A Short Note on

Machine Learning

September 2024

The Machine Learning Landscape

What Is Machine Learning?

- Machine Learning is the science (and art) of programming computers so they can learn from data.
- Machine Learning is the field of study that gives computers the ability to learn without being explicitly programmed. **—Arthur Samuel, 1959**
- A computer program is said to learn from experience E with respect to some task T and some performance measure P, if its performance on T, as measured by P, improves with experience E. **— Tom Mitchell, 1997**

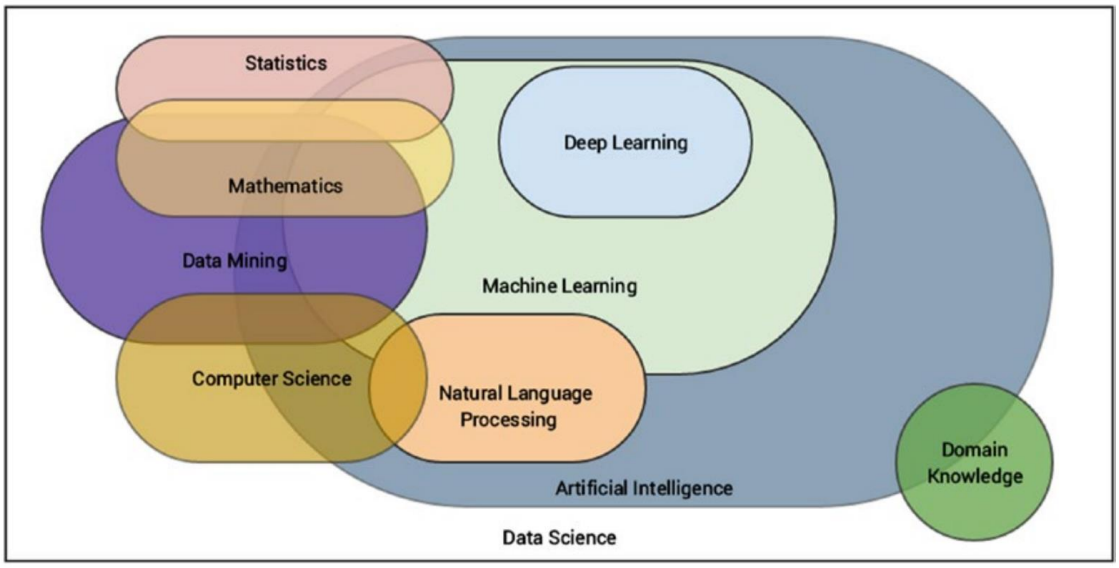


Figure 1-4. *Machine Learning: a true multi-disciplinary field*

- Example: Email SPAM Filtering
  - The task T is to flag spam for new emails
  - the experience E is the training data, and
  - the performance measure P needs to be defined:
    - the ratio of correctly classified emails (Accuracy)

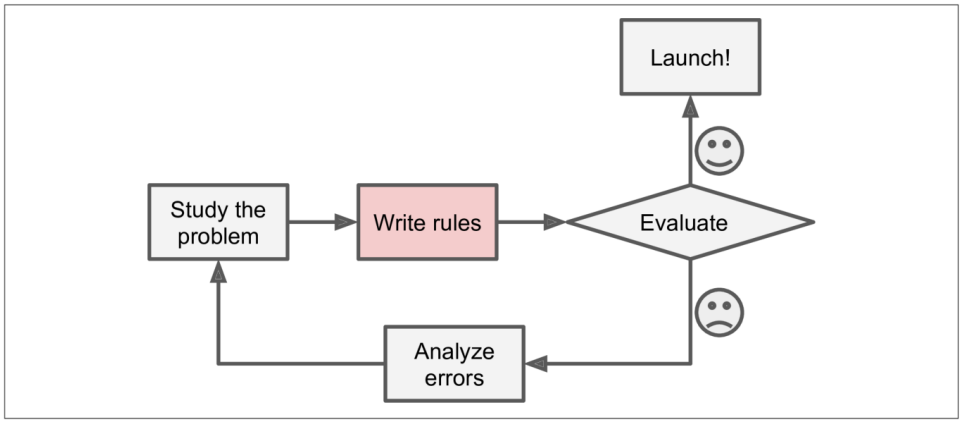


Figure 1-1. The traditional approach

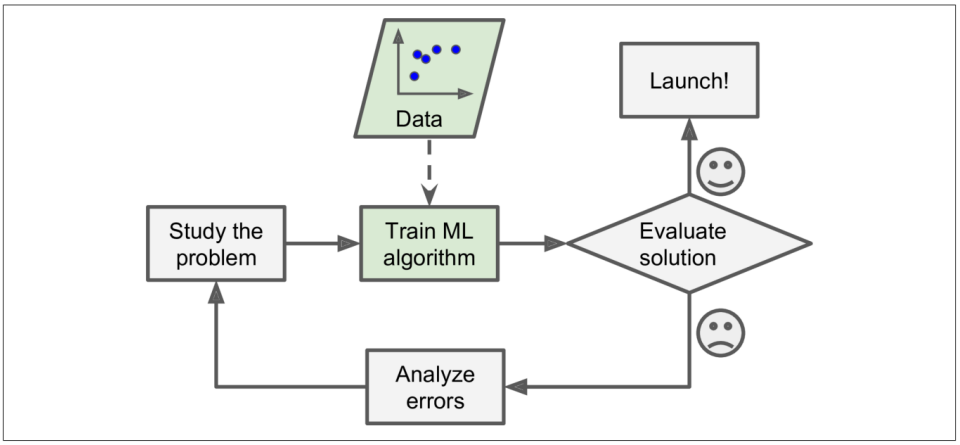


Figure 1-2. Machine Learning approach

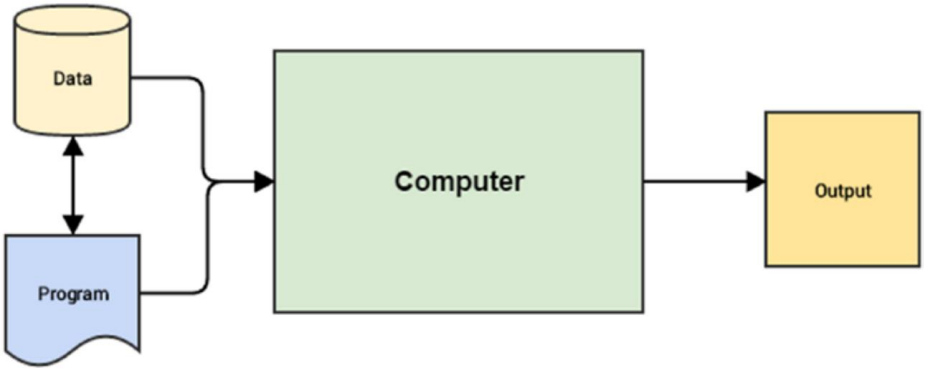


Figure 1-1. *Traditional programming paradigm*

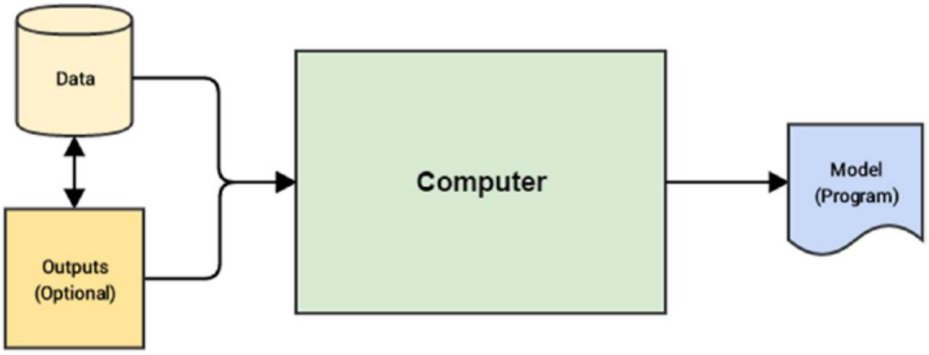
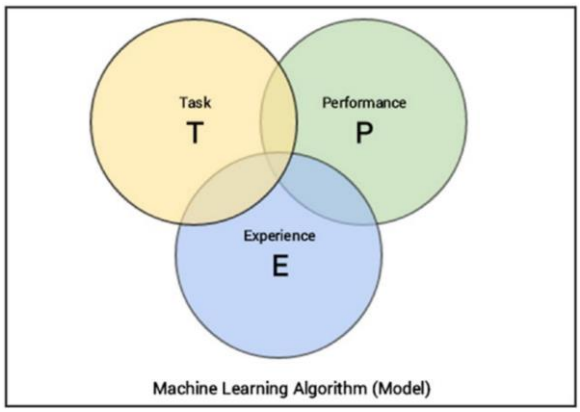


Figure 1-2. *Machine Learning paradigm*



We can simplify the definition as follows.
Machine Learning is a field that consists of learning algorithms that:

- Improve their performance P
- At executing some task T
- Over time with experience E

Machine Learning is great for:

- Problems for which existing solutions require a lot of hand-tuning or long lists of rules: one Machine Learning algorithm can often simplify code and perform better.
- Complex problems for which there is no good solution at all using a traditional approach: the best Machine Learning techniques can find a solution.
- Fluctuating environments: a Machine Learning system can adapt to new data.
- Getting insights about complex problems and large amounts of data.

Types of features in Machine Learning

In machine learning, features (or attributes/variables) are the inputs used to train a model. They can be of various types, each playing a different role in the learning process. Here are the main types of features.

Feature Type	Description	Examples
Numerical Features	Continuous or discrete numbers that can be measured on a scale.	Age, height, weight, income, temperature
Categorical Features	Discrete values that can be grouped into categories.	Gender, color, zip code, brand
Binary Features	A special case of categorical features where the data takes on one of two possible values.	Yes/No, True/False, 0/1
Text Features	Features derived from textual data, often requiring preprocessing like tokenization or embedding.	Reviews, comments, articles
Time-based Features	Features that represent temporal data, often used in time series analysis.	Timestamps, dates, time intervals
Interaction Features	Features created by combining two or more features to capture interactions between them.	Age * Income, Price * Quantity

Derived Features	Features created from existing features through transformations or aggregations.	Log-transformed values, moving averages, polynomial features
Image Features	Features extracted from images, often using techniques like convolutional neural networks (CNNs).	Pixel values, edges, textures
Audio Features	Features extracted from audio signals, often using techniques like Fourier transforms.	Frequency, amplitude, pitch, MFCC (Mel-frequency cepstral coefficients)
Geospatial Features	Features that represent spatial data, often used in geographic information systems (GIS).	Latitude, longitude, altitude, distance

1. Numerical Features

- Continuous: These are numerical values that can take any value within a range. Examples include age, temperature, and salary.
- Discrete: These are numerical values that take distinct, separate values. Examples include the number of children in a family or the number of cars in a garage.

2. Categorical Features

- Nominal: These are categories with no intrinsic ordering. Examples include gender, marital status, or colors (red, blue, green).
- Ordinal: These are categories with a meaningful order but without consistent differences between categories. Examples include education level (high school, bachelor's, master's) or rating scales (poor, fair, good, excellent).

3. Binary Features

These are a special case of categorical features with only two possible values, often represented as 0 and 1. Examples include true/false, yes/no, or male/female.

4. Text Features

These are features based on textual data. Text features often require preprocessing and transformation, such as tokenization, stemming, and converting to numerical vectors using techniques like TF-IDF or word embeddings.

5. Date and Time Features

These features involve time-related data, such as timestamps, dates, and durations. They often need to be converted into meaningful components like day, month, year, hour, minute, or calculated intervals.

6. Derived or Engineered Features

These are new features created from the existing ones to provide more information to the model. Examples include ratios, interactions between features, or polynomial transformations.

7. Spatial Features

These features involve geographic or spatial data. Examples include latitude and longitude, distance between locations, or spatial patterns.

8. Sequence and Time Series Features

These features involve sequential data points collected over time. Examples include stock prices over time, sensor readings, or historical weather data.

9. Image Features

These features are extracted from image data. Techniques such as convolutional neural networks (CNNs) are used to automatically detect and extract relevant features from images.

10. Audio Features

These features are derived from audio signals. Examples include frequency components, pitch, and spectrograms. Techniques like Mel-frequency cepstral coefficients (MFCCs) are commonly used.

11. Interaction Features

These features are created by combining multiple features to capture interactions between them. For example, creating a feature that is the product of two numerical features.

12. Aggregated Features

These features are aggregated statistics from groups of data points. Examples include average purchase amount per customer, total sales per region, or count of transactions per day.

