

# Data Preprocessing

The majority of the datasets available are called Raw Datasets. The reason they are labelled raw datasets is that they contain many anomalies which further implies that, the dataset is not suitable to train our Machine Learning and Deep Learning Models. The dataset needs to be nurtured and structured via a series of steps commonly called the Data Preprocessing Steps, to make it suitable for the training purpose of the proposed models.

The anomalies associated with the Raw Dataset are listed as follows –

### Missing Values

### Skewness

### Kurtosis

### Outliers

### Feature Selection or Data Reduction

Once the dataset is Preprocessed, it improves the proposed models' overall accuracy, precision, recall and F1-Score.

## Missing Values

In the dataset, some values might be missing from some or all of the attributes. These missing values are represented with a ‘Blank’, ‘null’ and ‘NaN’ (Not a Number). The standard procedures for the effective removal/replacement of the missing values are listed below –

1. *Drop down the entire row column containing at least one missing value*
2. *Replace the missing value(s) with the median of that attribute if applicable*
3. *Replace the missing value(s) with the mean of that attribute if applicable*
4. *Replace the missing value(s) with the Forward Fill technique*
5. *Replace the missing value(s) with the Backward Fill technique*

The forward Fill technique puts in the last known value before the first missing cell of that particular attribute, and each missing cell of that particular attribute is then replaced by the same last known value. Think of it as, surfing through each row from top to bottom, identifying the last known cell value before the missing cell and then replacing all the missing cells with that value.

The Backward Fill technique puts in the last known value before the first missing cell of that particular attribute while going backwards, and each missing cell of that particular attribute is then replaced by the same last known value. Think of it as, surfing through each row from bottom to top, identifying the last known cell value before the missing cell and then replacing all the missing cells with that value.

## Skewness

Before knowing what skewness is, the concept of Normal Distribution is important. Normal Distribution or commonly termed a Gaussian Distribution is a type of continuous probability distribution, with a bell-shaped curved. The probability density function can be defined as follows:

(1)

where, f(x) = probability density function,

= standard deviation, and

= mean

A typical symmetric Gaussian Distribution looks like follows:

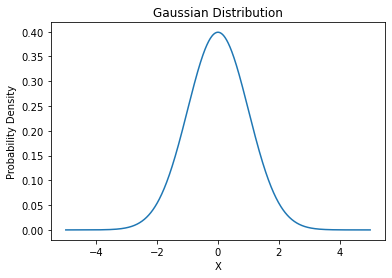


Fig. 1. Gaussian Distribution or Bell Curve

Now, skewness is a measure of how much the Gaussian Distribution is skewed or shifted from its normal position towards left or right and accordingly called Right Skewed or Left Skewed respectively. The Right Skewed value is represented using a positive value and for Left Skewed, it is represented using a negative value. The skewness can be calculated using the following formula:

(2)

Where is the skewness, N is the number of variables in the distribution, Xi random variable, is the mean of the distribution and is the standard deviation.

The industrial accepted skewness value ranges from -1.5 to +1.5. Anything greater than +1.5 or smaller than -1.5 needs to be reduced to fit within the range. For this we can apply the following methods:

1. *Box-Cox Transformation – It can be calculated using the following function*

(3)

*where <\*to be inserted\*>*

1. *Cube root Transformation - It can be calculated using the following function*

f(x) = (4)

1. *Log Transformation - It can be calculated using the following function*

f(x) = log(x) (5)

A normally distributed attribute helps to increase the overall accuracy, precision, recall and F1-Score of the proposed models.

## Kurtosis

It is a measure of how much the data clusters near the tails or the head of the curve. The Kurtosis value can be obtained using the stated equation:

(6)

Where is the mean of the given data, S is the standard deviation of the data and n is the total number of observations.

