**ADN**

**Machine Learning**

**Course Materials – Week 2**

**Authors: Rubaiyet Sadi, Galib Anwar**

Contents

[The Seven Steps of Machine Learning 4](#_Toc134899381)

[Data Preprocessing 6](#_Toc134899382)

[I. Data Collection 6](#_Toc134899383)

[II. Data Cleaning 6](#_Toc134899384)

[III. Data Transformation 6](#_Toc134899385)

[IV. Data Splitting 6](#_Toc134899386)

[V. Data Augmentation (Optional) 7](#_Toc134899387)

[VI. Handling Imbalanced Data (Optional) 7](#_Toc134899388)

[**Types of Machine Learning** 8](#_Toc134899389)

[Supervised Learning 8](#_Toc134899390)

[I. Types of Supervised Learning 8](#_Toc134899391)

[II. The Supervised Learning Process 8](#_Toc134899392)

[III. Model Selection and Evaluation 8](#_Toc134899393)

[IV. Types of Models 9](#_Toc134899394)

[Unsupervised Learning 9](#_Toc134899395)

[I. Types of Unsupervised Learning 9](#_Toc134899396)

[- Clustering: Grouping similar data points together based on their features. 9](#_Toc134899397)

[- Dimensionality reduction: Reducing the number of features in the data while preserving its structure. 9](#_Toc134899398)

[II. The Unsupervised Learning Process 9](#_Toc134899399)

[III. Clustering 10](#_Toc134899400)

[K-means clustering: 10](#_Toc134899401)

[Hierarchical clustering: 10](#_Toc134899402)

[Density-based clustering: 10](#_Toc134899403)

[IV. Dimensionality Reduction 10](#_Toc134899404)

[Principal Component Analysis (PCA): 10](#_Toc134899405)

[t-Distributed Stochastic Neighbor Embedding (t-SNE) 10](#_Toc134899406)

[Linear Discriminant Analysis (LDA) 10](#_Toc134899407)

[Reinforcement Learning 11](#_Toc134899408)

[I. The Reinforcement Learning Process 11](#_Toc134899409)

[Agent and Environment 11](#_Toc134899410)

[Action: 11](#_Toc134899411)

[Reward: 11](#_Toc134899412)

[Policy: 11](#_Toc134899413)

[II. Markov Decision Processes (MDPs) 12](#_Toc134899414)

[III. Exploration and Exploitation 12](#_Toc134899415)

[IV. Q-Learning 12](#_Toc134899416)

[Neural Networks 13](#_Toc134899417)

[Two categories of Neural Networks 13](#_Toc134899418)

[I. Artificial Neurons 13](#_Toc134899419)

[II. Feedforward Neural Networks 13](#_Toc134899420)

[III. Convolutional Neural Networks (CNNs) 13](#_Toc134899421)

[IV. Recurrent Neural Networks (RNNs) 13](#_Toc134899422)

[V. Deep Learning 14](#_Toc134899423)

[Model Evaluation and Selection 14](#_Toc134899424)

[I. Overfitting and Underfitting 14](#_Toc134899425)

[II. Cross-Validation 15](#_Toc134899426)

[III. Hyperparameter Tuning 15](#_Toc134899427)

[IV. Model Selection 15](#_Toc134899428)

[V. Bias/Variance Tradeoff 15](#_Toc134899429)

[Deployment 17](#_Toc134899430)

[I. Model Export 17](#_Toc134899431)

[II. Model Optimization 17](#_Toc134899432)

[III. Model Serving 17](#_Toc134899433)

[IV. Infrastructure Setup 17](#_Toc134899434)

[V. Monitoring and Maintenance 17](#_Toc134899435)

[Ethics and Privacy in Machine Learning 18](#_Toc134899436)

[I. Bias and Fairness 18](#_Toc134899437)

[II. Privacy 18](#_Toc134899438)

[III. Transparency and Explainability 18](#_Toc134899439)

[IV. Accountability 18](#_Toc134899440)

[V. Regulation and Governance 19](#_Toc134899441)

Machine Learning (ML)

Machine learning is a subset of artificial intelligence that enables systems to learn predict possibilities and improve its prediction capability from experience. ML differs from AI in that it is not explicitly programmed to perform its tasks, like old school AI was. Moreover, ML can learn from experience, while AI is mostly static or human enhanced at best.