Types of Machine Learning Systems

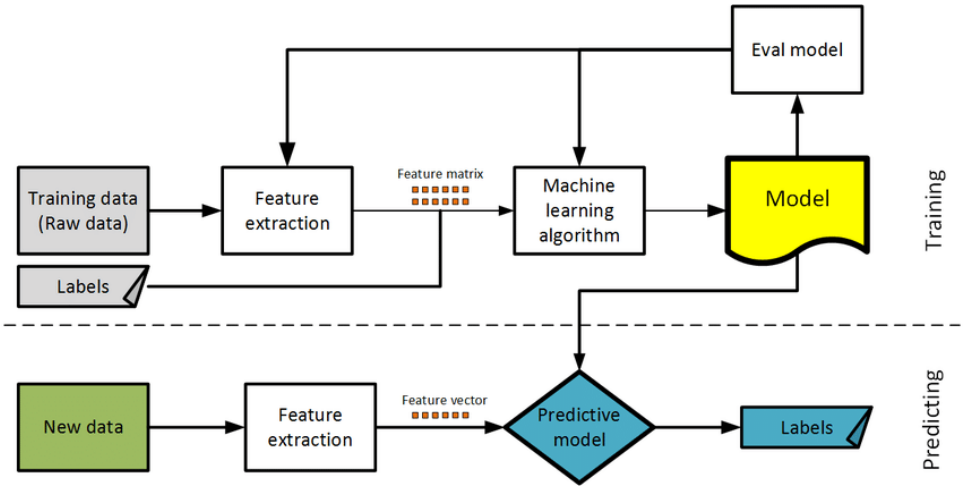
Category	Type	Description	Examples
By Learning Approach	Supervised Learning	Trained with labelled data to map inputs to outputs.	Linear Regression, Decision Trees, SVM, Neural Networks
	Unsupervised Learning	Given input data without labelled responses; finds patterns or groupings.	K-means Clustering, PCA, Association Rule Learning
	Semi-Supervised Learning	Combines labelled and unlabelled data for training.	Semi-Supervised SVM
	Reinforcement Learning	Learns through trial and error by receiving feedback in the form of rewards/penalties.	Q-Learning, Deep Q-Networks (DQN), AlphaGo
By Type of Output	Regression	Predicts continuous values.	Predicting house prices
	Classification	Predicts discrete categories or classes.	Spam Detection
	Clustering	Identifies groups or clusters within data.	Customer Segmentation
	Anomaly Detection	Identifies unusual data points that don't fit the general pattern.	Fraud Detection
	Recommendation Systems	Suggests products or content based on user behaviour.	Netflix or Amazon Recommendations
By Training Method	Batch Learning	Trained on the entire dataset at once; doesn't learn further unless retrained.	Static Data Models
	Online Learning	Trained incrementally with data instances sequentially; adapts to changing data.	Dynamic, Real-time Systems
By Similarity to Human Brain	Artificial Neural Networks (ANN)	Layers of interconnected nodes inspired by the human brain.	Feedforward Neural Networks, CNN, RNN
	Deep Learning	Deep neural networks with multiple layers to extract high-level features.	Image Recognition with CNNs, NLP with Transformers
By Application	Predictive Analytics	Uses historical data to predict future outcomes.	Time Series Forecasting, Predictive Maintenance
	Computer Vision	Enables machines to interpret visual information.	Image Classification, Object Detection, Facial Recognition
	Natural Language Processing (NLP)	Enables machines to understand and generate human language.	Chatbots, Sentiment Analysis, Machine Translation
Other Models	**Ensemble Learning Models**	Combine multiple models to improve overall performance.	Bagging, Boosting, Stacking

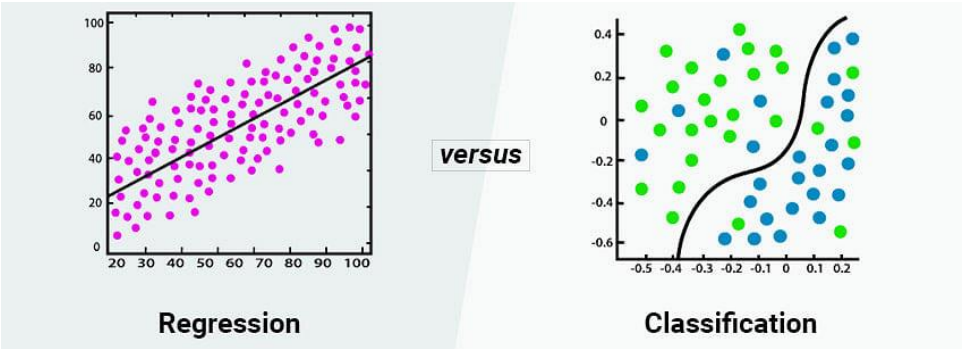
Category	Type	Description	Examples
	Transfer Learning Models	Models leverage knowledge gained from one task to improve learning in a different but related task.	Fine-Tuning Pre-Trained Models like ResNet, VGG, BERT.

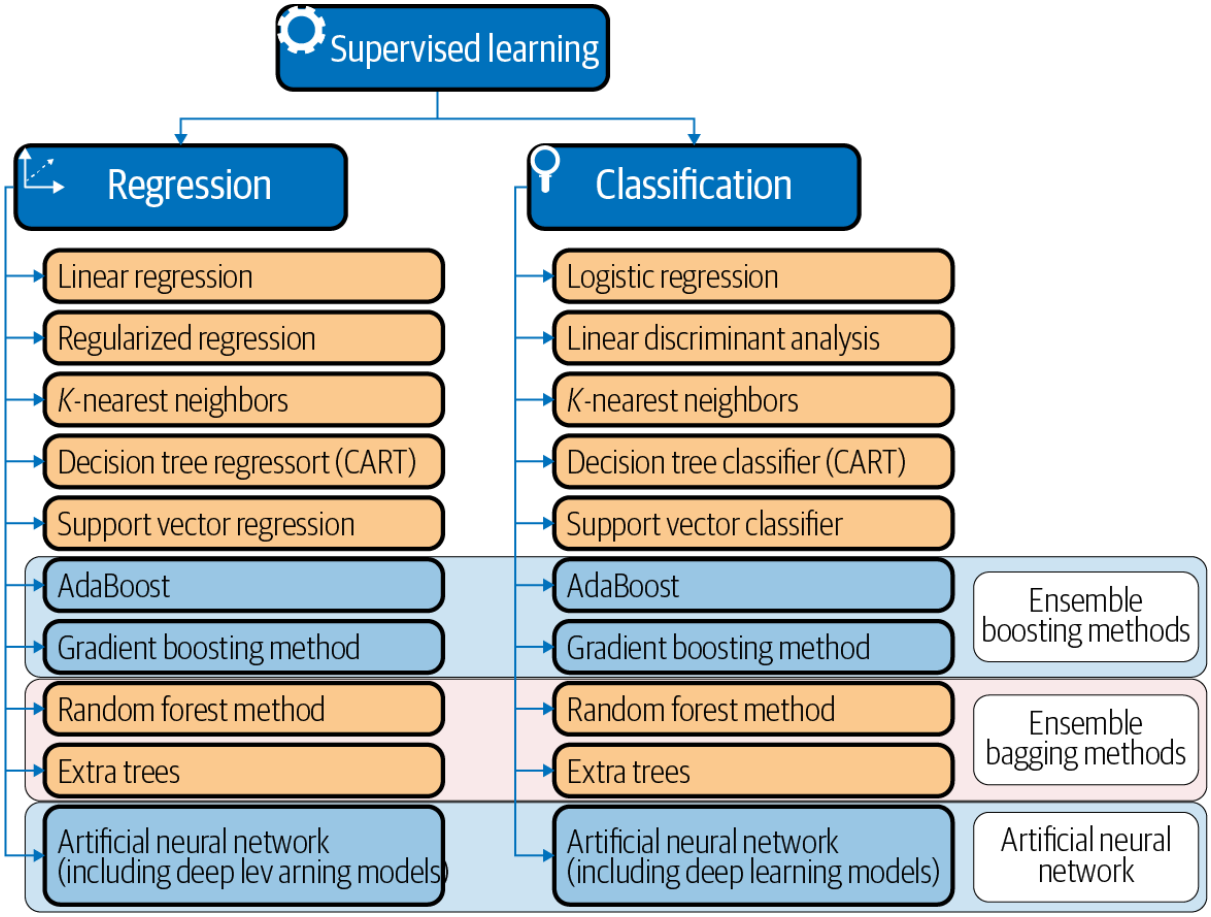
There are so many different types of Machine Learning systems that it is useful to classify them in broad categories based on:

Whether or not they are trained with human supervision

- **Supervised Learning**
  - In supervised learning, the training data you feed to the algorithm includes the desired solutions, called labels.
  - Two types of supervised learning
    - Classification or categorization
      - This typically encompasses the list of problems or tasks where the machine has to take in data points or samples and assign a specific class or category to each sample.
    - Regression
      - These types of tasks usually involve performing a prediction such that a real numerical value is the output instead of a class or category for an input data point.



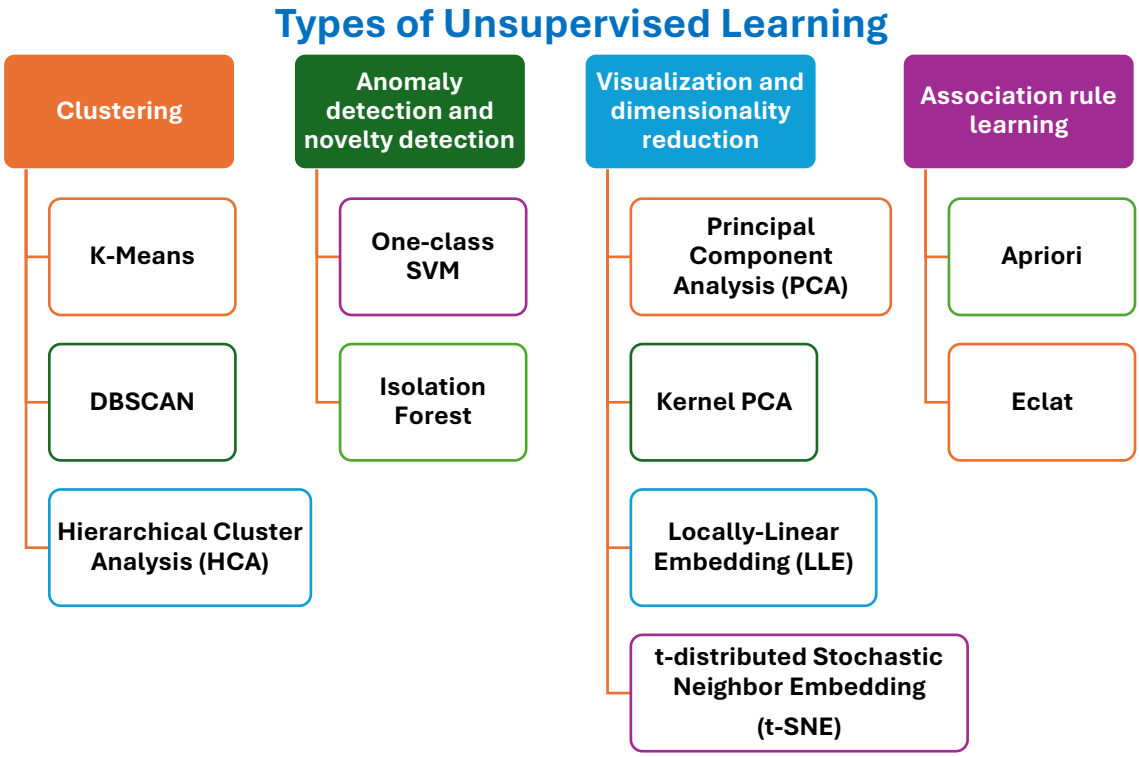




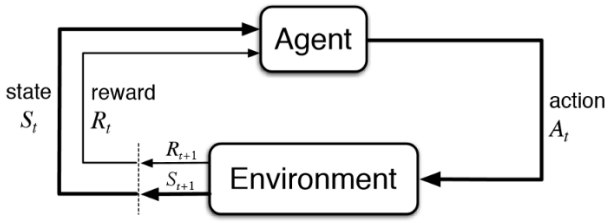
Key Concepts in Supervised Learning

Key Concepts in Supervised Learning
•**Features** • input variables used to make predictions. •**Labels** • output variables or target values •**Training Set** • portion of the data used to train the model •**Test Set** • portion of the data used to evaluate the model •**Model** • mathematical representation that maps inputs to outputs •**Prediction** • mathematical representation that maps inputs to outputs

- **Unsupervised Learning**
  - In unsupervised learning, as you might guess, the training data is unlabelled. The system tries to learn without a teacher.



- **Semi-supervised Learning**
  - Some algorithms can deal with partially labelled training data, usually a lot of unlabelled data and a little bit of labelled data. This is called semi-supervised learning.
- **Reinforcement Learning**
  - The learning system, called an agent in this context, can observe the environment, select and perform actions, and get rewards in return (or penalties in the form of negative rewards)
  - It must then learn by itself what is the best strategy, called a policy, to get the most reward over time. A policy defines what action the agent should choose when it is in a given situation.



