Fachhochschule Aachen
Campus Jülich

Fachbereich: Medizintechnik und Technomathematik
Studiengang: Scientific Programming

Autonomous Fault Detection Using Artificial Intelligence
Applied to CLAS12 Drift Chamber Data

Eine Bachelorarbeit von Christian Peters

Jülich, den 26. Juni 2018

Contents

1 Introduction

2 The CLAS12 Particle Detector

3 Deep Learning Fundamentals

3.1 Artificial Neural Networks

Artificial neural networks (ANNs) are a class of machine learning algorithms that are loosely inspired by the structure of biological nervous systems. To be precise, each ANN consists of a collection of artificial neurons that are connected with each other. The neurons are able to exchange information along their connections. A common way to arrange artificial neurons within a network is to organize them in layers as depicted in figure 3.1.
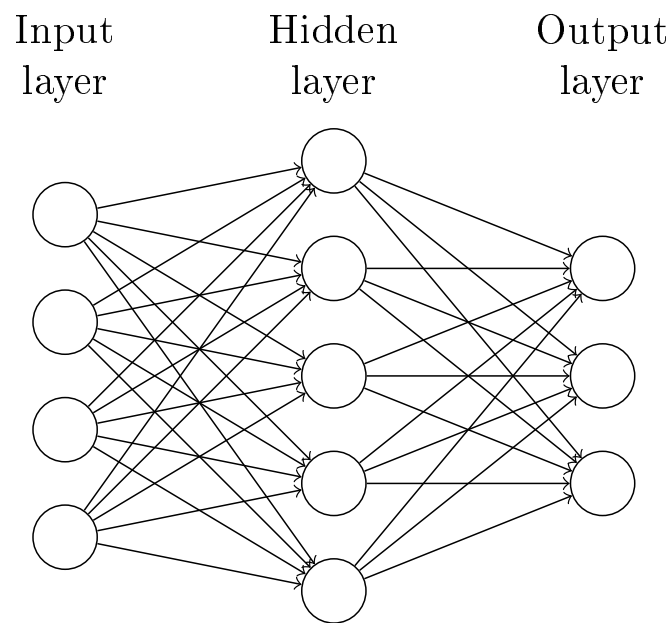

Figure 3.1: The structure of an ANN can be described by a directed graph. The nodes represent the neurons, the edges represent their connections, also indicating the flow of information.

When an artificial neuron receives signals on some of its incoming connections, it may

elect to become active based on the input it collects.[1] In this state it also influences all neurons it has an outgoing connection to by passing a signal along their channel. Those other neurons in turn may also elect to become active - this way a signal can propagate through the network along the connecting edges.

Usually, each ANN consists of at least one layer of neurons that is responsible for receiving signals from the environment - we call this an *input layer* (see figure 3.1 on the preceding page). When these neurons receive a signal from the environment, they propagate it to their connected neighbors in the next layer. This process repeats until the *output layer* is reached. The neurons in this layer represent the output of the whole network. Each layer in between is called a *hidden layer* because there is no direct communication between the neurons in this layer and the environment. Networks that satisfy this basic architectural model where each layer is fully connected with its following layer and signals only flow in one direction without cycles are called *fully connected feedforward networks*.

The goal behind this procedure usually is to convert an input signal into a meaningful output by feeding it through the network. If the network is able to detect relevant features or patterns in the input signal, it can be used to perform tasks such as classification or regression (i.e. approximate discrete or continuous functions). In order for this to be possible, some kind of learning has to take place which enables the network to capture the essence of the data it is confronted with. We will take a further look at these aspects as well as the mathematical model of a neural network in the following sections.

3.1.1 Modeling Artificial Neurons

To fully understand how each neuron processes the signals it receives, it is necessary to develop a mathematical model that describes all the operations taking place. The following descriptions are partially based on the explanations that are provided in [Hay08].[2] As shown in figure 3.2 on the next page, each artificial neuron basically consists of three components:

1. **A set of weighted inputs:** Each connection that is leading into the neuron has a weight w_{kj} associated with it where k denotes the neuron in question and j denotes the index of the neuron that delivers its input to the current neuron k.[3] The signal

---

[1] The details of this process are further illustrated in section 3.1.1.
[2] See chapter I.3: *Models of a Neuron* for more details.
[3] There might arise the question why the indexing of a weight from neuron j to neuron k is w_{kj} and *not* w_{jk}. This is the case because the weights are usually stored in matrices where each row corresponds to a neuron k and each column corresponds to an input j which allows for much faster computations by heavily utilizing matrix-multiplication.

that passes the connection is multiplied by the related weight of that connection before arriving at the next component.