Machine learning has a wide range of applications, from image and speech recognition to fraud detection and personalized recommendations. By enabling computers to learn from data, machine learning has the potential of transforming industries and driving innovation. However, with great power comes great responsibility, and it's important to ensure that machine learning is used ethically and responsibly to avoid perpetuating bias and discrimination.

We’ll begin by introducing the basic concepts of machine learning and the different types of learning, such as supervised, unsupervised, and reinforcement learning. Additionally, the module covers Neural Networks.

We’ll also cover key techniques in machine learning, such as data preprocessing, feature engineering, and model evaluation and selection. In addition, the course discusses important considerations in machine learning, such as ethics and privacy, model deployment, and interpretability. By the end of the course, students will have a solid understanding of the key concepts and techniques in machine learning, as well as the ethical and practical considerations involved in its use.

# The Seven Steps of Machine Learning

1. Data collection: Data collection is the process of gathering and measuring information from different sources that are relevant to the problem you want to solve. Data can be numerical, textual, image, audio, video, etc. Data can be obtained from various sources, such as databases, files, web pages, sensors, surveys, etc. Data collection is important because it provides the raw material for machine learning algorithms to learn from and make predictions or decisions.
2. Data preparation or processing: Data preparation is the process of cleaning, transforming, and organizing the data into a suitable format for machine learning algorithms. Data preparation may involve tasks such as removing missing values, outliers, or duplicates; encoding categorical variables; scaling or normalizing numerical variables; splitting or merging features; creating new features; etc. Data preparation is important because it improves the quality and usability of the data and reduces the noise and errors that may affect the performance of machine learning algorithms.
3. Choosing a model: Choosing a model is the process of selecting a machine learning algorithm or technique that can best fit the data and solve the problem. There are many types of machine learning models, such as linear regression, logistic regression, decision trees, neural networks, etc. Each model has its own assumptions, advantages, disadvantages, and parameters. Choosing a model may depend on factors such as the type and size of the data, the complexity and nature of the problem, the computational resources and time available, etc. Choosing a model is important because it determines how well the machine learning algorithm can learn from the data and make predictions or decisions.
4. Training a model: Training a model is the process of applying a machine learning algorithm to the data and finding the optimal values of the parameters that minimize a cost function or maximize an objective function. Training a model may involve techniques such as gradient descent, stochastic gradient descent, backpropagation, etc. Training a model may also require splitting the data into training and validation sets to avoid overfitting or underfitting. Training a model is important because it enables the machine learning algorithm to learn from the data and find the best solution for the problem.
5. Evaluating a model: Evaluating a model is the process of assessing how well the trained machine learning algorithm performs on new or unseen data that was not used for training. Evaluating a model may involve using metrics such as accuracy, precision, recall, F1-score, mean squared error, R-squared, etc. Evaluating a model may also require splitting the data into training and test sets to measure the generalization ability of the machine learning algorithm. Evaluating a model is important because it helps to measure the effectiveness and reliability of the machine learning algorithm and compare different models.
6. Hyperparameter tuning: Hyperparameter tuning is the process of finding the optimal values of the settings or knobs that control the behavior or complexity of the machine learning algorithm. Hyperparameters are different from parameters in that they are not learned from the data but are set by the user before training. Hyperparameters may include learning rate, number of iterations, number of hidden layers or nodes, regularization strength, etc. Hyperparameter tuning may involve techniques such as grid search, random search, Bayesian optimization, etc. Hyperparameter tuning is important because it helps to improve the performance and efficiency of the machine learning algorithm and avoid overfitting or underfitting.
7. Prediction: Prediction is the process of using the trained and tuned machine learning algorithm to make predictions or decisions on new or unseen data that was not used for training or evaluation. Prediction may involve applying the machine learning algorithm to individual data points or batches of data points and producing outputs such as labels, scores, probabilities, classifications, regressions, etc. Prediction is important because it helps to solve real-world problems and provide value or insights based on data.

