An Introduction to Deep Learning
Ludovic Arnold, Sébastien Rebecchi, Sylvain Chevallier, Hélène Paugam-Moisy

To cite this version:
Ludovic Arnold, Sébastien Rebecchi, Sylvain Chevallier, Hélène Paugam-Moisy. An Introduction to Deep Learning. European Symposium on Artificial Neural Networks (ESANN), Apr 2011, Bruges, Belgium. Proceedings of the European Symposium on Artificial Neural Networks (ESANN). <hal-01352061>

HAL Id: hal-01352061
https://hal.archives-ouvertes.fr/hal-01352061
Submitted on 5 Aug 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
An Introduction to Deep Learning

Ludovic Arnold¹,², Sébastien Rebecchi¹, Sylvain Chevallier³, Hélène Paugam-Moisy¹,³

1- Tao, INRIA-Saclay, LRI, UMR8623, Université Paris-Sud 11
F-91405 Orsay, France
2- LIMSI, UMR3251
F-91403 Orsay, France
3- Université Lyon 2, LIRIS, UMR5205
F-69676 Bron, France

Abstract. The deep learning paradigm tackles problems on which shallow architectures (e.g. SVM) are affected by the curse of dimensionality. As part of a two-stage learning scheme involving multiple layers of nonlinear processing a set of statistically robust features is automatically extracted from the data. The present tutorial introducing the ESANN deep learning special session details the state-of-the-art models and summarizes the current understanding of this learning approach which is a reference for many difficult classification tasks.

1 Introduction

In statistical machine learning, a major issue is the selection of an appropriate feature space where input instances have desired properties for solving a particular problem. For example, in the context of supervised learning for binary classification, it is often required that the two classes are separable by a hyperplane. In the case where this property is not directly satisfied in the input space, one is given the possibility to map instances into an intermediate feature space where the classes are linearly separable. This intermediate space can either be specified explicitly by hand-coded features, be defined implicitly with a so-called kernel function, or be automatically learned. In both of the first cases, it is the user’s responsibility to design the feature space. This can incur a huge cost in terms of computational time or expert knowledge, especially with highly dimensional input spaces, such as when dealing with images.

As for the third alternative, automatically learning the features with deep architectures, i.e. architectures composed of multiple layers of nonlinear processing, can be considered as a relevant choice. Indeed, some highly nonlinear functions can be represented much more compactly in terms of number of parameters with deep architectures than with shallow ones (e.g. SVM). For example, it has been proven that the parity function for \( n \)-bit inputs can be coded by a feed-forward neural network with \( O(\log n) \) hidden layers and \( O(n) \) neurons, while a feed-forward neural network with only one hidden layer needs an exponential number of the same neurons to perform the same task [1]. Moreover, in the case of highly varying functions, learning algorithms entirely based on local generalization are severely impacted by the curse of dimensionality [2]. Deep architectures address this issue with the use of distributed representations and as such may constitute a tractable alternative.
Unfortunately, training deep architectures is a difficult task and classical methods that have proved effective when applied to shallow architectures are not as efficient when adapted to deep architectures. Adding layers does not necessarily lead to better solutions. For example, the more the number of layers in a neural network, the lesser the impact of the back-propagation on the first layers. The gradient descent then tends to get stuck in local minima or plateaus [3], which is why practitioners have often preferred to limit neural networks to one or two hidden layers.

This issue has been solved by introducing an unsupervised layer-wise pre-training of deep architectures [3, 4]. More precisely, in a deep learning scheme each layer is treated separately and successively trained in a greedy manner: once the previous layers have been trained, a new layer is trained from the encoding of the input data by the previous layers. Then, a supervised fine-tuning stage of the whole network can be performed (see Fig. 1).

This paper aims at providing to the reader a better understanding of the deep learning through a review of the literature and an emphasis of its key properties. Section 2 details a widely used deep network model: the deep belief network or stacked restricted Boltzmann machines. Other models found in deep architectures are presented in Sect. 3, i.e. stacked auto-associators, deep kernel machines and deep convolutional networks. Section 4 summarizes the main results in the different application domains, points out the contributions of the deep learning scheme and concludes the tutorial.

2 Deep learning with RBMs

2.1 Restricted Boltzmann Machines

Restricted Boltzmann Machines (RBMs) are at the intersection of several fields of study and benefit from a rich theoretical framework [5, 6]. First, we will
Figure 2: The RBM architecture with a visible (v) and a hidden (h) layers.

present them as a probabilistic model before showing how the neural network equations arise naturally.