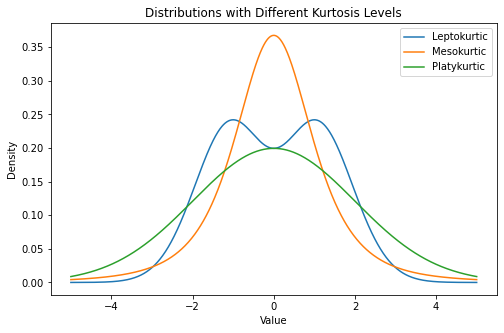


Fig. 2. Three types of Kurtosis

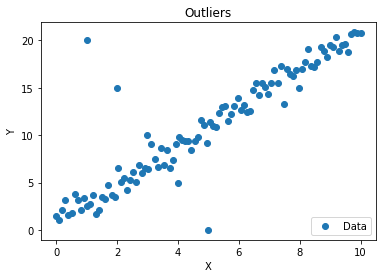
Based on this, there are three types of kurtosis:

1. *Mesokurtic – The data here is moderately spread, with a medium peak.*
2. *Leptokurtic – The majority of the data is concentrated near the tails, leading to a pointed peak.*
3. *Platykurtic – The data is evenly spread-out, implying a flat line almost with a little bump.*

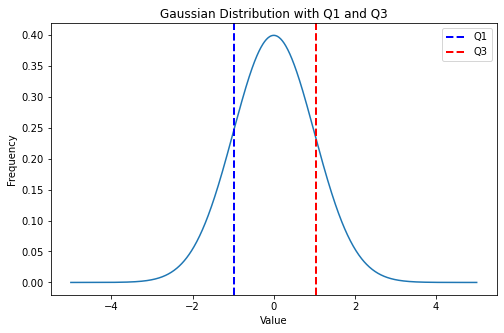
The permissible and the industrial standard accepted value is 3. Anything less than 3 or greater than 3 is not permissible.

## Outliers

To put it in simple words, Outlier means the odd one out. From Fig. 3 it is evident that the marked points have too much deviated from the rest of the pack. These points are labelled as Outliers. The best method/practice to find out the outlier of the attribute is the visual representation. From the distribution plot, the outliers can be identified easily.

 Fig. 3. Outliers present in a Linear Regression Plot

It is essential to remove or replace those outliers because they can interfere with the efficiency, accuracy, precision, recall and F1-Score of the proposed models. The industry-accepted and effective method to remove or replace those points is called Interquartile Range Function (IQR).

 Fig. 4. Interquartile Range of a Gaussian Distribution

IQR is a statistical dispersion that represents the range from the first quartile (Q1) to the third quartile (Q3), implying covering 50% of the distribution area. The IQR is defined as:

IQR = Q3 – Q1 (7)

The values lying within the IQR are considered to be in the safe zone. Any points not within the range are either dropped, if the dataset is very large, or the points are replaced by the median, which is a safer option and works well for large and relatively small datasets.

## Feature Selection or Data Reduction

A dataset comprises several attributes which are responsible for obtaining vital information to learn and understand the pattern and relationship between the input and output values. However, not all attributes contribute the same amount of information. Dropping down those specific attributes does not harm the goal of seeking the relationship between input and output variables and also reduces the training time of our proposed ML and DL models.

There are various techniques for feature selection, including:

1. *Filter methods involve selecting features based on statistical tests such as correlation, chi-square, or mutual information.*
2. *Wrapper methods: This involves selecting features based on the performance of a machine learning model using different subsets of features.*
3. *Embedded methods: This involves selecting features during the training process of a machine learning model, such as regularization techniques.*
4. *Dimensionality reduction: This involves transforming the original dataset into a lower-dimensional space, such as principal component analysis (PCA) or linear discriminant analysis (LDA).*

When selecting features, it is important to consider the trade-off between the accuracy and complexity of the model, as well as the interpretability of the features. Additionally, it is important to use a validation set or cross-validation to ensure that the selected features generalize well to new data.

Principal Component Analysis or PCA in short is a widely used statistical technique used to reduce the dimensionality of a dataset. Dimension Reduction is a very important problem in machine learning as for smaller datasets the number of attributes can be higher than the number of instances which can lead to overfitting. PCA can be used to solve this problem by transforming the dataset into a different coordinate system where the dataset can be represented in a lower dimensional space.

