June-2023 [END SEM] [6003] - 544	Solved Paper

Course 2019

Time : $2\frac{1}{2}$ Hours] [Maximum Marks : 70

Instructions to the candidates :

1) *Answer Q.1 or Q.2, Q.3 or Q.4, Q.5 or Q.6, Q.7 or Q.8.*
2) *Neat diagram must be drawn wherever necessary.*
3) *Figures to the right indicate full marks.*
4) *Assume suitable data, if necessary.*

Q.1 **a)** *What is the Hopfield neural network ? What is a state transition diagram for Hopfield neural network ? Explain how to derive it in Hopfield model.* **(Refer Q.2 and Q.3 of Chapter - 3)** **[8]**

b) *Explain the concept of associative learning in artificial neural networks. How is it related to pattern recognition ?*
(Refer Q.1 of Chapter - 3) **[6]**

c) *Explain the architecture of Boltzmann machine.*
(Refer Q.9 of Chapter - 3) **[4]**

OR

Q.2 **a)** *Describe the Boltzmann machine and Boltzmann learning law. What are the limitations of the Boltzmann learning ?*
(Refer Q.9 and Q.10 of Chapter - 3) **[8]**

b) *Write a short note on : i) Stochastic network ii) Simulated annealing.* **[10]**

Ans. : i) Stochastic networks : Stochastic neural networks are a type of Artificial Neural Networks (ANNs) constructed by introducing stochastic components into their architectures that allow the estimation of uncertainty of their predictions.

Stochastic artificial neural network is a Bayesian Neural Network (BNN) that is trained using Bayesian inference.

For BNNs, the network parameters θ are usually considered stochastic and this allows the networks to simulate multiple model parameter configurations according to their associated probability distribution p(θ).

While training a BNN, instead of training one single model, a set of models is trained and their predictions are aggregated into probabilistic distributions. This characteristic avoids problems of overfitting for the neural network and gives access to uncertainty estimates of its predictions.

To design and train a BNN denoted by $y = F_\theta(x)$, the following Bayesian inference process is carried out. Given a training dataset with $X = [x_1, \ldots, x_N]$ as its input variables and $Y = [y_1, \ldots, y_N]$ as their respective target outputs, based on the problem first a proper neural network architecture is chosen (i.e. feed-forward, recurrent, convolutional).

Next step is to choose a prior distribution p(θ) over the model parameters, that describe the prior beliefs about the parameters before analyzing the dataset and a likelihood distribution p(Y|X, θ), that describes a prior confidence in the predictive power of the model F_θ.

Predictive distribution is summarized by a few statistics computed using a Monte Carlo sampling approach. In this approach T samples of θ are sampled from the posterior distribution p(θ|X, Y) and then used to compute statistics of the predictive distribution.

To summarize the prediction of a BNN used in regression problem, the usual procedure is to perform model averaging is as follows,

$$\tilde{y} = \frac{1}{T}\sum_{i=1}^{T} F_{\theta_i}(x^*)$$

The uncertainty of the prediction is computed as follows,

$$\tilde{\sigma}^2 = \frac{1}{T}\sum_{t=1}^{T} (F_{\theta_i}(x^*) - \tilde{y}^*)^2$$

Main problem while training a BNN is that the posterior distribution computation is usually an intractable problem, since computing the evidence $\int p(Y|X, \theta')p(\theta')d\theta'$ cannot be done analytically.

To handle this problem, Bayesian inference approximation methods are normally used to train BNNs in practice.

ii) Simulated annealing :

