Date
Page

Assignment - 1

Name: Kaushal kumar Rai
Branch: B.Tech CSE with AI & ML
PRN: 240205241029
Semester: III

Short questions:

① What do we mean by machine learning in the field of artificial intelligence?

→ Machine Learning (ML) is a subfield of artificial intelligence (AI) where algorithms are designed to learn patterns and make predictions or decisions from data, rather than being explicitly programmed for a specific task.
Furthermore it is about creating systems that can improve their performance automatically through experiences (i.e by being exposed to more data).

② How can learning be defined from a machine's perspective?

→ From a machine's perspective learning is defined by improving its performance on a specific task through experience. This is often formalized by computer scientist Tom mitchell's definition:

A computer Program is said to learn from experience (E) with respect to some class of tasks (T) and a performance measure (P). if its performance at tasks in T, as measured by P, improves with experience E.

- Task (T): The problem the machine needs to solve. (e.g classifying emails as spam or not spam).
- Experience (E): The data used to train the model. (e.g a dataset of labeled emails).
- Performance Measure (P): The metric used to evaluate how well the machine performs the task (e.g the percentage of emails correctly classified).

③ What methods are commonly used to evaluate the performance of machine learning models?

→ The performance of a machine learning model is evaluated using various metrics, which depends on the type of task (e.g classification or regression).

For classification model:

- These model predict a category (spam or not spam)

- Accuracy: The ratio of correct predictions to the total no of predictions

∴ Accuracy = $\frac{\text{Number of correct Predictions}}{\text{Total Number of predictions}}$

- Confusing matrix:
- A table that summarize the performance of a classification model, showing true positives, true negatives, false positive and false negative.

- Precision: Measures the accuracy of positive predictions.

Precission = $\frac{\text{True Positives}}{\text{True positives + False positives}}$

For Regression model:
These models predict a continuous value (e.g house price).

- Mean Absolute Error (MAE): The average of the absolute difference between the predicted and actual values

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

- Mean Square Error (MSE): The average of the squared difference between the predicted and actual values.

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

- Root mean squared Error (RMSE): The squared root of the MSE, which brings the metric back to the original unit of the target variable

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

(4) Why is it important to divide data into training and testing sets during model development?

⇒ Dividing data into training and testing sets is a fundamental practice in ML to prevent overfitting

- Training set
  - This portion of the data (typically 70-80%) is used to train the model. The model learns the underlying patterns and realtionship from this data.

- Testing set:
  - This portion of the data (typically 20-30%) is held back and used to evaluate the model's performance

after it has been trained. Since the model has never seen this data before, the testing set provides an unbiased estimate of how the model will perform on new, real-world data

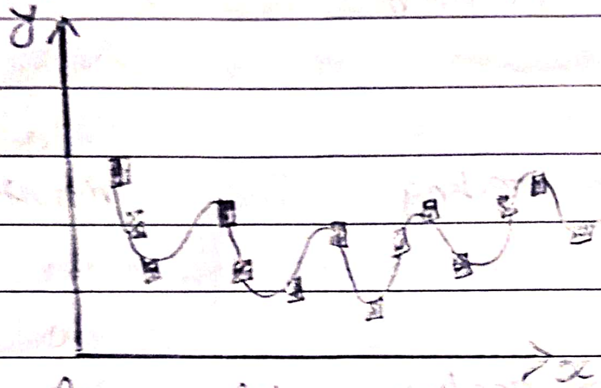


fig: overfitting

(5) What does the process of cross-validation involve in model evaluation?

→ Cross-validation is a robust technique used during model evaluation and tuning, particularly for assessing how well a model generalizes to unseen data and preventing overfitting. Instead of a single train-test split, cross validation involves.

I) Partitioning the data into multiple subsets (folds).

II) Training ~~the~~ and testing the model multiple times, using different folds for training and testing in each iteration.

III) Aggregating the results (e.g averaging performance metrics) to provide a more reliable estimate of the model's performance and to make hyperparameter tuning decisions.