# Data Preprocessing

## I. Data Collection

* Identifying data sources: Determining where the data is coming from and the available data type.
* Gathering data from various sources: Collecting data from multiple sources such as databases, APIs, or web scraping.
* Storing data in a suitable format: Choosing an appropriate format such as CSV, JSON, or a database for easy analysis and retrieval.

## II. Data Cleaning

* Handling missing values: Determining the best method to handle missing data such as imputation, deletion, or interpolation.
* Handling duplicate values: Identifying and removing duplicate data that can skew analysis results.
* Handling outliers: Identifying and removing outliers that can negatively impact machine learning models.
* Handling noisy data: Identifying and removing noisy data that can introduce errors into the analysis.

## III. Data Transformation

* Feature scaling: Scaling data to ensure that all features are on the same scale and have equal importance.
* Feature encoding: Transforming categorical data into numerical data that machine learning models can process.
* Feature extraction: Extracting new features from existing data to provide additional information to machine learning models.
* Feature selection: Selecting the most relevant features to improve the accuracy and efficiency of machine learning models.

## IV. Data Splitting

* Splitting the data into training and testing sets: Separating the data into two sets, one for training the machine learning model and the other for testing the model's accuracy.
* Setting a random seed for reproducibility: Ensuring that the analysis results can be replicated by setting a random seed.
* Choosing an appropriate ratio of training and testing data: Determining the best proportion of the data for training and testing the machine learning model.
* Stratified sampling for imbalanced datasets: Ensuring that each class in an imbalanced dataset is represented in the training and testing sets.

## V. Data Augmentation (Optional)

* Generating new data from existing data: Creating additional data points from existing data to improve the quality and quantity of the dataset.
* Flipping, rotating, or cropping images: Transforming images to create new variations of the same data.
* Adding noise to audio or text data: Introducing random variations in the data to create new data points.
* Creating synthetic data: Generating new data that is similar to the existing data to augment the dataset.

## VI. Handling Imbalanced Data (Optional)

* Undersampling the majority class: Reducing the number of data points in the majority class to balance the dataset.
* Oversampling the minority class: Increasing the number of data points in the minority class to balance the dataset.
* Generating synthetic samples using SMOTE or other techniques: Creating new data points that are similar to the minority class to balance the dataset.
* Combining undersampling and oversampling techniques: Using a combination of techniques to balance the dataset.

# **Types of Machine Learning**

# Supervised Learning

As the name suggests this type of learning involves human intervention. The machine or the algorithm learns incrementally by adjusting against human assessments on its predictions.

Let’s discuss how a machine may be trained using different popular algorithms applying the to real-world datasets.

## I. Types of Supervised Learning

* Classification: Predicting categorical or discrete values.
* Regression: Predicting continuous numerical values.

## II. The Supervised Learning Process

* Collecting and preparing the data: Gathering data and preparing it for analysis using data preprocessing techniques.
* Splitting the data into training and testing sets: Separating the data into two sets, one for training the machine learning model and the other for testing the model's accuracy.
* Choosing a suitable model: Select a model that is appropriate for the problem at hand and the type of data being analyzed.
* Training the model: Using the training data to adjust the model's parameters and minimize the error between the predicted and actual values.
* Evaluating the model: Using the testing data to evaluate the model's accuracy and generalization.
* Fine-tuning the model: Adjusting the model's hyperparameters to improve its performance.
* Making predictions: Using the trained model to make predictions on new, unseen data.

## III. Model Selection and Evaluation

* Metrics for classification: Accuracy, precision, recall, F1 score, AUC-ROC curve.
* Metrics for regression: Mean squared error, mean absolute error, R-squared score.
* Cross-validation: Evaluating the model's performance on multiple subsets of the data to ensure that it is generalizing well.
* Regularization: Techniques to prevent overfitting, such as L1 and L2 regularization.

## IV. Types of Models

* Linear models: Models that assume a linear relationship between the input and output variables.
* Decision trees: Models that make decisions based on a tree-like structure of if-then statements.
* Ensemble models: Models that combine multiple models to improve their performance, such as random forests and gradient boosting.
* Neural networks: Models that use layers of interconnected nodes to learn complex relationships between the input and output variables.