- Simulated annealing is a **method for solving unconstrained and bound-constrained optimization problems.** The method models the physical process of heating a material and then slowly lowering the temperature to decrease defects, thus minimizing the system energy.
- The simulated annealing algorithm is based upon physical annealing in real life. Physical annealing is the process of heating up a material until it reaches an **annealing temperature** and then it will be **cooled down** slowly in order to change the material to a desired structure. When the material is hot, the molecular structure is weaker and is more susceptible to change. When the material cools down, the molecular structure is harder and is less susceptible to change.
- Another important part of this analogy is the following equation from thermal dynamics,

$$P(\Delta E) = e^{-\frac{\Delta E}{k * t}}$$

- This equation calculates the probability that the energy magnitude will increase. One can calculate this value given some energy magnitude and some temperature t along with the Boltzmann constant k.
- **From AI point of view, simulated annealing** is a stochastic global search optimization algorithm.
- This means that it makes use of randomness as part of the search process. This makes the algorithm appropriate for nonlinear objective functions where other local search algorithms do not operate well.
- Simulated Annealing (SA) mimics the physical annealing process but is used for optimizing parameters in a model. This process is very useful for situations where there are a lot of local minima such that algorithms like Gradient Descent would be stuck at.

- It modifies a single solution and searches the relatively local area of the search space until the local optima is located. It may accept worse solutions as the current working solution.
- The likelihood of accepting worse solutions starts high at the beginning of the search and decreases with the progress of the search, giving the algorithm the opportunity to first locate the region for the global optima, escaping local optima, then hill climb to the optima itself.

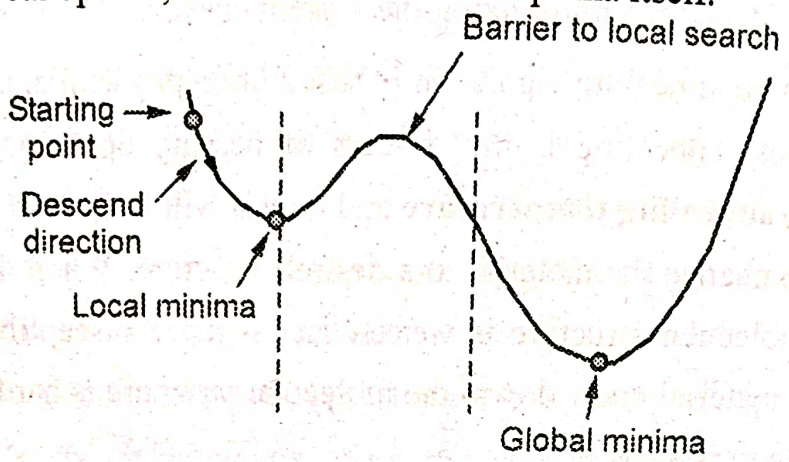


Fig. 1

- In problems like the one in Fig. 1, if gradient descent started at the starting point indicated, it would be stuck at the local minima and not be able to reach the global minima.

Objective function : The objective function is the function that is to be optimized.

Temperature

- The *temperature* is a parameter in simulated annealing that affects two aspects of the algorithm :
  - The distance of a trial point from the current point.
  - The probability of accepting a trial point with higher objective function value.
- Temperature can be a vector with different values for each component of the current point. Typically, the initial temperature is a scalar.
- Temperature decreases gradually as the algorithm proceeds. One can specify the initial temperature as a positive scalar or vector in the

InitialTemperature option. One can specify the temperature as a function of iteration number as a function handle in the TemperatureFcn option. The temperature is a function of the annealing parameter, which is a proxy for the iteration number. The slower the rate of temperature decrease, the better the chances are of finding an optimal solution, but the longer the run time.

Annealing parameter

- The *annealing parameter* is a proxy for the iteration number. The algorithm can raise temperature by setting the annealing parameter to a lower value than the current iteration. One can specify the temperature schedule as a function handle with the TemperatureFcn option.

Reannealing

- *Annealing* is the technique of closely controlling the temperature when cooling a material to ensure that it reaches an optimal state. Reannealing raises the temperature after the algorithm accepts a certain number of new points, and starts the search again at the higher temperature. Reannealing avoids the algorithm getting caught at local minima. Specify the reannealing schedule with the ReannealInterval option.