PCA works by representing the original dataset in a new coordinate system where each dimension is a linear combination of the original attributes. This new coordinate system is selected in such a way that the first component captures the maximum variance in the dataset, the second component captures the maximum variance that is orthogonal to the first component and so on.

To perform PCA we first standardize the data points by subtracting the mean and divide by the standard deviation. We then compute the covariance matrix of the dataset which measures the relative variance of the attributes of the dataset.

Next we compute the eigenvectors and eigenvalues of the covariance matrix. The eigenvectors represent the directions of the original feature space along which the variance of the data points are the highest, the eigenvalues represent how much the data points vary.

Finally we select the highest N eigenvalues and the corresponding eigenvectors and use them as the basis of the new coordinate system. We then project the data along the new coordinate system to obtain the lower dimensional representation of the dataset.

The algorithm for computing PCA can be represented as:

1. *Standardize the data by subtracting the mean and dividing it by the standard deviation.*

(8)

*Where*

1. *Compute the covariance matrix of the standardized dataset.*
2. *Compute the eigenvalues and eigenvectors of the covariance matrix.*
3. *Sort the eigenvalues and eigenvectors according to the eigenvalues in descending order*
4. *Select N largest eigenvalues and corresponding eigenvectors and use them as the basis for the new coordinate system to represent the dataset in a lower dimensional feature space.*

# Machine Learning Models

## K-Nearest Neighbors Classifier

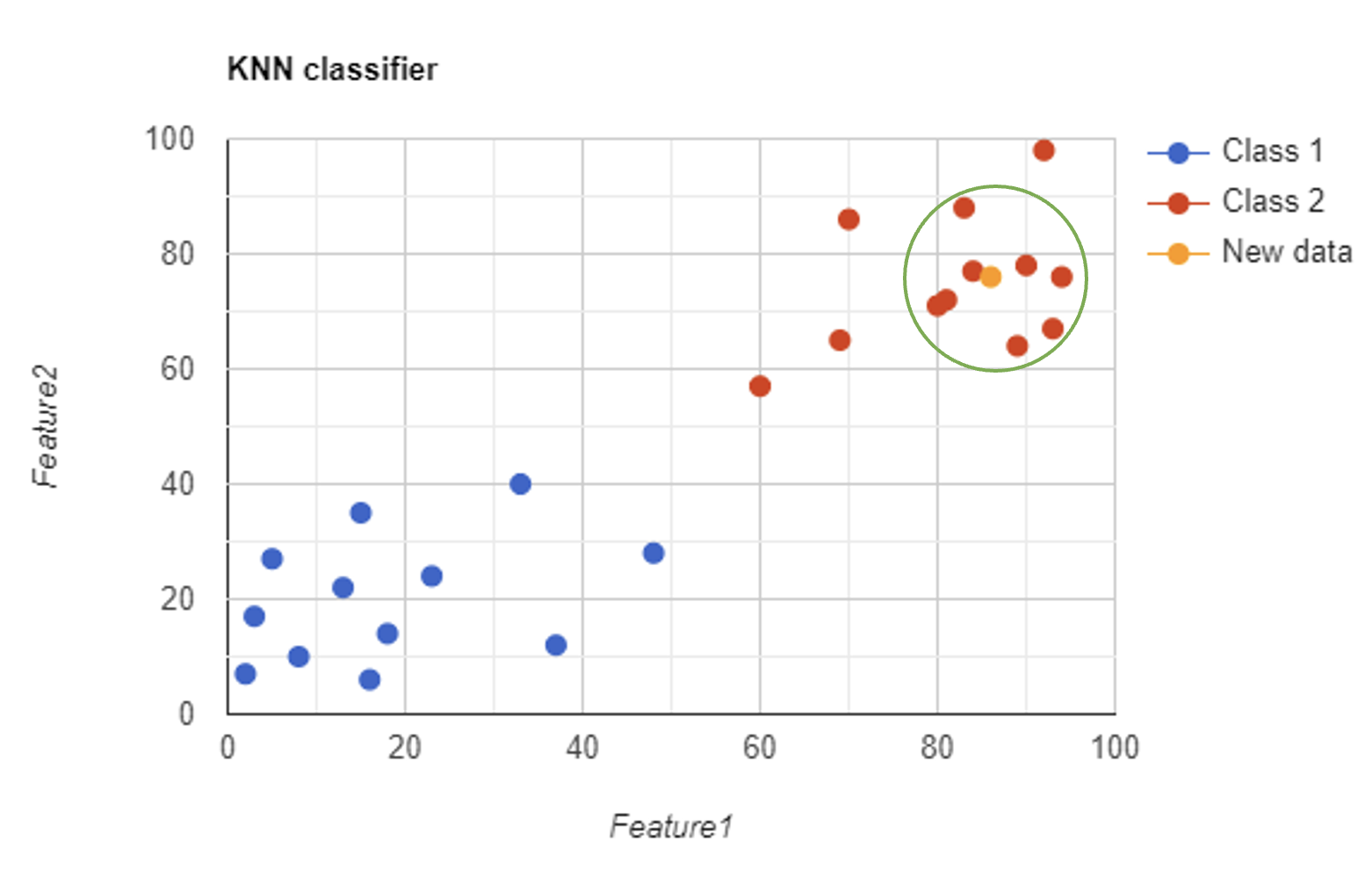
K-nearest neighbours classifier is a supervised learning technique which is non-parametric i.e. it makes no assumptions about the underlying distributions of the data. The working principle of the algorithm is the prediction of the classes based on some similarity measures (generally Euclidian distance). The new data point is classified by observing the k nearest data points around it and the most common class among the k neighbours is assigned the class to the new data point.