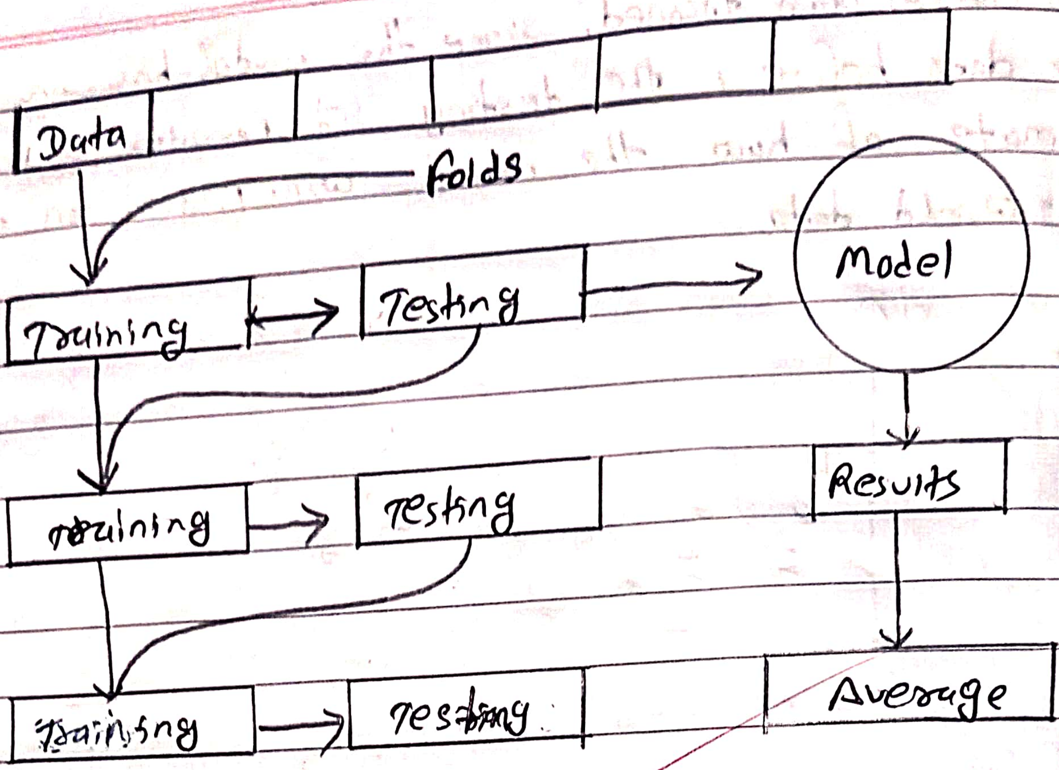


Fig:- Cross-Validation

⑥ What are feature sets, and how do they influence the learning process of a model?

→ A feature set is the collection of measurable input variables (or attributes) used to train a ML model. The selection and quality of these features are critical as they directly influence a model's ability to learn.

Influence: Models learn by identifying patterns between the input features and the output target. If the features are relevant and informative, the model can easily detects these patterns. If the features are noisy (e.g to predic credit score using someone's shoe size), the model will strugel to learn and will perform poorly. In short, better features lead to better models.

Date
Page

(7) Why is a validation set necessary, and how it is different from test and training sets?

→ A validation set is a subset of the data used to tune the model's hyperparameters and make decisions about the model's architecture. It's different from the training and test sets.

- Training set: used for the model to learn its parameters (e.g weights)
- Validation set: used to evaluate the model during training to tune hyperparameters (e.g learning rate, no of layers) and prevent overfitting. It acts as unbaised check during the model development phase.

- Test set: used only once at the very end to provide a final, unbaised assessment of the fully trained and tuned model's performance on unseen data.

Using a validation set prevents 'leaking' information from the test set into model tuning process, which would make the final evaluation overlay optimistic.