Q.3 **a)** *Draw and explain competitive learning network.*
(Refer Q.1 and Q.2 of Chapter - 4) **[7]**

b) *Describe the Self-Organization Map (SOM) algorithm and explain how it can be used for feature mapping.*
(Refer Q.12, Q.13, Q.14 of Chapter - 4) **[6]**

c) *Explain how ART can be used for character recognition task.*
(Refer Q.11 of Chapter - 4) **[4]**

OR

Q.4 **a)** *Explain briefly ART network. What are the features of ART network ?* **(Refer Q.6 and Q.7 of Chapter - 4)** **[7]**

b) *Describe the components of a competitive learning neural network and explain how they contribute to the network function.* **(Refer Q.2 and Q.3 of Chapter - 4)** [6]

c) *What is vector quantization ? How it is used for pattern clustering ?* **(Refer Q.16 of Chapter - 4)** [4]

Q.5 **a)** *Explain the role of pooling layer in convolution neural network.* **(Refer Q.7 and Q.10 of Chapter - 5)** [8]

b) *Explain the concept of transfer learning and its importance in deep learning.* **(Refer Q.31 and Q.32 of Chapter - 5)** [6]

c) *Explain padding in neural network.* **(Refer Q.11 of Chapter - 5)** [4]

OR

Q.6 **a)** *Explain residual network in convolution neural network.* **(Refer Q.39 of Chapter - 5)** [8]

b) *Explain the concept of SoftMax regression and its significance in CNN models.* **(Refer Q.17 of Chapter - 5)** [10]

Q.7 **a)** *Explain how ANN can be used for the recognition of printed characters.* **(Refer Q.3 of Chapter - 6)** [7]

b) *Describe the Neocognitron model and its significance in the recognition of handwritten characters.* **(Refer Q.4 of Chapter - 6)** [6]

c) *Explain example of pattern recognition in everyday life.* **(Refer Q.1 of Chapter - 6)** [4]

OR

Q.8 **a)** *Discuss the application of ANN in pattern classification and recognition of olympic game symbols.* **(Refer Q.2 of Chapter - 6)** [7]

b) *Explain texture classification and segmentation in ANN.* [6]

Ans. : For segmentation : Refer Q.6 of Chapter - 6.

Texture : Texture analysis which consists of texture classification, segmentation and synthesis has a wide variety of applications in image processing, e.g., industrial and biomedical surface inspection, ground classification and segmentation of satellite imagery and content-based image retrieval. Texture, even though humans can effortlessly recognize texture, is very difficult to define. Classification refers to as assigning a physical object or incident into one of a set of predefined categories. In texture classification the goal is to assign an unknown sample image to one of a set of known **texture classes**. Texture classification is one of the four problem domains in the field of texture analysis. The other three are texture segmentation (partitioning of an image into regions which have homogeneous properties with respect to texture; supervised texture segmentation with a priori knowledge of textures to be separated simplifies to texture classification), texture synthesis (the goal is to build a model of image texture, which can then be used for generating the texture) and shape from texture (a 2D image is considered to be a projection of a 3D scene and apparent texture distortions in the 2D image are used to estimate surface orientations in the 3D scene). Texture analysis is important in many applications of computer image analysis for classification or segmentation of images based on local spatial variations of intensity or color. A successful classification or segmentation requires an efficient description of image texture. Important applications include industrial and biomedical surface inspection, for example for defects and disease, ground classification and segmentation of satellite or aerial imagery, segmentation of textured regions in document analysis and content-based access to image databases. However, despite many potential areas of application for texture analysis in industry there is only a limited number of successful examples. A major problem is that textures in the real world are often not uniform, due to changes in orientation, scale or other visual appearance. In addition, the degree of computational complexity of many of the proposed texture measures is very high.

c) *Discuss the application of ANN in the recognition of Consonant Vowel (CV) segments.* **(Refer Q.6 of Chapter - 6)** **[4]**

December-2023 [END SEM] [6180] - 70 **Solved Paper**

Course 2019

Time : $2\frac{1}{2}$ Hours] **[Maximum Marks : 70**

Q.1 **a)** *What do you understand by associative memory ? Also mention characteristics and applications for the same.* **(Refer Q.1 of Chapter - 3)** [5]

b) *Write short notes on the following :*

i) State transition diagram **(Refer Q.27 of Chapter - 3)**

ii) False minima problem. **(Refer Q.28 of Chapter - 3)** [5]

c) *Illustrate the architecture of Boltzmann machine and its learning also its applications.* **(Refer Q.9 of Chapter - 3)** [8]