Euclidian distance is the measure of distance between two points in a Cartesian coordinate system. For instance, let us assume two data points M and N having coordinates (xm, ym) and (xn, yn) respectively. Then the Euclidian distance between the points can be calculated as:

D(M, N) = (9)

For classification using the knn algorithm, the dataset is first split into the training and testing part. Then for each new data point, the k nearest neighbours are considered and assigned the most common class among the neighbours.

The number of neighbours i.e. K is the hyperparameter that needs to be adjusted carefully to avoid problems like overfitting or underfitting.

Fig. 5. Working mechanism of KNN

## Support Vector Classifier

Support vector classifier (SVC) is a classification technique used for supervised learning problems. SVC finds out the optimal separating hyperplane also called the decision boundary that separates the data points belonging to different classes. The goal of SVC is to maximise the distance between data points close to the margin and the separating hyperplane. The data points closest to the margin are called support vectors and hence the name.

SVC has a few important parameters which need to be tuned carefully for proper results:

1. ***c:*** *Regularization parameter with default value 1.0, type float.*
2. ***kernels:*** *Out of several choices for the kernels the appropriate one must be chosen (more on kernels later).*

Popular choices for kernels:

1. ***Linear:*** *It calculates the dot product of input vectors.*

*(10)*

1. ***Radial Basis Function (RBF):*** *It uses a Gaussian function to map the input vectors to an infinite dimensional feature space.*

*(11)*

1. ***Polynomial:*** *It is a non-linear kernel that calculates the similarity between two vectors using the following relation:*

*(12)*

1. ***Sigmoid****: It uses a tan hyperbolic function to compute the similarity between the inputs. It is a non-linear kernel.*

*(13)*

Where x,x’ are the input vectors, is the hyperparameter controlling the width of the Gaussian kernel, d is the hyperparameter degree and coef0 is the coefficient hyperparameter.

The Support Vector machine uses hinge loss as a loss function. The goal of SVM is to minimise hinge loss. The loss function is given as:

(14)

Where yi and xi are the ith instances in the training set and b is the bias.

