

**ANNAMACHARYA INSTITUTE OF TECHNOLOGY AND SCIENCES
RAJAMPET**

(Autonomous)

Department of ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

Lecture Notes



Name of the Faculty: D.SAI SHIREESHA

Class: III B.Tech II Sem.

Branch : AIDS

Name of the Course: DEEP LEARNING

Subject Code: 23A3062T

Academic Year: 2025-2026

UNIT-1

Linear Algebra: Scalars, Vectors, Matrices and Tensors, Matrix operations, types of matrices, Norms, Eigen decomposition, Singular Value Decomposition, Principal Components Analysis. Probability and Information Theory: Random Variables, Probability Distributions, Marginal Probability, Conditional Probability, Expectation, Variance and Covariance, Bays' Rule, Information Theory. Numerical Computation: Overflow and Underflow, Gradient-Based Optimization, Constrained Optimization, Linear Least Squares.

Introduction

Linear Algebra forms the **mathematical foundation of Deep Learning and Machine Learning**. Almost every operation in a neural network — such as input representation, weight computation, forward propagation, and gradient calculation — is expressed using **scalars, vectors, matrices, and tensors**. Among these, **scalars and vectors** are the most fundamental building blocks. A clear understanding of these two concepts is essential to analyze and design deep learning models effectively.

Scalars

Definition

A scalar is a single numerical value that represents **magnitude only** and has **no direction**. Scalars belong to the set of real numbers or integers.

$$a \in \mathbb{R} \setminus \mathbb{Z} \quad a \in \mathbb{R}$$

Characteristics of Scalars

- One-dimensional
- No direction
- Represent constants or parameters
- Can be positive, negative, or zero

Examples of Scalars

- Temperature = 30°C
- Learning rate in neural networks = 0.01
- Bias term in a neuron
- Loss value produced by a neural network

Role of Scalars in Deep Learning

In Deep Learning, scalars are widely used in:

- Learning rate during optimization
- Regularization parameters (λ)
- Bias values added to neurons
- Output loss values such as Mean Squared Error

Thus, scalars control the **behavior and performance** of neural networks.

Vectors

Definition

A **vector** is an ordered collection of numbers arranged either as a **row** or **column**, representing both **magnitude and direction**.

$$x = [x_1 \ x_2 \ \dots \ x_n] \in \mathbb{R}^n \quad \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{R}^n$$

Types of Vectors

1. Row Vector

$$x = [x_1 \ x_2 \ x_3] \quad \mathbf{x} = [x_1 \ x_2 \ x_3]$$

2. Column Vector

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \quad \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

Vector Operations

1. Vector Addition

Two vectors can be added only if they have the same dimension.

$$\mathbf{a} + \mathbf{b} = [a_1 + b_1 \ a_2 + b_2] \quad \mathbf{a} = [a_1 \ a_2] \quad \mathbf{b} = [b_1 \ b_2]$$

Example:

$$[12] + [34] = [46] \quad \begin{bmatrix} 1 \\ 2 \end{bmatrix} + \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 4 \\ 6 \end{bmatrix}$$

2. Scalar Multiplication

A vector can be multiplied by a scalar.

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

3. Dot Product (Inner Product)

The dot product of two vectors is defined as:

$$\mathbf{a} \cdot \mathbf{b} = \sum_{i=1}^n a_i b_i$$

Example:

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 4 \end{bmatrix} = 1(3) + 2(4) = 11$$

Geometrical Interpretation of Vectors

Vectors can be represented geometrically as arrows:

- Length → magnitude
- Direction → orientation

The dot product measures **similarity** between vectors and is used extensively in:

- Cosine similarity
- Attention mechanisms
- Classification task

Importance of Vectors in Deep Learning

Vectors are used to represent:

- Input features
- Word embeddings
- Image pixels (flattened)
- Activations in neural networks
- Gradients during backpropagation

Every layer in a neural network processes vectors to learn patterns from data.

Python Example (Vector Operations)

```
import numpy as np
x = np.array([1, 2, 3])
```

```

y=np.array([4,5,6])

print("Addition:", x + y)
print("DotProduct:", np.dot(x, y))

```

Common Mistakes by Students

- Mixing row and column vectors
- Ignoring vector dimensions
- Applying dot product on incompatible vectors

Scalars and vectors are the **basic mathematical entities** used in Deep Learning. Scalars control learning behavior, while vectors represent data and parameters. A strong understanding of these concepts enables students to understand more advanced topics such as matrices, tensors, eigen decomposition, and optimization.

After understanding scalars and vectors, the next fundamental concepts in Linear Algebra are **matrices and tensors**. These structures allow us to represent **multiple vectors together** and handle **high-dimensional data** efficiently. In Deep Learning, almost every operation — from storing dataset to representing neural network weights — relies heavily on matrices and tensors.

2. Matrices

Definition

A **matrix** is a two-dimensional rectangular array of numbers arranged in **rows and columns**.

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

Where:

- m = number of rows
- n = number of columns

Matrix Dimensions

Represented as $m \times n$

- Example:
 - $3 \times 2 \times 2 \rightarrow 3 \text{ rows}, 2 \text{ columns}$

Examples of Matrices

- Studentmarkstable
- Imagepixels(2Dgrid)
- Weightmatrixinneuralnetworks

3. TypesofMatrices(Overview)

- RowMatrix
- ColumnMatrix
- SquareMatrix
- ZeroMatrix
- DiagonalMatrix
- IdentityMatrix
- SymmetricMatrix

4. MatrixOperations(Basic)

Matrix Addition

Twomatricescanbeadded

onlyiftheyhavethesamedimensions. $A+B=[a_{ij}+b_{ij}]$ $A + B =$

$[a_{ij} + b_{ij}]$ $A+B=[a_{ij}+b_{ij}]$ **Example:**

$[1234]+[5678]=[681012]$ $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} + \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} = \begin{bmatrix} 6 & 8 \\ 10 & 12 \end{bmatrix}$ $[1324]+[5768]=[610812]$

ScalarMultiplication

Eachelementofthematrixismultipliedbyascalar.

$cA=[c \cdot a_{ij}]$ $cA = [c \cdot a_{ij}]$ $cA=[c \cdot a_{ij}]$

MatrixMultiplication

If:

- AAA is $m \times n$ $m \times n$ $m \times n$
- BBB is $n \times p$ $n \times p$ $n \times p$

Then:

$AB=C(m \times p)$ $AB=C \quad (m \times p)$ $AB=C(m \times p)$

Matrix multiplication is **not commutative**.

5. Importance of Matrices in Deep Learning

Matrices are used to represent:

- Input data batches
- Weight parameters
- Bias values
- Activation outputs

Example:

For a neural layer:

$$y = Wx + b \quad \mathbf{y} = W\mathbf{x} + b \quad y = Wx + b$$

Where:

- W → weight matrix
- x → input vector
- b → bias vector

This shows that **matrix multiplication is the core operation in neural networks**.

6. Tensors

Definition

A **tensor** is a generalization of scalars, vectors, and matrices to **higher dimensions**.

Object Dimension

Scalar 0-D

Vector 1-D

Matrix 2-D

Tensor ≥ 3 -D

Examples of Tensors

1. **3-D Tensor**
 - Color image: (Height \times Width \times Channels)
2. **4-D Tensor**

- Batchofimages:
(Batchsize×Height×Width×Channels)

TensorRepresentation

T_{ijk} (3-D tensor) $\quad \text{(3-D tensor)}$ T_{ijk} (3-D tensor)

7. TensorinDeepLearning

Tensorsaretheprimarydatastructureindeeplearningframeworkssuchas:

- TensorFlow
- PyTorch

Used for:

- Inputdata
- Featuremaps inCNNs
- Gradients
- Modelparameters

8. PythonExample(Matrix&Tensor)

```
importnumpyasnp

#Matrix
A=np.array([[1,2],[3, 4]])

#3DTensor
T=np.array([
    [[1,2],[3,4]],
    [[5,6],[7,8]]
])

print("MatrixA:\n",A)
print("TensorT:\n",T)
```

9. CommonMistakesbyStudents

- Confusingmatrixandtensordimensions
- Invalid matrix multiplication
- Ignoringshapecompatibility

10. ApplicationsinDeepLearning

- CNNsuse4-D tensors

- RNNs process 3-D tensors
- Backpropagation uses tensor operations

Matrices and tensors enable efficient representation and computation of high-dimensional data. They form the **structural backbone of Deep Learning models**, making them indispensable for modern AI systems.

Matrices are the **core computational structures** in Linear Algebra and Deep Learning. Once matrices are defined, various **matrix operations** are performed on them to manipulate data, transform features, and train neural networks. Additionally, **special types of matrices** possess unique properties that simplify computations and improve efficiency. Understanding matrix operations and types is essential for building, analyzing, and optimizing deep learning models.

2. Matrix Operations

Matrix operations allow us to combine, transform, and analyze matrices mathematically.

Matrix Addition

Definition

Two matrices can be added

only if they have the same dimensions. $A+B=[a_{ij}+b_{ij}]$ $A+B=$

$[a_{ij} + b_{ij}]$ $A+B=[a_{ij}+b_{ij}]$ **Example**

$A=\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $B=\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}$ $A+B=\begin{bmatrix} 6 & 8 \\ 10 & 12 \end{bmatrix}$

Properties

- Commutative: $A+B=B+A$
- Associative: $(A+B)+C=A+(B+C)$
- Identity element: Zero matrix

Scalar Multiplication

Definition

Each element of the matrix is multiplied by a scalar value. $cA=[c \cdot a_{ij}]$

$cA=[c \cdot a_{ij}]$

Example

$$2 \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix}$$

Matrix Multiplication Definition

Matrix multiplication is possible when:

- A is of size $m \times n$
- B is of size $n \times p$

Resulting matrix:

$$AB = C \quad (m \times p) \quad c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$$

Example

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, B = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \quad AB = \begin{bmatrix} 19 & 22 \\ 43 & 50 \end{bmatrix}$$

Important Properties

- **Not commutative:** $AB \neq BA$
- Associative
- Distributive over addition

Transpose of a Matrix**Definition**

The transpose of matrix A is obtained by interchanging rows and columns. $A^T = [a_{ji}]$

$$A^T = [a_{ji}]$$

Example

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \Rightarrow A^T = \begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}$$

Inverse of a Matrix

Definition

The inverse of a square matrix A is denoted as A^{-1} such that:

$$AA^{-1} = I \quad A^{-1}A = I$$

Conditions

- Matrix must be square
- Determinant must be non-zero

3. Types of Matrices**Row Matrix**

- Single row
- Dimension: $1 \times n$

Column Matrix

- Single column
- Dimension: $m \times 1$

Square Matrix

- Same number of rows and columns
- Required for determinant and inverse

Zero (Null) Matrix

- All elements are zero
- Additive identity

Diagonal Matrix

- Non-zero elements only on main diagonal

$$D = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix}$$

Identity Matrix

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
 Acts as

multiplicative identity.

Symmetric Matrix

$$A=ATA= A^TA=AT$$

Used in covariance matrices and PCA.

Orthogonal Matrix

$$ATA=IA^TA=IATA=I$$

Used in rotation and PCA.

Singular and Non-Singular Matrix

- Singular: determinant=0
- Non-singular: determinant \neq 0

4. Importance in Deep Learning

- Weight matrices define neural connections
- Transpose used in backpropagation
- Symmetric matrices in covariance computation
- Identity matrix in initialization and normalization
- Matrix multiplication drives forward propagation

5. Python Example

```
import numpy as np

A=np.array([[1,2],[3, 4]])
B=np.array([[5,6],[7, 8]])

print("Addition:\n", A + B)
print("Multiplication:\n", np.dot(A,B))
print("Transpose:\n", A.T)
```

6. Common Student Mistakes

- Invalid matrix multiplication
- Assuming commutativity
- Forgetting dimension rules

Matrix operations and types form the **computational engine** of Deep Learning. Correct usage ensures efficient learning, numerical stability, and accurate model implementation.