OR

Q.2 **a)** *Explain Boltzmann machine. How does it differ from Hopfield net ?* **(Refer Q.9 of Chapter - 3)** [8]

b) *How does simulated annealing algorithm work ?* **(Refer Q.7 of Chapter - 3)** [5]

c) *Write short notes on the following :*

i) Applications of Hopfield network for travelling sales man problem

ii) Associative memory **(Refer Q.1 of Chapter - 3)** [5]

Ans. : i. Applications of Hopfield network for travelling sales man problem

Hopfield networks are used for the Traveling Salesman Problem (TSP) for training the network to represent the optimal tour for a given set of cities.

The problem can be represented as below :

- TSP is represented as a set of cities and the distances between them. Create a matrix where each element represents the distance between two cities.

The Hopfield network configuration is as below :

- Hopfield network is set with as many neurons as there are cities in the defined TSP.

Weight matrix initialization is as below :

- The weights are initialized based on the distances between cities. The weight between neurons (i, j) should correspond to the distance between cities i and j.

To train the network below process is followed :

- Train the Hopfield network using a set of input patterns that correspond to possible tours. The goal is to associate the patterns with low energy states, representing optimal solutions.

Energy function is defined as below :

- An energy function represents the objective function of the TSP. In the context of TSP, the objective is to minimize the total tour distance.
- Updating neuron states is done by implementing the update rule for neuron states. An iterative process is used to converge to a state where the energy function is minimized.
- Extracting the solution Once the network has converged. The state of neurons represents a solution to the TSP. Decode the solution from the network's neuron states.
- **Post-processing process :** Any necessary post-processing steps are applied, such as rounding the solution to the nearest city or checking if it satisfies the TSP constraints.
- It is important to note that Hopfield networks may not guarantee an optimal solution for large TSP instances and the quality of the solutions may vary. The approach is more suitable for smaller TSP instances or as part of a hybrid solution combining multiple optimization techniques to get an optimal solution.

Q.3 a) *What is competitive learning in neural networks ?* **[5]**

(Refer Q.1 of Chapter - 4)

b) *Consider an ART-I network with input vector [1,1,0,0], [0,0,1,0], [1,1,1,0] and [1,1,1,1], want to produce clustering with following data, number of inputs n = 4, clusters to be formed m = 3 and vigilance parameter ρ = 0.5, compute the result of the first iteration and comment on clustering.* [8]

Ans. : ART networks implement a clustering algorithm. **Input is presented to the network and the algorithm checks whether it fits into one of the already stored clusters.**

Binary-based input vector - ART1 is designed for binary 0/1 inputs, where each input vector may have more 0/1 elements.

Unsupervised learning - In unsupervised learning, no external teacher or critic oversees the learning process and provides feedback information. Moreover, no environmental feedback exists to indicate the nature or correctness of the outputs. The network must discover its own patterns, features, regularities, correlations, or categories in the input data and code for them in the output.

Quick learning capability - When an input pattern is not sufficiently similar to any existing prototype and a new node is created to represent a new category involving the input pattern as the prototype.

Concept of vigilance parameter - The "sufficiently similar" idea depends on a vigilance parameter r, with $0 < r < 1$. The similarity condition is easier to meet if r is small, leading to coarse categorization. On the other hand, if r is 1, numerous finely divided categories are formed. The vigilance parameter value can be adjusted during learning such that increasing it can lead to subdivision of existing categories.

Stability and plasticity - The ART1 network is sufficiently stable to preserve significant past prototype vectors and thus are also binary 0 or 1 vectors, where i indicates the output nodes or categories, each of which can be enabled or disabled.

