increasingly costly with larger amounts of data points, as correct labeling requires ground-truth or a human who can hand-label the data. Consequently, classifiers leveraging information from both labeled and unlabeled data have in recent years shifted into the focus of many research groups (Liu et al., 2010; Weston et al., 2012; Pitelis et al., 2014; Kingma et al., 2014; Forster et al., 2015; Rasmus et al., 2015; Miyato et al., 2015). Typically, a supervised deep neural network (DNN) is used in combination with additional mechanisms that allow usability when labels are limited. However, such systems generally come with large numbers of free parameters, which in the semi-supervised setting increases the risk of overfitting to very small validation sets. Alternatively, standard probabilistic networks, e.g., in the form of deep directed graphical models (DDMs) can in principle be trained using unlabeled and labeled data. However, while being potentially very powerful information processors, typical directed models are limited in size (compare, e.g. Larochelle and Murray, 2011; Bornschein and Bengio, 2015; Gan et al., 2015).

In contrast to DNNs and SVMs, DDMs are primarily used for unsupervised learning. For the targeted limit of few labels, DDMs thus appear as a more natural starting point if we are able to address scalability for classification applications. In order to do so, we base our study on a directed graphical model which is sufficiently richly structured to give rise to a good classifier, while it allows for efficient training on large data sets and with large network sizes. Scalability will be realized by the derivation of a neural network equivalent for maximum likelihood learning of the considered graphical model. The emerging compact and local inference and learning equations of the network can then be parallelized and scaled using the same tools as were originally developed for conventional deep neural networks. By additionally considering a minimalistic network architecture, the number of free parameters will, at the same time, be kept low and easily tunable on few labels.

LLD Workshop, 31st Conf. on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA.
2 A Hierarchical Neural Network for Learning with Limited Labels

A classification problem can be modeled as an inference task based on a probabilistic hierarchical mixture model (e.g., Duda et al., 2001). For our goal of semi-supervised learning with limited labels, we restrain the model complexity to the minimum of no more than three layers:

\[
p(k) = \frac{1}{K}, \quad p(l|k) = \delta_{lk} \\
p(c|k, R) = R_{kc}, \quad \sum_c R_{kc} = 1 \tag{1} \\
p(\tilde{y} | c, W) = \prod_d \text{Poisson}(y_d; W_{cd}). \tag{2}
\]

The parameters of the model, \(W \in \mathbb{R}^{C \times D}_{\geq 0}\) and \(R \in \mathbb{R}^{K \times C}_{\geq 0}\), will be referred to as generative weights, which are normalized to constants \(A\) and 1, respectively. The top node represents \(K\) abstract concepts or super classes \(c\) (for example, ten classes of digits). The middle node represents any of the occurring \(C\) subclasses \(s\) (like different writing styles of the digits). And the bottom nodes represent an observed data sample \(\tilde{y}\) with an according data label \(l\) (e.g., ranging from ‘0’ to ‘9’). Our model assumes non-negative observed data, and we use the Poisson distribution as an elementary distribution for non-negative observations.

For the purposes of this study, we specify a neural network formulation that corresponds to learning and inference in this hierarchical generative model. Consider the neural network in Fig. 1 with neural activities \(\tilde{y}, \tilde{s}\) and \(\tilde{t}\) and learning rules as in Tab. 1. We assume the values of \(\tilde{y}\) to be obtained from a set of unnormalized data points \(\vec{y}\) by Eq. (T1.3), and the label information to be presented as top-down input vector \(\vec{u}\) as given in Eq. (T1.2). For the neural weights \((W, R)\) of the network, we consider Hebbian learning with a subtractive synaptic scaling term (see for example Abbott and Nelson, 2000) as in Eqs. (T1.7) and (T1.8), where \(\epsilon_W > 0\) and \(\epsilon_R > 0\) are learning rates. These learning rules are local, can integrate both supervised and unsupervised learning, are highly parallelizable and they result in normalized neural weights \((W, R)\). Those we can relate to the generative weights \((W, R)\) by identifying \(s_c\) with the posterior probability \(p(c|\tilde{y}^{(n)}, t^{(l)}, \Theta)\) by Eq. (T1.4) and \(t_k\) with the neural weights as model parameters \(\Theta\). Such neural learning converges to the same fixed points as EM for the hierarchical Poisson mixture Keck et al., 2012; Forster et al., 2015; Forster and

\[\text{Figure 1: Graphical illustration of the hierarchical recurrent neural network.}\]

\[
\text{Table 1: Neural network formulation of probabilistic inference and maximum likelihood learning.}
\]