Supervised learning is a type of machine learning where the input data is labeled and the goal is to learn a function that maps the input to the output. By following the supervised learning process, you can train machine learning models to make accurate predictions on new, unseen data. Choosing a suitable model and evaluating its performance are crucial steps in the process, and there are various metrics and techniques that can be used to ensure that the model is accurate and generalizes well.

# Unsupervised Learning

Let us find out how a machine is made to learn on its own. And how we humans make use of what it has learnt - to answer real world question and to solve real world problems.

Let’s also learn about some effective and popular algorithms used by the industry.

## I. Types of Unsupervised Learning

### Clustering: Grouping similar data points together based on their features.

### Dimensionality reduction: Reducing the number of features in the data while preserving its structure.

## II. The Unsupervised Learning Process

* Collecting and preparing the data: Gathering data and preparing it for analysis using data preprocessing techniques.
* Choosing a suitable model: Select a model that is appropriate for the problem at hand and the type of data being analyzed.
* Training the model: Learning the underlying patterns and structure of the data using unsupervised learning techniques.
* Evaluating the model: Assessing the model's performance based on its ability to find meaningful patterns and structure in the data.
* Applying the model: Using the trained model to gain insights into the data, such as identifying clusters of similar data points or reducing the dimensionality of the data.

## III. Clustering

### K-means clustering:

Dividing the data into k clusters based on their similarity to the cluster centroid.

### Hierarchical clustering:

Dividing the data into clusters based on their similarity to each other, forming a tree-like structure.

### Density-based clustering:

Dividing the data into clusters based on their density, with each cluster containing a high-density region.

## IV. Dimensionality Reduction

### Principal Component Analysis (PCA):

Finding the principal components that explain the majority of the variance in the data and projecting the data onto a lower-dimensional space.

### t-Distributed Stochastic Neighbor Embedding (t-SNE)

Reducing the dimensionality of the data while preserving its local structure, is useful for visualizing high-dimensional data.

### Linear Discriminant Analysis (LDA)

LDA, similar to PCA, aids in reducing the dimensionality of data, but its primary focus is on enhancing the separability among known categories. This is accomplished by creating a new linear axis and projecting the data points onto it, resulting in greater distinguishability among the categories.

Unsupervised learning is a type of machine learning where the input data is unlabeled and the goal is to learn the underlying structure and patterns in the data. By following the unsupervised learning process, you can gain insights into the data and identify meaningful clusters or reduce the dimensionality of the data while preserving its structure. Clustering is a common unsupervised learning technique that involves grouping similar data points together based on their features, while dimensionality reduction involves reducing the number of features in the data while preserving its structure. Various techniques such as k-means clustering, hierarchical clustering, PCA, LDA, and t-SNE can be used to perform unsupervised learning on different types of data.

# Reinforcement Learning

## I. The Reinforcement Learning Process

### Agent and Environment

The agent interacts with the environment and takes actions based on its current state.

State: The current condition of the environment that the agent observes.

### Action:

The decision made by the agent in response to the observed state.

### Reward:

The feedback signal received by the agent after taking an action, indicating how well the action performed in achieving the goal.

### Policy:

The mapping between the observed state and the action taken by the agent.

Value function: The expected amount of future rewards that the agent will receive from a given state or action.

## II. Markov Decision Processes (MDPs)

A formal framework for modeling reinforcement learning problems.

The environment is represented as a set of states, actions, and transition probabilities between states.

The goal is to find the optimal policy that maximizes the expected cumulative reward.

## III. Exploration and Exploitation

Exploration: Taking actions that may not be optimal in order to learn more about the environment and discover better strategies.

Exploitation: Taking actions that are currently believed to be optimal based on previous experience.

## IV. Q-Learning

An off-policy reinforcement learning algorithm for learning the optimal action-value function.

Uses a Q-table to store the expected future rewards for each state-action pair.

Updates the Q-values using the Bellman equation and an exploration-exploitation strategy such as epsilon-greedy.