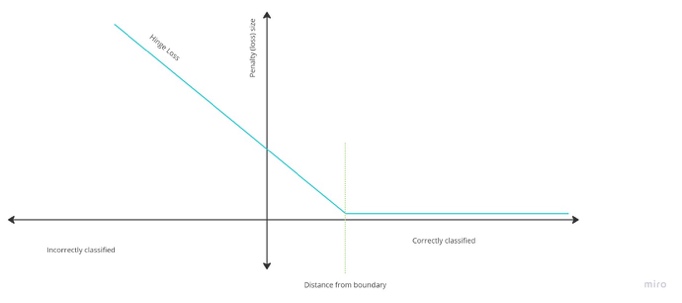


Fig. 6. Hinge Loss of SVM

## Decision Tree Classifier

The decision tree classifier is a supervised learning technique used for the classification of input. It works by continuously separating the input space into several segments and making decisions based on certain criteria. This algorithm can be easily visualised as a tree of decisions which has consequences at each decision node.

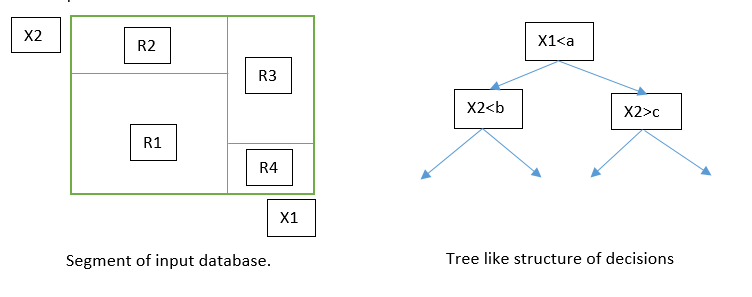


Fig. 7. Working Principle of Decision Tree

After building the tree, sometimes it tends to take a very complex form which has very high computational complexity. In order to reduce the computational load the tree is pruned which also avoids overfitting.

The decision tree algorithm uses various metrics to select the feature for the best split. Some of the commonly used metrics are:

1. *Information Gain:*

*(15)*

*(16)*

*(17)*

1. *Gini Index:*

*(18)*

*Where D is the instance of the dataset, c is the number of possible classes and pi is the probability that Di belongs to class i.*

## Random Forest Classifier

Random forest classifier is a bit different classification algorithm. It is an ensemble learning technique which uses multiple decision trees to generate its output (a group of trees is called a forest).

Bagging of these individual trees is done to reduce the correlation between trees. This algorithm creates multiple decision trees where each tree constructed uses a different subset of features, selected with replacement also called Bootstrapping.

After all, the trees are constructed and output generated, the final output is obtained by taking the majority voting or the mean of all predictions. A random forest works similarly to the decision tree and hence is mathematically identical. However, prediction is generated as follows:

## Naïve Bayes Classifier

Naïve Bayes classifier is a probabilistic machine learning algorithm used for classification. The backbone for this algorithm is the Bayesian network, also known as the Bayes network or Belief network.

A Bayesian network is a directed probability graph which depicts the conditional dependency of the random variables on one another. The Bayesian network has to be an acyclic graph.

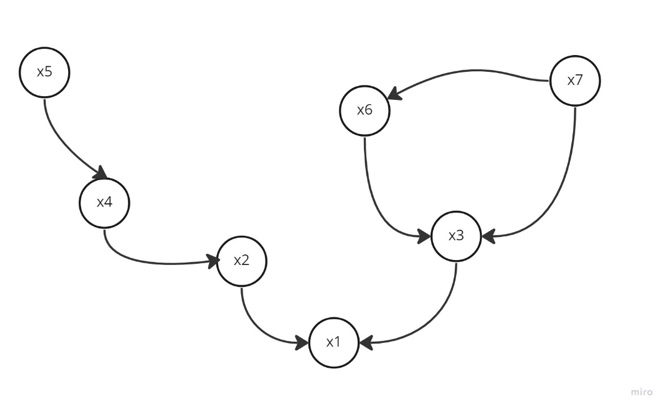


Fig. 8. Bayesian Network

Let us consider the above Bayesian network. This network shows that x5 is an independent variable and x4 depends on x5 which is shown by an arrow from a random variable to the dependent variable. The joint probability distribution of the network can be factorized by using the chain rule. The factorization of the above network can be observed to be:

(19)

From this graph we can also say, knowing x2 (say) separates x1 and x4 i.e. x1 and x4 are conditionally independent if x2 is known.