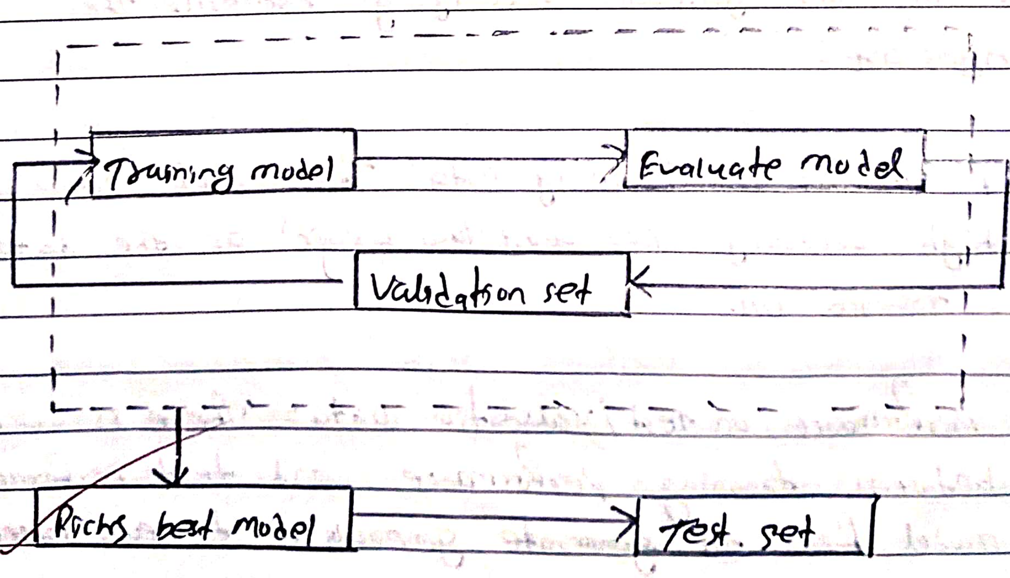


fig: Training data / validation / test

⑧ What is the purpose of splitting a dataset into multiple subsets before training a model.

→ Splitting a dataset into multiple subsets (training, validation and testing) is essential for developing a reliable and generalizable model. The primary purpose is to simulate how the model will perform on new, real-world data and to avoid overfitting. This separation allows you to:

i) train the model on one portion of data.
ii) Tune and select the best model using a separate validation portion.
iii) Evaluate the model its final performance honestly on a completely unseen test portion.

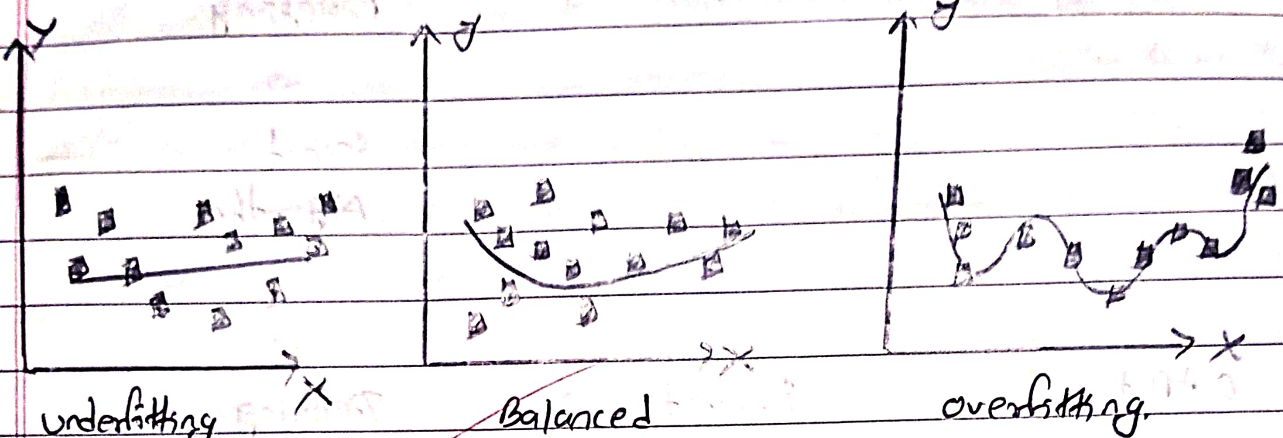
⑨ What are the key signs that a model is overfitting the training data?

→ A model is overfitting when it learns the training data too well. including its noise and random fluctuations, instead of the general underlying pattern. The key signs are:

- High Performance on Training Data:- The model achieves very high accuracy (or very low error) on the data it was trained on.

- Poor Performance on test / validation Data: There is a large gap between training performance and test performance. The model fails to ~~generate~~ generalize to new, unseen data.

- Excessive model complexity: The model might be too complex for the amount of data available (e.g. a deep neural network for a ~~long~~ simple problem).



(10) How does a machine learning model learn from patterns in data?