First iteration of the ART 1 network with the given parameters are as follows :

Input vectors - (1, 1, 0, 0), (0, 0, 1, 0), (1, 1, 1, 0), (1, 1, 1, 1)

Number of inputs (n) - 4

Number of clusters to be formed (m) = 3

Vigilance parameter (p) = 0.5

Initialize weights for the first cluster using the first input vector - (1, 1, 0, 0)

Calculate the similarity between the input vector and the weight vector using the cosine similarity measure.

If the similarity is greater than or equal to the vigilance parameter (0.5), assign the input to the cluster.

If the similarity is less than the vigilance parameter, create a new cluster with the input vector as the weight vector.

Based on the above steps, each input vector is considered as follows :

For the first input vector (1, 1, 0, 0) the steps are applied as follows,

Cosine similarity with the initial weight vector (1, 1, 0, 0) is 1.

Since the similarity is equal to 1, the input vector is assigned to the first cluster.

For the second input vector (0, 0, 1, 0) the steps are applied as follows,

Cosine similarity with the initial weight vector (1, 1, 0, 0) is 0.

Since the similarity is less than 0.5, a new cluster is created with the input vector as the weight vector.

For the third input vector (1, 1, 1, 0) the steps are applied as follows,

Cosine similarity with the initial weight vector (1, 1, 0, 0) is 0.816.

Since the similarity is greater than or equal to 0.5, the input vector is assigned to the first cluster.

For the fourth input vector (1, 1, 1, 1) the steps are applied as follows,

Cosine similarity with the initial weight vector (1, 1, 0, 0) is 0.816.

Since the similarity is greater than or equal to 0.5, the input vector is assigned to the first cluster.

After the first iteration, two clusters formed, as follows,

Cluster 1 - (1, 1, 0, 0), (1, 1, 1, 0), (1, 1, 1, 1)

Cluster 2 - (0, 0, 1, 0)

There are two unassigned input vectors, but they will be considered in subsequent iterations.

This initial clustering shows that the network tends to group vectors with similar patterns together while creating new clusters for dissimilar patterns.

Clustering is the act of organizing similar objects into groups. Assigning related objects into clusters is beneficial for AI models. Clustering has many uses in data science, like image processing, knowledge discovery in data, unsupervised learning and various other applications.

Cluster analysis, or clustering, is done by scanning the unlabeled datasets in a machine learning model and setting measurements for specific data point features. The cluster analysis will then classify and place the data points in a group with matching features. Once data has been grouped together, it will be assigned a cluster ID number to help identify the cluster characteristics. Breaking down large, intricate datasets using the clustering technique can improve stress when deciphering complex data.

c) *Draw the network architecture of ART network. Explain the algorithm for designing the weights of ART network.*

(Refer Q.7 of Chapter - 4) **[5]**

OR

Q.4 **a)** *Explain ART under the following headings : i) Architecture ii) Working iii) Training iv) Implementation.*

(Refer Q.6 and Q.7 of Chapter - 4) **[5]**

b) *Draw the architecture of Kohonen network and explain the algorithm for training the weights of the network.*

(Refer Q.12 and Q.13 of Chapter - 4) **[5]**

c) *Define following :*

i) Learning vector quantization **(Refer Q.16 of Chapter - 4)**

ii) Adaptive pattern classification. **[8]**

Ans. : ii. Adaptive pattern classification

- Adaptive pattern classification is **the assignment of patterns to classes based on typical patterns or training samples, used by the system to determine the decision procedure.**
- Pattern classification **involves building a function that maps the input feature space to an output space of two or more than two classes.** Neural Networks (NN) are an effective tool in the field of pattern classification, using training and testing data to build a model.
- The system is adaptive means the decision procedure is optimized according to some criterion of the system's performance on the training samples. An adaptive pattern classification system is described that does not require a priori knowledge of the probability density of the pattern vectors for each class, as do the classical statistical techniques. Any decision rule, consisting of a discriminant function, that is a linear combination of arbitrary scalar functions of the pattern vector, may be chosen on the basis of a priori knowledge about the classes, engineering judgment and economic considerations.
- The system optimizes itself by adjustment of the decision parameters according to a weighted mean-square-error performance criterion, using a multivariable search technique.