In Linear Algebra, **norms** measure the **size or magnitude** of vectors and matrices. Norms are widely used in Deep Learning to:

- Measure **distance between vectors**
- Regularize neural networks (L1, L2 regularization)
- Ensure numerical stability
- Control overfitting

Formally, norms provide a **mathematical framework for “length” or “size”** in multi-dimensional space.

2. Vector Norms

Definition

A **vector norm** is a function $\|\cdot\|: \mathbb{R}^n \rightarrow \mathbb{R}$ that satisfies:

1. **Non-negativity:** $\|\mathbf{x}\| \geq 0$
2. **Definiteness:** $\|\mathbf{x}\| = 0 \iff \mathbf{x} = \mathbf{0}$
3. **Homogeneity:** $\|\alpha \mathbf{x}\| = |\alpha| \|\mathbf{x}\|$
4. **Triangle inequality:** $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$

Common Vector Norms

a) L1 Norm (Manhattan norm)

$$\|\mathbf{x}\|_1 = \sum_{i=1}^n |x_i|$$

- Measure **sum of absolute values**
- Used in **Lasso regression / L1 regularization**

Example:

$$\mathbf{x} = [3, -4, 1] \implies \|\mathbf{x}\|_1 = 3 + 4 + 1 = 8$$

$$\mathbf{x} = [3, -4, 1] \implies \|\mathbf{x}\|_1 = 3 + 4 + 1 = 8$$

b) L2 Norm (Euclidean norm)

$$\|\mathbf{x}\|_2 = \sqrt{\sum_{i=1}^n x_i^2} \quad \|\mathbf{x}\|_2 = \sqrt{3^2 + 4^2} = 5$$

- Measures **straight-line distance from origin**
- Used in **weight decay/ L2 regularization**
- Most common in Deep Learning

Example:

$$\mathbf{x} = [3, 4] \Rightarrow \|\mathbf{x}\|_2 = \sqrt{3^2 + 4^2} = 5$$

c) Infinity Norm

$$\|\mathbf{x}\|_\infty = \max_i |x_i| \quad \|\mathbf{x}\|_\infty = \max\{3, 4\} = 4$$

- Measures **largest magnitude component**
- Useful in **robust optimization**

Geometric Interpretation

- L1 norm → “city block distance”
- L2 norm → “straight line”
- Infinity norm → “maximum component magnitude”

Python Example

```
import numpy as np

x = np.array([3, -4, 1])

print("L1 norm:", np.linalg.norm(x, 1))
print("L2 norm:", np.linalg.norm(x))
print("Infinity norm:", np.linalg.norm(x, np.inf))
```

3. Matrix Norms

Definition

Matrix norms measure the **size of matrices**. Some common norms:

a) Frobenius Norm

$$\|A\|_F = \sqrt{\sum_{i,j} a_{ij}^2}$$

- Generalizes L2 norm for matrices
- Used to **measure weight magnitude in neural networks**

b) L1 Norm (Maximum column sum)

$$\|A\|_1 = \max_j \sum_i |a_{ij}| \quad \|A\|_{-1} = \max_j \sum_i |a_{ij}| \quad \|A\|_1 = \max_i \sum_j |a_{ij}|$$

c) Infinity Norm (Maximum row sum)

$$\|A\|_\infty = \max_i \sum_j |a_{ij}| \quad \|A\|_{-\infty} = \max_i \sum_j |a_{ij}| \quad \|A\|_\infty = \max_j \sum_i |a_{ij}|$$

Python Example (Matrix Norms)

```
A=np.array([[1,2],[3,4]])

print("Frobenius norm:", np.linalg.norm(A, 'fro'))
print("L1 norm:", np.linalg.norm(A, 1))
print("Infinity norm:", np.linalg.norm(A, np.inf))
```

4. Properties of Norms

- Non-negativity: $\|x\| \geq 0$ and $\|x\| = 0$ if and only if $x = 0$
- Scalability: $\|\alpha x\| = |\alpha| \|x\|$ and $\|\alpha x\| = |\alpha| \|x\|$
- Triangle inequality: $\|x+y\| \leq \|x\| + \|y\|$ and $\|x+y\| \leq \|x\| + \|y\|$
- Sub-multiplicative (for matrices): $\|AB\| \leq \|A\| \cdot \|B\|$ and $\|AB\| \leq \|A\| \cdot \|B\|$

5. Importance in Deep Learning

- **Regularization:** Prevent overfitting (L1, L2)
- **Gradient normalization:** Ensures stable updates
- **Distance computation:** Clustering, nearest neighbors
- **Weight scaling:** Controls magnitude in neural networks

Example:

Weight decay in L2 regularization:

$$\text{Loss} = \text{MSE} + \lambda \|W\|_2^2 \quad \text{Loss} = \text{MSE} + \lambda \|W\|_2^2$$

6. Common Mistakes

- Confusing vector norm with matrix norm
- Ignoring dimensionality
- Using wrong norm in optimization

Eigendecomposition is a **fundamental concept in linear algebra** whereas square matrix is expressed in terms of its **eigenvalues and eigenvectors**. It is extensively used in:

- Dimensionality reduction (PCA)
- Covariance analysis
- Stability analysis of neural networks

Eigendecomposition simplifies matrix operations, especially in **diagonalization**, which helps in faster computation and better understanding of linear transformations.

2. Definitions

- **Eigenvector** (\mathbf{v}): A non-zero vector that only **changes in magnitude** when a linear transformation is applied.

$$A\mathbf{v} = \lambda\mathbf{v}$$

- **Eigenvalue** (λ): Scalar representing the **factor by which the eigenvector is scaled**.

Eigen Decomposition

For a square matrix A :

$$A = V\Lambda V^{-1}$$

Where:

- V = matrix of eigenvectors
- Λ = diagonal matrix of eigenvalues

Note: Eigendecomposition exists for **diagonalizable matrices**.

3. Computing Eigenvalues and Eigenvectors

1. Solve **characteristic equation**:

$$\det(A - \lambda I) = 0$$

2. Solve $(A - \lambda I)\mathbf{v} = 0$ for eigenvectors.

Example

$$A = \begin{bmatrix} 4 & 1 \\ 2 & 3 \end{bmatrix}$$

1. Characteristic equation: $\det(A - \lambda I) = 0$

$$\det\begin{bmatrix} 4-\lambda & 1 \\ 2 & 3-\lambda \end{bmatrix} = (4-\lambda)(3-\lambda) - 2 = \lambda^2 - 7\lambda + 10 = 0$$

$$\det\begin{bmatrix} 4-\lambda & 1 \\ 2 & 3-\lambda \end{bmatrix} = (4-\lambda)(3-\lambda) - 2 = \lambda^2 - 7\lambda + 10 = 0$$

2. Eigenvalues: $\lambda_1 = 5, \lambda_2 = 2$
3. Eigenvectors: Solve $(A - \lambda I)v = 0$ for each λ

4. Importance in Deep Learning

- **Principal Component Analysis (PCA)** uses eigendecomposition of covariance matrix to reduce dimensionality
- Analyze stability of recurrent neural networks
- Used in diagonalization of weight matrices for efficient computation

Python Example

```
import numpy as np

A = np.array([[4, 1], [2, 3]])

eigenvalues, eigenvectors = np.linalg.eig(A)
print("Eigenvalues:", eigenvalues)
print("Eigenvectors:\n", eigenvectors)
```

5. Common Mistakes

- Forgetting that eigenvectors must be non-zero
- Confusing eigenvalues with singular values
- Using non-square matrices

SVD and PCA are **powerful linear algebra tools** for:

- Dimensionality reduction
- Feature extraction
- Data compression

They transform data into a **simpler, more informative space** while retaining essential features.

2. Singular Value Decomposition (SVD)

Definition

For any matrix $A \in \mathbb{R}^{m \times n}$

$$A = U \Sigma V^T$$

Where:

- $U \in \mathbb{R}^{m \times m}$ orthogonal matrix (left singular vectors)
- $\Sigma \in \mathbb{R}^{m \times n}$ diagonal matrix of singular values
- $V \in \mathbb{R}^{n \times n}$ orthogonal matrix (right singular vectors)

Steps of SVD

1. Compute $A^T A$ and $A A^T$
2. Find eigenvectors of $A^T A$ (columns of V)
3. Compute singular values ($\sigma_i = \sqrt{\lambda_i}$)
4. Find columns of U using $u_i = A v_i / \sigma_i$

Importance in Deep Learning

- Dimensionality reduction for large datasets
- Image compression and reconstruction
- Data denoising
- Feature extraction before training

Python Example

```
import numpy as np

A = np.array([[1, 2], [3, 4], [5, 6]])
U, S, Vt = np.linalg.svd(A)
print("U:\n", U)
print("S:", S)
print("Vt:\n", Vt)
```

3. Principal Component Analysis (PCA)

Definition

PCA is a statistical technique that transforms high-dimensional data into a lower-dimensional space while preserving maximum variance.

Steps of PCA

1. Center data: $X \leftarrow X - \text{mean}(X)$
2. Compute covariance matrix: $C = X^T X$
3. Compute eigenvalues and eigenvectors of C
4. Select top- k eigenvectors \rightarrow principal components
5. Project data onto new subspace

Importance in Deep Learning

- Reduces dimensionality → faster training
- Removes redundant features
- Helps visualize high-dimensional data
- Preprocessing for neural networks, clustering, and ML models

Python Example

```
from sklearn.decomposition import PCA
import numpy as np

X = np.array([[2.5, 2.4], [0.5, 0.7], [2.2, 2.9]])

pca = PCA(n_components=1)
X_pca = pca.fit_transform(X)
print(X_pca)
```

4. Common Mistakes

- Forgetting to center data before PCA
- Confusing singular values and eigenvalues
- Selecting too few or too many components

Probability theory provides a **framework to quantify uncertainty**, which is crucial in Deep Learning, ML, and AI for:

- Modeling predictions
- Handling stochastic data
- Optimizing probabilistic models

Random variables, expectations, variance, and Bayes' rule are core concepts.

2. Random Variables

- **Random Variable (RV):** A variable whose value depends on chance.
- Types:
 1. **Discrete RV** – finite or countable outcomes (e.g., dice roll)
 2. **Continuous RV** – infinite outcomes (e.g., height, temperature)

3. Probability Distributions

- **Discrete Distribution:** Probability mass function (PMF)

$$P(X=x) = p$$

- **Continuous Distribution:** Probability density function (PDF)

$$P(a \leq X \leq b) = \int_a^b f(x) dx$$

Examples:

- Binomial, Poisson (Discrete)
- Gaussian/ Normal (Continuous)

4. Marginal and Conditional Probability

- **Marginal Probability:** Probability of single event ignoring others

$$P(X) = \sum_y P(X, Y) \quad P(X) = \sum_y P(X, Y)$$

- **Conditional Probability:** Probability of X given Y

$$P(X|Y) = \frac{P(X, Y)}{P(Y)} \quad P(X|Y) = \frac{P(X, Y)}{P(Y)}$$

5. Expectation, Variance, Covariance

- **Expectation:** Average value

$$E[X] = \sum_x x P(X=x) \quad \text{or} \quad \int x f(x) dx \quad E[X] = \sum_x x P(X=x) \quad \text{or} \quad \int x f(x) dx$$

- **Variance:** Spread of

$$\text{distribution} \quad \text{Var}(X) = E[(X - E[X])^2] \quad \text{Var}(X) = E[(X -$$

$$E[X])^2] \quad \text{Var}(X) = E[(X - E[X])^2]$$

- **Covariance:** Measure of relationship between X and Y

$$\text{Cov}(X, Y) = E[(X - E[X])(Y - E[Y])] \quad \text{Cov}(X, Y) = E[(X - E[X])(Y - E[Y])]$$

6. Bayes' Rule

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \quad P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

- Used in **Naive Bayes classifiers**, probabilistic inference

7. Information Theory Basics

- **Entropy:** Measure of uncertainty

$$H(X) = -\sum P(x) \log_2 P(x) \quad H(X) = -\sum P(x) \log_2 P(x)$$

- **KL-Divergence:** Measure of difference between distributions

$$DKL(P||Q)=\sum P(x)\log\frac{P(x)}{Q(x)}D_{\{KL\}}(P||Q)=\sum P(x)\log\frac{P(x)}{Q(x)}$$

8. Applications in Deep Learning

- Probabilistic modeling (Bayesian Neural Networks)
- Loss functions (Cross-Entropy Loss)
- Uncertainty quantification
- Reinforcement learning

Python Example (Probability & Expectation)

```
import numpy as np

X = np.array([1, 2, 3, 4, 5])
p = np.array([0.1, 0.2, 0.3, 0.2, 0.2])

expectation = np.sum(X * p)

print("Expectation:", expectation)
```

9. Common Mistakes

- Misunderstanding discrete vs continuous RV
- Forgetting to normalize probabilities
- Confusing marginal and conditional probability

Numerical computation and optimization are **core to training deep learning models**. Understanding overflow, underflow, gradient-based optimization, and constrained optimization ensures **stability and efficiency** of learning algorithms.