2. **A summation unit:** This component adds up all the weighted signals that arrive at the neuron as well as a constant bias value b_k that is independent of the inputs. The reason for adding the bias term is explained in section 3.1.3 on page 10.

3. **An activation function:** The activation function $\phi(\cdot)$ applies a transformation to the output of the summation unit that is usually non-linear. The value of the activation function is the output of the neuron which will travel further through the network alongside the corresponding connections. In section 3.1.2 on the next page, a more detailed explanation of activation functions as well as some commonly used examples will be provided.
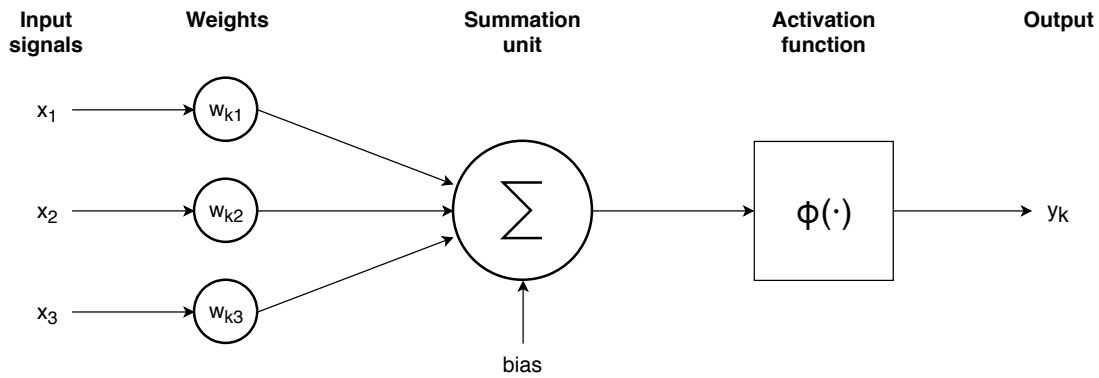

Figure 3.2: The components of a single artificial neuron. This neuron k receives three input signals that are first multiplied by the associated weights, summed up including a bias and then fed into an activation function that will determine the ouput signal.

Transforming this model into mathematical equations, the output of the summation unit of a particular neuron k with n input signals x_j can be described by the following formula:

$$z_k = \sum_{j=1}^{n} x_j \cdot w_{kj} + b_k \tag{3.1}$$

where b_k denotes the bias term of neuron k and z_k describes the result of the summation unit.

As a consequence, the output signal y_k of neuron k can be computed by applying the activation function $\phi(\cdot)$ to the output of the summation unit which can be described by

the following expression:

$$y_k = \phi(z_k) \tag{3.2}$$

3.1.2 Activation Functions

The basic task of an activation function is to determine the level of activity that a neuron emits based on the input it receives. Because the incoming signals are first weighted and summed up by the summation unit, they arrive at the activation function as a single value z. Since the output y of the neuron is also a scalar, each activation function can be described as $\phi : \mathbb{R} \to \mathbb{R}$. In the following paragraphs, an overview of the most popular activation functions will be presented that is based on the descriptions found in [PG17].[4]

The Sigmoid Function This activation function transforms an input z into a range between 0 and 1 based on the following equation:

$$\phi(z) = \frac{1}{1 + e^{-\theta \cdot z}} \tag{3.3}$$

The θ parameter is used to adjust the sensitivity of the sigmoid function with respect to its input signal. High values of θ lead to steep slopes around $z = 0$ while smaller values will lead to smoother slopes. An illustration of this relationship is presented in figure 3.3.
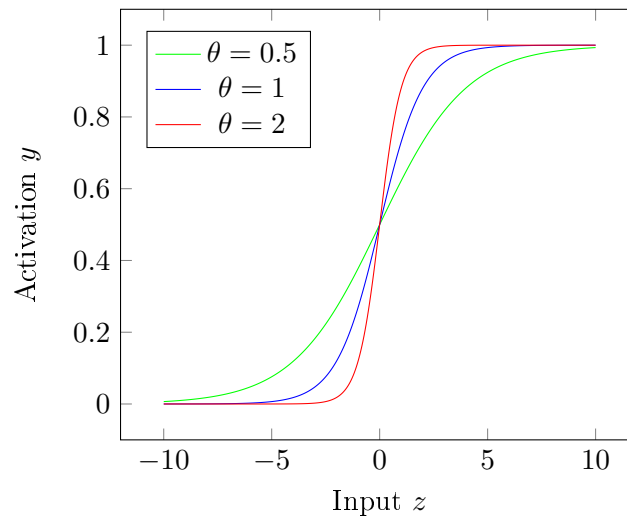

Figure 3.3: The sigmoid activation function plotted for different values of θ.

