Fundamentals of Neural Networks

Seminar Data Mining

Mathias Jackermeier
Fakultät für Informatik
Technische Universität München
Email: mathias.jackermeier@tum.de

***Abstract*— Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrumCurabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.**

***Index Terms*— test**

I. Introduction

Artificial intelligence systems have been becoming more and more powerful over the last 10 years. We have seen outstanding advances in a variety of fields including computer vision, natural language processing and fraud detection, which power many end-user technologies such as digital assistants or self-driving cars. Much of the recent progress can be attributed to *deep learning*, a powerful set of techniques that enable computers to understand the world by decomposing complex concepts into a hierarchy of simpler abstractions.

While numerous other approaches to machine learning exist, deep learning has shown to outperform other methods in a wide variety of applications. To name a few examples, deep learning models dominate the task of object recognition in images [1], even surpassing human-level performance [2], have been successfully applied to sentiment analysis [3], and have significantly improved speech recognition systems [4]. Deep learning has also been used in problems such as style transfer between images [5], image description generation [6], and learning to play video games [7].

By learning everything required to solve a task purely from raw data, these techniques have alleviated the need for problem-specific expert knowledge. Thus, very similar models building on the same core ideas can be applied to a vast array of different tasks with outstanding success.

One such core idea that is fundamental to deep learning is the *neural network*, a computing model loosely inspired by neuroscience. While neural networks are not new, it was not until recently that enough data and computational resources became available to train them effectively and fully appreciate their power [8, Ch. 1, pp. 18-21].

Since neural networks have become so prevalent in modern machine learning applications, many libraries exist that abstract their concepts and provide simple programming interfaces. However, it does not suffice to be familiar with such libraries to use neural networks effectively; in order to understand which architectures perform well, and why, one must also know their mathematical foundations.

In this paper we thus aim to give a thorough overview of neural networks and the fundamental techniques and algorithms associated with them. We first briefly examine the motivation and history behind neural networks in Section II by introducing the *perceptron* model. Section III then shows how this model has been adjusted and extended to obtain the neural network, focusing in particular on *feedforward neural networks*. In Section IV, we then proceed to explain how these networks can be trained, introducing ideas such as *stochastic gradient descent* and *back-propagation*. Subsequently, Section V discusses the effectiveness of neural networks from a theoretical point of view. In Section VI we examine several extensions to the basic feedforward neural network that are often used in practice, before we conclude our paper in Section VII.

II. The Perceptron

When researchers developed the first machine learning models, they often used ideas based closely on our understanding of the brain. One such model, inspired by the biological neuron, is the perceptron [9].

Like its biological counterpart, the perceptron receives information and produces an output. More specifically, it accepts n input values $x_1, \dots, x_n$ and calculates a corresponding output value $\hat{y} \in \{-1, 1\}$ by computing

$$\hat{y} = \operatorname{sign}\left(\sum_{i=1}^{n} w_i x_i\right), \tag{1}$$

where the weights w_i are the parameters of the model, and $\operatorname{sign}(x)$ is defined as

$$\operatorname{sign}(x) = \begin{cases} 1 & \text{if } x > 0 \\ -1 & \text{if } x \leq 0. \end{cases} \tag{2}$$

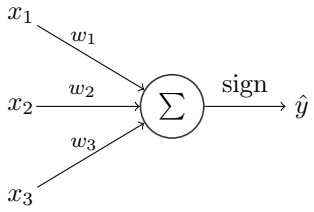

Fig. 1. An illustration of the perceptron model. In this example, the perceptron accepts three inputs x_1, x_2, x_3, has the parameters w_1, w_2, w_3, and computes $\hat{y} = \text{sign}(w_1 x_1 + w_2 x_2 + w_3 x_3)$.

By representing the input values and weights as vectors $\boldsymbol{x}$ and $\boldsymbol{w}$, we can rewrite Eq. (1) as

$$\hat{y} = \text{sign}(\boldsymbol{w}^\top \boldsymbol{x}). \tag{3}$$

For a visual representation of this model, see Fig. 1.

Perceptron models can be used to solve binary classification problems. In this scenario, we are given a set of m training examples $\mathbb{X} = \{\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(m)}\}$ and their corresponding binary labels $\mathbb{Y}$, and wish to predict the most probable label for an unseen vector $\boldsymbol{x} \notin \mathbb{X}$.