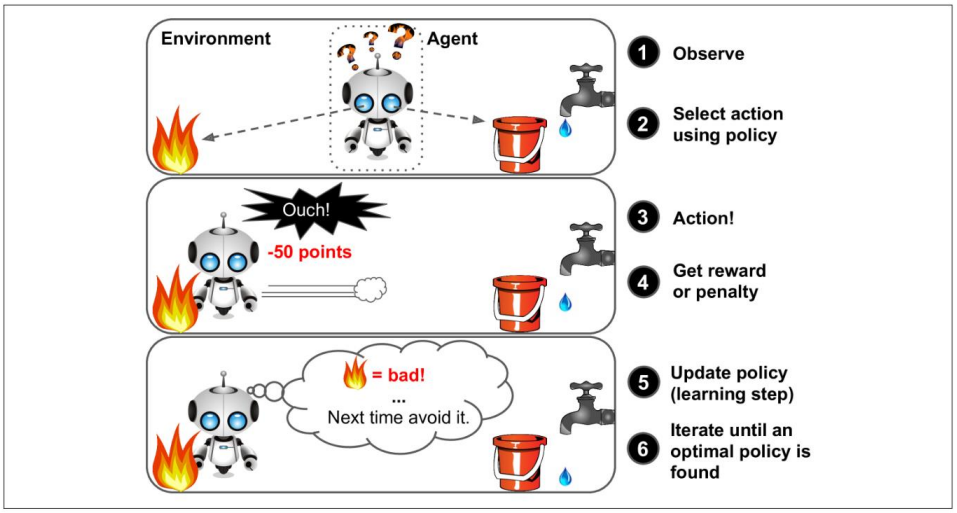


Figure 1-12. Reinforcement Learning

Whether or not they can learn incrementally on the fly

- **Online learning**
  - In online learning, you train the system incrementally by feeding it data instances sequentially, either individually or by small groups called mini batches.
  - Each learning step is fast and cheap, so the system can learn about new data on the fly, as it arrives.
  - Online learning is great for systems that receive data as a continuous flow (e.g., stock prices) and need to adapt to change rapidly or autonomously.
  - It is also a good option if you have limited computing resources: once an online learning system has learned about new data instances, it does not need them anymore, so you can discard them.
- **Batch learning**
  - In batch learning, the system is incapable of learning incrementally: it must be trained using all the available data. This will generally take a lot of time and computing resources, so it is typically done offline. This is called offline learning.

Whether they work by simply comparing new data points to known data points, or instead detect patterns in the training data and build a predictive model, much like scientists do

- **Instance-based learning**
  - The system learns the examples by heart, then generalizes to new cases by comparing them to the learned examples (or a subset of them), using a similarity measure like distance or correlation.
  - Advantages of instance-based learning:
    - No explicit model training is required, so it's easy to adapt to new data.
    - Can handle complex relationships and adapt well to varying data distributions.
  - Disadvantages of instance-based learning:
    - Can be computationally expensive, especially with large datasets.
    - Sensitive to irrelevant or noisy features in the data.
    - Lack of a learned model makes it harder to interpret or explain predictions.

- **Model-based learning**
    - Another way to generalize from a set of examples is to build a model of these examples, then use that model to make predictions. This is called model-based learning.
    - Model-based learning involves creating a model that generalizes from the training data to make predictions on new, unseen data. This model can capture patterns, relationships, and features within the data to provide a way to understand and predict outcomes.

Prerequisites and Tools for Machine Learning

To begin with machine learning, it's essential to have a foundational understanding and access to key tools:

1. Mathematics:

- **Linear Algebra**: Understanding vectors and matrices is crucial for many ML algorithms.
- **Probability and Statistics**: Helps in interpreting data and building probabilistic models.
- **Calculus**: Useful for optimization techniques, particularly in deep learning.

2. Programming Skills:

- **Python**: The most popular language for ML due to its simplicity and extensive libraries like **Scikit-learn**, **TensorFlow**, and **PyTorch**.
- **R**: Often used for statistical analysis and data visualization.
- Familiarity with **SQL** for database management and retrieving data.

3. Data Handling Tools:

- **Pandas**: For data manipulation and analysis.
- **NumPy**: For handling large datasets and performing mathematical operations efficiently.

4. Development Environments:

- **Jupyter Notebook**: A widely-used tool for coding and visualizing results interactively.
- **Google Colab**: Provides a cloud-based environment with free GPU access for running ML models.

5. Machine Learning Libraries and Frameworks:

- **Scikit-learn**: Ideal for beginners to practice standard algorithms like regression and clustering.
- **TensorFlow and PyTorch**: Popular frameworks for building deep learning models.

6. Version Control:

- **Git**: Essential for managing code, tracking changes, and collaborating with others.

7. Cloud Platforms:

- **AWS, Azure, Kaggle and Google Cloud**: Offer scalable resources and tools like AutoML for deploying and managing ML models efficiently.

Category	Details
Mathematics	• **Linear Algebra**: Understanding vectors and matrices is crucial for many ML algorithms. • **Probability and Statistics**: Helps in interpreting data and building probabilistic models. • **Calculus**: Useful for optimization techniques, particularly in deep learning.
Programming Skills	• **Python**: Popular for ML with libraries like Scikit-learn, TensorFlow, and PyTorch. • **R**: Used for statistical analysis and data visualization. • **SQL**: Familiarity with SQL for database management and data retrieval.

Data Handling Tools	• **Pandas**: For data manipulation and analysis. • **NumPy**: For handling large datasets and performing mathematical operations efficiently.
Development Environments	• **Jupyter Notebook**: Tool for coding and visualizing results interactively. • **Kaggle, Google Colab**: Cloud-based environment with free GPU access for running ML models.
ML Libraries and Frameworks	• **Scikit-learn**: Ideal for beginners to practice standard algorithms like regression and clustering. • **TensorFlow and PyTorch**: Frameworks for building deep learning models.
Version Control	• **Git**: For managing code, tracking changes, and collaborating.
Cloud Platforms	• **AWS, Azure, Google Cloud**: Scalable resources and tools like AutoML for ML model deployment.

Main Challenges of Machine Learning

Main Challenges of Machine Learning	
	Inadequate Training Data
	Poor Quality of Data
	Non-Representative Training Data
	Overfitting and Underfitting
	Monitoring and Maintenance
	Data Bias
	Lack of Explainability
	Lack of Skilled Resources
	Process Complexity of Machine Learning
	Slow Implementations and Results
	Irrelevant Features
	Getting Bad Recommendations

1. Inadequate Training Data

One of the primary challenges in machine learning is the availability of **adequate training data**. Machine learning models require large amounts of high-quality data to learn effectively. However, in many domains, obtaining such data is difficult due to factors like **privacy concerns**, **costs of data collection**, and **data sparsity**.

When the training dataset is too small, models can struggle to capture meaningful patterns, resulting in poor performance on unseen data. This problem becomes particularly pronounced in fields like healthcare, where collecting large, diverse datasets is challenging.

Solutions:

- **Data Augmentation**: Techniques such as data augmentation, which artificially increases the size of the dataset by modifying existing data, can help mitigate the problem of limited data.
- **Synthetic Data Generation**: Tools like **GANs (Generative Adversarial Networks)** can generate synthetic data to expand training datasets.
- **Transfer Learning**: Transfer learning allows models to leverage knowledge from other related tasks, reducing the need for large amounts of data.

Addressing the challenge of inadequate training data is essential for building robust and accurate machine learning models.

2. Poor Quality of Data

The quality of data directly impacts the performance of machine learning models. **Poor-quality data**, which may be incomplete, noisy, or inconsistent, can lead to inaccurate predictions and flawed outcomes. **Data preprocessing** is a crucial step to ensure that data is clean and ready for analysis.

Common Issues in Data Quality:

- **Missing Values**: Gaps in data can cause models to make incorrect predictions.
- **Outliers**: Extreme values can skew the model's understanding of normal behavior.
- **Noisy Data**: Unreliable or incorrect data points can reduce the accuracy of the model.

Best Practices for Data Quality:

- **Data Cleaning**: Techniques like **imputation** (filling missing values) and **outlier detection** are essential for improving data quality.
- **Normalization and Scaling**: Ensuring that data is on a consistent scale can improve the model's ability to learn patterns.
- **Feature Engineering**: Creating new features from existing data can provide the model with more meaningful information.

Ensuring high-quality data through proper preprocessing steps is key to improving model performance.

3. Non-Representative Training Data

Non-representative training data occurs when the training dataset does not accurately reflect the **real-world distribution** of data. This can result in models that perform well on the training data but fail to generalize to new, unseen data.

Consequences:

- **Poor Generalization**: Models trained on biased or unrepresentative data may perform well in controlled environments but poorly in real-world applications.
- **Bias in Predictions**: If the training data is not representative, the model's predictions will be biased toward certain outcomes, potentially leading to unfair or inaccurate results.

Solutions:

- **Data Sampling**: Use **stratified sampling** techniques to ensure the training dataset accurately reflects the distribution of the target population.
- **Cross-Validation**: Employ cross-validation methods to test the model's generalization capabilities across different subsets of the data.

Addressing non-representative data is essential for ensuring that models can make accurate predictions in real-world scenarios.

4. Overfitting and Underfitting

Overfitting occurs when a machine learning model becomes too complex and fits the noise in the training data rather than the underlying patterns. This results in poor generalization to new data. **Underfitting**, on the other hand, occurs when a model is too simple to capture the underlying patterns in the data.

Causes:

- **Overfitting**: Caused by models with too many parameters or when there is insufficient regularization.
- **Underfitting**: Occurs when the model is too simple or lacks the capacity to capture complex patterns.

Strategies to Address Overfitting and Underfitting:

- **Cross-Validation**: Regularly test models on unseen data during training to prevent overfitting.
- **Regularization Techniques**: Methods like **L1** and **L2 regularization** can prevent the model from becoming too complex.
- **Early Stopping**: Stop the training process when the model's performance on a validation set starts to degrade, preventing overfitting.

Balancing model complexity is essential to avoid both overfitting and underfitting, ensuring optimal model performance.

5. Monitoring and Maintenance

Once a machine learning model is deployed, **continuous monitoring** is essential to ensure that it remains accurate and relevant. As the data landscape changes, models may begin to drift from their original performance levels.

Challenges:

- **Model Drift**: Over time, changes in the data distribution can lead to model performance degradation, a phenomenon known as model drift.

- **Retraining Needs**: Models require periodic updates and retraining to ensure they continue to deliver accurate predictions as new data becomes available.

Solutions:

- **Automated Monitoring**: Implement monitoring systems to detect when a model's performance starts to decline.
- **Scheduled Retraining**: Regularly retrain models using new data to keep them up to date.

Effective monitoring and maintenance strategies are critical for ensuring that machine learning models remain accurate over time.

6. Data Bias

Data bias occurs when the training data used to build a model is not representative of the broader population, leading to biased predictions. This can result in models that **discriminate against certain groups** or fail to generalize to all users.

Examples:

- **Gender Bias in Hiring Models**: Algorithms trained on biased hiring data may favour one gender over another, perpetuating inequalities.
- **Facial Recognition**: Systems trained predominantly on lighter-skinned individuals often fail to accurately identify people with darker skin tones.

Detecting and Reducing Bias:

- **Bias Detection Tools**: Tools like **IBM AI Fairness 360** can help identify and reduce bias in machine learning models.
- **Diverse Training Data**: Ensuring that the training dataset includes diverse examples can help mitigate bias.

Addressing data bias is critical for building **fair and equitable machine learning models**, especially in industries like healthcare, finance, and criminal justice.

7. Lack of Explainability

Many machine learning models, especially **deep learning** models, are often described as "**black boxes**" due to the difficulty in understanding how they make decisions. This **lack of explainability** presents challenges in industries where transparency is crucial, such as **healthcare** and **finance**.

Consequences:

- **Regulatory Compliance**: In some industries, regulations require that models provide clear explanations for their decisions. Lack of explainability can hinder the adoption of machine learning in these fields.
- **Trust**: Without understanding how a model arrives at a decision, stakeholders may be reluctant to trust its predictions.

Methods to Improve Explainability:

- **LIME (Local Interpretable Model-agnostic Explanations)**: LIME explains individual predictions by approximating the model locally.
- **SHAP (SHapley Additive exPlanations)**: SHAP values provide insights into how each feature contributes to a prediction.

Improving explainability is essential for increasing trust in machine learning models and ensuring compliance with industry regulations.

8. Lack of Skilled Resources

The demand for skilled machine learning professionals far exceeds the available supply, creating a **skills gap** that slows the adoption of machine learning technologies.

Impact:

- **Delayed Adoption**: Organizations may struggle to implement machine learning solutions due to a lack of qualified personnel.