2. Overflow and Underflow

- **Overflow:** Values exceed maximum representable number \rightarrow infinity
- **Underflow:** Values approach zero too closely \rightarrow loss of precision

Example:

Sigmoid function $\sigma(x) = \frac{1}{1 + e^{-x}}$ may cause overflow for large $|x|$.

- Solution: Numerical stability techniques, e.g., log-sum-exp trick.

3. Gradient-Based Optimization

- **Objective:** Minimize loss $L(\theta)$
- **Gradient Descent:**

$$\theta := \theta - \eta \nabla_{\theta} L(\theta)$$

- Variants:
 - Stochastic GD
 - Mini-batch GD
 - Momentum, RMSProp, Adam

4. Constrained Optimization

- Solve optimization with constraints:

$$\min_{\mathbf{x}} f(\mathbf{x}) \text{ s.t. } g(\mathbf{x}) = 0$$

- Lagrange multipliers:

$$L(\mathbf{x}, \lambda) = f(\mathbf{x}) + \lambda g(\mathbf{x})$$

- Used in regularization and resource-constrained learning

5. Linear Least Squares

- Objective: Fit linear model

$$y = X\beta + \epsilon$$

- Minimizes sum of squared errors:

$$\min_{\beta} \|X\beta - y\|_2^2$$

- Solution:

$$\beta = (X^T X)^{-1} X^T y$$

- Used in linear regression and as initialization in neural networks

Python Example

```
import numpy as np

X = np.array([[1, 1], [1, 2], [2, 2]])
y = np.array([6, 8, 9])
beta = np.linalg.inv(X.T @ X) @ X.T @ y
print("Least squares solution:", beta)
```

6. Importance in Deep Learning

- Ensures **numerical stability**
- Efficient **training of neural networks**
- Handles **large datasets** without errors
- Optimizes performance with constraints

7. Common Mistakes

- Ignoring learning rate scaling
- Not normalizing data → overflow/underflow
- Using wrong gradient formulas

UNIT-2

Machine Learning: Basics and Under fitting, Hyper parameters and Validation Sets, Estimators, Bias and Variance, Maximum Likelihood, Bayesian Statistics, Supervised and Unsupervised Learning, Stochastic Gradient Descent, Challenges Motivating Deep Learning. Deep Feed forward Networks: Learning XOR, Gradient-Based Learning, Hidden Units, Architecture Design, Back-Propagation and other Differentiation Algorithms.

1. Introduction to Machine Learning:
Machine Learning (ML) is a field of Artificial Intelligence that enables computer systems to learn patterns from data and improve their performance on a specific task without being explicitly programmed. Instead of following rigid rules, ML models adapt based on experience.

Importance of Machine Learning

- * Handles large volumes of data
- * Automates decision making
- * Learns complex patterns
- * Improves accuracy over time

Machine Learning Process

1. Data Collection
2. Data Preprocessing
3. Feature Extraction
4. Model Selection
5. Training
6. Evaluation
7. Deployment

Data → Preprocessing → Model → Training → Evaluation → Prediction

2. Basics of Machine Learning

Machine Learning systems learn a mapping between input variables (features) and output variables (targets). The goal is to generalize well to unseen data.

Key Components

- * Dataset
- * Features
- * Labels
- * Model
- * Loss function
- * Optimization algorithm

Applications

- * Spam detection
- * Face recognition
- * Medical diagnosis
- * Recommendation systems

3. Underfitting

Definition

Underfitting occurs when a model is too simple to capture the underlying structure of the data. It fails to learn meaningful relationships.

Characteristics

- * High training error
- * High testing error
- * Poor prediction accuracy

Causes

- * Simple model
- * Insufficient training time
- * Lack of important features

Example

Using a straight line to fit curved data.

Diagram

Datapoints: **

**

Model line: -----

-

4. Hyperparameters and Validation Sets

Hyperparameters

Hyperparameters are configuration values set before training begins. They control the learning process.

Examples

- * Learning rate
- * Number of epochs

- * Numberofhiddenlayers

- * Regularizationparameter

Validation Set

Avalidationsetisusedtotunehyperparametersandavoidoverfitting. Data

Split

- * Trainingset:70%

- * Validationset:15%

- * Testset:15%

5. Estimators

Definition

Anestimatorisaruleoralgorithmusedtoestimateunknownparametersfromdata.

Types

- * PointEstimator

- * IntervalEstimator

PropertiesofGood Estimators

- * Unbiasedness

- * Consistency

- * Efficiency

Example

Samplemeanasanestimatorofpopulationmean

6. BiasandVariance

Bias

Biasistheerrorduetooverlysimplicassumptionsinthemodel.

Variance

Variance is the error caused by sensitivity to fluctuations in the training data. Bias–

Variance Tradeoff

* High Bias → Underfitting

* High Variance → Overfitting

Diagram

Error

^

| \ Variance

| \

| \ _____ Bias

| _____ > Model Complexity

7. Maximum Likelihood Estimation (MLE)

Definition

MLE is a method used to estimate model parameters by maximizing the likelihood of observing the given data.

Likelihood Function

$P(\text{Data} | \text{Parameters})$

Key Points

* Widely used in statistics and ML

* Assumes data distribution

* Sensitive to outliers

Example

Estimating mean of Gaussian distribution

8. Bayesian Statistics

Definition

Bayesian statistics treats model parameters as random variables and updates beliefs using probability.

Bayes Theorem

$$P(\theta|X) = [P(X|\theta) \times P(\theta)] / P(X)$$

Components

- * Prior probability
- * Likelihood
- * Posterior probability

Advantages

- * Incorporates prior knowledge
- * Handles uncertainty

Diagram

Prior + Data → Posterior

9. Supervised Learning

Definition

Supervised learning uses labeled data to learn a mapping from inputs to outputs. Types

- * Classification
- * Regression

Algorithms

- * Linear Regression
- * Logistic Regression
- * Support Vector Machines

- * K-NearestNeighbors

Diagram

Input→Model→ Output

10. UnsupervisedLearning

Definition

Unsupervisedlearningworkswithunlabeleddatatodiscoverhiddenpatterns.

Tasks

- * Clustering

- * DimensionalityReduction

Algorithms

- * K-Means

- * HierarchicalClustering

- * PCA

Diagram

Data→PatternDiscovery

11. StochasticGradientDescent(SGD)

GradientDescent

Anoptimizationalgorithmusedtominimizelossfunction.

SGD

SGDupdatesmodelparametersusingonedatapointatatime.

Update

Rule $\theta = \theta - \eta \nabla$

$L(\theta)$

Advantages

- * Fast

- * Scalable

Disadvantages

- * Noisy convergence

Diagram

Loss

\wedge^*

|**

|*

|____> Parameters`

12. Challenges Motivating Deep Learning

Limitations of Traditional ML

- * Manual feature extraction
- * Poor performance on unstructured data

Challenges

- * High dimensionality
- * Non-linear relationships
- * Large datasets

Motivation for Deep Learning

- * Automatic feature learning
- * Handles complex patterns

Diagram

Input → Hidden Layers → Output

Deep Feed-Forward Networks:

Introduction to Deep Feed-Forward Networks:

Deep Feed-Forward Networks (DFFNs), also known as Multilayer Perceptrons (MLPs), are one of the most fundamental architectures in deep learning. These networks form the backbone of many modern artificial intelligence systems. A feed-forward network is characterized by the unidirectional flow of information, meaning that data moves strictly from the input layer through one or more hidden layers to the output layer without forming cycles or feedback loops.

The main motivation behind deep feed-forward networks is their ability to approximate complex nonlinear functions. Unlike traditional machine learning algorithms that rely heavily on handcrafted features, deep networks can automatically learn hierarchical representations from raw data. Lower layers typically learn simple patterns, while higher layers capture increasingly abstract features.

Basic Structure

A deep feed-forward network consists of the following components:

- * **Input Layer** **: Receives raw input features
- * **Hidden Layers** **: Perform nonlinear transformations
- * **Output Layer** **: Produces final prediction

Input Layer Hidden Layer 1 Hidden Layer 2

Output Layer $x_1 x_2 x_3 \rightarrow$ $ooo \rightarrow$

$oo \rightarrow$ o

Mathematical Model of Feed-Forward Networks

A feed-forward network computes a function $f(x; \theta)$, where x is the input and θ represents the parameters (weights and biases). Each neuron computes a weighted sum of its inputs followed by a nonlinear activation function.

For a single neuron:

$$z = w_1 x_1 + w_2 x_2 + \dots + w_n x_n + b$$

$\varphi(z)$

where:

* w_i are weights

* bias

* ϕ is an activation function

For deep networks, this computation is repeated layer by layer, forming a composition of functions.

Learning the XOR Problem

Definition of XOR

The XOR (Exclusive OR) problem is a classical example used to demonstrate the limitations of single-layer perceptrons and the power of multi-layer networks. XOR outputs true only when the two inputs are different.

[Input A | Input B | XOR Output]

| Input A | Input B | XOR Output |
|---------|---------|------------|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Linear Separability

A problem is linearly separable if a straight line (or hyperplane) can separate the classes. XOR is not linearly separable.

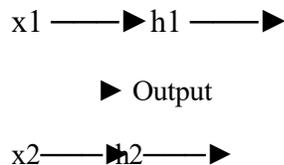
$(0,1)$ ● $(1,1)$ ○

$(0,0)$ ○ $(1,0)$ ●

No single straight line can separate the two classes.

XOR with a Hidden Layer

A feed-forward network with one hidden layer can learn XOR by transforming the input space.



Hidden neurons learn intermediate features such as AND and OR, which are combined to compute XOR. This demonstrates that **hidden layers enable nonlinear decision boundaries**

Gradient-Based Learning

Learning Objective

The objective of training a deep feed-forward network is to minimize a loss function that measures the discrepancy between predicted outputs and true targets.

Common loss functions include:

- * Mean Squared Error (MSE)

- * Cross-Entropy Loss

Gradient Descent Algorithm

Gradient descent is an optimization technique used to update network parameters iteratively.

$$w \leftarrow w - \eta (\partial L / \partial w)$$

where:

- * η is the learning rate

- * $\partial L / \partial w$ is the gradient of the loss

Types of Gradient Descent

- * **Batch Gradient Descent**: Uses entire dataset

- * **Stochastic Gradient Descent (SGD)**: Uses one sample at a time

- * **Mini-Batch Gradient Descent**: Uses small batches

Mini-batch gradient descent is most commonly used in practice due to efficiency and stability

Hidden Units and Activation Functions

Role of Hidden Units

Hidden units allow the network to learn internal representations of data. Each hidden layer extracts features at a different level of abstraction.

Without hidden layers, neural networks reduce to linear models and fail to capture complex patterns.

Activation Functions

Activation functions introduce nonlinearity into the network.

