Machine Learning

(Course Code: 18B1WCI634 / 18B11BI611)

Introduction to Machine Learning

Mr. Sandeep Kumar Patel

Assistant Professor

Jaypee University of Information Technology

Waknaghat, Solan, HP-173234

Machine Learning

Arthur Samuel coined the term *Machine Learning* as:

> *"Field of study that gives computers the ability to learn without being explicitly programmed."*

Definition: A program learns from **experience (E)** with respect to a class of **tasks (T)** and a **performance measure (P)**, if its performance at tasks in T, measured by P, improves with experience E. — Tom Mitchell, 1997,

Well-Defined Learning System

A **well-defined learning system** can be represented as:

$$\langle P, T, E\rangle$$

Example: Handwriting Recognition

- **Task (T):** Recognizing and classifying handwritten words in images.
- **Performance (P):** Percentage of correctly classified words.
- **Experience (E):** A database of handwritten words with correct labels.

Key Components of a Machine Learning Problem

- **Task (T):** What the system needs to do (e.g., classify emails, predict house prices).
- **Performance Measure (P):** How success is evaluated (e.g., accuracy, precision, recall).
- **Experience (E):** What data or interactions the system uses to improve (e.g., training datasets, user interactions, simulations).

Goals of Machine Learning

The main goals of Machine Learning (ML) are:

- **Automation:** Enable computers to perform tasks without explicit programming.
- **Prediction:** Accurately predict outcomes from data.
- **Recognition:** Identify patterns, objects, or events in data.
- **Adaptation:** Improve performance over time with experience.
- **Decision Making:** Support or automate decision-making processes.
- **Efficiency:** Reduce human effort in analyzing large and complex datasets.

Example: A recommendation system that improves suggestions based on user interactions.

Applications of Machine Learning

- **Healthcare:** Disease diagnosis, medical imaging analysis, drug discovery.
- **Finance:** Credit scoring, fraud detection, algorithmic trading.
- **Retail & E-commerce:** Recommendation systems, customer behavior analysis.
- **Transportation:** Self-driving cars, traffic prediction, route optimization.
- **Natural Language Processing:** Chatbots, language translation, sentiment analysis.
- **Computer Vision:** Face recognition, object detection, video surveillance.
- **Robotics:** Adaptive robots, industrial automation, intelligent agents.
- **Entertainment:** Personalized content recommendations (movies, music, games).

Example: Netflix recommends movies based on your past watching patterns.

Aspects of Developing a Learning System

When designing a Machine Learning system, several key aspects must be considered:

1. **Training Experience / Data:** Data provides experience.
2. **Choosing the Target Function:** Target function defines what to learn.
3. **Choosing a Representation for the Target Function:** Representation decides how it can be modeled.
4. **Choosing a Function Approximation Algorithm:**Algorithm teaches the model to approximate it.
5. **The final design:** constitutes the fully specified learning system

1. Training Experience / Data

- Dataset:instances of data used for learning or evaluation.

$$D = \{(x_i, y_i)\}_{i=1}^{N}$$

  - x_i : input feature vector
  - y_i : corresponding output label
  - N : total number of training samples
- (x_i, y_i) is assumed to be independently and identically distributed **(i.i.d.).** Formally,

$$(x_i, y_i) \sim P(X, Y)$$

- $P(X, Y)$: Probability that input X and label Y occur together

Feature Vectors and Labels (Example: Spam Detection)

Email ID	**Contains "Free"?**	**Length $>$ 100?**	**Contains Link?**	**Label**
1	Yes	No	Yes	Spam
2	No	Yes	No	Not Spam
3	Yes	Yes	Yes	Spam
4	No	No	No	Not Spam
5	Yes	No	No	Spam

2. Choosing the Target Function

- Target function f is the **true but unknown underlying rule** that maps inputs X to outputs Y.

$$f : X \to Y$$

- **Examples:**
  - Regression: $Y \in \mathbb{R}$ (continuous output)
  - Classification: $Y \in \{1, \ldots, K\}$ (discrete output)

3. Choosing a Representation for the Target Function

- **Representation learning** is an ML approach in which the system automatically learns the best way to represent data so that the target task (classification, prediction) becomes easier. Representation defines how the hypothesis h can be modeled.

- **Examples:**

$$h(x) = w^T x + b \quad \text{(linear model)}$$

$$h(x) = \mathrm{NN}(x; \theta) \quad \text{(neural network)}$$

- Representation limits the hypothesis space $\mathcal{H}$:

$$h \in \mathcal{H}$$

Your choice of representation decides what type of functions your model can learn.

Hypothesis Space

- The **hypothesis space** is the set of all models that a learning algorithm can represent, from which it selects the best-fit hypothesis to map inputs to outputs.