For example, the vectors $\boldsymbol{x}^{(i)}$ might describe features of an email using a *bag-of-words* representation. That is, we define a fixed vocabulary, and the j^{th} entry in the vector $\boldsymbol{x}^{(i)}$ specifies how often the j^{th} word of the vocabulary occurs in the particular email represented by $\boldsymbol{x}^{(i)}$. The corresponding label $y^{(i)} = 1$ then might signify that the email is a legitimate email, whereas a value of $y^{(i)} = -1$ might label the email as spam.

In the beginning, the weights are randomly initialized and the model thus makes arbitrary predictions. During the process of *training* the perceptron, we iteratively adjust the weights in order to improve the prediction accuracy on the training set.

One common method of training is the perceptron learning algorithm proposed by Rosenblatt [10]. Essentially, the algorithm iterates through the training data $\mathbb{X}$ and makes small adjustments to the weights if a particular training example $x^{(i)}$ is misclassified. For example, if the perceptron predicts $\hat{y} = 1$ and the actual label is $y^{(i)} = -1$, the weights are corrected in the negative direction. Since the perceptron learning algorithm is not directly applicable to neural networks, we will not discuss it further; a more in depth explanation can be found in Ref. [11, Ch. 8, pp. 265-267].

A major shortcoming of the perceptron is that it can only learn to classify linearly separable data [12]. For example, the XOR function, where

$$\text{XOR}(\boldsymbol{x}) = \begin{cases} 0 & \text{if } \boldsymbol{x} = [0,0] \vee \boldsymbol{x} = [1,1] \\ 1 & \text{if } \boldsymbol{x} = [1,0] \vee \boldsymbol{x} = [0,1], \end{cases} \tag{4}$$

cannot be learned with the perceptron. The discovery of these limitations has greatly reduced interest in the field of biological learning, until more sophisticated models, such as neural networks, were developed [8, Ch. 1, pp. 12-18].

III. Feedforward Neural Networks

A natural extension of the perceptron model is to combine multiple perceptrons in a network architecture called a neural network. It is intuitively clear that, much like in an organic brain, a complex arrangement of many simple computing units can learn much more complicated functions than those simple units alone. In this section, we will examine how such a network architecture based on perceptrons can be constructed. The ideas that we develop are mostly based on Ref. [8, Ch. 6].

A. Extensions to the Perceptron

Before explaining the composition of perceptrons to neural networks, we will first explore two common extensions to the perceptron model.

First, we introduce an additional term called *bias* to the output calculation. The new output $\hat{y}$ becomes

$$\hat{y} = \text{sign}(\boldsymbol{w}^\top \boldsymbol{x} + b), \tag{5}$$

where the scalar b is the bias. This additional learnable parameter shifts the function computed by the model independently of its input. If the bias is large and positive, the model is more inclined to predict a positive label, while a negative bias makes it more likely that negative labels are predicted.

Second, we generalize the perceptron by replacing the sign function with an arbitrary function f called *activation function*. In contrast to $\text{sign}(x)$, most activation functions used in neural networks are continuous, since this enables us to use a variety of *gradient-based* learning algorithms for training as we will see in Section IV. Concrete examples of activation functions will be discussed later in this section.

We also introduce the quantity z, the *weighted input*, which simply is defined as

$$z = \boldsymbol{w}^\top \boldsymbol{x} + b. \tag{6}$$

The computing units we have obtained with these modifications to the perceptron are generally called *neurons* or simply *units*.

B. Network architecture

Any arrangement of neurons in a network architecture can be considered a neural network. The most influential such architecture is the feedforward neural network, which forms the basis for many other more advanced neural networks [8, Ch. 6, p. 163]. Feedforward neural networks are sometimes also called *multilayer perceptrons* (MLPs).

In feedforward neural networks, the computing units are arranged in layers. We distinguish between the *output layer*, the *hidden layers*, and the *input layer*. The output layer is the final layer in the network were its actual output is produced. The input layer is the first layer in the network, and all layers in between are called hidden layers. The input layer is special in that it does not compute anything; it merely represents the input that is passed into the neural network. In general, a L-layer feedforward neural network consists of one input layer, $(L-2)$ hidden layers, and an output layer. We call the number of layers L the *depth* of the model.