→ A machine learning model learns by mathematically optimizing its internal parameters to map input data to correct outputs. The process generally involves these steps:-

i) Prediction: The model takes an input from the training data and makes a prediction.

ii) Error calculation: It compares its prediction to the actual known outcome and calculates an error or loss.

iii) Optimization: An optimization algorithm uses this error to slightly adjust the model's internal parameter in a direction that would reduce the error.

iv) Iteration: This process is repeated thousands or millions of times with all the data in the training set. With each iteration, the model's parameters get progressively better at capturing the patterns that connect the features to the correct outcomes.

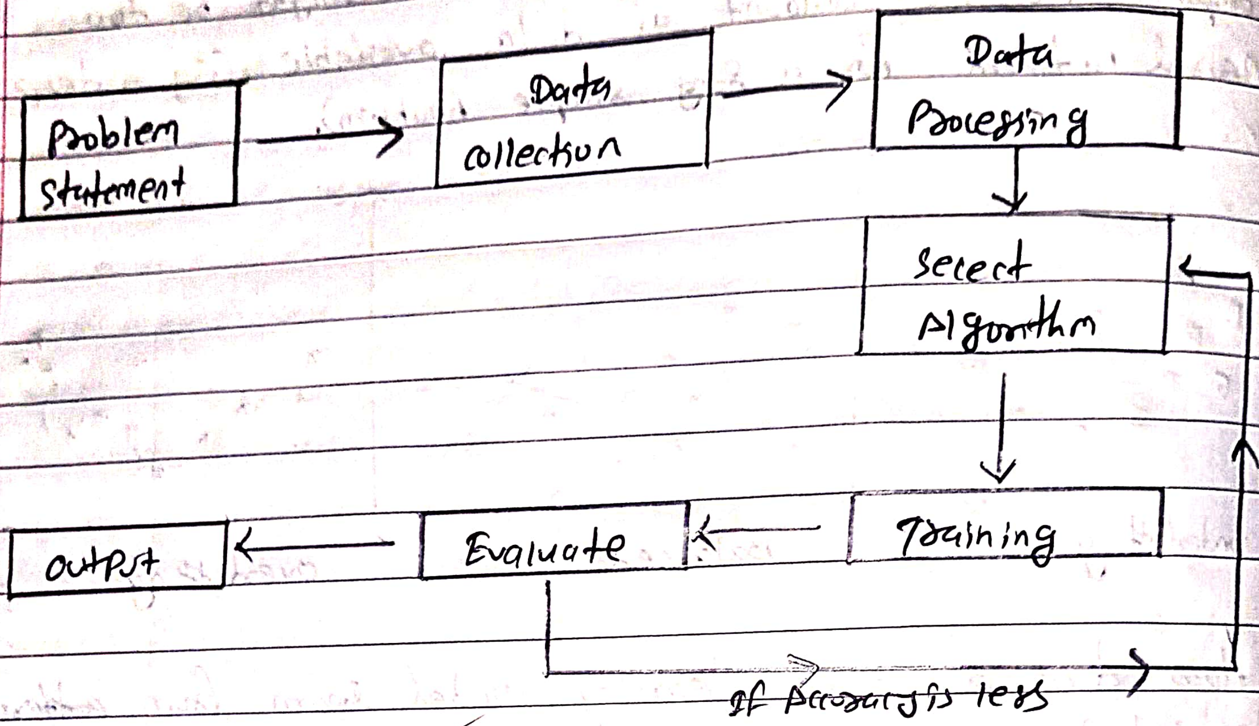


fig: Machine learning model

(11) In Machine learning, what consitutes a dataset and what elements does it typically include?

→ In ML, a dataset is a structured collection of examples, typically organised in a table format.

- Samples (or Instances): The rows of the tables. Each row represents a single observation or data point.
- Features: The columns of the table. Each column represents a characteristic or attribute of the sample.
- Target (or Label): A special column containing the outcome value that the model aims to predict. This is the 'answer' that the model learns from in supervised Learning.

(12) How does cross-validation improve the generalization ability of model?

→ Cross-validation improves a model's development process by providing a more reliable estimate of its generalization ability. By training and testing the model on multiple different subsets of the data, it averages out the performance metrics.

- This gives a more stable and less biased measure of how the model will likely perform on unseen data compared to a single train-test split. This better estimate helps developers select the best-performing model and hyperparameters, which indirectly leads to a final model that generalizes better.