---

[4]See section *Activation Functions* in chapter two.

One important reason why the sigmoid function is often used is that it reduces the impact of outliers in the data without removing them. When the input of a neuron is large, it is reduced to a number near one, when it is very negative, the activation evaluates to a number near zero. This behaviour adds to the overall robustness of the network.

The Rectified Linear Unit (ReLU)   Because it is not always desirable to reduce large signals to a smaller scale, this function will only replace negative values with zero and leave positive values untouched. This behaviour can be modeled by the following expression:

$$\phi(z) = \max(0, z) \tag{3.4}$$

When building deep neural networks, one of the problems that sometimes arise is that a signal will fade out when propagating through many hidden layers. This issue is remedied to some degree by using the ReLU function because large signals are not cut down. Due to the negative values being set to zero, the ReLU function is also non-linear when taking its whole domain into account. This is an important concept because non-linear activation functions are essential for a network to learn complex relationships. Another benefit of the ReLU function is that its derivative is either 1 or 0. This will turn out to be important when looking into the training of a neural network. Because of all these benefits, ReLUs are one of the state of the art activation functions in deep neural networks. A plot of the ReLU function is presented in figure 3.4.
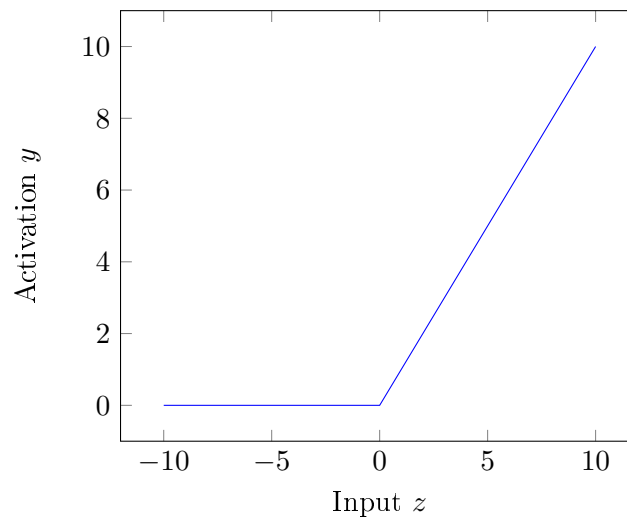

Figure 3.4: The ReLU activation function.

9

The Softmax Activation Function   This activation function is usually applied to the output neurons of a network. When a neural network is used to perform classification tasks, each output neuron is commonly associated with a specific class. In classification tasks it is highly desirable to assign a probability to each class that represents how likely it is that the input data belongs to that class. The softmax activation function is used to achieve this by setting up the output neurons to represent a probability distribution over all possible classes. In an output layer consisting of n output neurons, the softmax function for each neuron i of that layer can be described by the following equation, where z_i denotes the summation units' output of the i'th neuron:

$$\phi(z_i) = \frac{e^{z_i}}{\sum_{j=1}^{n} e^{z_j}} \tag{3.5}$$

The softmax activation function represents – loosely speaking – the percentage of the current neurons activation with respect to the compound activation of all neurons in the layer.

There might arise the question why each input z_i is first fed into the exponential function e^x before translating the activations into probabilities. This is done to further amplify the strongest signals and attenuate the weaker ones which results in more clear-cut values.[5]

3.1.3 The Role of the Bias Value

There still remains the question why in each artificial neuron there is a bias value b_k added to the weighted sum of the inputs. The reason for this is related to the activation function: The bias term acts like a parameter that determines how to shift the activation function along the x-axis. We already know from equation (3.1) on page 7 that for a neuron k with n inputs the toal input signal z_k adds up to:

$$z_k = \sum_{j=1}^{n} x_j \cdot w_{kj} + b_k$$

Let us denote the weighted sum of the input signals as a separate value $a_k = \sum_{j=1}^{n} x_j \cdot w_{kj}$ that describes the raw input of the neuron. This means that $z_k = a_k + b_k$ and using the

---

[5]Imagine the z_i inputs of the output layer are given by the following vector: $(2, 4, 2, 1)^T$. If we just normalize these values to obtain a probability for each neuron, we get $(0.22, 0.44, 0.22, 0.11)^T$. Using the exponential function first, we roughly get $(0.1, 0.75, 0.1, 0.05)^T$ which amplifies the most likely outcomes and attenuates the less likely ones. See `https://datascience.stackexchange.com/questions/23159/in-softmax-classifier-why-use-exp-function-to-do-normalization` for a nice explanation and the source of this example.