The Naïve Bayes classification algorithm uses the principle of Bayes theorem assuming that all the features are independent of each other and hence the name. The model calculates the probability of an instance belonging to a class based on the features associated with it. This is done by calculating the conditional probability of each feature given the class and then calculating the total probability using the Bayes theorem.

The instance having the highest probability of belonging to a class is classified to be a point in that class.

Conditional probability is calculated using Bayes theorem as follows:

(20)

Naive Bayes has different variations and can be used for both binary and multi-class classification.

## Logisitic Regression

Logistic regression is a classification algorithm for binary class problems using a statistical approach. This algorithm works very well where the prediction of the probability of events is involved. The logistic regression algorithm uses a logit transformation of the probability as follows:

(21)

Solving which gives us:

(22)

Which is nothing but a sigmoid.

Where β0 and β are the weights and p(x) is the probability of instance x of the dataset.

Logistic regression uses the maximum likelihood estimation method to estimate the parameters of the linear combination and maximises the likelihood of the observed data given the model. An iterative algorithm such as gradient descent is used to estimate the parameters.

## Extreme Gradient Boosting Classifier

Extreme Gradient boosting classifier, popularly known as XGBoost classifier, works using an ensemble of decision trees. This algorithm also uses multiple decision trees but in a sequential manner which is not the case in Random Forest. Here every subsequent tree tries to correct the errors of the previous tree.

The gradient-boosting algorithm is used to optimize an objective function:

(23)

Where loss is the loss function of the algorithm and Ω is the regularization function used for penalization. Actual and predicted are the vectors of actual labels and predicted labels respectively.

The loss function used can be any of the popular choices such as Mean Squared Error (MSE), log loss, hinge loss etc. The mean squared error can be calculated as:

(24)

(25)

Where yi is the actual label and f(xi) is the predicted label of the ith instance of the dataset having N data points.

The regularization parameter can use various methods like L1 or L2 norms. Here Ω using L2 norm is represented as:

(26)

Where Ὑ is the strength of regularization and w is the weight of the leaves.

XGBoost also uses pruning to decrease computational complexity and prevent overfitting.

## Gradient Boosting Classifier

The Gradient Boosting algorithm uses the idea of combining various weak classifiers to make a strong classifier altogether. It iteratively keeps on adding new trees to the ensemble and updates the weights of the training examples based on the errors of the previous trees.

The algorithm first initialises the ensemble with the mean of the target variables (say). Then for each iteration i, fits a regression tree to the negative gradient of the loss function. The negative gradient can be calculated as:

(27)

Where Loss() is the loss function used, yn is the actual label and Fn is the predicted label for the nth index of the training samples for the mth iteration.

Then the optimal leaf weight is calculated for the new tree minimises the loss function.

(28)

Where is the prediction of the current tree for the ith instance given that it falls in the jth leaf.

The weights are then updated with the new tree and the optimal weight.

(29)

These steps are repeated until the desired result is achieved.

# Neural Networks

## Multilayer Perceptron Model

This is based on the concept of the Perceptron Learning Algorithm (PLA), used for binary classification with the help of a single separating hyperplane. Note that, PLA is only able to classify linearly separable data. For non-linearly separable data, it needs to be shifted to a higher dimension to make it linearly separable on that particular plane.

Multilayer Perceptron Classifier (MLP Classifier) can be thought of as a network of elementary processors arranged in a very specific manner to mimic the neural structure of a human brain, capable of learning the hidden patterns and connections between the input and output values to classify them accordingly.