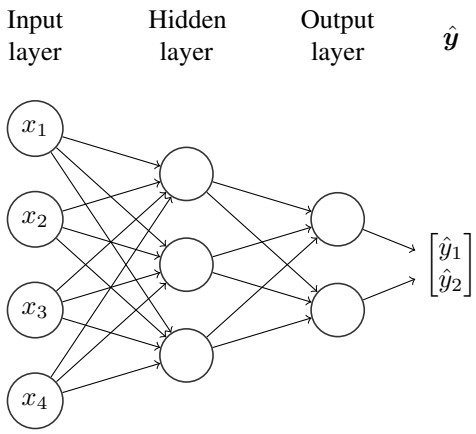

Fig. 2. A three-layer neural network. The network accepts an input $\boldsymbol{x} \in \mathbb{R}^4$, propagates it through its hidden layer consisting of three units, and finally produces an output $\hat{\boldsymbol{y}} \in \mathbb{R}^2$ in the output layer. The weights, sums, and activation functions have been omitted.

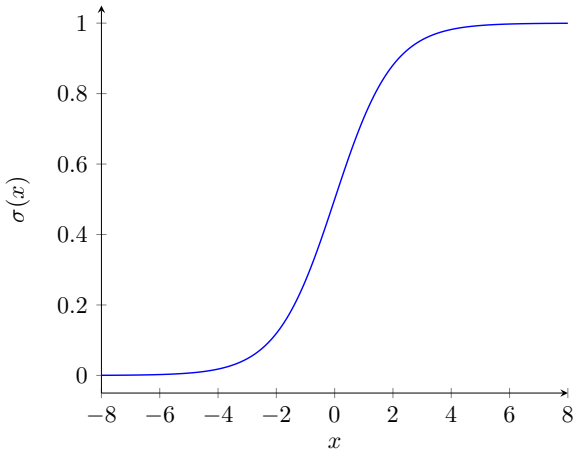

Fig. 3. The logistic sigmoid function.

Every neuron in a layer l receives input from all neurons in the $(l-1)^{\text{th}}$ layer. There are no connections between neurons in the same layer, and we also do not allow feedback connections into previous layers. Neurons in the hidden and output layers behave exactly like the modified perceptron; the only important detail is that their input is the output from the previous layer.

An illustration of a feedforward neural network can be found in Fig. 2.

In the remainder of this section, we will discuss the individual layers and corresponding design decisions in more detail.

1) Output layer: The design of the output layer depends mostly on the task that we wish to perform with the neural network.

If we want to predict a numerical value, a problem known as *regression*, we only use a single linear neuron in the output layer. A linear neuron simply uses the identity function as its activation function.

In *classification*, we wish to predict the class of an input vector $\boldsymbol{x}$, given a set of classes. For example, as with the perceptron, we might want to distinguish normal emails from spam emails. In this case of *binary* classification, it is common to use the activation function

$$\sigma(x) = \frac{1}{1+\exp(-x)}, \tag{7}$$

called the logistic sigmoid, in combination with a single output unit. As shown in Fig. 3, $\sigma(x)$ squashes its input to a value between 0 and 1, which can be interpreted as a Bernoulli distribution. Thus, it is an excellent choice for binary classification problems: the output $\hat{y}$ of the neural network is the probability that $\boldsymbol{x}$ belongs to class 1, while $(1-\hat{y})$ is the probability that $\boldsymbol{x}$ belongs to class 0.

In *multiclass* classification problems, where we wish to predict a probability distribution over k different classes, we construct an output layer with k units. A generalization of the logistic sigmoid, called the $\mathrm{softmax}$ function

$$\mathrm{softmax}(x) = \frac{\exp(x)}{\sum_{i=1}^{k}\exp(z_i)}, \tag{8}$$

is commonly used as activation function in this scenario. In Eq. (8), z_i represents the weighted input z of the i^{th} neuron in the output layer. We can easily see that the $\mathrm{softmax}$ function creates a valid probability distribution and that neurons that have a large weighted input are assigned a higher probability. The output $\hat{y}_i$ of the neural network is the probability it assigns to the i^{th} class.

Feedforward neural networks can also be applied to many other tasks such as *structured output prediction*, *anomaly detection*, and *synthesis* [8, Ch. 5, pp. 96-100]. Many specialized architectures exist for these types of problems, which we will not discuss further.