- **Increased Costs**: The scarcity of skilled professionals drives up salaries, making it costly for organizations to hire and retain talent.

Solutions:

- **Education and Training**: Companies can invest in training programs and partnerships with universities to upskill their current workforce.
- **Collaborations**: Partnering with **data science institutes** and offering internships can help build a pipeline of talent.

Closing the skills gap is crucial for accelerating the adoption of machine learning technologies across industries.

9. Process Complexity of Machine Learning

The **development and deployment** of machine learning models can be complex, requiring expertise in **data preprocessing**, **model selection**, and **hyperparameter tuning**. Scaling these processes for larger datasets or diverse use cases adds to the challenge.

Challenges:

- **Data Preparation**: Preprocessing large, complex datasets requires significant time and effort.
- **Model Scaling**: Adapting models to handle larger datasets or real-time applications can be difficult.

Solutions:

- **Automated Machine Learning (AutoML)**: AutoML platforms automate many of the tasks involved in building machine learning models, reducing the complexity of the process.
- **Pipeline Automation**: Automating data pipelines can streamline the process of moving from data collection to model deployment.

Simplifying the machine learning workflow through automation tools can help overcome the complexity of the process.

10. Slow Implementations and Results

Implementing machine learning models and obtaining actionable results can be a slow process, particularly for complex algorithms or large datasets.

Causes:

- **Data Processing Delays**: Preprocessing large datasets can take significant time.
- **Complexity of Algorithms**: Models like **deep learning** often require large amounts of computational resources, leading to delays.

Solutions:

- **Parallel Computing**: Using distributed computing frameworks like **Apache Spark** can speed up data processing and model training.
- **Simplified Models**: In some cases, simpler models can deliver faster results without sacrificing accuracy.

Streamlining the model-building process and optimizing algorithms for efficiency can help reduce the time it takes to implement machine learning solutions.

11. Irrelevant Features

Irrelevant or redundant features in the training data can negatively impact model performance. These features add noise, increase computational costs, and may lead to **overfitting**.

Solutions:

- **Feature Selection**: Techniques like **Principal Component Analysis (PCA)** and **Lasso regression** help reduce the number of features by selecting the most relevant ones.
- **Domain Knowledge**: Leveraging domain expertise can help identify which features are likely to be relevant and which can be discarded.

Reducing irrelevant features improves model accuracy and efficiency, leading to better results and lower computational costs.

12. Getting Bad Recommendations

Recommendation systems are widely used in platforms like **e-commerce** and **streaming services**. However, these systems can provide **bad recommendations** due to **data inaccuracies**, **user behavior changes**, or poorly designed algorithms.

Consequences:

- **User Dissatisfaction**: Poor recommendations can lead to a negative user experience, reducing engagement and customer retention.
- **Loss of Revenue**: Inaccurate recommendations can impact business outcomes by driving users away from the platform.

Solutions:

- **Collaborative Filtering**: Collaborative filtering techniques analyze user behavior to provide more personalized recommendations.
- **Reinforcement Learning**: Reinforcement learning allows recommendation systems to adapt and improve over time by learning from user feedback.

Improving recommendation systems with advanced algorithms can enhance user experience and drive better business outcomes.

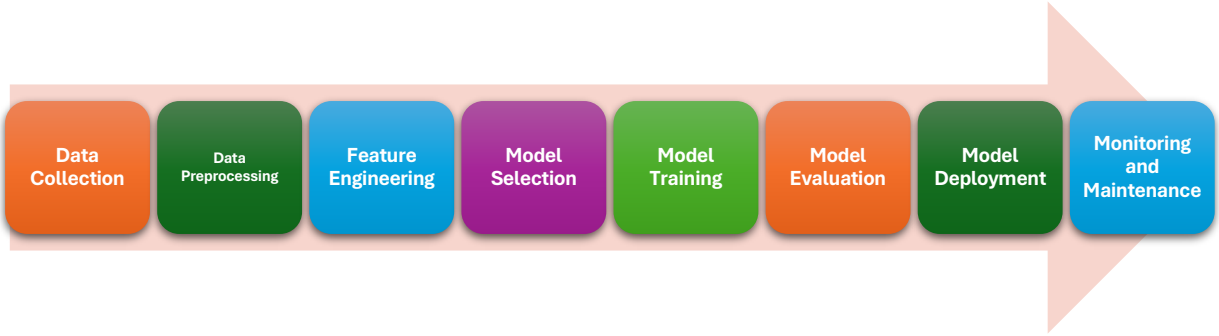
Challenge	Description	Solutions
Inadequate Training Data	Difficulty in obtaining large amounts of high-quality data. Models may struggle to capture patterns with small datasets.	• Data Augmentation • Synthetic Data Generation (GANs) • Transfer Learning
Poor Quality of Data	Incomplete, noisy, or inconsistent data impacts model performance.	• Data Cleaning (imputation, outlier detection) • Normalization and Scaling • Feature Engineering
Non-Representative Training Data	Training data not reflecting real-world distribution leads to poor generalization and biased predictions.	• Data Sampling (stratified) • Cross-Validation
Overfitting and Underfitting	Overfitting: Model fits noise, poor generalization. Underfitting: Model too simple, can't capture patterns.	• Cross-Validation • Regularization (L1, L2) • Early Stopping
Monitoring and Maintenance	Models need continuous monitoring and retraining as data changes over time to avoid performance degradation (model drift).	• Automated Monitoring • Scheduled Retraining
Data Bias	Biased training data leads to discriminatory predictions or failure to generalize.	• Bias Detection Tools (e.g., IBM AI Fairness 360) • Diverse Training Data
Lack of Explainability	Difficulty in understanding complex models' decisions, challenging for industries requiring transparency (e.g., healthcare).	• - LIME (Local Interpretable Model-agnostic Explanations)

Challenge	Description	Solutions
		• SHAP (SHapley Additive exPlanations)
Lack of Skilled Resources	High demand for skilled ML professionals creates a skills gap, slowing adoption and increasing costs.	• - Education and Training • Collaborations with academic and research institutions
Process Complexity of ML	Developing and deploying models requires expertise in data preprocessing, model selection, and hyperparameter tuning. Scaling adds complexity.	• Automated Machine Learning (AutoML) • Pipeline Automation
Slow Implementations and Results	Complex algorithms and large datasets can slow down implementation and result generation.	• Parallel Computing (e.g., Apache Spark) • Simplified Models
Irrelevant Features	Redundant or irrelevant features in data add noise, increase costs, and can cause overfitting.	• Feature Selection (PCA, Lasso regression) • Domain Knowledge
Getting Bad Recommendations	Poor recommendations impact user experience and revenue due to data inaccuracies, user behaviour changes, or poorly designed algorithms.	• Collaborative Filtering • Reinforcement Learning

End-to-End Machine Learning Project

The Machine Learning Pipeline

A machine learning pipeline is a set of repeatable, linked, and often automated steps you follow to engineer, train, and deploy ML models to production.



Data collection:

In this initial stage, new data is collected from various data sources, such as databases, APIs or files. This data ingestion often involves raw data which may require preprocessing to be useful. Here are a few places you can look to get data:

- **Popular open data repositories:**
  - UC Irvine Machine Learning Repository
  - Kaggle datasets
  - Amazon's AWS datasets
- **Meta portals (they list open data repositories):**
  - http://dataportals.org/
  - http://opendatamonitor.eu/
  - http://quandl.com/
- **Other pages listing many popular open data repositories:**
  - Wikipedia's list of Machine Learning datasets
  - Quora.com question
  - Datasets subreddit

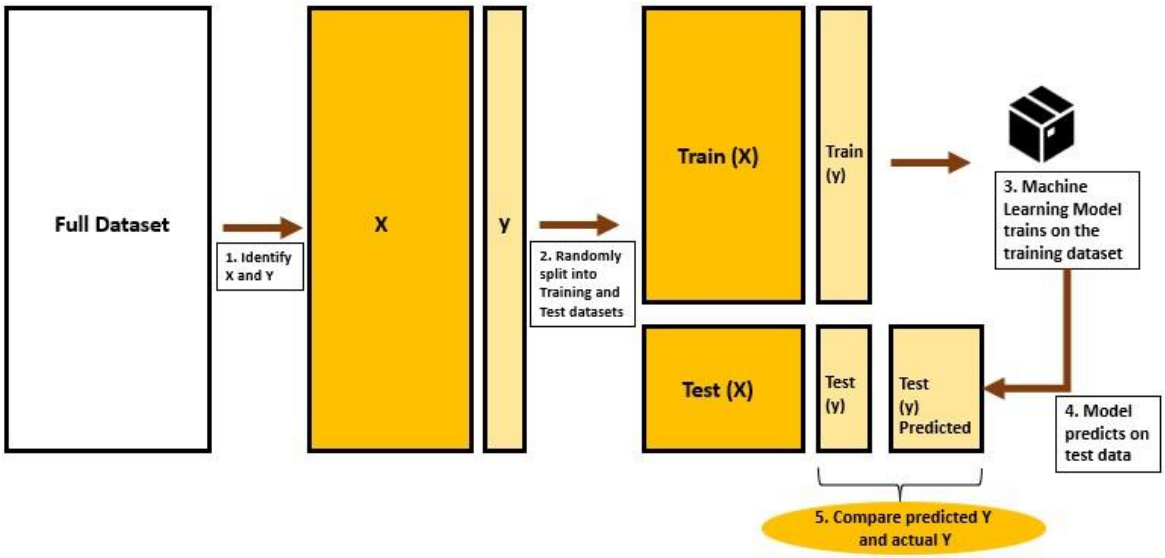
Data preprocessing:

This stage involves cleaning, transforming and preparing input data for modelling. Common preprocessing steps include

- **Exploratory Data Analysis**
  1. **Univariate Analysis**
     - **Summary Statistics**: Mean, median, mode, variance, standard deviation, and percentiles.
     - **Visualizations**: Histograms, bar plots, box plots, and density plots.
  2. **Bivariate Analysis**
     - **Comparative Statistics**: Correlation coefficients, covariance.
     - **Visualizations**: Scatter plots, pair plots, and joint plots.
  3. **Multivariate Analysis**
     - Techniques: Principal Component Analysis (PCA), clustering (e.g., k-means), and factor analysis.
     - Visualizations: Heatmaps, pair plots, and parallel coordinates plots.
  4. **Distribution Analysis**
     - Purpose: Understanding the distribution of data and identifying outliers.
     - Visualizations: Histograms, box plots, and QQ plots.

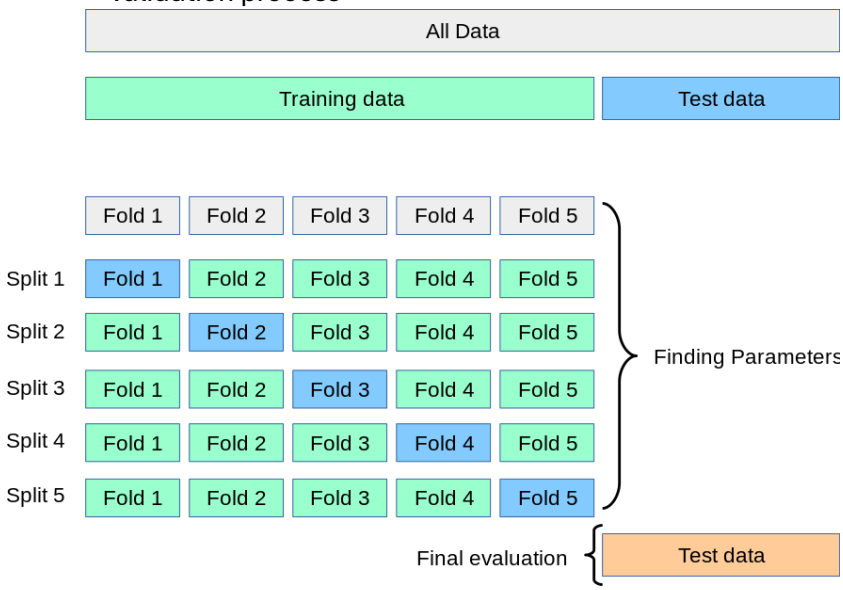
5. **Missing Value Analysis**
    - **Purpose**: Identifying and handling missing data.
    - **Techniques**: Imputation methods, visualization of missing data patterns.
6. **Outlier Detection**
    - **Purpose**: Identifying and analysing outliers.
    - **Techniques**: Z-scores, IQR (Interquartile Range) method, and visualizations like box plots.
7. **Correlation Analysis**
    - **Purpose**: Measuring the relationship between variables.
    - **Techniques**: Pearson, Spearman, and Kendall correlation coefficients.
    - **Visualizations**: Correlation heatmaps, scatter plots.
8. **Trend Analysis**
    - **Purpose**: Identifying patterns or trends over time.
    - **Techniques**: Time series analysis, moving averages.
    - **Visualizations**: Line plots, area plots.
9. **Data Aggregation and Grouping**
    - **Purpose**: Summarizing data based on categories or groups.
    - **Techniques**: Group by operations, pivot tables.
    - **Visualizations**: Bar plots, pie charts, box plots.
10. **Data Visualization**
    - **Purpose**: Creating graphical representations to understand data.
    - **Tools**: Matplotlib, Seaborn, Plotly, and other visualization libraries.
    - **Visualizations**: Various plots (scatter, line, bar, etc.), interactive dashboards.