The classical Perceptron (single layer) can find the separating hyperplane for linearly separable data. The first layer is called the Input Layer, comprising d number of nodes or processing units signifying d attributes present in the dataset. The final layer is called the Output Layer, comprising two nodes being a binary classifier. Each node of the Input Layer is connected to each node of the output layer, leading to a fully connected network. Refer to Fig. 9.

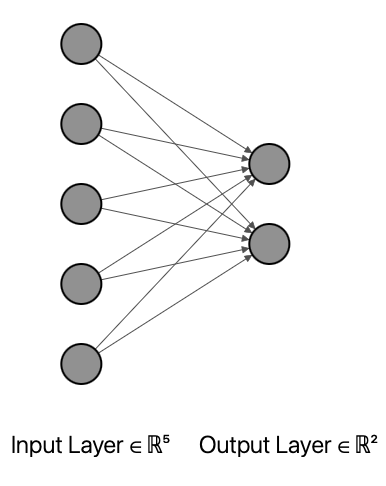


Fig. 9. Neural Network

Each Input Layer node takes in the value from each attribute. All the edges connected from the Input Layer to the Output Layer are assigned random weights. So, the total input of each node of the Output Layer is defined by

(30)

Where j = 1, 2, ..., c implying c number of classes, is the total input from the input layer to the jth node of the output layer, is the ith feature of the input layer, is the weight associated between the jth node of the output layer and ith node of the input layer for the nth instance of the dataset.

The value of , but the actual output has a value of 1 or 0, implying Class A and Class B respectively. Thus, a mapping is required to map the value of to {1,0} using a function. This function is called the Activation Function which maps the output value of the output node to {-1,1}. The most effective and commonly used Activation function is the sigmoid function.

(31)

Where, j = 1, 2, …, c, i = 0, 1, 2, …, d, is the output of the jth node of the output layer and is the activation function defined by

(32)

Where a is constant.

The learning technique associated with MLP is called the backpropagation algorithm which utilizes the concept of the Gradient Descent technique proposed by Newton. The aim is to come up with a corrected set of weights for each edge by minimizing the error using the backpropagation technique. The pointwise error is calculated as below:

(33)

Where en is the squared error for the nth data point of the dataset, ynj is the actual output of the nth data point of the dataset and jth node, vnj is the calculated output of the nth data point of the dataset and jth node of the output layer and c is the total number of classes.

Hence, the total error or the overall error (E) is calculated as

(34)

(35)

(36)

Where N is the number of entries in the dataset.

The aim is to reduce the total error (E) using the backpropagation algorithm. The only variable associated with E is the weights. So, the target is to optimize the weights to minimize the error. Thus, the Error(E) can be expressed as a function of weights.

(37)

Where wji is the weight between the jth node of the output layer and ith node of the input layer.

The backpropagation algorithm is stated as

Step 1 : Randomly assign weights (wji) for i = 0, 1, 2, …, d and j = 1, 2, …, c

Step 2 : Repeat loop starts

Step 3 : for loops starts for n = 1 to N

Step 4 : computer unj, vnj and en

Step 5 :

Step 6: for loop ends

Step 7: Repeat loop ends if the error has reduced to the permissible range or the iterations have reached their limit.

Since the error for each point is calculated and used for adjusting the weights, it is an extension of Gradient Descent known as Stochastic Gradient Descent (SGD). SGD takes care of the small local minima and ensures the algorithm is not stuck at those minima.

The MLP with a single layer can create a hyperplane to separate linearly separable data. For non-linearly separable data, it needs more than one layer called the Hidden Layer.

For MLP with one or more hidden layers, the concept remains the same. However, for each hidden layer, the weights need to be adjusted.

## Artificial Neural Network

Artificial Neural Networks (ANNs) are a type of machine learning model or to be precise a Deep Learning Model that mimics the structure and function of the human brain. ANNs consist of a large number of interconnected processing nodes known as neurons, which are arranged in a very specific format. Each neuron receives input from all the neurons of the previous layer and processes that input before passing it on to the next layer.