An RBM defines a probability distribution \( p \) on data vectors v as follows:

\[
p(v) = \sum_h \frac{e^{-E(v,h)}}{\sum_u e^{-E(u,g)}}.
\] (1)

The variable \( v \) is the input vector and the variable \( h \) corresponds to unobserved features [7] that can be thought of as hidden causes not available in the original dataset. An RBM defines a joint probability on both the observed and unobserved variables which are referred to as visible and hidden units respectively (see Fig. 2). The distribution is then marginalized over the hidden units to give a distribution over the visible units only. The probability distribution is defined by an energy function \( E \) (RBMs are a special case of energy-based models [8]), which is usually defined over couples \((v, h)\) of binary vectors by:

\[
E(v, h) = -\sum_i a_i v_i - \sum_j b_j h_j - \sum_{i,j} w_{ij} v_i h_j,
\] (2)

with \( a_i \) and \( b_j \) the biases associated to the input variables \( v_i \) and hidden variables \( h_j \) respectively and \( w_{ij} \) the weights of a pairwise interaction between them. In accordance with (1), configurations \((v, h)\) with a low energy are given a high probability whereas a high energy corresponds to a low probability.

The energy function above is crafted to make the conditional probabilities \( p(h|v) \) and \( p(v|h) \) tractable. The computation is done using the usual neural network propagation rule (see Fig. 2) with:

\[
p(v|h) = \prod_i p(v_i|h) \quad \text{and} \quad p(v_i = 1|h) = \text{sign} \left( a_j + \sum_j h_j w_{ij} \right),
\]

\[
p(h|v) = \prod_j p(h_j|v) \quad \text{and} \quad p(h_j = 1|v) = \text{sign} \left( b_j + \sum_i v_i w_{ij} \right),
\] (3)

where \( \text{sign}(x) = 1/(1 + \exp(-x)) \) is the logistic activation function.

The model with the energy function (2) defines a distribution over binary vectors and, as such, is not suitable for continuous valued data. To address this
issue, $E$ can be appropriately modified to define the Gaussian-Bernoulli RBM by including a quadratic term on the visible units [3]:

$$E(v, h) = \sum_i \frac{(v_i - a_i)^2}{\sigma_i^2} - \sum_j b_j h_j - \sum_{i,j} w_{ij} \frac{v_i}{\sigma_i} h_j,$$

where $\sigma_i$ represents the variance of the input variable $v_i$. Using this energy function, the conditional probability $p(h|v)$ is almost unchanged but $p(v|h)$ becomes a multivariate Gaussian with mean $a_i + \sigma_i \sum_j w_{ij} h_j$ and a diagonal covariance matrix:

$$p(v_i = x|h) = \frac{1}{\sigma_i \sqrt{2\pi}} e^{-\frac{(x - a_i - \sigma_i \sum_j w_{ij} h_j)^2}{2\sigma_i^2}},$$

$$p(h_j = 1|v) = \text{sigm}(b_j + \sum_i \frac{v_i}{\sigma_i} w_{ij}).$$

(4)

In a deep architecture using Gaussian-Bernoulli RBM, only the first layer is real-valued whereas all the others have binary units. Other variations of the energy function are given in [3, 9, 10] to address the issue of continuous valued inputs.

2.2 Learning with RBMs and Contrastive Divergence

In order to train RBMs as a probabilistic model, the natural criterion to maximize is the log-likelihood. This can be done with gradient ascent from a training set $D$ likewise:

$$\frac{\partial \log p(D)}{\partial w_{ij}} = \sum_{x \in D} \frac{\partial \log p(x)}{\partial w_{ij}} = \sum_{x \in D} \frac{\partial E(x, g)}{\partial w_{ij}} e^{-E(x, g)} - \sum_{u \in \mathcal{D}} \sum_{g} \frac{\partial E(u, g)}{\partial w_{ij}} e^{-E(u, g)}.$$

$$= E_{\text{data}} \left[ \frac{\partial E(x, g)}{\partial w_{ij}} \right] - E_{\text{model}} \left[ \frac{\partial E(u, g)}{\partial w_{ij}} \right],$$

where the first term is the expectation of $\frac{\partial E(x, g)}{\partial w_{ij}}$ when the input variables are set to an input vector $x$ and the hidden variables are sampled according to the conditional distribution $p(h|x)$. The second term is an expectation of $\frac{\partial E(u, g)}{\partial w_{ij}}$ when $u$ and $g$ are sampled according to the joint distribution of the RBM $p(u, g)$ and is intractable. It can however be approximated with a Markov chain Monte Carlo algorithm such as Gibbs sampling: starting from any configuration $(v^n, h^n)$, one
samples $h^t$ according to $p(h|v^{t-1})$ and $v^t$ according to $p(v|h^t)$ until the sample $(v^t, h^t)$ is distributed closely enough to the target distribution $p(v, h)$.