sigmoid function (see section 3.1.2 on page 8) as an example to demonstrate the effects of the bias value, we can slightly rewrite it as

$$\phi(a_k) = \frac{1}{1 + e^{-(a_k + b_k)}}$$

also setting $\theta = 1$ for demonstration purposes. Plotting the activation function for different values of b_k immediately reveals the effect of the bias value as a shift-parameter which can be seen in figure 3.5.
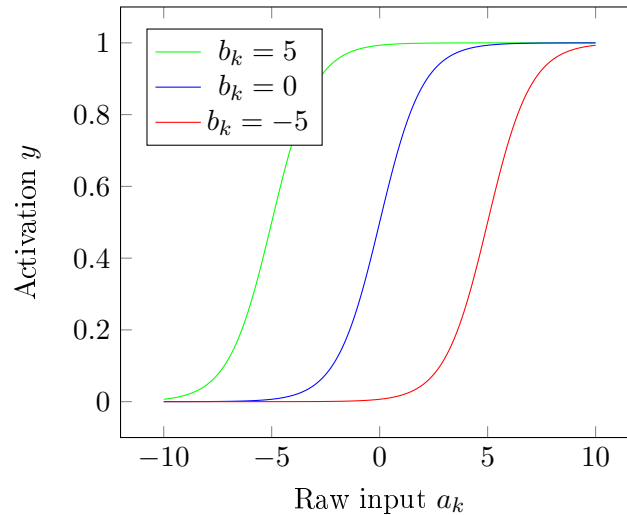

Figure 3.5: The sigmoid activation function plotted for different bias values.

What this shift means is that the bias term acts like a threshold that has to be overcome in order for the neuron to become active. Positive bias values lead to activity even when the raw input a_k is still negative and negative bias values require bigger input signals in order for the neuron to fire.

3.2 Neural Networks as Classifiers

After establishing a mathematical model that helps us to describe a neural network, there is still one problem to be solved: How to train the network to be able to successfully perform tasks such as classification? In order to figure this out, we will first take a look at classification tasks in general and then explore how to set up and train a neural network to perform classification.

3.2.1 Classification

The basis of a classification task is usually formed by a dataset that consists of features as well as labels. The goal of the classification algorithm is to predict the label of an instance of the dataset by only looking at its features. In order to achieve this, the classifier first has to build a model based on a training dataset. This procedure is called *training*. In the next step, the classifier is presented with some new examples that it did not see during training. The classifier is tested on these new examples to estimate its performance and to see if it was able to learn any concepts from the data, i.e. to *generalize*. This phase is also called *testing*. Because classification requires pre-labeled instances and the classifier acts like a learner who learns from a teacher, classification is an example of a broader domain called *supervised learning*.

3.2.1.1 Evaluating a Classifier

In order to find out how well a classifier generalizes after training, the results of the testing phase can be entered into a *confusion matrix* that is structured as shown in figure 3.6.[6]

	Class Positive (Predicted)	**Class Negative (Predicted)**
Class Positive (Actual)	True positives (TP)	False negatives (FN)
Class Negative (Actual)	False positives (FP)	True negatives (TN)

Figure 3.6: The structure of a confusion matrix for a classification task with two classes "positive" and "negative".

Each entry in this matrix describes how often the classifier was presented with an example of the row-class during testing and predicted that the example belongs to the column-class. The resulting measurements of true positives, true negatives, false positives and false negatives can be used to compute the following evaluation metrics:[7]

---

[6]It should be noted that this concept can be extended to classification tasks with more than two classes as well by simply adding new rows and columns for each new class.

[7]A collection of these metrics can also be found in [PG17], see chapter *Evaluating Models*.

Accuracy This measurement determines the percentage of examples in the testing set that the classifier predicted correctly. It can be denoted by the following equation:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3.6}$$

This metric works well if there is roughly an equal amount of examples for each class. However if one of the classes makes up most of the examples, the classifier can reach a high degree of accuracy by just predicting the label of the dominant class every single time. This impairs the significance of this metric when imbalances among the classes are present.