Sigmoid Function

$$\sigma(x) = \frac{1}{1 + e^{-x}}$$

- * Outputs values between 0 and 1

- * Suffers from vanishing gradient problem

Tanh Function

- * Outputs values between -1 and 1

- * Zero-centered

ReLU (Rectified Linear Unit)

$$f(x) = \max(0, x)$$

- * Computationally efficient

- * Reduces vanishing gradients

Leaky ReLU

$$f(x) = \max(0.01x, x)$$

- * Solves dying ReLU problem

Architecture Design of Deep Feed-Forward Networks

Design Considerations

Key architectural decisions include:

- * Number of layers (depth)

- * Number of neurons per layer (width)

- * Choice of activation functions

- * Regularization techniques

Depth vs Width

Deep architectures are preferred because they:

- * Learn hierarchical features
- * Require fewer parameters than very wide shallow networks
- * Generalize better when properly regularized

Universal Approximation Theorem

The theorem states that a feed-forward network with a single hidden layer containing a finite number of neurons can approximate any continuous function. However, deep networks achieve this more efficiently.

Back-Propagation Algorithm

High Overview:

Back-propagation is the core algorithm used to train deep feed-forward networks. It efficiently computes gradients of the loss function with respect to all parameters.

Phases of Back-Propagation

Forward Pass

- * Inputs propagated through the network
- * Output and loss computed

Backward Pass

- * Errors propagated backward
- * Gradients computed using chain rule
- * Weights updated

Forward: $x \rightarrow h_1 \rightarrow h_2 \rightarrow y$

Backward: $\leftarrow \delta_1 \leftarrow \delta_2 \leftarrow \delta_y$

Mathematical Explanation

For a weight w in layer l :

$$\frac{\partial L}{\partial w} = \left(\frac{\partial L}{\partial a}\right) \left(\frac{\partial a}{\partial z}\right) \left(\frac{\partial z}{\partial w}\right)$$

This layered decomposition makes training deep networks computationally feasible.

Other Differentiation Algorithms

Numerical Differentiation

Uses finite differences to approximate gradients.

- * Simple but inaccurate
- * Computationally expensive

Symbolic Differentiation

- * Computes exact derivatives
- * Suffers from expression explosion

Automatic Differentiation

Automatic differentiation is used in modern deep learning frameworks such as TensorFlow and PyTorch.

Advantages:

- * Exact gradients
- * Efficient computation
- * Scales to deep architecture

Challenges in Training Deep Feed-Forward Networks

- * Vanishing and exploding gradients
- * Overfitting
- * Choice of hyperparameters
- * Computational complexity

Techniques such as normalization, better initialization, and advanced optimizers help overcome these challenges.

Conclusion

Deep feed-forward networks form the foundation of deep learning. Their ability to learn nonlinear, hierarchical representations makes them powerful tools for solving complex real-world problems. Understanding XOR learning, gradient-based optimization, hidden units, architecture design, back-propagation, and differentiable algorithms is essential for mastering modern neural networks.

UNIT-III:RegularizationandOptimizationforDeepLearning

Regularization for Deep Learning: Parameter Norm Penalties, Norm Penalties as Constrained Optimization, Regularization and Under-Constrained Problems, Dataset Augmentation, Noise Robustness, Semi-Supervised Learning, Multi-Task Learning, Early Stopping, Parameter Tying and Parameter Sharing, Sparse Representations, Bagging and Other Ensemble Methods, Dropout, Adversarial Training, Tangent Distance, Tangent Prop and Manifold Tangent Classifier. Optimization for Training Deep Models: Pure Optimization, Challenges in Neural Network Optimization, Basic Algorithms, Parameter Initialization Strategies, Algorithms with Adaptive Learning Rates, Approximate Second-Order Methods, Optimization Strategies and Meta-Algorithms

Parameter Norm Penalties

Definition:

Parameter norm penalties are techniques used in deep learning to **prevent overfitting** by adding a penalty to the loss function based on the **size (norm) of the weights**. Large weights are discouraged, making the model simpler and more generalizable.

Key Points:

1. **L1 Regularization (Lasso):**
 - Adds the sum of absolute values of weights to the loss.
 - Encourages **sparsity** → some weights become exactly zero.
2. **L2 Regularization (Ridge):**
 - Adds the sum of squared weights to the loss.
 - Discourages **large weights** but rarely sets them exactly to zero.

Example (L2 Regularization):

Original loss function (Mean Squared Error, MSE):

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

With L2 penalty:

$$J(\theta) = MSE + \lambda \sum_{i=1}^n \theta_i^2 \quad J(\theta) = MSE + \lambda \sum_{i=1}^n \theta_i^2$$

Where:

- θ_i → weights of the model
- λ → regularization parameter (controls penalty strength)

Larger λ → stronger shrinkage of weights → prevent overfitting.

DiagramExplanation:

- **L1Regularization:** Weight values shrink toward zero, some become exactly **0** (sparse).
- **L2Regularization:** Weight values shrink **smoothly**, but rarely become exactly zero.

Conceptual Illustration:

Weight magnitude



- L1 → diamond-like penalty → sparsity
- L2 → circle-like penalty → smooth shrinkage

Norm Penalties as Constrained Optimization**Definition:**

Regularization can be interpreted as **minimizing the loss function while keeping the weights within a certain norm constraint**. This means we only allow weight values that satisfy a specific size limit, which helps prevent overfitting.

Mathematically:

$$\min_{\theta} L(\theta) \text{ subject to } \|\theta\|_p \leq c$$

Where $p=1$ for L1 and $p=2$ for L2.

Key Points:**1. L2 Regularization (Ridge):**

- Constraint: $\|\theta\|_2 \leq c \iff \|\theta\|_2 \leq c$
 - Geometrically \rightarrow **circular(spherical)region** in weight space.
 - Encourages small but non-zero weights.
2. **L1 Regularization (Lasso):**
- Constraint: $\|\theta\|_1 \leq c \iff \|\theta\|_1 \leq c$
 - Geometrically \rightarrow **diamond-shaped feasible region.**

- Encourages **sparse weights**, some exactly zero.
3. **Purpose:**
- Helps visualize how regularization limits weight growth.
 - Shows why L1 leads to sparsity and L2 to smooth shrinkage.

Example:

Suppose we want to minimize the loss subject to an L2 constraint:

$$\sum_i \theta_i^2 \leq 1$$

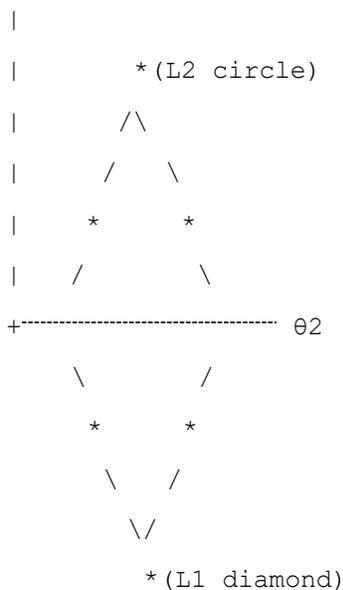
- Only weight combinations that satisfy $\sum_i \theta_i^2 \leq 1$ are allowed.
- The optimizer finds the best weights **inside the circle**.

Diagram Explanation:

- **L2 Constraint:** Circle in 2D weight space \rightarrow all points inside circle satisfy $\|\theta\|_2 \leq c$.
- **L1 Constraint:** Diamond in 2D weight space \rightarrow all points inside diamond satisfy $\|\theta\|_1 \leq c$.

Conceptual Illustration:

Weight θ_1



- The **circle** \rightarrow smooth weight shrinkage (L2)
- The **diamond** \rightarrow sparsity (L1)

3. Regularization and Under-Constrained Problems

Definition:

When the **number of model parameters exceeds the number of training samples**, the model is **under-constrained**—there are infinitely many solutions that fit the training data. Regularization helps **select simpler solutions** that generalize better.

KeyPoints:

1. **Reducesvariance:**Preventsthemodelfromfittingnoiseintraining data.
2. **Encouragesmoothnessandstability:** Solutionsaresimplerandless sensitivetosmall input changes.

Example:

- Polynomialregressionwith**degreehigherthan the numberof samples**.
- Withoutregularization→modelfitsallpointsexactly→ overfitting.
- WithL2 or L1regularization→ smoother curve,bettergeneralization.

DiagramExplanation:

- Overfittingcurve(high-degreepolynomial) →passsthroughallpoints.
- Regularizedcurve→smoother,approximates overalltrend.

ConceptualIllustration:

4. DatasetAugmentation

Definition:

Datetaugmentationinvolves **artificiallyexpandingthetrainingdataset**byapplying **transformations**toexistingsamples.Thisimprovesmodelgeneralizationandrobustness.

KeyPoints:

1. Commonimagetransformations:**rotation,flipping,cropping,scaling**.
2. Improvesmodelrobustnesstovariationsin input.
3. Reducesoverfittingonsmalldatasets.

Example:

- CIFAR-10 images:Originalimage→rotated,flipped,orcroppedversionsaddedto training set.

DiagramExplanation:

- Originalimage→rotated+flipped→multipleaugmented samples.

ConceptualIllustration:

[OriginalImage]→rotate15°→[RotatedImage]
 →horizontalflip→[FlippedImage]

5.NoiseRobustness

Definition:

Noiserobustnessinvolves**addingnoisetoinputsorlayersduringtraining**to improve model generalization. The model learns to be less sensitive to small variations.

KeyPoints:

1. Typesofnoise:**inputnoise**(e.g.,Gaussiannoise), **dropoutnoise**(randomlyturningoff neurons).
2. Helpsmode**lgeneralize**tounseenornoisydata.

Example:

- MNISThandwrittendigits: AddGaussiannoisetoinputimagesduringtraining→model learns to classify even noisy digits.

DiagramExplanation:

- Originalimagevs noisy image

ConceptualIllustration:

[OriginalImage]→+GaussianNoise→[NoisyImage]

- The modelseesbothversionsduringtraining→learnsrobustness.

6.Semi-SupervisedLearning

Definition:

Semi-supervised learning isa learningapproachthat usesa **smallamountoflabeleddata together with a large amount of unlabeled data** to improve model performance.

KeyPoints:

1. Combinessupervised (labeleddata)and **unsupervised** (unlabeleddata)learning.

2. Assumes unlabeled data helps reveal the **underlying data structure**.
3. Reduces labeling cost and improves generalization.
4. Common techniques:
 - **Pseudo-labeling**: Model assigns labels to unlabeled data.
 - **Consistency regularization**: Model predictions should remain stable under input perturbations.

Example:

- CIFAR-10 dataset with only a small portion of labeled images.
- The model learns from both labeled and unlabeled images to improve classification accuracy.

Diagram Explanation:

- Labeled data and unlabeled data are fed into the model.
- The model learns jointly and produces predictions.

LabeledData+UnlabeledData→Model→Predictions

7. Multi-Task Learning

Definition:

Multi-task learning is a technique where a model learns **multiple related tasks simultaneously** using shared internal representations.

Key Points:

1. Improves generalization by sharing knowledge across tasks.
2. Acts as a **regularizer**, reducing overfitting.
3. Shared features capture common patterns among tasks.

Example:

- Predicting **age and gender** from face images using a single neural network.

Diagram Explanation:

- Hidden layers are shared across tasks.
- Each task has a separate output layer.

Input→SharedHiddenLayers→AgeOutput
 →GenderOutput

8. Early Stopping

Definition:

Early stopping is a regularization technique where training is **stopped when validation loss stops improving**, even if training loss continues to decrease.

Key Points:

1. Prevents overfitting.
2. Acts as an **implicit regularizer**.
3. Uses validation set performance to decide stopping point.

Example:

- Training loss decreases continuously.
- Validation loss starts increasing → training is stopped.

Diagram Explanation:

- Graph shows training loss decreasing.
- Validation loss decreases initially, then increases → early stopping point.

```

Loss
|
|\Validation
|\StopHere
|  \
|Training
+----->Epochs
  
```

9. Parameter Tying/Parameter Sharing

Definition:

Parameter tying (or sharing) forces **multiple parameters to have the same value**, reducing model complexity.