In practice, the number of steps can be greatly reduced by starting the Markov chain with a sample from the training dataset and assuming that the model is not too far from the target distribution. This is the idea behind the Contrastive Divergence (CD) learning algorithm [11]. Although the maximized criterion is not the log-likelihood anymore, experimental results show that gradient updates almost always improve the likelihood of the model [11]. Moreover, the improvement to the likelihood tend to zero as the length of the chain increases [12], an argument which supports running the chain for a few steps only. Notice that the possibility to use only the sign of the CD update is explored in the present special session [13].

2.3 From stacked RBMs to deep belief networks

In an RBM, the hidden variables are independent conditionally to the visible variables, but they are not statistically independent. Stacking RBMs aims at learning these dependencies with another RBM. The visible layer of each RBM of the stack is set to the hidden layer of the previous RBM (see Fig. 3). Following the deep learning scheme, the first RBM is trained from the input instances and other RBMs are trained sequentially after that. Stacking RBMs increases a bound on the log-likelihood [14], which supports the expectation to improve the performance of the model by adding layers.

![Figure 3: The stacked RBMs architecture.](image)

A stacked RBMs architecture is a deep generative model. Patterns generated from the top RBM can be propagated back to the input layer using only the conditional probabilities as in a belief network. This setup is referred to as a Deep Belief Network [4].
3 Other models and variations

3.1 Stacked Auto-Associators

Another module which can be stacked in order to train a deep neural network in a greedy layer-wise manner is the Auto-Associator (AA) [15, 16].

An AA is a two-layers neural network. The first layer is the encoding layer and the second is the decoding layer. The number of neurons in the decoding layer is equal to the network’s input dimensionality. The goal of an AA is to compute a code $y$ of an input instance $x$ from which $x$ can be recovered with high accuracy. This models a two-stage approximation to the identity function:

$$ f_{\text{dec}}(f_{\text{enc}}(x)) = f_{\text{dec}}(y) = \hat{x} \simeq x, $$

with $f_{\text{enc}}$ the function computed by the encoding layer and $f_{\text{dec}}$ the function computed by the decoding layer (see Fig. 4).

An AA can be trained by applying standard back-propagation of error derivatives. Depending on the nature of the input data, the loss function can either be the squared error $L_{\text{SE}}$ for continuous values or the cross-entropy $L_{\text{CE}}$ for binary vectors:

$$ L_{\text{SE}}(x, \hat{x}) = \sum_i (\hat{x}_i - x_i)^2, $$

$$ L_{\text{CE}}(x, \hat{x}) = \sum_i [x_i \log \hat{x}_i + (1 - x_i) \log (1 - \hat{x}_i)]. $$

The AA training method approximates the CD method of the RBM [14]. Another important fact is that an AA with a nonlinear $f_{\text{enc}}$ differs from a PCA as it is able to capture multimodal aspects of the input distribution [17].

Similarly to the parametrization in an RBM, the decoder’s weight matrix $W_{\text{dec}}$ can be set to the transpose of the encoder’s weight matrix, i.e. $W_{\text{dec}} = W_{\text{enc}}^\top$. In such a case, the AA is said to have tied weights. The advantage of this constraint is to avoid undesirable effects of the training process, such as encoding the identity function, i.e. $f_{\text{enc}}(x) = x$. This useless result is possible when the encoding dimensionality is not smaller than the input dimensionality.

An interesting variant of the AA is the Denoising Auto-Associator (DAA) [18]. A DAA is an AA trained to reconstruct noisy inputs. To achieve this
Figure 5: The training scheme of a DAA. Noisy components are marked with a cross.

goal, the instance fed to the network is not $x$ but a corrupted version $\tilde{x}$. After training, if the network is able to compute a reconstruction $\hat{x}$ of $x$ with a small loss, then it is admitted that the network has learned to remove the noise in the data in addition to encode it in a different feature space (see Fig. 5).