<table>
<thead>
<tr>
<th>Neural Simpletron</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
</tr>
<tr>
<td>Bottom-Up: (\tilde{y}_d) unnormalized data                       (\text{(T1.1)})</td>
</tr>
</tbody>
</table>
| Top-Down: \(u_k\) = \[
\begin{cases} 
\delta_{lk} & \text{for labeled data} \\
\frac{1}{R} & \text{for unlabeled data}
\end{cases} \tag{T1.2} 
\]
| **Activation Across Layers** |
| Obs. Layer: \(y_d = (A - D) \frac{\tilde{y}_d}{\sum \tilde{y}_d} + 1\) \(\text{(T1.3)}\) |
| 1st Hidden: \(s_c = \frac{\exp(t_k)}{\sum \exp(t_k)}\), with \(I_c = \sum \log(W_{cd})y_d + \log(\sum_k u_k R_{kc})\) \(\text{(T1.4)}\) |
| 2nd Hidden: \(t_k = \{\begin{array}{ll} 
\frac{u_k}{\sum_{k, c} R_{kc} s_c} & \text{labeled data} \\
\sum_{k, c} R_{kc} s_c & \text{unlabeled data}
\end{array}\) \(\text{(T1.6)}\) |
| **Learning of Neural Weights** |
| 1st Hidden: \(\Delta W_{cd} = \epsilon_W (s_c y_d - s_c W_{cd})\) \(\text{(T1.7)}\) |
| 2nd Hidden: \(\Delta R_{kc} = \epsilon_R (t_k s_c - t_k R_{kc})\) labeled data \(\text{(T1.8)}\) |
2.1 Simpletron Variants

We investigate different NeSi versions for learning with limited labels. All variants accord with the likelihood objective and were chosen such that the number of tunable parameters remains small: (I) The complete formulas for the first hidden layer, given in Eqs. (T1.4) and (T1.5), define a recurrent network (‘r-NeSi’), i.e., combine both bottom-up and top-down information. By removing the second term in Eq. (T1.5), we gain a feedforward network (‘ff-NeSi’) that is equivalent to treating the $p(c|k, R)$ in the first hidden layer as uniform $1/C$. (II) Using the posterior $t_k$, the network can itself provide missing training labels (often termed ‘self-labeling’; see, e.g., Lee, 2013; Triguero et al., 2015) and the ‘Best versus Second Best’ (BvSB) measure on $t_k$ gives an index for classification certainty. We then train the top layer also on those inferred labels with high certainty, i.e., where the BvSB lies above a given threshold $\theta$. We mark NeSi networks using self-labeling by a superscript ‘+’ (‘r*-NeSi’ and ‘ff*-NeSi’). (III) We apply TV-EM (Lücke, 2016) to ff*-NeSi by keeping only the $C$ highest values in $s_c$ (Eq. T1.4) and setting lower values to hard zero with subsequent renormalization. Such truncation can be shown to maximize the variational free energy of the mixture model with a significantly lower computational cost (Forster and Lücke, 2017). We refer to simpletrons with truncated middle layer activations as ‘t-NeSi’. This represents a further development of the network in Forster et al. (2015) with enhanced training and significantly improved results.

3 Parameter Tuning with Limited Labels

It is customary to regard limited numbers of labels as restriction only on training itself and not on the preceding optimization of free model parameters by using validations sets with (much) more labels than available during training. For model comparison, this however introduces a bias towards more complex models, that would be otherwise more prone to overfitting to small validation sets. We therefore train our models given a strictly limited total number of labels for the complete tuning and training procedure. For parameter tuning, we use 10 labeled training data points per class (the setting with the lowest number of labels on which models are generally compared on MNIST) with a half/half split into training and validation set. Once optimized, we keep the free parameters fixed for all following experiments. In doing so, we ensure that all our results of 10 labels per class and more are achievable by using no more labels in total than provided within each training setting. Furthermore, using only training data for parameter tuning guarantees a fully blind test set, such that the test error gives a reliable index for generalization.

4 Numerical Experiments

We apply the NeSi networks to three standard benchmarks for classification on non-negative data: the 20 Newsgroups text data set (Lang, 1995), the MNIST data set of handwritten digits (LeCun et al., 1998) and the NIST Special Database 19 of handwritten characters (Grother, 1995). We perform experiments for different proportions of randomly chosen, class-balanced labeled data and measure the mean classification error on the blind test set.