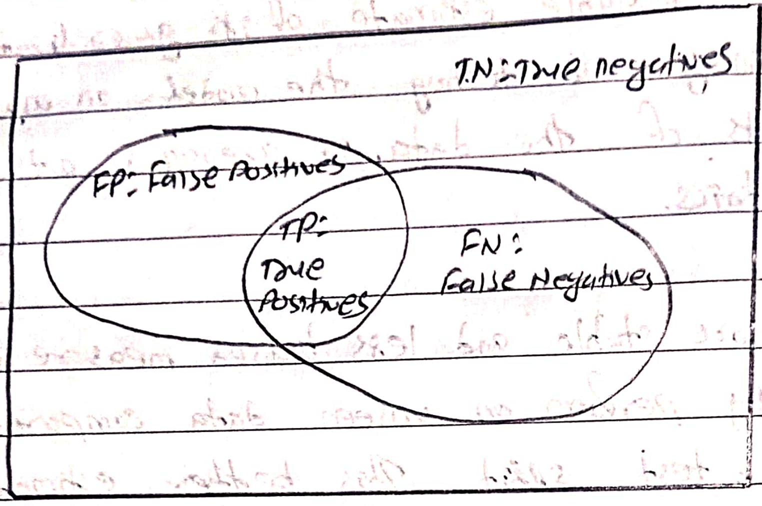
(13) What are the main evaluation metrics used to measure a model's accuracy and reliability?

→ The main metrics to measure a model's accuracy and reliability depends on the task.

1) For classification (Predicting categories).
- Accuracy : overall correctness
- Precision : Accuracy of positive predictions
- Recall : Ability to find all actual positives
- F1-score : A single score that balances precision and recall.

ii) For Regression (Predicting numerical values:)
- mean Absolute Error (MAE): Average absolute prediction error.

- Mean squared error: (MSE): Average squared error (Penalize large errors more)
- Root mean squared error: square root of MSE, expressed in the same units as target.



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

$$\text{Recall}(r) = \frac{TP}{TP+FN}$$

$$\text{F-measure}(F) = \frac{1}{\frac{1}{2}\left(\frac{1}{p}+\frac{1}{r}\right)} = \frac{2pr}{p+r}$$

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

(14) How do training and testing datasets differ in their roles and usage?

→ The roles of training and testing datasets are distinct and crucial for proper model development.

- Training dataset: This is the data used to teach the model. The model iterates over this data to learn the underlying patterns by adjusting its internal parameters. It is the "study material".

- Testing Dataset: This data is kept separate and is used to only at the end to evaluate the final, trained model. It acts as a "final exam" to get an unbaised measure of the model's performance on completely new data.

Date
Page

(15) What Datasets and we can explain it?

→ A classic example of dataset used in ML is the Iris flower dataset.

- A dataset is a collection of organized data - like a table or spreadsheet. Each row is an item, each column is a feature.

Types of Datasets:

- Structured - clean, like Excel files.
- unstructured - messy, like tweets or images
- semi - structured - in - between like JSON.

- Dataset Power AI, machine learning, and analytics. No data = no smart tech.

{Long Questions}

(1) Explain the history and evoluting of Machine Learning with examples.

→ ML journey begins long before computers. Its roots are in statistics and pattern recognition, with foundational ideas like Bayes' Theorem (1700s), and linear regression laying the mathematical groundwork.

The term 'Machine Learning' was coined in 1959 by Arthur Samuel, who created a checkers playing program that learned from its own games to improve its performance.

This field was revitalized in the 1980s with the rediscovery of backpropagation, an algorithm that made it practical to train more complex neural network. The 1990s saw the rise of powerful methods like support vector machine (SVMs). The modern era of deep learning exploded in the 2010s, driven by three key facts.

1) Big data: The availability of massive datasets to train on.
2) Powerful Hardware: The use of GPUs for parallel processing.
3) Algorithmic Advances: Innovations like AlexNet model in 2012, which revolutionized image recognition.

② What is machine learning, how does it differ from traditional rule-based programming, and why is it considered a core part of AI?

→ The core differences lies in the programming paradigm:

- Traditional programming
  - A developer writes explicit, step-by-step rules. The computer takes this program and input data to produce an answer. The logic is handcrafted.