Key Points:

1. Reduces number of free parameters.
2. Improves generalization.

3. Commonly used in **CNNs** and **RNNs**.

Example:

- In CNNs, the **same convolution filter** is applied across different spatial locations of an image.

Diagram Explanation:

- A single filter slides across the image to extract features.

[Filter] → → → across image

10. Sparse Representations

Definition:

Sparse representations encourage **most neuron activations to be zero or near zero**, allowing only a few neurons to be active at a time.

Key Points:

1. Improves computational efficiency.
2. Enhances generalization.
3. Often enforced using **L1 regularization**.
4. Common in **sparse autoencoders**.

Example:

- Sparse coding of image patches where only a few features represent each patch.

Diagram Explanation:

- Dense activation: many neurons active.
- Sparse activation: few neurons active.

Dense: [11111]

Sparse: [00100]

11. Bagging and Ensemble Methods

Definition:

Bagging (Bootstrap Aggregating) and ensemble methods combine the predictions of **multiple models** to produce a more accurate and stable final prediction.

KeyPoints:

1. Reduces **variance** of predictions.
2. Improves robustness and generalization.
3. Each model is trained on a different **bootstrap sample** of data.
4. Final output is obtained by **averaging or voting**.

Example:

- **Random Forest:** An ensemble of decision trees trained on different subsets of data and features.

Diagram Explanation:

- Multiple models make predictions.
- Predictions are aggregated to produce the final output.

Model 1 →
 Model 2 → Aggregation → Final Output Model 3

→

12. Dropout

Definition:

Dropout is a regularization technique where **random neurons are temporarily removed during training**, forcing the network to learn robust features.

KeyPoints:

1. Prevents **co-adaptation** of neurons.
2. Acts like training **many subnetworks**.
3. Controlled by **dropout probability (p)**.
4. Used only during training, not testing.

Example:

- Applying dropout to fully connected layers in a neural network.

Diagram Explanation:

- Some neurons are randomly removed during training.

OOO

\x/

OOO

D.SAISHIREESHA

DEEPEARNING

(X=droppedneuron)

13. Adversarial Training

Definition:

Adversarial training improves model robustness by **training on adversarial examples**, which are inputs slightly modified to fool the model.

Key Points:

1. Small perturbations added to inputs maximize loss.
2. Improves resistance to adversarial attacks.
3. Enhances model robustness and security.

Example:

- **FGSM (Fast Gradient Sign Method):** Adds perturbations in the direction of the gradient.

Diagram Explanation:

- Original image and adversarial image appear similar but cause different predictions.

Original Image → Correct Prediction
Adversarial Image → Wrong Prediction

14. Tangent Distance & Manifold Methods

Definition:

These methods capture **invariances along the data manifold**, allowing the model to ignore small transformations such as rotation or translation.

Key Points:

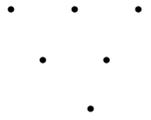
1. **Tangent Distance:** Measures similarity invariant to small transformations.
2. **Tangent Propagation:** Penalizes sensitivity along manifold directions.
3. Improves invariance and generalization.

Example:

- Handwritten digits that are rotated or shifted but represent the same number.

DiagramExplanation:

- Datapoints lie on a smooth curved manifold.



(Manifold)

PART B: Optimization for Deep Learning

15. Pure Optimization

Definition:

Pure optimization focuses solely on **minimizing the loss function**, without considering statistical or generalization properties.

Key Points:

1. Uses **gradient descent** and its variants.
2. Includes **second-order methods** like Newton's method.
3. Concerned only with finding minima.

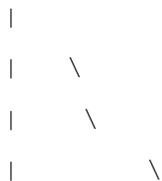
Example:

- Minimizing mean squared error in **linear regression**.

Diagram Explanation:

- Optimization moves downhill on the loss surface toward minimum.

Loss



+----->Parameters

16. Optimization Challenges

Definition:

Optimization challenges arise because **neural network loss surfaces are highly non-convex**, making training difficult and unstable.

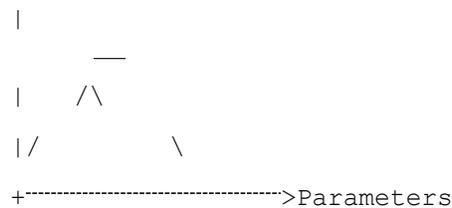
KeyPoints:

1. **Vanishinggradients:**Gradientsbecomeverysmall,slowing learningindeepnetworks.
2. **Explodinggradients:**Gradientsgrowtoolarge, causingunstableupdates.
3. **Saddlepoints:**Flatregionswheregradientsarenearzerobutnotminima.
4. **Localminima:** Optimizationmayconvergetosub-optimalsolutions.

DiagramExplanation:

- Losssurfaceshowsvalleys,peaks, andsaddlepointswhereoptimizationslows.

Loss



17. BasicOptimizationAlgorithms

Definition:

Basicoptimizationalgorithmsare**gradient-basedmethods**usedto minimizethelossfunction during training.

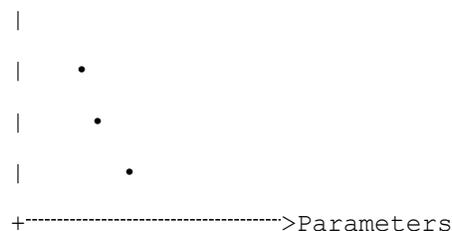
KeyPoints:

1. **BatchGradientDescent:**Usesentiredataset perupdate(slowbutstable).
2. **StochasticGradientDescent(SGD):**Updatesusingonesampleat a time(fast but noisy).
3. **Mini-batchGradientDescent:**Uses smallbatches;mostcommonlyused.

DiagramExplanation:

- Optimizationstepsmovedownhilltoward minimum.

Loss



18. ParameterInitialization

Definition:

Parameter initialization is the process of choosing **initial weight values** before training begins.

KeyPoints:

1. **Zeroinitializationfails:** Causesneuronstolearnidentical features.
2. **XavierInitialization:** Suitablefortanhorsigmoidactivations.
3. **HeInitialization:** Designed forReLUactivations.
4. Helpsprevent vanishingorexplodinggradients.

DiagramExplanation:

- Properinitializationmaintainsbalancedsignalflowacrosslayers.

Input→Layer1→Layer2→Output (Stable weight flow)

19. AdaptiveLearningRateAlgorithms

Definition:

Adaptivelearningratealgorithms**automaticallyadjustlearningrates**duringtrainingforfaster convergence.

KeyPoints:

1. **AdaGrad:** Adaptslearningrateperparameter.
2. **RMSProp:** FixesAdaGrad'saggressivedecay.
3. **Adam:** Combines momentumand RMSProp.
4. Providesfasterandmorestableconvergence.

DiagramExplanation:

- Learningratedecreasessmoothlyoveriterations.

LearningRate

|

| \

| \

| \

+----->Iterations

20. ApproximateSecond-OrderMethods

Definition:

Approximatesecond-ordermethodsuse**curvature(secondderivative)information** toimprove optimization efficiency.

KeyPoints:

1. **Newton's Method:** Uses Hessian matrix.
2. **Quasi-Newton Methods:** Approximate Hessian (e.g., BFGS).
3. Faster convergence but **computationally expensive**.
4. Rarely used for very deep networks.

Diagram Explanation:

- Curvature information helps take smarter steps toward minimum.

Loss Curve

|
|/\

+-----> Parameters

21. Optimization Strategies & Meta-Algorithms

Definition:

Optimization strategies and meta-algorithms enhance **convergence speed and training stability**.

KeyPoints:

1. **Momentum:** Accelerates learning in correct direction.
2. **Nesterov Accelerated Gradient:** Looks ahead before updating.
3. **Gradient clipping:** Prevents exploding gradients.
4. **Learning rate schedules:** Reduce learning rate over time.

Diagram Explanation:

- Momentum smooths optimization path compared to standard GD.

Standard GD: zig-zag path

Momentum: smooth curved path



UNIT-IV

Convolution Networks: The Convolution Operation, Pooling, Convolution, Basic Convolution Functions, Structured Outputs, Data Types, Efficient Convolution Algorithms, Random or Unsupervised Features, Basis for Convolution Networks.

1. Basis for Convolutional Networks

Definition:

CNNs are specialized deep neural networks for **grid-structured data** like images, video, and audio. They exploit spatial, temporal, or volumetric structure to reduce parameters and improve learning efficiency.

Key Principles:

1. **Sparse Connectivity (Local Receptive Fields)**
 - Each neuron connects only to a **small local region** in the input.
 - **Example:** In a 32×32 image, a 5×5 kernel connects to only 25 pixels at a time.
 - Captures **local features** like edges or corners.
 - Reduces parameters \rightarrow lowers computational cost and memory usage.
2. **Parameter Sharing (Weight Reuse)**
 - The same kernel/filter is applied across different input locations.
 - Ensure **translation invariance**: patterns are recognized regardless of location.
 - Reduces parameters drastically (e.g., $5 \times 5 \times 3$ kernel vs $32 \times 32 \times 3$ fully connected layer).
3. **Translation Equivariance**
 - Shifting input \rightarrow proportional shift in output feature map.
 - Critical for image and video tasks where objects may move slightly.
4. **Hierarchical Feature Learning**
 - Early layers detect **low-level features** (edges, textures).
 - Middle layers detect **mid-level features** (eyes, noses).
 - Deep layers detect **high-level concepts** (faces, objects).

Applications:

- Image classification, object detection, facial recognition, video understanding.

Example:

- Edge detection using a small filter remains effective regardless of edge position.

Diagram (ASCII)

| InputImage | ConvolutionFilter |
|--------------------------------|------------------------|
| [xxxxx] [www] [xxxxx] [www] | [xxxxx] ---> [www] |
| Aspect | FullyConnectedNN CNN |
| ----- | ----- |
| Connectivity Dense | Sparse |
| Parameters VeryHigh | Low |
| SpatialInfo Ignored | Preserved |
| Translation Poor | Excellent |

2. The Convolution Operation (Expanded)

Definition:

Convolution is a **mathematical operation** that combines an input signal (or image) with a kernel (filter) to produce a feature map. In CNNs, convolution is used to **extract local features** from data.

Mathematical Formulation:

- **1D Discrete Convolution:**

$$(f * g)(n) = \sum_m f(m)g(n-m) \quad (f * g)(n) = \sum_m f(m)g(n-m)$$

- **2D Convolution (for images):**

$$S(i,j) = \sum_m \sum_n I(i+m, j+n) \cdot K(m,n) \quad S(i,j) = \sum_m \sum_n I(i+m, j+n) \cdot K(m,n)$$

Where:

- I = input image
- K = convolution kernel
- S = output feature map

Cross-correlation in CNNs:

- CNNs typically use **cross-correlation**, not true convolution:

$$S(i,j) = \sum_m \sum_n I(i+m, j+n) \cdot K(m,n) \quad S(i,j) = \sum_m \sum_n I(i+m, j+n) \cdot K(m,n)$$

Kernel is not flipped, simplifies computation, same learning effect

Key Concepts:

1. **Receptive Field**
 - Area of input that a neuron “sees”
 - Larger kernels → larger receptive field
 - Deeper networks → larger effective receptive field
2. **Stride**
 - Determines step size of kernel
 - Larger stride → smaller feature map, less computation, but may miss fine details
3. **Padding**
 - Zero-padding maintains output dimensions
 - Types: **Valid padding** (no padding), **Same padding** (output size = input size)

Examples:

- Edge Detection: Vertical or horizontal edge detection filters highlight patterns in images.
- Smoothing: Average filter reduces noise.
- Sharpening: Kernel emphasizes transitions in pixel intensity.