- **Encoding Categorical Variables**
    - — Encoding categorical variables is a crucial step in preparing data for machine learning models. Since most algorithms require numerical input, we need to convert categorical data into a numerical format. Here are some common techniques:
        - One-Hot Encoding
        - Label Encoding
        - Ordinal Encoding
        - Binary Encoding
        - Target Encoding
        - Frequency Encoding
- **Scaling Numerical Features**
    - — Scaling numerical features is a key step in data preprocessing that can significantly improve the performance of machine learning models. It is scaling the data to be analysed to a specific range such as [0.0, 1.0] to provide better results. Here's a list of the most common techniques for scaling numerical features:
        - Standardization (Z-score Normalization)
        - Min-Max Scaling (Normalization)
        - Robust Scaling
        - Log Transformation
        - Square Root Transformation
        - Exponential Transformation
        - Maximum Absolute Scaling
- **Splitting The Data into Training and Testing Sets.**
    - — Splitting the data into training and testing sets is a fundamental step in building machine learning models. It ensures that the model's performance can be



evaluated on unseen data, providing a measure of its generalizability. Some of the data splitting are given as

- **Simple Split**
  A simple and common approach is to randomly split the dataset into two parts: the training set and the testing set. The training set is used to train the model, while the testing set is used to evaluate its performance.
- **Stratified Split**
  When dealing with imbalanced datasets, it's important to ensure that the split maintains the same proportion of classes in both the training and testing sets. This is known as stratified sampling.
- **Cross-Validation Split**
  Cross-validation is a more robust method that involves splitting the data into multiple folds. The model is trained and evaluated multiple times, each time using a different fold as the testing set and the remaining folds as the training set. This helps in getting a more reliable estimate of the model's performance. The diagram below shows the k-fold cross validation process



Feature engineering:

Feature engineering is the process of creating new features or selecting relevant features from the data that can improve the model's predictive power. This step often requires domain knowledge and creativity.

1. **Creation of New Features**
   - **Combining Features:** Creating new features by combining existing ones. For example, if you have height and weight, you might create a new feature BMI (Body Mass Index).
   - **Decomposition:** Splitting a feature into multiple components. For instance, a date feature can be decomposed into day, month, year, or even day of the week.
2. **Transformation of Features**
   - **Normalization/Standardization:** Scaling features so that they have a mean of 0 and a standard deviation of 1. This is especially useful for algorithms like gradient descent.
   - **Encoding Categorical Features:** Converting categorical variables into numeric values. Common methods include one-hot encoding and label encoding.
4. **Feature Selection**
   - **Filter Methods:** Using statistical tests to select features based on their relationship with the target variable.
   - **Wrapper Methods:** Employing algorithms to search for the best subset of features.
   - **Embedded Methods:** Methods like Lasso regression that perform feature selection during the model training process.
5. **Feature Interaction**
   - **Polynomial Features:** Creating new features by taking the polynomial combination of existing features.
   - **Interaction Terms:** Multiplying or combining features to capture interactions between them.
6. **Dimensionality Reduction**
   - **Principal Component Analysis (PCA):** Reducing the dimensionality of the data while retaining most of the variance.
   - **t-Distributed Stochastic Neighbour Embedding (t-SNE):** A technique for visualizing high-dimensional data by reducing it to two or three dimensions.

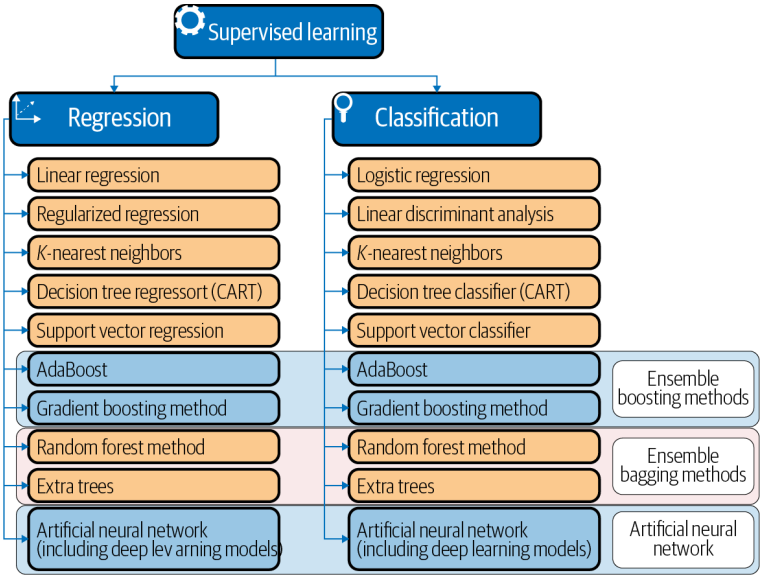
Model selection:

In this stage, you choose the appropriate machine learning algorithm(s) based on the problem type, data characteristics, and performance requirements. You may also consider hyperparameter tuning.

Model training:

The selected model(s) are trained on the training dataset using the chosen algorithm(s). This involves learning the underlying patterns and relationships within the training data.

- **Supervised learning:** When input data along with correct output is supplied to the model, the learning is known as supervised learning.
- **Unsupervised learning:** When unlabelled data is provided and the aim of the algorithm is to find patterns in data and cluster them or to find the association, this sort of learning is known as unsupervised learning.
- **Reinforcement learning:** It's basic aim is to learn to take some suitable action in a particular environment so as to maximise the reward.



Pre-trained models can also be used, rather than training a new model.

Model evaluation:

Validation Process

Before we evaluate our model onto a test dataset, it is a good idea to validate the model on the validation set. This is because when we have trained our model, we can't say for sure that our model works well on unseen dataset i.e. performs with required accuracy.

Thus, the process of validation is to get confidence that our model can give desired results on unseen data or to give us an assurance that the way we have assumed relations between data to produce some outputs are indeed correct.

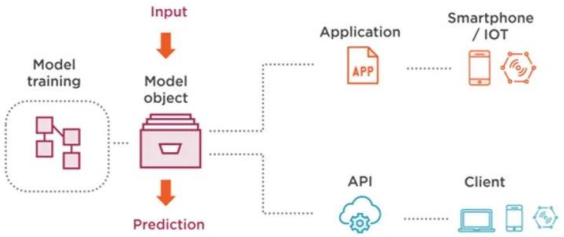
Testing Process

After training, the model's performance is assessed using a separate testing dataset or through cross-validation. The table provides different metrics usually used for regression and classification applications.

Regression Metrics	Classification Metrics
• Mean Absolute Error • Mean Squared Error • Root Mean Square Error • Root Mean Square Logarithmic Error • R^2 – Score	• Classification Accuracy • Logarithmic loss • Area under Curve • F1 score • Precision • Recall • Confusion Matrix

Model deployment:

Once a satisfactory model is developed and evaluated, it can be deployed to a production environment where it can make predictions on new, unseen data. Deployment may involve creating APIs and integrating with other systems.



Model serving platforms are programs or frameworks that make managing, scaling, and deploying machine learning models in real-world settings easier. Some of the popular platforms are listed below.

- Amazon SageMaker
- Google Cloud AI Platform
- Hugging Face
- IBM Watson Machine Learning
- KServe
- Kubeflow
- Microsoft Azure ML
- MLflow
- TensorFlow Serving

Monitoring and maintenance:

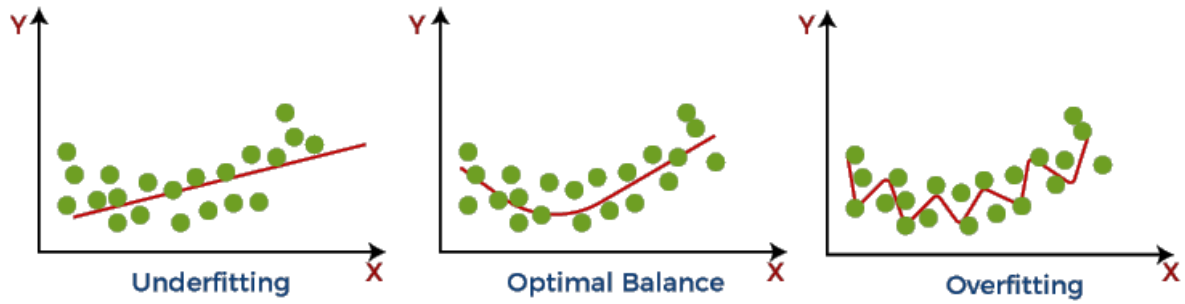
After deployment, it's important to continuously monitor the model's performance and retrain it as needed to adapt to changing data patterns. This step ensures that the model remains accurate and reliable in a real-world setting.

Bias – Variance Trade-off

Bias and variance are two sources of error in predictive models. Getting the right balance between the bias and variance trade-off is fundamental to effective machine learning algorithms. Here is a quick explanation of these concepts:

Bias

- Bias refers to error caused by a model for solving complex problems that is over simplified, makes significant assumptions, and misses important relationships in your data.
- Its also known as underfitting.
- Bias in ML is sometimes called the “too simple” problem. Bias is considered a systematic error that occurs in the machine learning model itself due to incorrect assumptions in the ML process.
- Technically, we can define bias as the error between average model prediction and the ground truth. Moreover, it describes how well the model matches the training data set:
    - **High bias.** A model with a higher bias would not match the data set closely.
    - **Low bias.** A low bias model will closely match the training data set.
- Characteristics of a high bias model include:
    - Failure to capture proper data trends
    - Potential towards underfitting
    - More generalized/overly simplified
    - High error rate



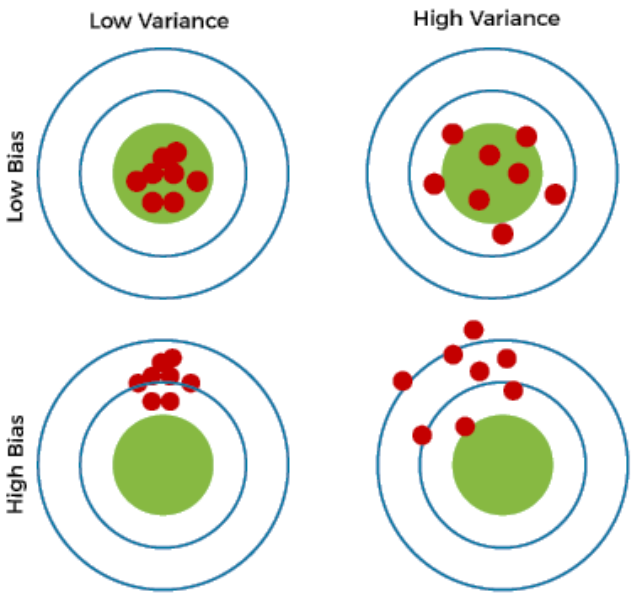
Variance

- Variance is an error caused by an algorithm that is too sensitive to fluctuations in data, creating an overly complex model that sees patterns in data that are actually just randomness.
- Variance in machine learning is sometimes called the “too sensitive” problem. Variance in ML refers to the changes in the model when using different portions of the training data set.
- Simply stated, variance is the variability in the model prediction—how much the ML function can adjust depending on the given data set. Variance comes from highly complex models with a large number of features.
    - **Low variance**. Models with high bias will have low variance.
    - **High variance**. Models with high variance will have a low bias.

- All these contribute to the flexibility of the model. For instance, a model that does not match a data set with a high bias will create an inflexible model with a low variance that results in a suboptimal machine learning model.
- Characteristics of a high variance model include:
    - Noise in the data set
    - Potential towards overfitting
    - Complex models
    - Trying to put all data points as close as possible

Different Combinations of Bias-Variance

There are four possible combinations of bias and variances, which are represented by the below diagram:



Low-Bias, Low-Variance:

The combination of low bias and low variance shows an ideal machine learning model. However, it is not possible practically.