Reinforcement learning is a type of machine learning where an agent learns to make decisions by interacting with an environment and receiving feedback in the form of rewards. The reinforcement learning process involves observing the current state, taking action, receiving a reward, and updating the policy and value function. Markov Decision Processes (MDPs) provide a formal framework for modeling reinforcement learning problems, and the goal is to find the optimal policy that maximizes the expected cumulative reward. Exploration and exploitation are important concepts in reinforcement learning, balancing between learning more about the environment and exploiting current knowledge to achieve the goal. Q-Learning is a popular reinforcement learning algorithm that uses a Q-table to learn the optimal action-value function, updating the Q-values using the Bellman equation and an exploration-exploitation strategy.

# Neural Networks

# Two categories of Neural Networks

1. Shallow Learning: a simple neural network, with a single hidden layer
2. Deep Learning: a complex neural network with more than one hidden layers

## I. Artificial Neurons

* Mimic the behavior of biological neurons in the brain.
* Receives input signals from other neurons or external stimuli.
* Processes the inputs using a set of weights and a bias term.
* Applies an activation function to the weighted sum of inputs to generate an output.

## II. Feedforward Neural Networks

* The most common type of neural network, where the information flows in one direction from the input layer through one or more hidden layers to the output layer.
* Each neuron in one layer is connected to every neuron in the next layer.
* Typically use backpropagation algorithm to adjust the weights and biases during training.

## III. Convolutional Neural Networks (CNNs)

* Designed for image and video recognition tasks.
* Apply convolutional filters to the input image to extract features and patterns.
* Use pooling layers to reduce the dimensionality of the feature maps.
* Often used in conjunction with fully connected layers for classification or regression tasks.

## IV. Recurrent Neural Networks (RNNs)

* Designed for sequential data processing tasks.
* Use a feedback loop that allows the network to retain information about previous inputs.
* Can process variable-length input sequences and produce variable-length output sequences.
* Useful for tasks such as speech recognition, natural language processing, and time series prediction.

## V. Deep Learning

* Refers to neural networks with multiple hidden layers.
* Can learn hierarchical representations of data, extracting higher-level features from lower-level features.
* Requires a large amount of training data and computational resources, but can achieve state-of-the-art performance on many tasks.

Neural networks are a type of machine learning model inspired by the structure and function of biological neurons in the brain. They consist of artificial neurons that process input signals and produce output signals through a series of weighted connections. Feedforward neural networks are the most common type of neural network and process information in a single direction through one or more hidden layers. Convolutional neural networks are designed for image and video recognition tasks, using convolutional filters and pooling layers to extract features. Recurrent neural networks are designed for sequential data processing tasks, using a feedback loop to retain information about previous inputs. Deep learning refers to neural networks with multiple hidden layers, enabling them to learn hierarchical representations of data.

# Model Evaluation and Selection

## I. Overfitting and Underfitting

* Overfitting occurs when a model is too complex and learns the training data too well, resulting in poor generalization performance on unseen data.
* Underfitting occurs when a model is too simple and does not capture the underlying patterns in the data, resulting in poor performance on both training and test data.
* Balancing the complexity of the model and the amount of available data is crucial for avoiding overfitting and underfitting.

## II. Cross-Validation

* A technique for assessing the performance of a model on unseen data.
* In k-fold cross-validation, the data is split into k subsets, and the model is trained and evaluated k times, each time using a different subset as the test set.
* Provides a more reliable estimate of the model's performance than using a single train-test split.

## III. Hyperparameter Tuning

* Many machine learning models have hyperparameters that need to be set before training.
* Hyperparameter tuning involves selecting the best hyperparameters for the model based on a validation set.
* Techniques for hyperparameter tuning include grid search, random search, and Bayesian optimization.

## IV. Model Selection

* In some cases, multiple models may be considered for a given task.
* Model selection involves comparing the performance of different models on a validation set and selecting the best one.
* Techniques for model selection include comparing the accuracy of different models, using information criteria such as Akaike information criterion (AIC) and Bayesian information criterion (BIC), and using ensemble methods such as stacking.