2) Hidden layers: In contrast to the output layer, the task that we want so solve does not give us any information about how to design the hidden layers. The first and foremost design decision that comes to mind is the depth of the neural network. While, in principle, any function can be learned with a neural network with just one hidden layer as we will see in Section V, networks with more hidden layers often perform much better in practice.

We can think of the hidden layers as a means to learn a different representation of the input. The neural network transforms the input by propagating it through its hidden layers until it obtains a representation where it can perform its assigned task much easier. For example, in object recognition, one can show that neural networks learn to detect different features such as edges or individual object parts in different hidden layers [13]. It is thus not surprising that deeper neural networks often perform better. On the other hand, deep neural networks are often difficult and computationally expensive to train.

Another important consideration is the activation function in hidden layers. Common activation functions are the logistic sigmoid, which we have already presented, the $\tanh$ function,

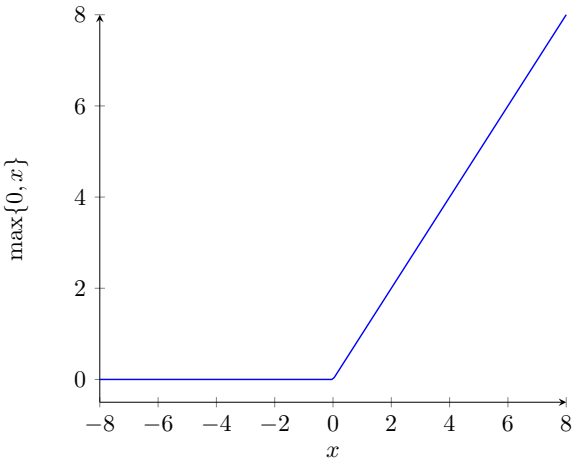

Fig. 4. The rectified linear function.

which is only a slight variation of the logistic sigmoid function, and the rectified linear function $g(x) = \max\{0, x\}$, a plot of which can be found in Fig. 4.

Activation functions are continuous, a property needed for the training algorithm, and generally non-linear, since a network consisting of only linear hidden layers is linear as a whole, suffering from the same drawbacks that we saw in the perceptron model [8, Ch. 6, p. 190].

The design of neural networks is mostly driven by experimentation and not many theoretical tools exist that justify the use of one architecture over another. For example, rectified linear units often outperform other types of hidden units, but we are far from a rigorous understanding of why this is the case. Thus, a network design for a particular task is mostly chosen via trial and error. [8, Ch. 6, pp. 185-187].

3) Input layer: Since the input layer only represents the input of the neural network, there are not many design choices to be made. We can only choose how we wish to represent the input. Often, this representation follows immediately from the raw data–for example, in image classification, we can simply represent an input image as a vector of pixel values. In other cases, the input representation might not be so obvious and we may need carefully hand-crafted features.

C. Mathematical formulation

As we have seen, a feedforward neural network is simply a combination of many perceptron-like computing units. We can combine all parameters of these neurons in weight matrices and bias vectors to obtain one single mathematical specification of the whole network.

For every layer l except the input layer we define a weight matrix $\boldsymbol{W}^{(l)}$ where the entry in the j^{th} row and k^{th} column equals the weight of the j^{th} neuron in the $(l-1)^{\text{th}}$ layer to the k^{th} neuron in the l^{th} layer. Sometimes we will also specify this weight with w^l_{jk}. We similarly define as bias vector $\boldsymbol{b}^{(l)}$ whose j^{th} entry simply contains the bias of the j^{th} neuron in the l^{th} layer. We denote the activation function used in the l^{th} layer with $f^{(l)}$. Activation functions are applied element-wise to vectors.

We can now denote the output $\boldsymbol{h}^{(l)}$ of the l^{th} hidden layer as

$$\boldsymbol{h}^{(l)} = f^{(l)}\left(\boldsymbol{W}^{(l)\top}\boldsymbol{h}^{(l-1)} + \boldsymbol{b}^{(l)}\right), \tag{9}$$

where we define $\boldsymbol{h}^{(0)} = \boldsymbol{x}$. The output of the whole network then is simply given by $\hat{\boldsymbol{y}} = \boldsymbol{h}^{(L)}$.

Note that this expression is very similar to the formulation of the perceptron model in Eq. (5). The only difference is that we now use matrices, since there are multiple neurons in a layer, and that the total output consists of a chain of multiple such functions.

