Lecture1a : Machine Learning

⚠️ **There might be errors, so please read with caution.**

Slide Link

What is Machine Learning?

Machine Learning (ML) is a subfield of Artificial Intelligence (AI) that allows machines to learn from data and improve their performance over time without needing explicit programming. It differs from traditional expert systems, where humans would write rule-based systems after consulting experts. In contrast, ML can make decisions and predictions by finding patterns in data.

Example:

Before ML, a medical diagnostic system might require a collection of rules written by medical experts, but with ML, the system can learn from patient data and improve its diagnosis ability over time.

Why is ML Important?

Some tasks that are simple for humans are difficult for computers, and vice versa.

- **Example 1 (easy for computers, hard for humans):** Sorting a million numbers is quick and easy for computers, but humans would struggle to do it manually.
- **Example 2 (easy for humans, hard for computers):** Recognizing an animal in a picture is easy for humans, but very challenging for a computer. With ML, computers can now do this at human-like accuracy.

Applications of ML

Machine Learning has applications in a variety of fields:

- **Disease Diagnosis:** ML can help doctors identify diseases by learning from medical data like images, lab results, and patient history.

- **Fraud Detection:** Banks use ML to detect fraudulent activity by analyzing transaction patterns.
- **Email Filtering:** ML helps in filtering spam by analyzing the characteristics of unwanted emails.
- **Computer Vision:** ML can recognize objects in images, like detecting faces or identifying animals.
- **Drug Design & Bioinformatics:** ML is used to find patterns in biological data that can aid in drug discovery or understanding genetic data.
- **Autonomous Vehicles:** Self-driving cars use ML to make decisions like when to change lanes or adjust speed.

Small Examples of ML Models

Here's a simplified example using two variables (X1, X2) to predict an outcome (Y):

- **Equation:** If `X1 * 0.5 + X2 * 0.5 - 0.25 >= 0`, then `Y = 1`; otherwise `Y = 0`.

X1	X2	Y
0	0	0
0	1	1
1	0	1
1	1	1

- This is an example of how a simple rule can be used to predict an outcome based on the input values.

▼ Types of Machine Learning

1. **Supervised Learning:**
    - **Classification:** Predicting a category label (e.g., spam or not spam).
    - **Regression:** Predicting a continuous value (e.g., house price based on features like area, number of rooms, etc.).
2. **Unsupervised Learning:**
    - **Clustering:** Grouping data into clusters based on similarity (e.g., customer segmentation).

- **Density Estimation:** Estimating the probability distribution of data points.

3. **Semi-Supervised Learning:**
    - A mix of both supervised and unsupervised learning where the model is trained using a small amount of labeled data and a large amount of unlabeled data.
4. **Reinforcement Learning (RL):**
    - In RL, an agent learns by interacting with an environment and receiving feedback in the form of rewards or penalties. The goal is to maximize the cumulative reward.

▼ Supervised Learning

In **Supervised Learning**, the model is trained on a labeled dataset. This means that each training example is paired with an output label. The goal is to learn a mapping from inputs (features) to outputs (labels).

- **Example:** In spam detection, the model is trained with emails labeled as either "spam" or "not spam."

Pros of Supervised Learning:

1. **Accurate Predictions:**

    Since the model is trained on known outputs, it can make highly accurate predictions on similar data.

2. **Easy to Evaluate:**

    It is easy to evaluate the performance of a model because you have ground-truth labels to compare with.

3. **Clear Objective:**

    The objective (classification or regression) is very clear, and you can use various algorithms like linear regression, decision trees, and neural networks.

4. **Wide Range of Applications:**

Supervised learning can be applied to a variety of real-world problems like email filtering, stock market prediction, medical diagnosis, etc.

Cons of Supervised Learning:

1. **Requires Labeled Data:**

   A major drawback is the need for labeled data, which can be time-consuming and expensive to obtain. In many cases, labeling data requires human effort and expertise.

2. **Overfitting Risk:**

   If the model is too complex, it may overfit to the training data, meaning it performs well on training data but poorly on unseen data (test data).

3. **Limited to the Training Data:**

   Supervised learning models can only learn patterns from the labeled examples provided. If the training data is unrepresentative of real-world conditions, the model's performance will suffer.

▼ Unsupervised Learning

In **Unsupervised Learning**, the model is trained on data without any labeled outputs. The goal is to identify underlying patterns, structures, or relationships in the data.

- **Example:** In customer segmentation, the model groups customers based on purchasing behavior, without knowing the predefined categories (e.g., high spender, low spender).

Pros of Unsupervised Learning:

1. **No Labeled Data Required:**

   Unsupervised learning can work with raw, unlabeled data, making it easier to apply in situations where labeling data is difficult or expensive.

2. **Discover Hidden Patterns:**

   Unsupervised learning is excellent for discovering hidden structures or patterns in data, such as finding groups (clusters) or reducing dimensions in data (e.g., Principal Component Analysis).

3. **Exploratory Analysis:**

   It's a good method for exploring large datasets and finding potential insights that may not be immediately obvious, such as identifying trends or anomalies.

4. **Data Reduction:**

   Techniques like clustering or dimensionality reduction (e.g., PCA) can reduce the complexity of the data, making it easier to visualize and analyze.

Cons of Unsupervised Learning:

1. **Harder to Evaluate:**

   Since there are no ground-truth labels, it's difficult to evaluate the performance of the model. There's no "right" answer to compare predictions with.

2. **Complex Interpretation:**

   The results can be harder to interpret. For instance, in clustering, the algorithm might produce groups, but understanding what those groups represent could require more in-depth analysis.

3. **Limited Use Cases for Specific Problems:**

   It might not work well for tasks that need specific outputs, such as classification or regression. In such cases, supervised learning is typically more appropriate.

4. **Sensitive to Initial Conditions:**

   Some unsupervised algorithms, like k-means clustering, are sensitive to initial conditions, such as the starting points of the clusters. This could lead to different outcomes depending on how the algorithm starts.

Summary:

Aspect	Supervised Learning	Unsupervised Learning
Training Data	Requires labeled data	No labeled data required

Aspect	Supervised Learning	Unsupervised Learning
Goal	Learn to map input to known output	Discover hidden patterns or structure
Evaluation	Easy to evaluate (comparing predictions with true labels)	Harder to evaluate (no labels)
Applications	Classification, regression (e.g., spam detection, price prediction)	Clustering, anomaly detection (e.g., customer segmentation, anomaly detection)
Data Requirement	High-quality labeled data is required	Can work with unlabeled data
Risk	Risk of overfitting	Difficult to interpret results

When to Use Each:

- **Supervised Learning** is ideal when you have labeled data and need to predict specific outcomes, like predicting disease or classifying emails.
- **Unsupervised Learning** is ideal when you have large amounts of unlabeled data and want to explore or identify patterns without predefined categories, like clustering customers or finding hidden structures in data.

▼ Reinforcement Learning

Reinforcement Learning is about teaching an agent how to make decisions through trial and error. The agent receives rewards or penalties based on its actions and learns to adjust its behavior over time.

Examples of RL:

1. **Game Playing (e.g., Chess or Go):** In these games, the RL agent learns which strategies lead to winning more games.
2. **Robotics:** A robot can learn tasks like walking or picking up objects by performing actions and receiving feedback. It refines its actions through repeated attempts.
3. **Self-driving Cars:** RL helps autonomous vehicles make decisions (e.g., when to change lanes or stop) by learning from real-time feedback about the environment and adjusting its actions for safety.