The working of an ANN involves following stages

1. *Initialization: The network is structured by setting up the architecture which includes the total number of layers, the total number of neurons in each layer and the activation function to be used. The weights associated with each node are randomly assigned initially.*
2. *Forward Propagation: The data is first processed by the input layer and passed on to the first hidden layer. The neurons take in all the inputs, pass the value through an activation function and yield an output which is passed onto the next hidden layer. This process is continued till the output layer.*
3. *Activation Function: At each neuron, an activation function is applied to the input before it is passed on to the next layer. The activation function introduces non-linearity into the model, allowing the network to learn complex patterns in the data. There are many types of Activation Functions such as relu, softmax, sigmoid etc. among which for the intermediate layers, relu (Recti linear unit) is preferred and for the output layer sigmoid is preferred.*
4. *Loss Function: The output produced by the network is compared with the true output, and the difference between them is calculated. Usually, the Mean Squared Error (MSE) is used for Error Calculation. This can also be labelled as the loss function. The loss function is further used for the adjustment of the weights to make the predictions more accurate.*
5. *Backward Propagation: The Backpropagation method is used to consider the feedback of the loss function. It uses the concept of the Gradient Descent Algorithm proposed by Newton to update the weights of each edge. However, the implementation of Gradient Descent, has some disadvantages, like getting stuck in local minima and not being able to find the global minima. So, the Genetic Algorithm can also be used to overcome the shortages of Backpropagation.*
6. *Repeat: The entire process discussed above is repeated until the error is within an acceptable range or the epochs have reached the limit.*

The working of the ANN is very similar to that of the MLP Model and it is safe to conclude, MLP Model is a sub-class of ANN.

## Residual Neural Network

Residual Neural Network (ResNet) is an extension of the Convolution Neural Network (CNN). ResNet and CNN are primarily deployed for image processing as an application of Computer Vision.

The CNN was able to handle a particular number of hidden layers. For updating the weights, the Backpropagation method is used. After going back, a certain number of layers, there is a shift down of loss function. Over a significant number of layers, the gradient “vanishes” leading to the vanishing gradient problem, leading to a saturation in the performance of the CNN model. To overcome this issue, the ResNet model is deployed.

ResNet developed a unique solution, known as “skip connections”. It stacks multiple identity mappings (convolutional layers that do nothing at first), ignores those particular sets of layers and again reuses the activation functions of the previous layer. Skipping or ignoring speeds up initial training by compressing the network into compact layers.

While the network is again trained, all the layers are uncompressed and the remaining parts of the network, known as the residual parts, are allowed to elaborate more on the feature space of the input image.

The majority of the ResNet models skip two or three layers at a time with nonlinearity and batch normalization in between. More advanced ResNet models, known as HighwayNets, can learn to “skip weights”, which dynamically determine the number of layers to skip.

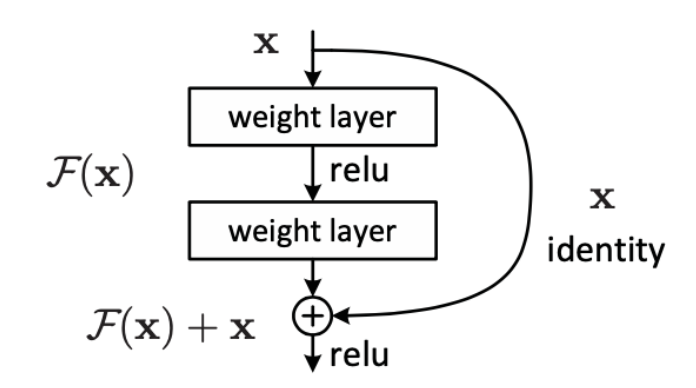


Fig. 10. Residual Block of ResNet

Fig. 10. shows the working of the Residual Block, which is responsible for skip connections in ResNet.