Low-Bias, High-Variance:

With low bias and high variance, model predictions are inconsistent and accurate on average. This case occurs when the model learns with a large number of parameters and hence leads to an **overfitting**

High-Bias, Low-Variance:

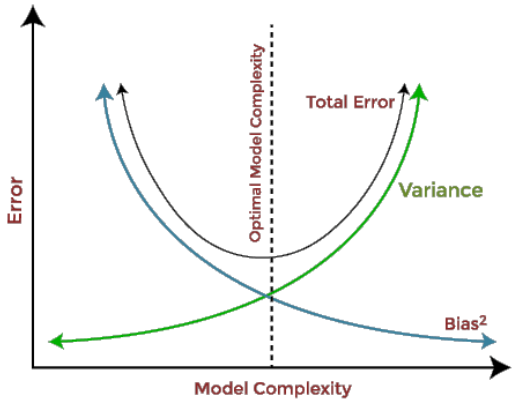
With High bias and low variance, predictions are consistent but inaccurate on average. This case occurs when a model does not learn well with the training dataset or uses few numbers of the parameter. It leads to **underfitting** problems in the model.

High-Bias, High-Variance:

With high bias and high variance, predictions are inconsistent and also inaccurate on average.

Bias–variance trade-off

- While building the machine learning model, it is really important to take care of bias and variance in order to avoid overfitting and underfitting in the model.
- If the model is very simple with fewer parameters, it may have low variance and high bias. Whereas, if the model has a large number of parameters, it will have high variance and low bias.
- So, it is required to make a balance between bias and variance errors, and this balance between the bias error and variance error is known as the Bias-Variance trade-off.



- For an accurate prediction of the model, algorithms need a low variance and low bias. But this is not possible because bias and variance are related to each other:
    - If we decrease the variance, it will increase the bias.
    - If we decrease the bias, it will increase the variance.
- Bias-Variance trade-off is a central issue in supervised learning.
- Ideally, we need a model that accurately captures the regularities in training data and simultaneously generalizes well with the unseen dataset.
- Unfortunately, doing this is not possible simultaneously. Because
    - a high variance algorithm may perform well with training data, but it may lead to overfitting to noisy data.
    - a high bias algorithm generates a much simple model that may not even capture important regularities in the data.
- So, we need to find a sweet spot between bias and variance to make an optimal model.

Classification

What is classification?

- In machine learning, classification solves the problem of identifying the category to which a new data point belongs. We build the classification model based on the training dataset containing data points and the corresponding labels.
- For example, let's say that we want to check whether the given image contains a person's face or not.
    - We would build a training dataset containing classes corresponding to these two classes: face and no-face.
    - We then train the model based on the training samples we have.
    - This trained model is then used for inference.
- A good classification system makes it easy to find and retrieve data.
- This is used extensively in face recognition, spam identification, recommendation engines, and so on.

Classification Steps

Data

- We will be using the MNIST dataset, which is a set of 70,000 small images of digits handwritten by high school students and employees of the US Census Bureau.
- Each image is labelled with the digit it represents.
- Datasets loaded by Scikit-Learn generally have a similar dictionary structure including:
    - A `DESCR` key describing the dataset
    - A `data` key containing an array with one row per instance and one column per feature
    - A `target` key containing an array with the labels
- There are 70,000 images, and each image has 784 features. This is because each image is 28×28 pixels, and each feature simply represents one pixel's intensity, from 0 (white) to 255 (black).

- To download the MNIST dataset the following code is used.

```
from sklearn.datasets import fetch_openml
mnist=fetch_openml('mnist_784',version=1)
```

Data Visualization

Model Selection

In this project, binary classification was performed to distinguish between zeros and non-zeros. The SGD classifier was used to perform the binary classification task.

Performance Evaluation

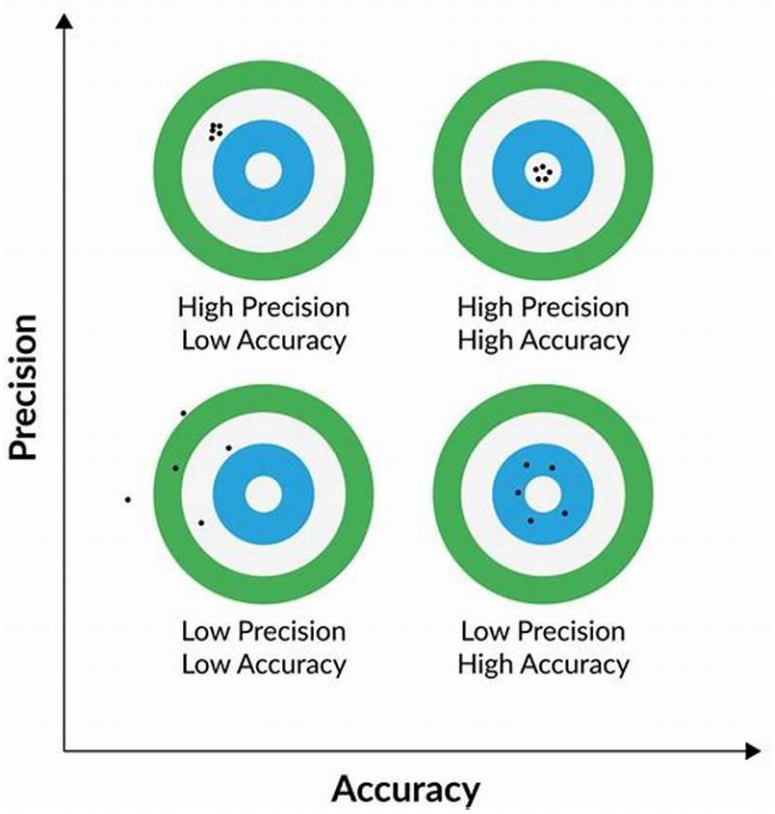
- Confusion Matrix
  - The confusion matrix is another performance measure used in classification. It is a table that allows visualization of the algorithm's performance.
  - Components of a Confusion Matrix
  - For binary classification, the confusion matrix summarizes 4 results in a 2x2 matrix.

	Predicted Positive	Predicted Negative
Actual Positive	True Positive	False Negative
Actual Negative	False Positive	True Negative

- Classification Report
  - It finds the parameters such as Accuracy, Precision, Recall, F1 Score.

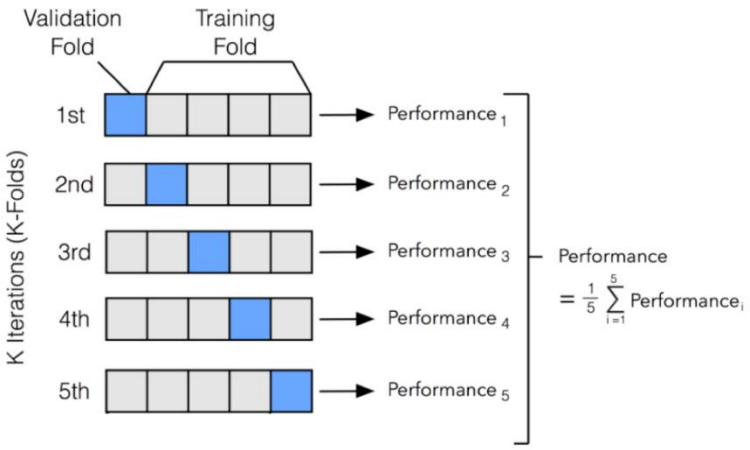
Parameter	Equation	Remark
Accuracy	$\frac{TN+TP}{TN+FP+TP+FN}$	• represents the number of correctly classified data instances over the total number of data instances. • may not be a good measure if the dataset is not balanced
Precision (Specificity)	$\frac{TP}{TP+FP}$	• Precision is a metric that gives you the proportion of true positives to the amount of total positives that the model predicts.

Recall (Sensitivity)	$\frac{TP}{TP + FN}$	• Also known as sensitivity or true positive rate • Recall focuses on how good the model is at finding all the positives.
F1-Score	$2 * \frac{Precision * Recall}{Precision + Recall}$	• Tells us how precise (It correctly classifies how many instances) and robust (does not miss any significant number of instances) our classifier is. • Useful in imbalanced datasets



- K-Fold Cross-Validation
  - K-fold cross-validation approach divides the input dataset into K groups of samples of equal sizes. These samples are called folds.
  - For each learning set, the prediction function uses k-1 folds, and the rest of the folds are used for the test set.
  - The brilliance of K-Fold Cross-Validation lies in its ability to mitigate the bias associated with the random shuffling of data into training and test sets, ensuring that every observation from the original dataset has the chance of appearing in the training and test set. This is crucial for models that are sensitive to the data on which they are trained.

- **Steps to Perform K-Fold Cross-Validation**
  - **Split the Dataset**: The dataset is divided into 'K' number of folds. Typically, K is set to 5 or 10, but the choice depends on the dataset size and the computational cost you're willing to incur.
  - **Iterate Through Folds**: For each iteration, select one fold as the test set and the remaining K-1 folds as the training set.
  - **Train and Evaluate**: Train the model on the training set and evaluate it on the test set. Record the performance score determined by your evaluation metric.
  - **Repeat**: Repeat this process K times, with each of the folds serving as the test set exactly once.
  - **Aggregate Results**: Calculate the average of the performance scores. This average is your model's performance metric.



- Precision-Recall Curve
  - Most imbalanced classification problems involve two classes:
    - a negative case with the majority of examples
    - a positive case with a minority of examples.
  - Two diagnostic tools that help in the interpretation of binary (two-class) classification predictive models are ROC Curves and Precision-Recall curves.
  - Plots from the curves can be created and used to understand the trade-off in performance for different threshold values when interpreting probabilistic predictions. Each plot can also be summarized with an area under the curve score that can be used to directly compare classification models.

Regression Example:
California Housing Price Prediction

Description:

The US Census Bureau has published California Census Data which has 10 types of metrics such as the population, median income, median housing price, and so on for each block group in California. The dataset also serves as an input for project scoping and tries to specify the functional and nonfunctional requirements for it.

Background of the Problem Statement:

The project aims at building a model of housing prices to predict median house values in California using the provided dataset. This model should learn from the data and be able to predict the median housing price in any district, given all the other metrics. Districts or block groups are the smallest geographical units for which the US Census Bureau publishes sample data (a block group typically has a population of 600 to 3,000 people). There are 20,640 districts in the project dataset.

Dataset Description:

Variable	Type	Description
longitude	signed numeric (float)	Longitude value for the block in California, USA
latitude	numeric (float)	Latitude value for the block in California, USA
housing_median_age	numeric (int)	Median age of the house in the block
total_rooms	numeric (int)	Count of the total number of rooms (excluding bedrooms) in all houses in the block
total_bedrooms	numeric (float)	Count of the total number of bedrooms in all houses in the block
population	numeric (int)	Count of the total number of population in the block
households	numeric (int)	Count of the total number of households in the block
median_income	numeric (float)	Median of the total household income of all the houses in the block
ocean_proximity	numeric (categorical)	Type of the landscape of the block ['NEAR BAY', '<1H OCEAN', 'INLAND', 'NEAR OCEAN', 'ISLAND']
median_house_value	numeric (int)	Median of the household prices of all the houses in the block

- **Dataset Size**: 20640 rows x 10 columns

Steps:

1. Load the data:

- Read the “housing.csv” file from the folder into the program.
- Print first few rows of this data.

2. Perform Exploratory Data Analysis

- Perform different EDA techniques such as
    - Statistical analysis
    - Histograms
    - Joint Plot
    - Pair Plot
    - Correlation Plot
    - Regression Plot
- Extract input (X) and output (y) data from the dataset.

3. Encode categorical data:

- Convert categorical column in the dataset to numerical data.

4. Handle missing values:

- Fill the missing values with the mean of the respective column.

5. Split the dataset:

- Split the data into 80% training dataset and 20% test dataset.

6. Standardize data:

- Standardize training and test datasets.

7. Perform Linear Regression:

- Perform Linear Regression on training data.
- Predict output for test dataset using the fitted model.
- Print root mean squared error (RMSE) from Linear Regression.

8. Perform other regression methods and compare the results

- Predict using Decision Tree
- Predict using Random Forest

Types of Regression Metrics

- Mean Absolute Error (MAE)
- Mean Squared Error (MSE)
- Root Mean Squared Error (RMSE)
- R Squared (R2)

Mean Absolute Error (MAE)

MAE is a very simple metric which calculates the absolute difference between actual and predicted values.

$$MAE = \frac{1}{N}\sum_{i=1}^{N}|y_i - \hat{y}_i|$$

Advantages of MAE

- The MAE you get is in the same unit as the output variable.
- It is most Robust to outliers.

Disadvantages of MAE

- The graph of MAE is not differentiable so we have to apply various optimizers like Gradient descent which can be differentiable.

Python Code

```
from sklearn.metrics import mean_absolute_error
print("MAE",mean_absolute_error(y_test,y_pred))
```

Mean Squared Error (MSE)

MSE is a most used and very simple metric with a little bit of change in mean absolute error. Mean squared error states that finding the squared difference between actual and predicted value.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2$$

Advantages of MSE

- The graph of MSE is differentiable, so you can easily use it as a loss function.