Diagram (ASCII):

| Input Patch (3x3) | * | Filter (3x3) |
|-------------------|---|--------------|
| [123] | | [10-1] |
| [456] | * | [10-1] |
| [789] | | [10-1] |

Output = sum of element-wise products

Applications:

- Image processing: Edge detection, blur, sharpening
- Feature extraction in CNNs
- Audio processing (1D convolution)

Table: Convolution Parameters

| Parameter | Description | Effect |
|-------------------|---------------------------|------------------------------|
| KernelSize | Dimensionsofthe filter | Determinesreceptive field |
| Stride | Stepsizeforkernelmovement | Controlsoutputsize |
| Padding | Zero-padding ofinput | Maintainsoutputsize |
| Number of Filters | Number of kernels | Determinesdepthoffeature map |

3. ConvolutioninCNNs(Expanded)**Definition:**

InCNNs,convolutionlayersapplymultiple **learnedfilter**stoinputstoproduce**featuremaps**, capturing hierarchical patterns in the data.

KeyDetails:

1. **Multi-channelInputs**
 - RGBimages:kernelspansall3 channels
 - Eachfilterproducess**singlefeaturemap**
 - Multiple filters→ multi-channelfeaturemaps
2. **HierarchicalFeatureLearning**
 - **Shallowlayers**:Detectedges,corners,textures
 - **Intermediatelayers**:Detectmotifs,objectparts
 - **Deeplayes**:Detectcomplexobjects(faces,vehicles)
3. **Strideand PaddinginCNNs**
 - Stridereducescomputationalloadand featuremapsize
 - Paddingpreventsshinkingoffeaturemapsafter convolution
4. **ParameterEfficiency**
 - Convolutionuses **weight sharing**→fewerparametersthanfullyconnected layers
 - Reducesoverfitting

Example:

- Facedetection:
 - Earlylayers→horizontal/verticaledges
 - Middle layers→eyes,nose,mouth
 - Finallayers→completefacerepresentation

Diagram(ASCII):

Input Image (RGB)

↓
ConvolutionFilters (3x3) applied

↓
FeatureMaps (MultipleChannels)

Applications:

- Imageclassification
- Object detection
- Sceneunderstanding

Table:Convolution LayerParameters

| Parameter | Description | Example |
|------------|------------------------|------------------------|
| Filters | Numberoflearnedkernels | 32filtersforfirstlayer |
| KernelSize | Size ofeachkernel | 3x3,5x5 |
| Stride | Stepsizeofconvolution | 1,2 |
| Padding | Zero-padding method | Same,Valid |

4. BasicConvolutionFunctions(Expanded)

Definition:

- CNNsuse**1D, 2D, or3Dconvolutions** dependingoninput type.
- ThesefunctionsallowCNNstohandlesequential,spatial,andspatiotemporaldata.

Typesof Convolution:

- 1DConvolution**
 - Input:Sequentialdata
 - Example:Audiowaveform
 - Capture**temporalcorrelations**
- 2DConvolution**
 - Input:Images(height×width)
 - Example:MNISTdigit classification
 - Capture**spatialfeatures**likeedgesandtextures
- 3DConvolution**
 - Input:Videoframesorvolumetricdata
 - Example:Actionrecognitioninvideosequences
 - Capture**spatiotemporaldependen**

cies Extended Concepts:

- **DepthwiseConvolution:**
 - Separateconvolutionper channel→ reducescomputation
 - UsedinMobileNet
- **SeparableConvolution:**
 - Factorizesconvolutionintodepthwise+pointwise
 - Reducesparameterswhilemaintaining performance

Examples:

- 1D:Heartbeatanomalydetection
- 2D:Dogvscatimageclassification
- 3D:Predictinghumanmotionfromvideoframes

Diagram(ASCII):

```

1D: [x1x2x3x4x5] 2D: [
x11 x12 x13 ]
      [x21x22x23]
3D: [x111x112x113] (time/depth)

```

Table:Convolution Types

| Type | Input | CNN Function | Application |
|------|-------|--------------|-------------------|
| 1D | Audio | 1DConv | Speechrecognition |
| 2D | Image | 2DConv | Classification |
| 3D | Video | 3DConv | Actionrecognition |

5. Pooling(Expanded)

Definition:

- Poolingreducesspatialsizeoffeaturemapswhileretaining**important features**.
- Provides**translationinvariance** andreducescomputation.

PoolingTypes:

1. **Max Pooling**
 - Selects maximumvalueineachregion
 - Preservesstrongestfeature
 - Commoninimagerecognition
2. **AveragePooling**
 - Computesaveragevalueineachregion
 - Smoothsfeaturemaps

3. Global Pooling

- Reduces entire feature map to a single value per channel
- Often used before fully connected layers

Key Concepts:

- **Stride and Pool Size:**
 - Pooling window size (2x2, 3x3) determines the downsampling factor
 - Stride controls movement of pooling window
- **Effect on Feature Maps:**
 - Reduces overfitting
 - Reduces computational load
 - Slight loss of spatial resolution

Example:

- In CIFAR-10 classification, 2x2 max pooling reduces feature map from 32x32 → 16x16, retaining key features.

Diagram (ASCII):

```

Input Feature Map (4x4)      2x2 Max Pooling
[1 3 2 1]                    [3 4]
[4 6 5 2]                    [8 9]
[7 2 8 3]                    ----->
[1 4 9 0]

```

Table: Pooling Comparison

| Type | Operation | Effect | Use Case |
|---------|-----------------|------------------------------|----------------------------------|
| Max | Max value | Retains strongest activation | Classification, object detection |
| Average | Mean | Smooths features | Less common, regression |
| Global | Mean/Max of all | Single vector | Fully connected layers input |

Applications:

- Image classification (MNIST, CIFAR-10)
- Object detection (YOLO, SSD)
- Reducing memory and computation in deep CNNs

6. Structured Outputs

Definition:

Structured outputs in CNNs are **outputs that preserve the spatial or temporal structure** of the

input, instead of collapsing it into a single scalar or class label. This is crucial for tasks where every element (pixel, time-step, voxel) requires a prediction.

Key Concepts:

1. **Fully Convolutional Networks (FCNs)**
 - Replace fully connected layers with convolutional layers.
 - Maintain **spatial correspondence** between input and output.
 - Can handle **arbitrary-sized inputs**.
2. **Applications of Structured Outputs:**
 - **Semantic Segmentation:** Pixel-level classification (e.g., labeling roads, cars, pedestrians in self-driving datasets).
 - **Depth Estimation:** Predict depth for each pixel in an image.
 - **Heatmap Prediction:** Locate objects or keypoints (e.g., facial landmarks).
 - **Object Detection/Localization:** Predict bounding boxes or probability maps.
3. **Techniques for Maintaining Resolution:**
 - **Upsampling/Transposed Convolution:** Increases feature map size to match input.
 - **Skip Connections:** Combines high-level semantic information with low-level spatial details.
 - **Dilated Convolutions:** Expands receptive field without losing resolution.

Example:

- In medical imaging, a CNN with structured output identifies tumor regions **pixel-by-pixel**, instead of just classifying the image as “tumor” or “no tumor.”

Diagram (ASCII):

```

Input Image (HxW)
    ↓
Conv+Pool Layers → Feature Maps
    ↓
Upsampling/Transposed Conv
    ↓
Pixel-wise Output Map (HxW)

```

Table: Structured vs Scalar Output

| Output Type | Description | Example |
|-------------|-----------------------------|---|
| Scalar | Single label | Image classification |
| Vector | Multiple labels | Multi-label classification |
| Structured | Pixel-wise or sequence-wise | Semantic segmentation, video prediction |

Importance:

- Maintains **spatial dependencies**.
- Enables **dense prediction tasks** that are essential for robotics, autonomous driving, and medical imaging.

7. Data Types in Convolutional Networks

Definition:

CNNs are designed to handle **grid-structured data**, which can be 1D, 2D, or 3D depending on the application.

Key Concepts:

- 1D Data:**
 - Examples: Audio signals, time-series data, sensor readings.
 - Processed using **1D convolution** along the temporal axis.
 - Captures local temporal correlations.
- 2D Data:**
 - Examples: Images (height × width).
 - Processed using **2D convolution** (spatial filters).
 - Captures edges, corners, textures, and patterns.
- 3D Data:**
 - Examples: Video (height × width × time), volumetric MRI/CT scans.
 - Processed using **3D convolution** (spatiotemporal or volumetric filters).
 - Captures movement patterns, depth features, and spatial-temporal correlations.
- Mini-Batching:**
 - Inputs are processed in **batches** for computational efficiency.
 - Standard tensor format: (batch_size, channels, height, width) for 2D,
(batch_size, channels, depth, height, width) for 3D.

Example:

- Video action recognition uses 3D convolution to capture motion across frames.
- ECG signal classification uses 1D convolution along the time axis.

Diagram (ASCII):

```

1D: [x1x2x3x4x5]  2D: [
x11 x12 x13 ]
      [x21x22x23]
3D: [x111x112x113] (time/depth)

```

Table: Data Types and Applications

| Data Type | Dimensionality | CNN Type | Application |
|-----------|----------------|----------------|--|
| Audio | 1D | 1D Convolution | Speech recognition, ECG analysis |
| Image | 2D | 2D Convolution | Object detection, image classification |
| Video | 3D | 3D Convolution | Action recognition, medical imaging |

Importance:

- Understanding the **datatype** ensures correct convolution design and architecture choice.
- Enables CNNs to adapt to **varied real-world inputs** across domains.

8. Efficient Convolution Algorithms

Definition:

Convolutions are computationally intensive, especially for **deep networks and large inputs**. Efficient algorithms accelerate training and inference.

Key Techniques:

- 1. Naive Convolution:**
 - Direct computation → high computational cost.
 - Suitable only for small datasets or prototypes.
- 2. im2col Transformation:**
 - Converts convolution into **matrix multiplication**.
 - Allows highly optimized GPU linear algebra libraries (BLAS).
 - Widely used in modern CNN frameworks.
- 3. FFT-based Convolution:**
 - Applies **Fast Fourier Transform** to input and kernel.
 - Reduces computational complexity for **large kernels**.
 - Less efficient for small kernels (3×3) commonly used in CNNs.
- 4. Winograd Algorithm:**
 - Reduces the number of **multiplications** required.
 - Very effective for small kernels ($3 \times 3, 5 \times 5$).
 - Used extensively in **high-performance CNN libraries**.

Example:

- A ResNet50 model with 3×3 convolution layers uses **Winograd algorithm** to reduce GPU computation.

Table: Efficient Convolution Methods

| Method | Description | Best UseCase |
|----------|------------------------------------|---------------------|
| Naive | Direct convolution | Small networks |
| im2col | Transform to matrix multiplication | GPU acceleration |
| FFT | Convolution in frequency domain | Large kernels |
| Winograd | Reduce multiplications | Small kernels (3x3) |

Importance:

- Allows **real-time inference** in image/video applications.
- Enables **deeper CNNs** to be trained on large datasets.

9. Random or Unsupervised Features

Definition:

- Random or unsupervised features are **learned without explicit labels**.
- Useful when labeled data is scarce or unavailable.

Key Points:

- 1. Random Filters:**
 - Initial layers with **random weights** can capture basic patterns (edges, textures).
 - Surprisingly effective due to natural statistics of images.
- 2. Unsupervised Feature Learning:**
 - Techniques: Autoencoders, Sparse coding, K-means clustering.
 - Learn **filters** from data distribution instead of labels.
 - Can pretrain CNN layers, followed by supervised fine-tuning.
- 3. Comparison with Supervised Learning:**
 - Supervised learning generally outperforms unsupervised methods on large labeled datasets.
 - Unsupervised pretraining is useful for **representation learning** when labels are limited.

Example:

- Autoencoder trained on unlabeled images produces Gabor-like filters in early layers.

Table: Feature Learning Methods

| Method | Labels Required | Performance | Example |
|--------|-----------------|-------------|---------------------|
| Random | No | Limited | Random edge filters |

| Method | LabelsRequired | Performance | Example |
|---------------|-----------------------|--------------------|----------------------------------|
| Unsupervised | No | Moderate | Autoencoderforfeature extraction |
| Supervised | Yes | Best | CNNclassification |

Importance:

- Supports**semi-supervisedlearning,pretraining,**andunderstanding**statistical properties** of natural images.
- Basisfor**transferlearning**indeepCNNs.