  Example: For a **linear regression** problem, the hypothesis space includes all possible lines:

  $$y = mx + b$$

  where:

  - m = slope of the line
  - b = y-intercept
- Different combinations of (m, b) represent different hypotheses in the space.
- **Goal:** The learning algorithm searches through the hypothesis space to find the **single best hypothesis** $h \in H$ that minimizes error on the training data.

Hypothesis

A **hypothesis** is a candidate function or model chosen by the learning algorithm to approximate the unknown target function:

$$h : X \to Y$$

- X = input features
- Y = output labels
- $h(x)$ = predicted label for input x

Goal:

$$h \approx f \quad \text{(target function)}$$

4. Choosing a Function Approximation Algorithm

Algorithm A searches $\mathcal{H}$ to find h minimizing empirical risk:

$$\hat{h} = \arg\min_{h \in \mathcal{H}} \frac{1}{N} \sum_{i=1}^{N} L(h(x_i), y_i)$$

where:

- $\hat{h}$ = the hypothesis (model) that minimizes the average loss over all training data.
- $h \in \mathcal{H}$ = the hypothesis space (all possible functions defined by the representation, e.g., linear functions)
- $L = L(h(x_i), y_i)$ measures prediction error

5. Final Design

- The final design constitutes the fully specified learning system, integrating:
  - Training dataset $D = \{(x_i, y_i)\}_{i=1}^{N}$
  - Target function $f : X \to Y$
  - Choose a hypothesis $h \in \mathcal{H}$ such that $h \approx f$
  - Choose Function approximation algorithm A

Issues in Machine Learning

- **Learning Algorithms**
  - Identify algorithms that learn target functions from examples.
  - Performance depends on problem type and representation.
- **Training Data and Generalization**
  - How much data is sufficient?
  - Larger hypothesis spaces require more data.
- **Role of Prior Knowledge**
  - Guides learning by restricting hypothesis. space
  - Improves efficiency and generalization.
- **Function Approximation**
  - Decide which functions should be learned
  - Can this decomposition be automated?

Performance Metrics

A bank develops a model to detect fraudulent transactions. The model was tested on 200 transactions with the following results:

$$\textbf{TP} = \textbf{50}, \quad \textbf{TN} = \textbf{120}, \quad \textbf{FP} = \textbf{20}, \quad \textbf{FN} = \textbf{10}$$

Tasks:

- Calculate the **Accuracy**, **Precision**, **Recall**

Formulas:

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

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

Solution

Given:

$$\mathrm{TP} = 50, \quad \mathrm{TN} = 120, \quad \mathrm{FP} = 20, \quad \mathrm{FN} = 10$$

Formulas:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}, \quad \text{Precision} = \frac{TP}{TP + FP}, \quad \text{Recall} = \frac{TP}{TP + FN}$$

Calculations:

$$\text{Accuracy} = \frac{50 + 120}{50 + 120 + 20 + 10} = \frac{170}{200} = 0.85 = 85\%$$

$$\text{Precision} = \frac{50}{50 + 20} = \frac{50}{70} \approx 0.714 = 71.4\%$$

$$\text{Recall} = \frac{50}{50 + 10} = \frac{50}{60} \approx 0.833 = 83.3\%$$

Q2.

A model is used to predict whether a student will **pass or fail an exam**.

- Total students: 50
- Actual failed: 20
- Actual passed: 30
- Model predicted 15 students will fail
- Out of these 15, 10 students actually failed

Tasks:

1. Fill in the confusion matrix
2. Identify TP, FP, TN, FN
3. Calculate Accuracy, Precision, Recall, F1-score

Step 1: Confusion Matrix

Step 1: Identify values

- True Positive (TP) $= 10$
- False Positive (FP) $= 5$
- False Negative (FN) $= 10$
- True Negative (TN) $= 25$

Confusion Matrix:

	Predicted Fail	Predicted Pass	Total
Actual Fail	10	10	20
Actual Pass	5	25	30
Total	15	35	50

Step 2: Metrics Calculation

Accuracy:

$$\text{Accuracy} = \frac{TP + TN}{Total} = \frac{10 + 25}{50} = 0.7 = 70\%$$

Precision:

$$\text{Precision} = \frac{TP}{TP + FP} = \frac{10}{10 + 5} \approx 66.7\%$$

Recall:

$$\text{Recall} = \frac{TP}{TP + FN} = \frac{10}{10 + 10} = 50\%$$

F1-Score:

$$\text{F1} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} = 2 \cdot \frac{0.667 \cdot 0.5}{0.667 + 0.5} \approx 57.1\%$$