Disadvantages of MSE

- The value you get after calculating MSE is a squared unit of output. for example, the output variable is in meter(m) then after calculating MSE the output we get is in meter squared.
- If you have outliers in the dataset then it penalizes the outliers most and the calculated MSE is bigger. So, in short, It is not robust to outliers which were an advantage in MAE.

Python Code

```
from sklearn.metrics import mean_squared_error
print("MSE",mean_squared_error(y_test,y_pred))
```

Root Mean Squared Error (RMSE)

As RMSE is clear by the name itself, that it is a simple square root of mean squared error.

$$RMSE = \sqrt{MSE} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2}$$

Advantages of RMSE

- The output value you get is in the same unit as the required output variable which makes interpretation of loss easy.

Disadvantages of RMSE

- It is not that robust to outliers as compared to MAE.

Python Code

```
print("RMSE",np.sqrt(mean_squared_error(y_test,y_pred)))Copy Code
```

R Squared Score (R2)

- R2 score is a metric that tells the performance of your model, not the loss in an absolute sense that how many wells did your model perform.

$$R2 = 1 - \frac{SST}{SSR}$$

Where:

  - $R2$ is the R-Squared.
  - SSR represents the sum of squared residuals between the predicted values and actual values.
  - SST represents the total sum of squares, which measures the total variance in the dependent variable.

- In contrast, MAE and MSE depend on the context as we have seen whereas the R2 score is independent of context.
- So, with help of R squared we have a baseline model to compare a model which none of the other metrics provides.
- So basically, R2 squared calculates how must regression line is better than a mean line.
- Hence, R2 squared is also known as Coefficient of Determination or sometimes also known as Goodness of fit.
- If the R2 score is zero then the above regression line by mean line is equal means 1 so 1-1 is zero. So, in this case, both lines are overlapping means model performance is worst, It is not capable to take advantage of the output column.
- If R2 score is 1, it means when the division term is zero and it will happen when the regression line does not make any mistake, it is perfect. In the real world, it is not possible.
- The regression line moves towards perfection, R2 score move towards one. And the model performance improves.

Python Code

```
from sklearn.metrics import r2_score
r2 = r2_score(y_test,y_pred)
print(r2)
```

Binary Classification Example: PIMA Indian Diabetes Dataset Classification

Description:

The Pima Indian Diabetes Dataset, originally from the National Institute of Diabetes and Digestive and Kidney Diseases, contains information of 768 women from a population near Phoenix, Arizona, USA.

The objective of the dataset is to diagnostically predict whether or not a patient has diabetes, based on certain diagnostic measurements included in the dataset. Several constraints were placed on the selection of these instances from a larger database. In particular, all patients here are females at least 21 years old of Pima Indian heritage.

Background of the Problem Statement:

The outcome tested was Diabetes, 268 tested positive and 500 tested negative. Therefore, there is one target (dependent) variable and the 8 attributes: pregnancies, OGTT (Oral Glucose Tolerance Test), blood pressure, skin thickness, insulin, BMI (Body Mass Index), age, pedigree diabetes function. The Pima population has been under study by the National Institute of Diabetes and Digestive and Kidney Diseases at intervals of 2 years since 1965. As epidemiological evidence indicates that T2DM results from interaction of genetic and environmental factors, the Pima Indians Diabetes Dataset includes information about attributes that could and should be related to the onset of diabetes and its future complications.

Dataset Description:

Features

Table 1. The attributes of PIMA dataset.

Attribute	Description	Type	Average/Mean
Preg	Number of times pregnant.	Numeric	3.85
Glucose	Plasma glucose concentration 2 h in an oral glucose tolerance test.	Numeric	120.89
BP	Diastolic blood pressure (mm Hg).	Numeric	69.11
SkinThickness	Triceps skinfold thickness (mm).	Numeric	20.54
Insulin	2-hour serum insulin (µlU/mL).	Numeric	79.80
BMI	Body mass index (kg/m^2).	Numeric	32
DPF	Diabetes pedigree function.	Numeric	0.47
Age	Age (years).	Numeric	33
Outcome	Diabetes diagnose results (tested_positive: 1, tested_negative: 0)	Nominal	–

Dataset Size: 768 rows x 9 columns

Steps:

1. Load the data:

- Read the “diabetes.csv” file from the folder into the program.
- Print first few rows of this data.

2. Perform Exploratory Data Analysis

- Perform different EDA techniques such as
    - Statistical analysis
    - Histograms
    - Joint Plot
    - Pair Plot
    - Correlation Plot
    - Regression Plot
- Extract input (X) and output (y) data from the dataset.

3. Encode categorical data:

- Convert categorical column in the dataset to numerical data.

4. Handle missing values:

- Fill the missing values with the mean of the respective column.

5. Split the dataset:

- Split the data into 80% training dataset and 20% test dataset.

6. Standardize data:

- Standardize training and test datasets.

7. Perform Classification using Logistic Regression:

- Perform Logistic Regression on training data.
- Predict output for test dataset using the fitted model.
- Find different performance parameters for classification.
- Generate the ROC-AUC graph
- Perform k-fold cross validation

8. Test with other classification methods and compare the results

- Classify using Random Forest

Performance Measures

Confusion Matrix

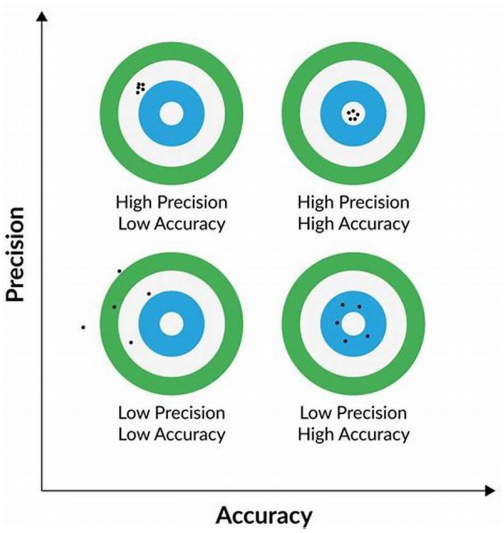
- The confusion matrix is another performance measure used in classification. It is a table that allows visualization of the algorithm’s performance.
- For binary classification, the confusion matrix summarizes 4 results in a 2x2 matrix.

	Actual Positive	Actual Negative
Predicted Positive	True Positive	False Positive
Predicted Negative	False Negative	True Negative

Classification Report

- It finds the parameters such as Accuracy, Precision, Recall, F1 Score.

Parameter	Equation	Remark
Accuracy	$\frac{TN + TP}{TN + FP + TP + FN}$	• represents the number of correctly classified data instances over the total number of data instances. • may not be a good measure if the dataset is not balanced
Precision (Specificity)	$\frac{TP}{TP + FP}$	• Precision is a metric that gives you the proportion of true positives to the amount of total positives that the model predicts.
Recall (Sensitivity)	$\frac{TP}{TP + FN}$	• Also known as sensitivity or true positive rate • Recall focuses on how good the model is at finding all the positives.
F1-Score	$2 * \frac{Precision * Recall}{Precision + Recall}$	• Tells us how precise (correctly classifies how many instances) and robust (does not miss any significant number of instances) our classifier is. • Useful in imbalanced datasets
False Positive Rate	$\frac{FP}{FP + TN}$	• Corresponds to the proportion of negative data points that are mistakenly considered as positive, wrt all negatives • The higher FPR, the more negative data points will be misclassified.

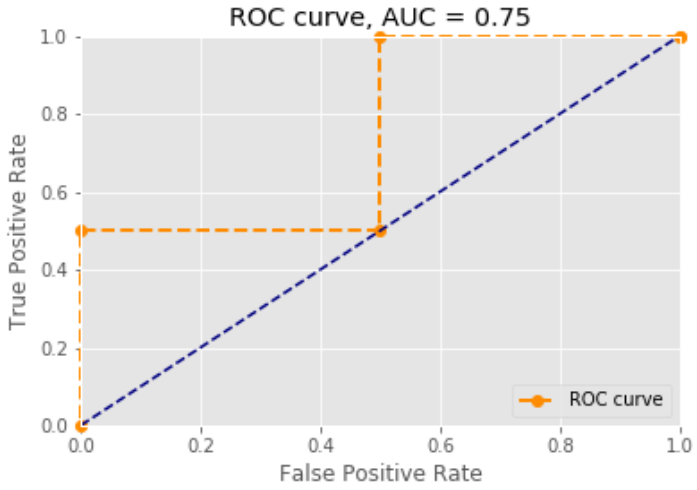


ROC - AUC Curve

- Most imbalanced classification problems involve two classes:
  - a negative case with the majority of examples
  - a positive case with a minority of examples.
- Two diagnostic tools that help in the interpretation of binary (two-class) classification predictive models are ROC Curves and Precision-Recall curves.
- Plots from the curves can be created and used to understand the trade-off in performance for different threshold values when interpreting probabilistic predictions.
- Each plot can also be summarized with an area under the curve score that can be used to directly compare classification models.
- The **ROC AUC score** is a crucial metric in machine learning, particularly for evaluating the performance of binary classification models. It stands for **Receiver Operating Characteristic - Area Under the Curve** and provides a graphical representation of a model's ability to distinguish between positive and negative classes.
- **ROC Curve**
  - The **ROC curve** is a plot that illustrates the performance of a binary classifier system as its discrimination threshold is varied. It is created by plotting the **True Positive Rate (TPR)** against the **False Positive Rate (FPR)** at various threshold settings.

		Threshold					
Actual Class (y)	**Predicted Probabilities ($\hat{y}$)**	($\hat{y}_0$)	($\hat{y}_{0.2}$)	($\hat{y}_{0.4}$)	($\hat{y}_{0.6}$)	($\hat{y}_{0.8}$)	($\hat{y}_1$)
1	*0.8*	1	1	1	1	1	0
0	*0.6*	1	1	1	1	0	0
1	*0.4*	1	1	1	0	0	0
0	*0.2*	1	1	0	0	0	0

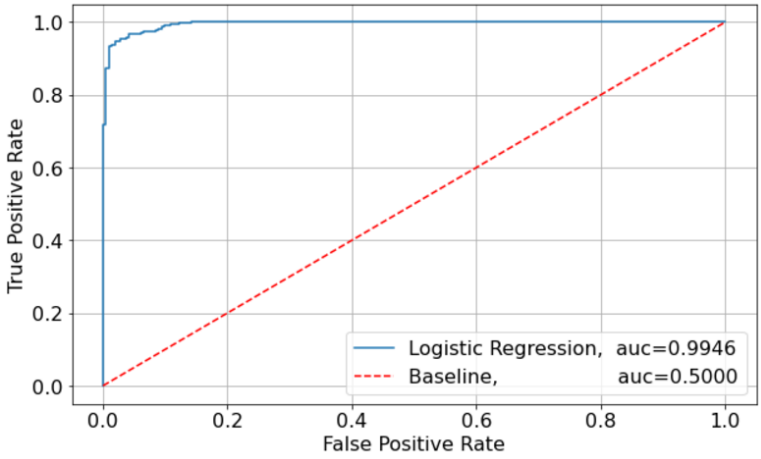
TPR	1	1	1	0.5	0.5	0
FPR	1	1	0.5	0.5	0	0



- **AUC (Area Under the Curve)**
  - The **AUC** represents the area under the ROC curve and provides a single scalar value to summarize the performance of the classifier. An AUC of 1.0 indicates a perfect model, while an AUC of 0.5 suggests a model with no discriminative power, equivalent to random guessing.
  - For example, let's have a binary classification problem with 4 observations. We know true class and predicted probabilities obtained by the algorithm. All we need to do, based on different threshold values, is to compute True Positive Rate (TPR) and False Positive Rate (FPR) values for each of the thresholds and then plot TPR against FPR.