Unit-5

Sequence Modelling: Recurrent and Recursive Neural Networks

Sequence Modelling: Recurrent and Recursive Nets: Unfolding Computational Graphs, Recurrent Neural Networks, Bidirectional RNNs, Encoder-Decoder Sequence-to-Sequence Architectures, Deep Recurrent Networks, Recursive Neural Networks, Echo State Networks, LSTM, Gated RNNs, Optimization for Long-Term Dependencies, Auto encoders, Deep Generative Model

Introduction

Sequence modelling refers to learning from data where the **order of inputs matters**. In many real-world problems, the current output depends not only on the current input but also on **previous inputs**. Examples include natural language sentences, speech signals, and time-series data. To handle such data, **Recurrent Neural Networks (RNNs)** and **Recursive Neural Networks** are used.

1. Recurrent Neural Networks (RNNs)

Definition

A Recurrent Neural Network is a neural network designed to process **sequential data** by maintaining a **hidden state** that stores information from previous time steps.

Working Principle

At each time step:

- The network takes the current input
- Combines it with the previous hidden state
- Produces a new hidden state and

$$\text{output}_t = f(Wx_t + Uh_{t-1} + b) \quad h_t = f(Wx_t + Uh_{t-1} + b)$$

$$h_t = f(Wx_t + Uh_{t-1} + b)$$

Here, the same weights are **shared across all time steps**, enabling the model to remember past information.

Characteristics

- Has feedback connections

- Maintains memory through hidden state
- Handles variable-length sequences

Advantages

- Suitable for sequential data
- Parameter sharing reduces complexity

Limitations

- Suffers from vanishing and exploding gradients
- Poor at learning long-term dependencies

Applications

- Language modeling
- Speech recognition
- Time-series prediction

2. Recursive Neural Networks

Definition

Recursive Neural Networks are neural networks that operate on **hierarchical or tree-structured data** instead of linear sequences.

Working Principle

- The same neural network is applied **recursively** to smaller parts of a structure
- Parent node representations are computed from child node representations
- Weight sharing occurs across all tree nodes

Characteristics

- Works on tree structures
- Captures hierarchical relationships
- Uses recursive composition

Advantages

- Effective for structured data
- Models syntactic and semantic relationships

Limitations

- Requires predefined tree structure
- Computationally complex

Applications

- Sentence parsing
- Sentiment analysis
- Natural language understanding

Comparison Between Recurrent and Recursive Neural Networks

| Aspect | Recurrent NN | Recursive NN |
|--------------|--------------|--------------------|
| Data Type | Sequential | Tree-structured |
| Processing | Time-based | Hierarchical |
| Memory | Hidden state | Node composition |
| Applications | Speech, text | Parsing, sentiment |

Unfolding Computational Graphs

Introduction

Unfolding computational graphs is a technique used in **Recurrent Neural Networks (RNNs)** to represent their behavior over time. Since RNNs process sequential data using the same network repeatedly, unfolding helps visualize and understand how the network operates across multiple time steps.

Concept of Unfolding

In an RNN, the same set of weights is applied at every time step. Unfolding converts this cyclic structure into **a linear chain of identical network copies**, one for each time step in the sequence.

Each copy represents the network at a particular time step, while sharing the same parameters.

Working Principle

- The input sequence is fed step by step into the RNN
- Each time step produces a hidden state
- When unfolded, the RNN becomes a deep feed-forward network. The depth of the network equals the length of the input sequence

This unfolded representation allows the network to track how information flows through time.

Mathematical Representation

For each timestep t :

$h_t = f(Wx_t + Uh_{t-1} + b)$ Here:

- x_t = input at time t
- h_t = hidden state
- W, U, b = shared parameters

Role in Training

Unfolding is essential for training RNNs using **Backpropagation Through Time (BPTT)**.

Backpropagation Through Time

- Error is computed at each timestep
- Gradients are propagated backward through the unfolded network
- Weights are updated based on accumulated gradients

Advantages of Unfolding

- Makes RNN computation understandable
- Enables gradient calculation
- Helps analyze temporal dependencies

Limitations

- Long sequences increase computational cost
- Causes vanishing and exploding gradient problems
- Requires large memory for long sequences

Application

- Language modeling
- Speech recognition
- Time-series prediction

Recurrent Neural Networks (RNNs)

Introduction

Recurrent Neural Networks (RNNs) are a class of neural networks specially designed to process **sequential and time-dependent data**. Unlike feed-forward neural networks, RNNs have **recurrent connections** that allow information to persist across time steps, enabling the network to capture temporal dependencies.

Definition

A Recurrent Neural Network is a neural network in which the output from the previous time step is fed back as input to the network, allowing it to maintain a **hidden state (memory)**.

Architecture

An RNN consists of:

- Input layer
- Hidden layer with recurrent connections
- Output layer

The hidden layer stores information from past inputs and passes it forward in time.

Working Principle

At each time step t :

- The current input x_t and previous hidden state h_{t-1} are combined
- A new hidden state h_t is produced
- Output is generated based on h_t

$h_t = f(Wx_t + Uh_{t-1} + b)$ Here:

- W, U, b are weight matrices
- b is bias
- f is an activation function

These weights are **shared across all time steps**.

Unfolding in Time

When unfolded, an RNN becomes a **deep feed-forward network** with one layer per time step. This representation is used during training.

Training of RNNs

RNNs are trained using **Backpropagation Through Time (BPTT)**, where:

- Error is calculated at each timestep
- Gradients are propagated backward through the unfolded network
- Weights are updated accordingly

Advantages

- Suitable for sequential data
- Handles variable-length inputs
- Parameter sharing reduces model size

Limitations

- Vanishing and exploding gradient problems
- Difficulty in learning long-term dependencies
- Training is computationally expensive

Applications

- Language modeling and text generation
- Speech recognition
- Time-series forecasting
- Sentiment analysis

Bidirectional Recurrent Neural Networks

Introduction

Bidirectional Recurrent Neural Networks (Bidirectional RNNs) are an extension of standard RNNs that improve sequence modelling by processing data in **both forward and backward directions**. In many sequence problems, the prediction at a particular timestep depends not only on past inputs but also on **future context**. Bidirectional RNNs are designed to capture this complete context.

Definition

A Bidirectional RNN is a recurrent neural network that consists of **two separate RNN layers**: one that processes the sequence from left to right (forward direction) and another that processes it from right to left (backward direction).

Architecture

The architecture of a Bidirectional RNN includes:

- **Forward RNN**: processes input sequence from $t=1$ to $t=T$
- **Backward RNN**: processes input sequence from $t=T$ to $t=1$
- **Output layer**: combines outputs from both directions

The hidden states from both directions are concatenated or summed to produce the final output.

Working Principle

At each time step t :

- Forward hidden state captures information from past inputs
- Backward hidden state captures information from future inputs
- Combined hidden state provides richer contextual representation

$h_t = [h_{t \rightarrow}, h_{t \leftarrow}]$

Training of Bidirectional RNNs

Bidirectional RNNs are trained using **Backpropagation Through Time (BPTT)** in both forward and backward directions. The same principles of RNN training apply, but with increased computational cost.

Advantages

- Captures both past and future context
- Improves prediction accuracy
- Effective for complex sequence tasks

Limitations

- Cannot be used for real-time or online prediction
- Requires complete input sequence
- Higher computational and memory cost

Applications

- Speech recognition
- Handwriting recognition
- Named entity recognition
- Part-of-speech tagging

Encoder–Decoder Sequence-to-Sequence Architectures

Introduction

Encoder–Decoder Sequence-to-Sequence (Seq2Seq) architectures are designed to map an **input sequence to an output sequence**, even when the input and output lengths are different. These models are widely used in tasks such as machine translation, speech recognition, and text summarization, where one sequence needs to be transformed into another.

Definition

A Seq2Seq model consists of two main components:

- **Encoder:** converts the input sequence into a fixed-length representation
- **Decoder:** generates the output sequence from this representation

Both encoder and decoder are usually implemented using **RNNs, LSTMs, or GRUs**.

Architecture

1. **Encoder**
 - Reads the input sequence one element at a time
 - Updates its hidden state at each time step
 - Final hidden state represents the entire input sequence (called context vector)
2. **Decoder**
 - Takes the context vector as input
 - Generates the output sequence step by step
 - Uses its previous output as input for the next step

Working Principle

- The encoder processes the input sequence and produces a **context vector**
- The decoder uses this context vector to predict the output sequence
- At each decoding step, the decoder predicts one output token

Mathematically:

$$h_t = f(Wx_t + Uh_{t-1}) \quad h_t = f(Wx_t + Uh_{t-1})$$

Training of Seq2Seq Models

- Trained using **Backpropagation Through Time (BPTT)**
- Use **teacher forcing**, where the actual output is given as input during training
- Loss is computed over the entire output sequence

Advantages

- Handles variable-length input and output sequences
- Flexible and powerful
- Suitable for many sequence transformation tasks

Limitations

- Fixed-length context vector can cause information loss
- Performance degrades for long sequences
- Computationally expensive

Attention Mechanism (Improvement)

To overcome the fixed-length context limitation, the **attention mechanism** allows the decoder to focus on relevant parts of the input sequence at each time step, improving performance significantly.

Applications

- Machine translation
- Text summarization
- Chatbots
- Speech-to-text system

Conclusion

Encoder–Decoder Seq2Seq architectures provide a powerful framework for sequence transformation problems. With improvements like attention mechanisms, they form the foundation of modern natural language processing systems.

Deep Recurrent Networks

Introduction

Deep Recurrent Networks are an extension of standard Recurrent Neural Networks in which **multiple recurrent layers are stacked on top of each other**. While a single-layer RNN can model simple temporal dependencies, deep RNNs are capable of learning **complex and hierarchical temporal patterns** present in sequential data.

Definition

A Deep Recurrent Network is a recurrent neural network that contains **more than one hidden recurrent layer**, where the output of one recurrent layer is fed as input to the next recurrent layer.

Architecture

- Consists of **input layer, multiple recurrent hidden layers, and an output layer**
- Each recurrent layer maintains its own hidden state
- The hidden state of a lower layer at time t is passed to the next layer at the same time step. This

stacking increases the depth of the network **in both time and space**.

Working Principle

At each time step:

1. Input is processed by the first recurrent layer
2. The output of this layer is passed to the next recurrent layer
3. This process continues through all layers
4. Final layer produces the output

Mathematically:

$$h_t^{(l)} = f(W^{(l)}h_{t-1}^{(l)} + U^{(l)}h_{t-1}^{(l-1)}) \quad h_t^{(l)} = f(W^{(l)}h_{t-1}^{(l)} + U^{(l)}h_{t-1}^{(l-1)})$$

Where l denotes the layer number.

Training of Deep RNNs

- Trained using **Backpropagation Through Time (BPTT)**
- Gradients are propagated through **multiple layers and time steps**
- Often combined with LSTM or GRU units to improve learning stability

Advantages

- Learn high-level and abstract temporal features

- Better performance on complex sequence tasks
- Higher representational power

Limitations

- Computationally expensive
- Difficult to train due to vanishing gradients
- Requires large datasets

Applications

- Speech recognition
- Language modeling
- Machine translation
- Audio signal processing

Recursive Neural Networks

Introduction

Recursive Neural Networks are a class of neural networks designed to process **hierarchical or structured data** rather than linear sequences. Unlike Recurrent Neural Networks, which operate over time steps, Recursive Neural Networks work on **tree-structured representations**, making them suitable for modeling data with inherent hierarchical relationships such as natural language syntax trees.

Definition

A Recursive Neural Network is a neural network that applies the **same set of weights recursively** over a structured input, typically represented as a tree, to compute representations for parent nodes from their child nodes.

Architecture

- Input data is represented as a **tree structure**
- Leaf nodes represent basic input units (words or features)
- Internal nodes represent compositions of child nodes
- The same neural network is used at every node in the tree

This weight sharing enables the model to generalize across different structures.