Precision The precision score shows the percentage of examples that were correctly classified as positive among all examples that the classifier labeled positive:

$$Precision = \frac{TP}{TP + FP} \tag{3.7}$$

This metric can also be interpreted as an estimate of the conditional probability that the classifier is right given that it predicted a positive class:

$$Precision = P(\text{Classifier is right}|\text{Classifier predicted POSITIVE})$$

Recall This measurement remedies the imbalance issues of the accuracy metric by determining the percentage of correctly classified examples for each separate class. It can be denoted by the following expression:

$$Recall = \frac{TP}{TP + FN} \tag{3.8}$$

The recall score can also be interpreted as an estimate of the conditional probability that the classifier is right given a specific class:

$$Recall = P(\text{Classifier is right}|\text{Class is POSITIVE})$$

F1 Score This metric combines precision and recall to calculate their so called *harmonic mean*. It is often used when evaluating classification models, thus its equation is also displayed here:

$$\text{F1 Score} = \frac{2 * Precision * Recall}{Precision + Recall} \tag{3.9}$$

It should be noted that all these measurements can be extended to classification tasks with more than two classes as well. This is done by first computing the metrics for each class separately and then taking the average of these values to estimate a global score.

3.2.2 Network Architecture for Classification

The architecture of the neural network that will be used to perform the classification task is highly dependent of the structure of the dataset. Remembering that a neural network consists of an *input layer* as well as *hidden layers* and an *output layer*, the question is how to assemble these layers to fit the task well.

The first consideration is that each feature in the dataset will correspond to an input signal that is fed into the network. Thus the amount of neurons in the input layer must be equal to the amount of features in the dataset. Because the only responsibility of the input units is to receive a signal from the environment and pass it on to the next layer, these neurons don't have a special activation function that transforms the input. The activation of these neurons is simply the identity of the incoming signal.

As already hinted at in section 3.1.2 on page 10 about the softmax activation function, it is highly useful if the network is able to not only to predict the correct label but also to indicate how certain it is about it. This is why the output layer will consist of as many neurons as there are classes in the dataset which will enable us to use the softmax function on this layer to retrieve a set of probabilities for each example that is presented to the network. The neuron that shows the highest degree of activity, i.e. assigns the highest probability, determines the label the network will assign to the example.

The number of hidden layers that are inserted between the input and the output layer highly depends on the complexity of the task. As the number of hidden neurons grows, there are more parameters (weights and biases) left to be adjusted during training which means more capacity for the network to learn. The danger lays in the fact that if there are too many hidden neurons, the network will just use this capacity to memorize the training examples and not extract general concepts from them which will lead to low accuracy on unseen examples. This problem can also be described by the more general term *overfitting*. On the contrary, if there are not enough hidden neurons, the network won't be able to capture all concepts that are present in the data which will lead to an opposite effect: *underfitting*. Both overfitting and underfitting harm the ability of the network to generalize well beyond the training data.

Because there are no general rules up to this point on how to structure the hidden layers of a neural network, it is recommended to apply the basic rule of thumb of increasing

the amount of hidden layers with the complexity level of the problem. It also helps to try out different structures during the training phase to see which one produces the best results.

3.2.3 Training the Network

In order to be able to improve the quality of the networks' predictions, i.e. training the network, we first have to introduce a way of measuring the performance of the network.

Let x be an example input from the training dataset and $y'(x)$ the desired output of the network that corresponds to the example. Both x and $y'(x)$ are vectors. The element x_i represents the input signal of the i'th input neuron and the element $y_i'(x)$ represents the desired activation of the i'th output neuron. To measure how close the actual output $y(x)$ of the network is to the desired output $y'(x)$, we can use the *sum of the squared errors*:

$$L_x = \sum_{i=1}^{n} (y_i(x) - y_i'(x))^2 = \left\| y(x) - y'(x) \right\|^2 \tag{3.10}$$

where n is the number of output neurons and L_x resembles the *loss of the network* for a single example x.

The *average total loss* of the network over all examples in the dataset (the total number of examples will be denoted by N) can be computed by just averaging the losses of every single example:

$$L = \frac{1}{N} \cdot \sum_{x} L_x \tag{3.11}$$

We can also express this value in terms of the current configuration of the neural network that is represented by the set of weights w and the set of biases b that is currently used as the *loss function* $L(w, b)$. Being now able to measure the training performance of the network with respect to its configuration by calculating the average loss $L(w, b)$, we can now define the training problem as follows:

Find a set of weights w and biases b such that $L(w, b) \rightarrow min$

This implies that training the network is nothing but an optimization problem where the weights and biases of the network are adjusted to find the minimum of the loss function $L(w, b)$.

3.3 Deep Networks

4 Convolutional Neural Networks

5 Implementing and Testing a CNN-Model in DL4J

6 Discussion

7 Conclusion

Bibliography

[Hay08]   Simon Haykin. *Neural Networks and Learning Machines*. 3rd ed. Prentice Hall
          International, 2008. ISBN: 978-0131471399.

[PG17]   Josh Patterson and Adam Gibson. *Deep Learning: A Practitioner's Approach*.
          1st ed. O'Reilly Media, 2017. ISBN: 978-1491914250.

List of Figures