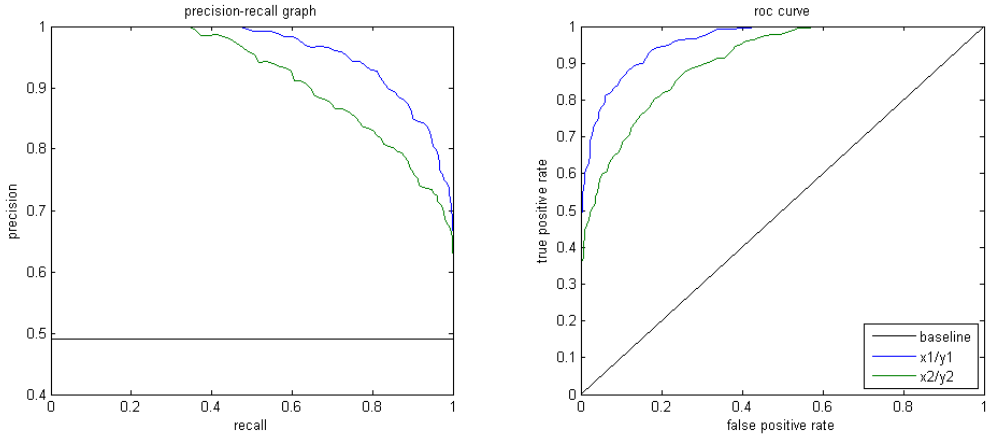
  - **ROC-AUC for Binary Classification**

```
from sklearn.datasets import load_breast_cancer
from sklearn.linear_model import LogisticRegression
from sklearn.metrics import roc_auc_score, roc_curve
import matplotlib.pyplot as plt

# Load data
X, y = load_breast_cancer(return_X_y=True)

# Train model
clf = LogisticRegression(solver="liblinear", random_state=0).fit(X, y)

# Compute ROC AUC score
roc_auc = roc_auc_score(y, clf.predict_proba(X)[:, 1])

y_pred_proba = clf.predict_proba(X)[::,1]
fpr, tpr, _ =roc_curve(y,  y_pred_proba)
auc =roc_auc_score(y, y_pred_proba).round(4)
plt.plot(fpr,tpr,label="Logistic Regression,  auc="+str(auc))
plt.plot([0, 1], [0, 1], 'r--', label='Baseline,
auc=0.5000')
plt.xlabel('False Positive Rate')
plt.ylabel('True Positive Rate')
plt.grid()
plt.legend(loc=4)
plt.show()
```



Precision Recall Curve

- **Precision** is the proportion of *correct* positive classifications (true positive) divided by the total number of *predicted* positive classifications that were made (true positive + false positive).
- **Recall** is the proportion of *correct* positive classifications (true positive) divided by the total number of the *truly* positive classifications (true positive + false negative).
- It is important to note that Precision is also called the Positive Predictive Value (PPV).
- The recall is also called Sensitivity, Hit Rate, or True Positive Rate (TPR).
- A PR curve is simply a graph with Precision values on the y-axis and Recall values on the x-axis.



- **Interpreting PR Curve**
  - It is desired that the algorithm should have both high precision and high recall.
  - However, most machine learning algorithms often involve a trade-off between the two. A good PR curve has greater AUC (area under the curve).
  - In the figure above, the classifier corresponding to the blue line has better performance than the classifier corresponding to the green line.
  - It is important to note that the classifier that has a higher AUC on the ROC curve will always have a higher AUC on the PR curve as well.
  - Precision-Recall curves are preferable when dealing with imbalanced datasets, focusing on positive class prediction performance.
  - Precision-Recall provides insights into the model's ability to correctly classify positive instances.

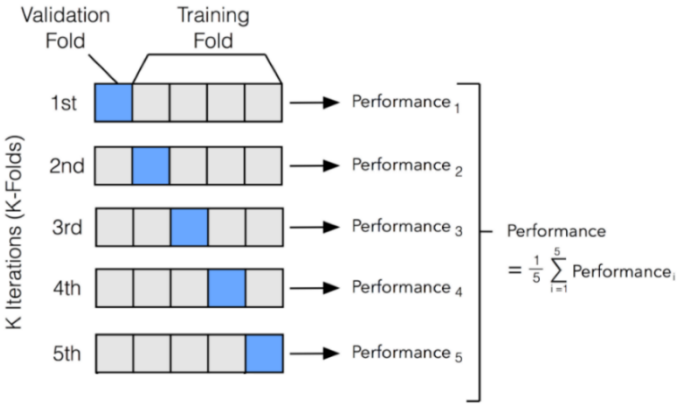
```
from sklearn.datasets import load_breast_cancer
from sklearn.linear_model import LogisticRegression
from sklearn.metrics import roc_auc_score
from sklearn.metrics import precision_recall_curve, auc

# Load data
X, y = load_breast_cancer(return_X_y=True)

# Train – Test Split
X_train, X_test, y_train, y_test = train_test_split(
    X, y, test_size=0.2, random_state=42)

# Train a logistic regression model (you can replace this with your own
classifier)
model = LogisticRegression()
model.fit(X_train, y_train)

# Predict probabilities for positive class
y_scores = model.predict_proba(X_test)[:, 1]

# Calculate precision and recall
precision, recall, thresholds = precision_recall_curve(y_test, y_scores)

# Calculate Area Under the Curve (AUC) for precision-recall curve
auc_score = auc(recall, precision)
no_skill = len(y[y==1]) / len(y)

# Plot precision-recall curve
plt.figure(figsize=(10, 6))
plt.plot(recall, precision, label=f'Precision-Recall Curve (AUC =
{auc_score:.4f})')
plt.plot([0, 1], [no_skill, no_skill], linestyle='--', label='No
Skill(%ge of positive samples)')
plt.xlabel('Recall')
plt.ylabel('Precision')
plt.title('Precision-Recall Curve')
plt.legend()
plt.grid()
plt.show()
```

K-Fold Cross-Validation

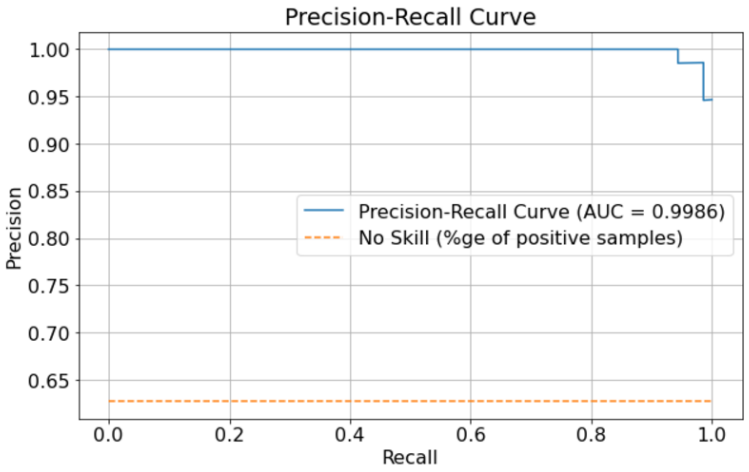
- K-fold cross-validation approach divides the input dataset into K groups of samples of equal sizes. These samples are called folds.
- For each learning set, the prediction function uses k-1 folds, and the rest of the folds are used for the test set.
- The brilliance of K-Fold Cross-Validation lies in its ability to mitigate the bias associated with the random shuffling of data into training and test sets, ensuring that every observation from the original dataset has the chance of appearing in the training

and test set. This is crucial for models that are sensitive to the data on which they are trained.

- **Steps to Perform K-Fold Cross-Validation**
    i. **Split the Dataset**: The dataset is divided into 'K' number of folds. Typically, K is set to 5 or 10, but the choice depends on the dataset size and the computational cost you're willing to incur.
    ii. **Iterate Through Folds**: For each iteration, select one fold as the test set and the remaining K-1 folds as the training set.
    iii. **Train and Evaluate**: Train the model on the training set and evaluate it on the test set. Record the performance score determined by your evaluation metric.
    iv. **Repeat**: Repeat this process K times, with each of the folds serving as the test set exactly once.
    v. **Aggregate Results**: Calculate the average of the performance scores. This average is your model's performance metric.

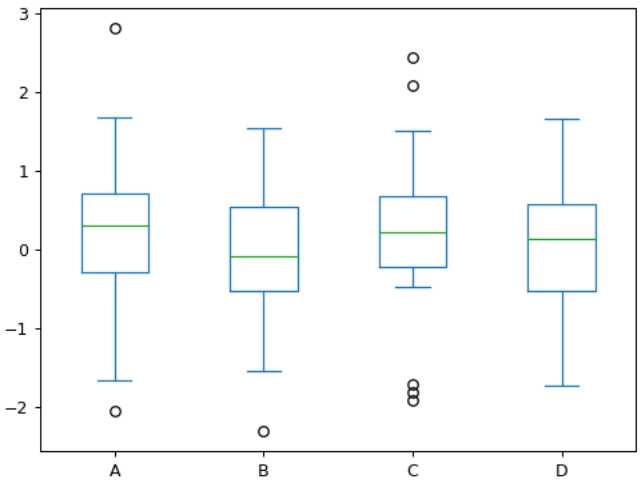



```
from sklearn.datasets import load_breast_cancer
from sklearn.model_selection import KFold, cross_val_score
from sklearn.linear_model import LogisticRegression
import numpy as np

# Load data
X, y = load_breast_cancer(return_X_y=True)

# Train model
model = LogisticRegression(solver="liblinear").fit(X, y)

# Define cross-validation method to use
cv = KFold(n_splits=5, random_state=1, shuffle=True)

# Use k-fold CV to evaluate model
scores = cross_val_score(model, X, y, cv=cv, n_jobs=-1)

# View mean performance
mean_score = np.mean(np.absolute(scores))

print('Foldwise Score:',scores.round(4))
print('Average  Score: ',mean_score.round(4))
```



Outlier handling

- A data point that varies greatly from other results is referred to as an outlier.
- An outlier may also be described as an observation in our data that is incorrect or abnormal as compared to other observations.
- **Causes and Consequences**
  - **Measurement errors:** Errors in data collection or measurement processes can lead to outliers.
  - **Sampling errors:** In some cases, outliers can arise due to issues with the sampling process.
  - **Natural variability:** Inherent variability in certain phenomena can also lead to outliers. Some systems may exhibit extreme values due to the nature of the process being studied.
  - **Data entry errors:** Human errors during data entry can introduce outliers.
  - **Experimental errors:** In experimental settings, anomalies may occur due to uncontrolled factors, equipment malfunctions, or unexpected events.
  - **Sampling from multiple populations:** Data is inadvertently combined from multiple populations with different characteristics.
  - **Intentional outliers:** Outliers are introduced intentionally to test the robustness of statistical methods.
- To find outliers, we can simply plot the box plot. Outliers are points that are outside of the minimum and maximum values, as seen in the image below.



Visualizing and Removing Outliers Using Box Plot

- Boxplot summarizes sample data using 25th, 50th, and 75th percentiles.
- One can just get insights (quartiles, median, and outliers) into the dataset by just looking at its boxplot.

```
# Importing
import sklearn
from sklearn.datasets import load_diabetes
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns


# Load the dataset
diabetics = load_diabetes()

# Create the dataframe
column_name = diabetics.feature_names
df = pd.DataFrame(diabetics.data)
df.columns = column_name
print(df.shape)
df.head()

# Create the Box Plot
sns.boxplot(df_diabetics['bmi'])

# Choose a threshold from Boxplot and remove the outliers
threshold = 0.12
df_no_outliers1 = df[df['bmi'] <= threshold]

df_no_outliers1.shape
```

Removal of Outliers with Z-Score

- Z- Score is also called a standard score.

$$Zscore = \frac{(data_{point} - mean)}{std.deviation}$$

- This value/score helps to understand that how far is the data point from the mean. And after setting up a threshold value one can utilize z score values of data points to define the outliers.

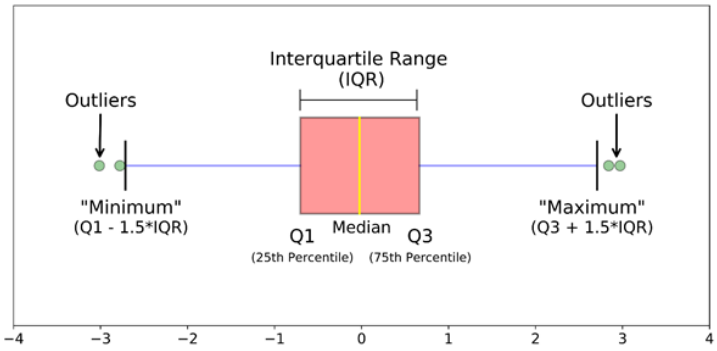
```
from scipy import stats
import numpy as np

z = np.abs(stats.zscore(df['bmi']))
sns.boxplot(z)
print(z)

threshold_z = 2.3

outlier_indices = np.where(z > threshold_z)[0]
df_no_outliers2 = df.drop(outlier_indices)
```

```
print("Original DataFrame Shape:", df.shape)
print("DataFrame Shape after Removing Outliers:", df_no_outliers2.shape)
```

Handling Outliers using IQR (Inter Quartile Range)

- IQR (Inter Quartile Range) Inter Quartile Range approach to finding the outliers is the most commonly used and most trusted approach used in the research field.

$$IQR = Quartile_3 - Quartile_1$$




```
# IQR
Q1 = df['bmi'].quantile(0.25)
Q3 = df['bmi'].quantile(0.75)
IQR = Q3 - Q1
print('IQR = ',IQR.round(4))

upper = Q3+1.5*IQR
lower = Q1-1.5*IQR

# Create arrays of Boolean values indicating the outlier rows
upper_index = np.where(df['bmi'] >= upper)[0]
lower_index = np.where(df['bmi'] <= lower)[0]

# Removing the outliers
df.drop(index=upper_index, inplace=True)
df.drop(index=lower_index, inplace=True)

# Print the new shape of the DataFrame
print("New Shape: ", df.shape)
```