Working Principle

- The network starts computation from the **leaf nodes**
- Child node representations are combined using a neural function
- This process continues recursively until the root node is formed
- The root representation captures the meaning of the entire structure

Mathematically:

$$h_{\text{parent}} = f(W[h_{\text{child1}}, h_{\text{child2}}] + b)$$

$$h_{\text{parent}} = f(W[h_{\text{child1}}, h_{\text{child2}}] + b)$$

Training of Recursive Neural Networks

- Trained using **Backpropagation Through Structure (BPTS)**
- Errors are propagated from the root node to leaf nodes
- Requires known tree structures during training

Advantages

- Effectively model hierarchical relationships
- Suitable for structured and compositional data
- Capture syntactic and semantic information

Limitations

- Requires predefined tree structures
- Computationally expensive
- Difficult to scale to large datasets

Applications

- Sentence parsing
- Sentiment analysis
- Natural language understanding
- Semantic relationship modeling

Echo State Networks

Introduction

Echo State Networks (ESNs) are a special type of **Recurrent Neural Network (RNN)** designed to simplify training while still capturing temporal dependencies in sequential data. Unlike

traditional RNNs, ESNs use a large, fixed recurrent layer called a **reservoir**, which eliminates the need to train recurrent connections.

Definition

An Echo State Network is a recurrent neural network in which the **recurrent weights are randomly initialized and kept fixed**, and **only the output layer weights are trained**.

Architecture

An ESN consists of three main components:

1. **Input Layer**—feeds input signals into the reservoir
2. **Reservoir**—a large, sparsely connected recurrent network with fixed weights
3. **Output Layer**—trained using supervised learning

The reservoir acts as a dynamic memory that transforms the input into a high-dimensional representation.

Working Principle

- Input signals are projected into the reservoir
- The reservoir creates rich, dynamic internal states
- These states are combined linearly at the output layer to generate predictions

State update equation:

$$x(t) = f(W_{in}u(t) + Wx(t-1)) \quad x(t) = f(W_{in}\{u(t)\} + Wx(t-1)) \quad x(t) = f(W_{in}u(t) + Wx(t-1)) \quad \text{Where:}$$

- $u(t)$ $u(t)$ $u(t)$ is input
- $x(t)$ $x(t)$ $x(t)$ is reservoir state
- W_{in} W_{in} W_{in} , W W W are fixed weight matrices

Echo State Property

The **echo state property** ensures that:

- The influence of initial states fades over time
- The reservoir state depends mainly on recent inputs

This property is achieved by controlling the **spectral radius** of the reservoir weight matrix.

Training of ESNs

- Only output weights are trained
- Training is fast and efficient
- Typically uses linear regression or ridge regression

Advantages

- Very fast training
- Avoids vanishing and exploding gradients
- Simple and stable learning

Limitations

- Performance depends on reservoir design
- Not optimal for all tasks
- Limited adaptability since reservoir is fixed

Applications

- Time-series prediction
- Speech recognition
- Signal processing
- Control systems

Long Short-Term Memory (LSTM)

Introduction

Long Short-Term Memory (LSTM) is a special type of **Recurrent Neural Network (RNN)** developed to overcome the **long-term dependency problem** faced by traditional RNNs. Standard RNNs struggle to learn information over long sequences due to the **vanishing gradient problem**. LSTM addresses this issue by introducing a memory cell and gating mechanisms that control information flow.

Definition

An LSTM is a recurrent neural network architecture that uses a **memory cell and three gates** to selectively remember, update, and output information over long periods of time.

Architecture

An LSTM unit consists of:

1. **CellState (CtC_tCt)**–stores long-term information
2. **ForgetGate (ftf_tft)** –decides what information to discard
3. **InputGate (iti_tit)** –decides what new information to store
4. **OutputGate (oto_tot)**–decides what information to output

These gates use **sigmoid** and **tanh** activation functions.

Working Principle

At each time step t :

ForgetGate

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f)$$

InputGate and Candidate Memory

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i)$$

$$\tilde{C}_t = \tanh(W_c[h_{t-1}, x_t] + b_c)$$

CellState Update

$$C_t = f_t \cdot C_{t-1} + i_t \cdot \tilde{C}_t$$

OutputGate

$$o_t = \sigma(W_o[h_{t-1}, x_t] + b_o)$$

$$h_t = o_t \cdot \tanh(C_t)$$

Training of LSTM

- Trained using **Backpropagation Through Time (BPTT)**
- Gates help maintain stable gradients
- Learns long-term dependencies effectively

Advantages

- Solves vanishing gradient problem
- Captures long-term dependencies
- Stable and powerful sequence learning

Limitations

- Complex architecture
- High computational cost
- Requires more memory

Applications

- Speech recognition
- Machine translation
- Text generation
- Time-series forecasting

Gated Recurrent Neural Networks (GRUs)

Introduction

Gated Recurrent Neural Networks are an improved form of **Recurrent Neural Networks (RNNs)** designed to overcome the **vanishing gradient problem** and to better capture **long-term dependencies** in sequential data. By using gating mechanisms, Gated RNNs control the flow of information through the network.

Definition

A Gated Recurrent Neural Network is a recurrent neural network that uses **gates** to regulate how much past information is retained and how much new information is added at each time step. The most common gated RNN is the **Gated Recurrent Unit (GRU)**.

Architecture

A GRU consists of two main gates:

1. **Update Gate (z_t)** – decides how much past information to keep
2. **Reset Gate (r_t)** – decides how much past information to forget

Unlike LSTM, GRU does **not** have a separate memory cell, making it simpler.

Working Principle

At each time step t :

Update Gate

$$z_t = \sigma(W_z[h_{t-1}, x_t] + b_z)$$

Reset Gate

$$r_t = \sigma(W_r[h_{t-1}, x_t] + b_r) \quad \tilde{h}_t = \tanh(W_h[r_t \cdot h_{t-1}, x_t] + b_h)$$

CandidateHiddenState

$$\tilde{h}_t = \tanh(W_h[r_t \cdot h_{t-1}, x_t] + b_h)$$

FinalHiddenState

$$h_t = (1 - z_t) \cdot h_{t-1} + z_t \cdot \tilde{h}_t$$

TrainingofGatedRNNs

- Trainedusing**BackpropagationThroughTime(BPTT)**
- Gatesallowgradientstoflow smoothly
- FasterconvergencethantraditionalRNNs

Advantages

- Solvesvanishinggradientproblem
- Fewer parametersthan LSTM
- Fastertrainingand lessmemoryusage

Limitations

- SlightlylessexpressivethanLSTM
- Performancedependson task

Applications

- Textandspeechprocessing
- Machinetranslation
- Time-seriesprediction

OptimizationforLong-TermDependencies

Introduction

Insequence modellingtasks, **long-termdependencies**occurwheninformationfromearliertime steps in a sequence significantly influences outputs at much later time steps. Standard Recurrent Neural Networks (RNNs) face difficulty in learning such dependencies due to optimization

problems during training. Efficient optimization techniques are therefore required to ensure stable learning over long sequences.

Long-Term Dependency Problem

When training RNNs using gradient-based methods, gradients are propagated backward through time. As the sequence length increases:

- Gradients may **shrink exponentially** (vanishing gradient problem)
- Gradients may **grow uncontrollably** (exploding gradient problem)

These issues prevent the network from learning relationships between distant time steps.

Vanishing Gradient Problem

- Gradients become very small
- Early layers or time steps receive almost no updates
- Network fails to learn long-term patterns

Exploding Gradient Problem

- Gradients grow excessively large
- Causes unstable learning
- Leads to numerical overflow

Optimization Techniques for Long-Term Dependencies

1. Gated Architectures (LSTM and GRU)

- LSTM uses **gates and memory cells** to preserve information
- GRU uses **update and reset gates**
- These architectures allow gradients to flow smoothly over long time steps

2. Gradient Clipping

- Gradients are clipped to a fixed range
- Prevents exploding gradients
- Ensures stable training

3. Proper Weight Initialization

- Initializes weights carefully to avoid extreme values
- Helps maintain stable gradients
- Improves convergence

4. Truncated Backpropagation Through Time (TBPTT)

- Backpropagation is limited to a fixed number of time steps
- Reduces computational cost
- Controls gradient instability

5. Use of Better Activation Functions

- ReLU and gated activations reduce gradient decay
- Sigmoid and tanh allow new ways to handle vanishing gradients

6. Regularization and Normalization

- Techniques like dropout and layer normalization
- Improve generalization and stability

Advantages of Optimization Techniques

- Enables learning of long-ranged dependencies
- Improves model stability
- Enhances convergence speed

Applications

- Speech recognition
- Machine translation
- Language modeling
- Time-series forecasting

Autoencoders

Introduction

Autoencoders are a type of **artificial neural network** used for **unsupervised learning**, where the objective is to learn an efficient representation of input data. They work by compressing the input into a lower-dimensional representation and then reconstructing it back to the original form. Autoencoders are widely used for feature learning and dimensionality reduction.

Definition

An autoencoder is a neural network that is trained to **reproduce its input at the output layer** by passing it through a compressed hidden representation.

Architecture

An autoencoder consists of three main parts:

1. **Encoder**—compresses the input data into a latent representation
2. **Latent Space (Bottleneck Layer)**—holds compressed features
3. **Decoder**—reconstructs the original input from the latent representation

The encoder and decoder are usually symmetric.

Working Principle

- Input data is fed into the encoder
- Encoder reduces dimensionality
- Decoder attempts to reconstruct the original input
- The network minimizes reconstruction error

Mathematically:

$$z = f(Wx + b) \quad \hat{x} = g(W'z + b')$$

Where:

- x is input
- z is latent representation
- \hat{x} is reconstructed output

Training of Autoencoders

- Trained using **backpropagation**
- Uses loss functions like **Mean Squared Error (MSE)**
- Does not require labeled data

Types of Autoencoders

1. Undercomplete Autoencoder

- Latent space smaller than input
- Forces feature learning

2. Sparse Autoencoder

- Uses sparsity constraints
- Learns meaningful representations

3. Denoising Autoencoder

- Trained to remove noise from data

4. Variational Autoencoder (VAE)

- Probabilistic generative model
- Used in data generation

Advantages

- Learns features automatically
- Reduces dimensionality
- Works without labeled data

Limitations

- May learn trivial identity mapping
- Requires careful tuning
- Not ideal for supervised tasks

Applications

- Dimensionality reduction
- Noise removal
- Feature extraction
- Anomaly detection

Deep Generative Models

Introduction

Deep Generative Models are a class of deep learning models that learn the **underlying probability distribution of data**. Unlike discriminative models that only make predictions, generative models can **generate new data samples** that are similar to the training data. These models are widely used in image, audio, and text generation tasks.

Definition

A Deep Generative Model is a neural network that learns to model the **data-generating process** and can generate new data samples by sampling from the learned distribution.

Basic Idea

- Learn how data is distributed
- Capture hidden patterns and structure
- Generate realistic news samples

These models are usually trained using **unsupervised** or **semi-supervised learning**.

Types of Deep Generative Models

1. Variational Autoencoders (VAE)

- Encoder maps input to a probability distribution
- Decoder generates data from sampled latent variables
- Uses probabilistic learning

Advantage: Stable training

Limitation: Slightly blurry outputs

2. Generative Adversarial Networks (GANs)

- Consist of two networks: **Generator** and **Discriminator**
- Generator creates faked data
- Discriminator distinguishes real vs faked data
- Trained using adversarial learning

Advantage: High-quality data generation

Limitation: Training instability

3. Autoregressive Models

- Generate data one element at a time
- Each output depends on previous outputs

Examples: PixelRNN, WaveNet

Training of Deep Generative Models

- Uses gradient-based optimization
- Minimizes likelihood or adversarial loss
- Requires large datasets and high computation

Advantages

- Can generate realistic data
- Useful for data augmentation

- Learns complex data distributions

Limitation

- Training can be unstable
- Computationally expensive
- Difficult to evaluate performance

Applications

- Image and video generation
- Speech synthesis
- Data augmentation
- Anomaly detection