4.1 Document Classification (20 Newsgroups)

We preprocess the newsgroups data using only tf-idf weighting (Sparck Jones, 1972). No stemming, removals of stop words or frequency cutoffs were applied. We investigate semi-supervised settings of 20, 40, 200, 800 and 2000 labels in total – that is 1, 2, 10, 40 and 100 labels per class – as well as the fully labeled setting. For each setting, we present the mean test error averaged over 100 independent runs and the standard error of the mean (SEM). On each new run, a new set of class balanced labels is chosen randomly from the training set. We train our model on the full 20-class problem without any feature selection.

As reported results on the full 20-class task in the semi-supervised setting are rare, we here only compare to a hybrid of generative and discriminative RBMs (HDRBM) trained by Larochelle and Bengio (2008) using stochastic gradient descent to perform semi-supervised learning. The test errors of the methods are compared in Tab. 2. For results marked with ‘(*)’, free parameters were optimized.

<table>
<thead>
<tr>
<th>#labels</th>
<th>ff-NeSi</th>
<th>r-NeSi</th>
<th>HDRBM</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>70.64 ± 0.68 (*)</td>
<td>68.68 ± 0.77 (*)</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>55.67 ± 0.54 (*)</td>
<td>54.24 ± 0.66 (*)</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>30.59 ± 0.22</td>
<td>29.28 ± 0.21</td>
<td></td>
</tr>
<tr>
<td>800</td>
<td>28.26 ± 0.10</td>
<td>27.20 ± 0.07</td>
<td>31.8 (*)</td>
</tr>
<tr>
<td>2000</td>
<td>27.87 ± 0.07</td>
<td>27.15 ± 0.07</td>
<td></td>
</tr>
<tr>
<td>11269</td>
<td>28.08 ± 0.08</td>
<td>17.85 ± 0.01</td>
<td>23.8</td>
</tr>
</tbody>
</table>

Table 2: Test error on 20 Newsgroups.
using additional labels: NeSi used the same parameter setting in all semi-supervised experiments on 20 Newsgroups, which was tuned with 200 labels in total; HDRBM used 1000 labels in total for tuning in the semi-supervised setting (200 additional labels for the validation set).

4.2 Handwritten Digit Recognition (MNIST)

We perform experiments on MNIST in the semi-supervised setting using 10, 100, 600, 1000 and 3000 labels in total – that is 1, 10, 60, 100 and 300 labels per class →, which are randomly and class balanced chosen from the 10 classes. Results are given as the mean and standard error (SEM) over 100 independent repetitions, with randomly drawn, class-balanced labels.

Tab. 3 shows the results of the NeSi algorithms. Again, for results marked with ‘(+)*’, the free parameters were optimized using more labels than available in the given setting. We used the same parameter setting for all experiments shown here, which was tuned using 100 labels in total. As the NeSi model has no prior knowledge about spatial relations in the data, the given results are invariant to pixel permutation.

Fig. 2 shows a comparison to standard and recent state-of-the-art approaches for 100 labels and more. The performance of the models is given with respect to the number of labels used during training (left-hand side) and with respect to the total number of labels used for the complete tuning and training procedure (right-hand side). For the NeSi algorithms, these plots are identical, as we only use maximally as many labels in the tuning phase as in the training phase for the shown results of 100 labels and more. All other algorithms (for lack of more comparable findings) either use a validation set with a substantial amount of additional labels than available during training or (explicitly) use the test set for parameter tuning. Also, some of the shown results (namely the TSVM, AGR, AtlasRBF and the Em-networks) were achieved in the transductive setting, where the (unlabeled) test data is included into the training process. The NeSi approaches are to our knowledge so far the closest to our goal of a competitive algorithm in the limit of as few labels as possible. Regarding classification performance, the NeSi networks achieve competitive results, surpassing even deep belief networks (‘DBN-rNCA’) and other recent approaches (like the ‘Embed’-networks,
‘AGR’ and ‘AtlasRBF’). In the light of reduced model complexity and effectively used labels, we can furthermore compare to the few very recent algorithms with a lower error rate (‘M1+M2’, ‘VAI’ and the ‘Ladder’-networks).

One competing model that so far comes closest to our limit setting of as few labels as possible is an approach which combines 10 generative adversarial networks (GANs) (Salimans et al., 2016) with 5 layers each. With down to 20 labels for training (and an however unknown additional number of labels for the validation set) the classification error of the full ensemble of 10 GANs the error was reported to be (11.34 ± 4.45)%). This compares to an error of (7.22 ± 0.53)% for t-NeSi which was trained with only 10 labels (one per class) and used 100 labels during parameter tuning.