IV. Training Feedforward Neural Networks

Given: Set of training data, labels, wie beim Perzeptron...

V. Universal Approximation Capabilities

VI. Extensions and Applications

VII. Conclusion

References

[1] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. S. Bernstein, A. C. Berg, and F. Li, "Imagenet large scale visual recognition challenge," *International Journal of Computer Vision*, vol. 115, no. 3, pp. 211–252, 2015. [Online]. Available: https://doi.org/10.1007/s11263-015-0816-y

[2] K. He, X. Zhang, S. Ren, and J. Sun, "Delving deep into rectifiers: Surpassing human-level performance on imagenet classification," in *2015 IEEE International Conference on Computer Vision, ICCV 2015, Santiago, Chile, December 7-13, 2015*. IEEE Computer Society, 2015, pp. 1026–1034. [Online]. Available: https://doi.org/10.1109/ICCV.2015.123

[3] A. Severyn and A. Moschitti, "Twitter sentiment analysis with deep convolutional neural networks," in *Proceedings of the 38th International ACM SIGIR Conference on Research and Development in Information Retrieval, Santiago, Chile, August 9-13, 2015*, R. A. Baeza-Yates, M. Lalmas, A. Moffat, and B. A. Ribeiro-Neto, Eds. ACM, 2015, pp. 959–962. [Online]. Available: http://doi.acm.org/10.1145/2766462.2767830

[4] A. Mohamed, G. E. Dahl, and G. E. Hinton, "Acoustic modeling using deep belief networks," *IEEE Trans. Audio, Speech & Language Processing*, vol. 20, no. 1, pp. 14–22, 2012. [Online]. Available: https://doi.org/10.1109/TASL.2011.2109382

[5] L. A. Gatys, A. S. Ecker, and M. Bethge, "Image style transfer using convolutional neural networks," in *2016 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2016, Las Vegas, NV, USA, June 27-30, 2016*. IEEE Computer Society, 2016, pp. 2414–2423. [Online]. Available: https://doi.org/10.1109/CVPR.2016.265

[6] A. Karpathy and L. Fei-Fei, "Deep visual-semantic alignments for generating image descriptions," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 4, pp. 664–676, 2017. [Online]. Available: https://doi.org/10.1109/TPAMI.2016.2598339

[7] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, J. Veness, M. G. Bellemare, A. Graves, M. A. Riedmiller, A. Fidjeland, G. Ostrovski, S. Petersen, C. Beattie, A. Sadik, I. Antonoglou, H. King, D. Kumaran, D. Wierstra, S. Legg, and D. Hassabis, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529–533, 2015. [Online]. Available: https://doi.org/10.1038/nature14236

[8] I. J. Goodfellow, Y. Bengio, and A. C. Courville, *Deep Learning*, ser. Adaptive computation and machine learning. MIT Press, 2016. [Online]. Available: http://www.deeplearningbook.org/

[9] W. McCulloch and W. Pitts, "A logical calculus of the ideas immanent in nervous activity," *The Bulletin of Mathematical Biophysics*, vol. 5, no. 4, pp. 115–133, 1943. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-51249194645&doi=10.1007%2fBF02478259&partnerID=40&md5=edb67afceee33d22eaabbf1f8c1dca90

[10] F. Rosenblatt, “The perceptron: A probabilistic model for information storage and organization in the brain,” *Psychological Review*, vol. 65, no. 6, pp. 386–408, 1958. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-11144273669&doi=10.1037%2fh0042519&partnerID=40&md5=f6ad02750f121e6d5d33566003d5ac8b

[11] K. P. Murphy, *Machine learning - a probabilistic perspective*, ser. Adaptive computation and machine learning series. MIT Press, 2012.

[12] M. Minsky and S. Papert, *Perceptrons - an introduction to computational geometry*. MIT Press, 1987.

[13] M. D. Zeiler and R. Fergus., “Visualizing and understanding convolutional networks,” in *Computer Vision - ECCV 2014 - 13th European Conference, Zurich, Switzerland, September 6-12, 2014, Proceedings, Part I*, ser. Lecture Notes in Computer Science, D. J. Fleet, T. Pajdla, B. Schiele, and T. Tuytelaars, Eds., vol. 8689. Springer, 2014, pp. 818–833. [Online]. Available: https://doi.org/10.1007/978-3-319-10590-1_53