Finally, a Stacked Auto-Associator (SAA) [3, 19, 18, 20] is a deep neural network trained following the deep learning scheme: an unsupervised greedy layer-wise pre-training before a fine-tuning supervised stage, as explained in Sect. 2.3 (see also Fig. 1). Surprisingly, for $d$ dimensional inputs and layers of size $k \geq d$, a SAA rarely learns the identity function [3]. In addition, it is possible to use different regularization rules and the most successful results have been reported with adding a sparsity constraint on the encoding unit activations [20, 21, 22]. This leads to learning very different features (w.r.t RBM) in the intermediate layers and the network performs a trade-off between reconstruction loss and information content of the representation [21].

3.2 Deep Kernel Machines

The Multilayer Kernel Machine (MKM) [23] has been introduced as a way to learn highly nonlinear functions with the iterative application of weakly nonlinear kernel methods.

The authors use the Kernel Principal Component Analysis (KPCA) [24] for the unsupervised greedy layer-wise pre-training stage of the deep learning scheme. From this method, the $\ell + 1^{th}$ layer learns a new representation of the output of the layer $\ell$ by extracting the $n_{\ell}$ principal components of the projection of the output of $\ell$ in the feature space induced by the kernel.

In order to lower as much as possible the dimensionality of the new representation in each layer, the authors propose to apply a supervised strategy devoted to selecting the best informative features among the ones extracted by the KPCA. It can be summarized as follows:

1. rank the $n_{\ell}$ features according to their mutual information with the class labels;

2. for different values of $K$ and $m_{\ell} \in \{1 \ldots n_{\ell}\}$, compute the classification error rate of a $K$-NN classifier using only the $m_{\ell}$ most informative features on a validation set;
3. the value of $m_l$ with which the classifier has reached the lowest error rate determines the number of features to retain.

However, the main drawback of using KPCA as the building block of an MKM lies in the fact that the feature selection process must be done separately and thus requires a time-expensive cross validation stage. To get rid of this issue when training an MKM it is proposed in this special session [25] to use a more efficient kernel method, the Kernel Partial Least Squares (KPLS).

KPLS does not need cross validation to select the best informative features but embeds this process in the projection strategy [26]. The features are obtained iteratively, in a supervised manner. At each iteration $j$, KPLS selects the $j$th feature the most correlated with the class labels by solving an updated eigenproblem. The eigenvalue $\lambda_j$ of the extracted feature indicates the discriminative importance of this feature. The number of features to extract, i.e. the number of iterations to be performed by KPLS, is determined by a simple thresholding of $\lambda_j$.

3.3 Deep Convolutional Networks

Convolutional networks are the first examples of deep architectures [27, 28] that have successfully achieved a good generalization on visual inputs. They are the best known method for digit recognition [29]. They can be seen as biologically inspired architectures, imitating the processing of “simple” and “complex” cortical cells which respectively extract orientations information (similar to a Gabor filtering) and compositions of these orientations.

The main idea of convolutional networks is to combine local computations (convolution of the signal with weight sharing units) and pooling. The convolutions are intended to give translation invariance to the system, as the weights depend only on spatial separation and not on spatial position. The pooling allows to construct a more abstract set of features through nonlinear combination of the previous level features, taking into account the local topology of the input data. By alternating convolution layers and pooling layers, the network successively extracts and combines local features to construct a good representation of the input. The connectivity of the convolutional networks, where each unit in a convolution or a pooling layer is only connected to a small subset of the preceding layer, allows to train networks with as much as 7 hidden layers. The supervised learning is easily achieved, through an error gradient backpropagation.

On the one hand, convolutional framework has been applied to RBM and DBN [10, 30, 31]. In [31] the authors derive a generative pooling strategy which scales well with image size and they show that the intermediate representations are more abstract in the higher layer (from edges in the lower layers to object parts in the higher). On the other hand, the unsupervised pre-training stage of deep learning have been applied to convolutional networks [32] and can greatly reduce the number of labeled examples required. Furthermore, deep convolutional networks with sparse regularization [33] yield very promising results for difficult visual detection tasks, such as pedestrian detection.
4 Discussion

4.1 What are the applicative domains for deep learning?

Deep learning architectures express their full potential when dealing with highly varying functions, requiring a high number of labeled samples to be captured by shallow architectures. Unsupervised pre-training allows, in practice, to achieve good generalization performance when the training set is of limited size by positioning the network in a region of the parameter space where the supervised gradient descent is less likely to fall in a local minimum of the loss function. Deep networks have been largely applied to visual classification databases such as handwritten digits\(^1\), object categories\(^2\), pedestrian detection [33] or off-road robot navigation [34], and also on acoustic signals to perform audio classification [35]. In natural language processing, a very interesting approach [36] gives a proof that deep architectures can perform multi-task learning, giving state-of-the-art results on difficult tasks like semantic role labeling. Deep architectures can also be applied to regression with Gaussian processes [37] and time series prediction [38]. In the latter, the conditional RBM have given promising results.