## V. Bias/Variance Tradeoff

* Bias refers to the difference between the expected predictions of the model and the true values.
* Variance refers to the variability of the model's predictions for different training sets.
* The bias-variance tradeoff is the balance between overfitting (low bias, high variance) and underfitting (high bias, low variance).
* Regularization techniques such as L1/L2 regularization, dropout, and early stopping can be used to control the bias-variance tradeoff.

Model evaluation and selection is an important part of machine learning, ensuring that the model can generalize well to unseen data. Overfitting and underfitting are common problems that can be addressed by balancing the complexity of the model and the amount of available data. Cross-validation is a technique for assessing the performance of a model on unseen data, while hyperparameter tuning involves selecting the best hyperparameters for the model. Model selection involves comparing the performance of different models on a validation set and selecting the best one. The bias-variance tradeoff is the balance between overfitting and underfitting, which can be controlled by regularization techniques.

# Deployment

## I. Model Export

* Once a model is trained and evaluated, it needs to be exported into a format that can be used for deployment.
* Common formats include TensorFlow's SavedModel format, ONNX format, and PMML.

## II. Model Optimization

* Models can be optimized for deployment by reducing their size, increasing their speed, and improving their accuracy.
* Techniques for model optimization include quantization, pruning, and model distillation.

## III. Model Serving

* Once a model is exported and optimized, it can be deployed for serving.
* Model serving involves setting up an API for receiving input data, making predictions with the model, and returning the predictions to the user.

## IV. Infrastructure Setup

* Model serving requires infrastructure for running the model and handling incoming requests.
* Infrastructure can be set up using cloud services such as AWS, Google Cloud, or Azure, or using on-premise solutions.

## V. Monitoring and Maintenance

* Once a model is deployed, it needs to be monitored to ensure that it is performing as expected.
* Monitoring involves tracking metrics such as accuracy, latency, and throughput, and alerting if any issues arise.
* Maintenance involves updating the model as new data becomes available and re-evaluating the model's performance over time.

Model deployment is the process of taking a trained machine-learning model and making it available for use in production environments. This involves exporting the model into a format that can be used for deployment, optimizing the model for size, speed, and accuracy, setting up infrastructure for running the model, monitoring the model's performance, and maintaining the model over time. By successfully deploying a machine learning model, it can provide valuable insights and predictions for real-world applications.

# Ethics and Privacy in Machine Learning

## I. Bias and Fairness

* Machine learning models can inadvertently perpetuate bias and discrimination against certain groups.
* Fairness is important in ensuring that the model treats all groups fairly and does not discriminate based on sensitive attributes such as race, gender, or age.

## II. Privacy

* Machine learning models can collect and process personal data, which can potentially be used for malicious purposes.
* Ensuring privacy involves protecting personal data and ensuring that it is only used for its intended purpose.

## III. Transparency and Explainability

* Machine learning models can be opaque and difficult to understand, which can make it challenging to assess their behavior and decisions.
* Transparency and explainability involve making the model's behavior and decisions more understandable to users and stakeholders.

## IV. Accountability

* Machine learning models can have significant impacts on individuals and society, so it's important to ensure that those responsible for the model are accountable for its behavior.
* This involves identifying who is responsible for the model's behavior and ensuring that they are held accountable for any negative impacts.

## V. Regulation and Governance

* As machine learning becomes more pervasive in society, there is a need for regulation and governance to ensure that it is used ethically and responsibly.
* This includes developing frameworks for responsible AI and establishing guidelines and regulations for the use of machine learning.

Ensuring the ethical and responsible use of machine learning is critical for building trust with users and stakeholders. This involves addressing issues related to bias and fairness, privacy, transparency, explainability, accountability, and regulation and governance. By taking these considerations into account, we can help ensure that machine learning is used for the benefit of society and does not perpetuate harm or injustice.

In conclusion, machine learning is a powerful tool that has the potential to transform industries and drive innovation. By enabling computers to learn from data, machine learning can automate tasks and make predictions that were previously impossible. However, as with any technology, there are potential risks and challenges associated with machine learning, such as the perpetuation of bias and discrimination. It is important for researchers, developers, and policymakers to address these challenges and ensure that machine learning is used ethically and responsibly to benefit society as a whole. By taking a thoughtful and responsible approach to machine learning, we can unlock its full potential and make the world a better place.