### 4.3 Large Scale Handwriting Recognition (NIST SD19)

To show large scale applicability, we show experiments on the NIST Special Database 19, containing over 800 000 binary 128 × 128 images. We preprocess the data similar to MNIST, which allows us to use the same setting for our free model parameters without retuning, and perform experiments on digit recognition (10 classes) and case-sensitive letter recognition (52 classes). The experiments are done using 1, 10, 60, 100, 300, or all labels per class. In Tab. 4, we report the mean and standard error over 10 experiments and compare to the state-of-the-art 35c-MCDNN (Cireşan et al., 2012). For the NeSi networks, the results are given for the permutation invariant task. To the best of our knowledge, this is the first system to report results for NIST SD19 in the semi-supervised setting.

| Table 4: Test error on NIST SD19 data set on the task of digit and letter recognition for different total amounts of labeled data. |
|---|---|---|---|---|---|
| #lbls/class | 1 | 10 | 60 | 100 | 300 | fully labeled |
| digits (10 classes) |
| #lbls total | 10 | 100 | 600 | 1000 | 3000 | 344 307 |
| t-NeSi | 7.6 ± 1.8 | 6.2 ± 0.2 | 6.0 ± 0.1 | 6.0 ± 0.1 | 5.70 ± 0.03 | 5.11 ± 0.01 |
| r-NeSi | 9.8 ± 2.4 | 6.1 ± 0.2 | 5.8 ± 0.1 | 5.9 ± 0.1 | 5.7 ± 0.1 | 4.52 ± 0.01 |
| t-NeSi | 5.7 ± 0.4 | 5.3 ± 0.2 | 4.84 ± 0.02 | 4.86 ± 0.03 | 4.84 ± 0.02 | 4.50 ± 0.01 |
| 35c-MCDNN | 0.77 |
| letters (52 classes) |
| #lbls total | 52 | 520 | 3120 | 5000 | 15 000 | 387 361 |
| t-NeSi | 55.7 ± 0.6 | 46.2 ± 0.4 | 44.2 ± 0.2 | 43.7 ± 0.2 | 43.0 ± 0.3 | 34.66 ± 0.05 |
| r-NeSi | 65.0 ± 0.9 | 54.1 ± 0.4 | 43.7 ± 0.2 | 41.6 ± 0.1 | 38.0 ± 0.1 | 31.93 ± 0.06 |
| t-NeSi | 52.1 ± 1.1 | 45.6 ± 0.4 | 41.9 ± 0.3 | 41.8 ± 0.4 | 41.1 ± 0.3 | 33.34 ± 0.04 |
| 35c-MCDNN | 21.01 |

### 5 Discussion

In this study, we explored classifier training on data sets with limited labels. We put a special emphasize on adhering to this restriction not only for the training phase, but the complete tuning, training and testing procedure. Our tool was a novel neural network with learning rules based on a maximum likelihood objective. Starting from hierarchical Poisson mixtures, the derived three layer directed data model can be observed to take on a form similar to learning in standard DNNs. The parameters of the network can be optimized with a very limited amount of labels and training in the same setting showed to achieve competitive results, giving the first network shown to operate using no more than 10 labels per class in total and down to a single training label per class on the investigated data sets.

Our main empirical results for the NeSi systems were obtained using the 20 Newsgroups, the MNIST and the NIST SD19 datasets. Tabs. 2 to 4 and Fig. 2 summarize the results and provide comparison to other approaches. The r-NeSi system is the best performing system for the 20 Newsgroups data set (Tab. 2), but comparative results were only available for HDRBM in the semi-supervised setting. Both on MNIST and NIST the performance of our 3-layer network in the fully labeled setting is not competitive to state-of-the-art fully supervised algorithms. Our results however do apply for the permutation invariant setting and do not take prior knowledge about two-dimensional image data into account (like convolutional networks do). More importantly, we only see a relatively mild decrease in test error when we strongly decrease the total number of used labels, with the t-NeSi consistently performing best. It has so far not been shown that other classifiers can be trained with similarly low total numbers of labels, as all comparable approaches use at least 1000 additional labels to optimize the free parameters of their respective systems (Fig. 2, right-hand-side). Furthermore, as all better performing approaches on MNIST combine different objectives to perform well with limited labels, the NeSi networks can be considered as the best performing non-hybrid approaches even if we only consider exclusively the labels for training (Fig. 2, left-hand-side).
References