Another interesting application area is highly nonlinear data compression. To reduce the dimensionality of an input instance, it is sufficient for a deep architecture that the number of units in its last layer is smaller than its input dimensionality. In practice, limiting the size of a neuron layer can promote interesting nonlinear structure of the data. Moreover, adding layers to a neural network can lead to learning more abstract features, from which input instances can be coded with high accuracy in a more compact form. Reducing the dimensionality of data has been presented as one of the first application of deep learning [39]. This approach is very efficient to perform semantic hashing on text documents [22, 40], where the codes generated by the deepest layer are used to build a hash table from a set of documents. Retrieved documents are those whose code differs only by a few bits from the query document code. A similar approach for a large scale image database is presented in this special session [41].

4.2 Open questions and future directions

A significant part of the ongoing research aims at improving the deep networks building blocks For RBMs, several propositions have been made to use real-valued units rather than binary ones either by integrating the covariance of the visible units in the hidden units update [42] or by approximating real-valued units by noisy rectified linear units [9, 10]. For AAs, the denoising criterion is particularly investigated since it achieves very good results on visual classification tasks [43].

\(^1\)MNIST: http://yann.lecun.com/exdb/mnist/
\(^2\)Caltech-101: http://www.vision.caltech.edu/Image_Datasets/Caltech101/
\(^3\)NORB: http://www.cs.nyu.edu/~ylclab/data/norb-v1.0/
\(^4\)CIFAR-10: http://www.cs.utoronto.ca/~kriz/cifar.html
Because the construction of good intermediate representations is a crucial part of deep learning, a meaningful approach is to study the response of the individual units in each layer. An effective strategy is to find the input pattern that maximizes the activation of a given unit, starting from a random input and performing a gradient ascent [44].

A major interrogation underlying the deep learning scheme concerns the role of the unsupervised pre-training. In [44], the authors argue that pre-training acts as an unusual form of regularization. By selecting a region in the parameter space which is not always better than a random one, pre-training systematically leads to better generalization. The authors provide results showing that pre-training does not act as an optimization procedure which selects the region of the parameter space where the basins of attraction are the deepest. Pre-training only modifies the starting point of supervised training and the regularization effect does not vanish when the number of data increases. Deep learning breaks down the problem of optimizing lower layers given that the upper layers have not yet been trained. Lower layers extract robust and disentangled representations of the factors of variations (e.g. on images: translation, rotation, scaling), whereas higher layers select and combine these representations. A fusion of the unsupervised and supervised paradigms in one single training scheme is an interesting way to explore.

Choosing the correct dimensions of a deep architecture is not an obvious process and the results shown in [29] open new perspectives on this topic. A convolution network with a random filter bank and with the correct nonlinearities can achieve near state-of-the-art results when there is few training labeled data (such as in the Caltech-101 dataset). It has been shown that the architecture of convolutional network has a major influence on the performance and that it is possible to achieve a very fast architecture selection using only random weights and no time-consuming learning procedure [45]. This, along with the work of [46], points toward new directions for answering the difficult question of how to efficiently set the sizes of layers in deep networks.

4.3 Conclusion

The strength of deep architectures is to stack multiple layers of nonlinear processing, a process which is well suited to capture highly varying functions with a compact set of parameters. The deep learning scheme, based on a greedy layer-wise unsupervised pre-training, allows to position deep networks in a parameter space region where the supervised fine-tuning avoids local minima. Deep learning methods achieve very good accuracy, often the best one, for tasks where a large set of data is available, even if only a small number of instances are labeled. This approach raises many theoretical and practical questions, which are investigated by a growing and very active research community and casts a new light on our understanding of neural networks and deep architectures.
Acknowledgements

This work was supported by the French ANR as part of the ASAP project under grant ANR_09_EMER_001_04.

References