- Machine Learnings
  - A developer provides a model, input data and the corresponding answers. The sys uses this to learn the underlying rules that connect the inputs to the answers. The logic is inferred from data.

ML is considered a core part of AI because learning from experience is a fundamental characteristics of intelligence.

3. How do we define "learning" in the context of ML systems, and what are the key components that enables a model to learn from data?

→ In ML 'learning' is defined as a process of improving performing on a task through experience. A system learns if its ability to perform a task gets better as it's exposed to more data.

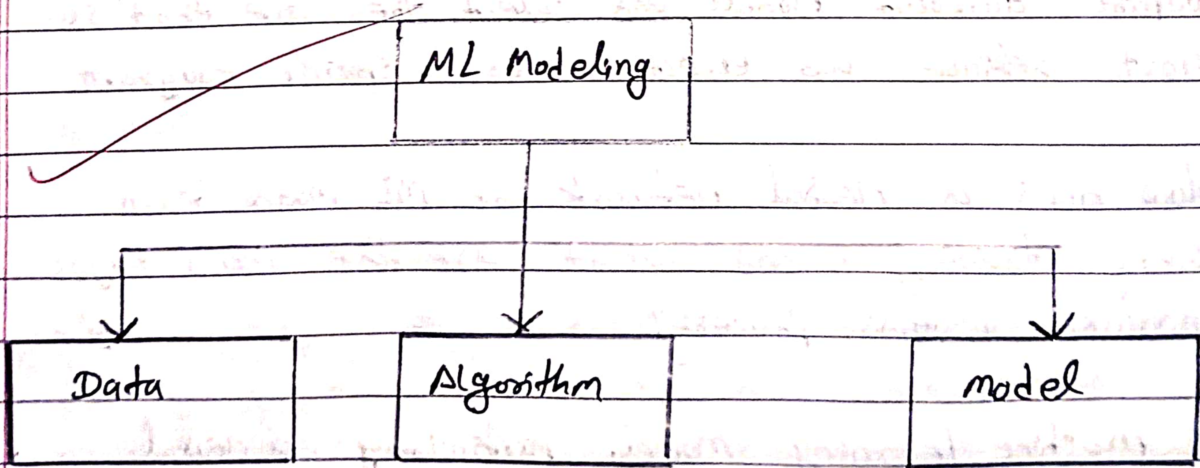
The key components that enables a model to learn are:-

i) Data :- The 'experience' the model uses to find patterns. This includes input features and, in supervised learning the correct output labels.

ii) model :- A mathematical framework with adjustable parameters that tries to represent the relationship between the data's features and its labels.

iii) Loss functions :- A function that measures the model's error by comparing its prediction to the actual label.

4.



(4) What are the different evaluation methods used in machine learning, and how to they help in assessing the quality and performance of a model?

→ Evaluation methods are used to assess a model's quality and performance on unseen data, ensuring it generalizes well and isn't just 'memorizing' the training set. The choice of methods depends on the task.

For classification Task
- Accuracy
- Precision
- Recall
- F1-score

For Regression Tasks
- mean Absolute Error (MAE)
- Root mean Squared Error (RMSE)

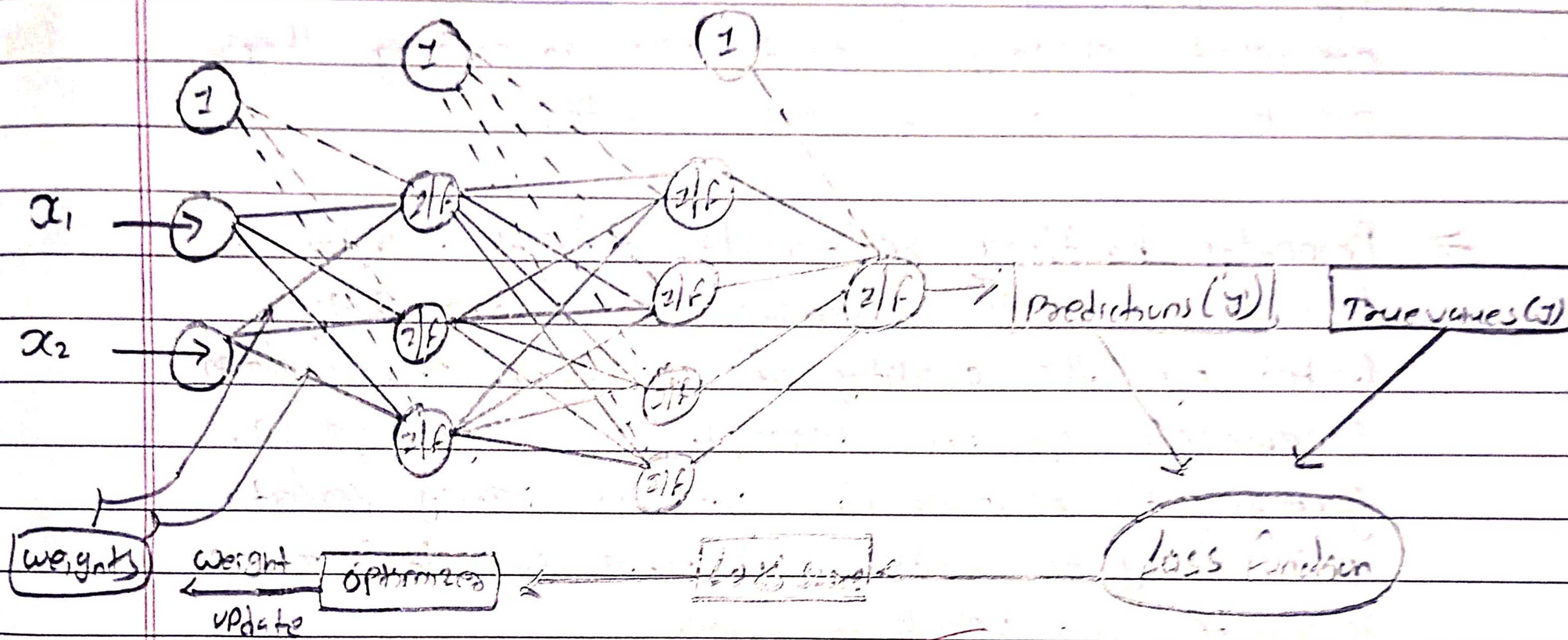
These metrics helps us quantify a model's performance, compare different models and select the one that is most reliable and effective for a specific Program.

(5) How does a neural network or ML model learn during training, and what are the main stages involved in this Process?

- A machine learning model, particularly a neural network, learns during training through an iterative optimization process. This process, often called the training loop, involves several main stages:

- initialization
- Forward Pass
- Loss Calculation
- Backward Pass
- Parameter update.

Forward Propagation



Backward Propagation

⑥ What exactly are datasets in machine learning, and how should they be collected, cleaned, and structured for effective model training?

→ In ML, a dataset is a structured collection of examples used to train and evaluate a model. It's typically organized as a table where rows represent individual samples customer, a house, and columns represent features. often, one column is the target or label.

Preparing a dataset for effective model training involves three key steps:

1) Collection
11) Cleaning
111) Structuring

⑦ Why is proper handling of real-world datasets important, and what challenges might arise in ensuring they are balanced, relevant, and accurate?

→ Properly handling real-world datasets is vital because a model's performance is fundamentally limited by the quality of its data. This is often summarized by the principle of "garbage in, garbage out". Real-world data is rarely perfect, and failing to address its flaws will lead to an inaccurate and unreliable model

Key challenges in ensuring data quality includes.

- Imbalanced data
- Relevance
- Accuracy
- Errors

⑧ What are features sets in machine learning, and how does the selection, transformation or extraction of features impact model performance?

→ A feature set is the group of input variables selected from the dataset to train a model. The process of selecting and modifying these features, known as feature engineering, has a massive impact on a model performance.

- Feature transformation: This means modifying existing features to make them more useful for the model.

- Feature selection: This involves choosing the most relevant features and discarding irrelevant or redundant ones

- Feature extraction: This involves a model's creating entirely new features from raw data

9) How is a dataset typically divided into training, validation, and testing sets and what specific roles does each set play in model development and evaluation?

→ A dataset is typically divided into three distinct subsets to ensure robust model development and evaluation. The split is usually done randomly to maintain a similar data distribution across all sets. A common split ratio 70% for training, 15% for validation, 15% for testing.

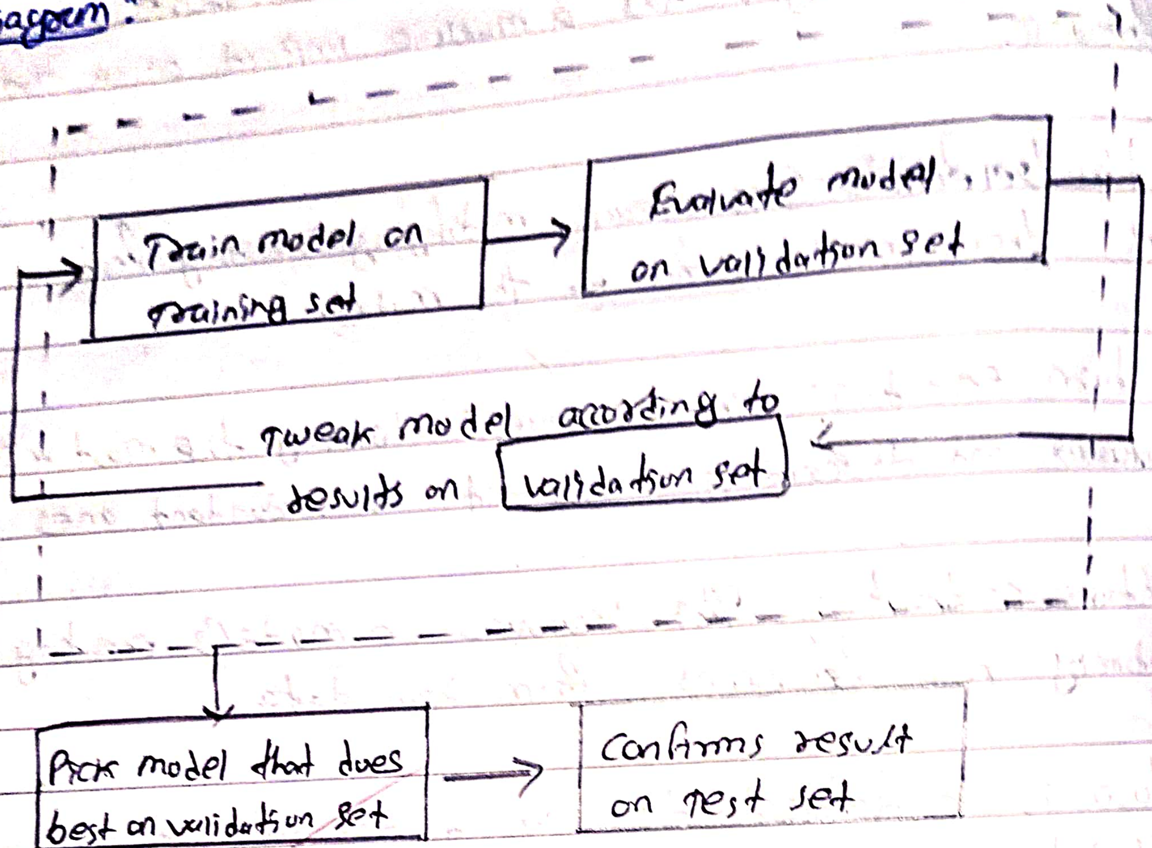
The steps are as:

i) Training set

ii) Validation set

iii) Testing set

Diagram:



(10) What is cross-validation, how is it performed, and why is it considered a reliable technique for model evaluation and tuning?

→ Cross-validation is a powerful and reliable evaluation technique that provides a more stable estimate of model's performance than a single train-validation split.
The most common method is k-fold cross-validation

Here's how it's performed (ex with k=5).

1) Split: The dataset is randomly shuffled and split into 5 equal-sized folds.

ii) Iterate:- The process runs for 5 iterations. In each iteration:

- one fold is held out as the test set.
- The remaining 4 fold are combined to form the training set
- The model is trained and then evaluated on the test fold

iii) Average: The final performance metric (e.g accuracy) is the average of the scores from all 5 iterations.

It's considered a reliable technique because every data point gets to be in a test set exactly once. This minimize the risk that the evaluation is skewed by a single "lucky" or "unlucky" split, giving a much better sense of how the model will generalize to unseen data.

28/7/25