Q.5 **a)** *Illustrate with example convolution and max pooling.* **(Refer Q.5 and Q.10 of Chapter - 5)** **[6]**

b) *What frameworks are used in deep learning ? Define any seven.* **[5]**

Ans. : Widely-used DL frameworks, such as PyTorch, TensorFlow, PyTorch Geometric, DGL, keras, Caffe and Shogun. Also refer Q.19, Q.21 and Q.23 of Chapter - 5.

c) *Explain the softmax regression with respect to hypothesis and cost function and write down its properties.* [6]

Ans. : The properties of softmax (all output values in the range (0, 1) and sum up to 1.0) make it suitable for a probabilistic interpretation that's very useful in machine learning. Also refer Q.17 of Chapter - 5.

OR

Q.6 **a)** *Exemplify convolution over volume with convolution on RGB images. Also illustrate multiple filters used in it.*
(Refer Q.16 of Chapter - 5) [6]

b) *Consider a LeNet-5 a convolutional neural network, we want to perform the classification of digits, write down the complete procedure followed in its architecture.* **(Refer Q.38 of Chapter - 5)** [5]

c) *What is transfer learning models for image classification ? What are the five types of transfer learning ?* [6]

Ans. : Transfer learning generally refers to a process where a model trained on one problem is used in some way on a second related problem.

- In deep learning, transfer learning is a technique whereby a neural network model is first trained on a problem similar to the problem that is being solved. Transfer learning has the advantage of decreasing the training time for a learning model and can result in lower generalization error.
- Transfer learning is about leveraging feature representations from a pre-trained model, so we don't have to train a new model from scratch.
- The pre-trained models are usually trained on massive datasets that are a standard benchmark in the computer vision frontier. The weights obtained from the models can be reused in other computer vision tasks.
- These models can be used directly in making predictions on new tasks or integrated into the process of training a new model. Including the pre-trained models in a new model leads to lower training time and lower generalization error.

Steps for transfer learning models for image classification :

- **Obtain pre-trained model :** The first step is to choose the pre-trained model we would like to keep as the base of our training, depending on the task. Transfer learning requires a strong correlation between the knowledge of the pre-trained source model and the target task domain for them to be compatible.
- **Create a base model :** The base model is one of the architectures such as ResNet which we have selected in the first step to be in close relation to our task. We can either download the network weights which saves the time of additional training of the model. Else, we will have to use the network architecture to train our model from scratch.
- **Freeze layers :** Freezing the starting layers from the pre-trained model is essential to avoid the additional work of making the model learn the basic features. If we do not freeze the initial layers, we will lose all the learning that has already taken place. This will be no different from training the model from scratch and will be a loss of time, resources, etc.
- **Add new trainable layers :** The only knowledge we are reusing from the base model is the feature extraction layers. We need to add additional layers on top of them to predict the specialized tasks of the model. These are generally the final output layers.
- **Train the new layers :** The pre-trained model's final output will most likely differ from the output we want for our model. For example, pre-trained models trained on the ImageNet dataset will output 1000 classes. However, we need our model to work for two classes. In this case, we have to train the model with a new output layer in place.
- **Fine-tune the model :** Fine-tuning involves unfreezing some part of the base model and training the entire model again on the whole dataset at a very low learning rate. The low learning rate will increase the performance of the model on the new dataset while preventing overfitting.

- Types of transfer learning are Domain Adaptation, Domain Confusion, Multi-task Learning, One-shot Learning and Zero-shot Learning.

  Also refer Q.32 of Chapter - 5.

Q.7 **a)** *Which device recognize a pattern of handwritten or printed characters ? And also illustrate it's working.* **(Refer Q.3 of Chapter - 6)** **[7]**

b) *Explain texture classification using convolution neural network.* **[5]**

Ans. : Texture classification is a fundamental issue in computer vision and image processing that plays a significant role in many applications such as medical image analysis, remote sensing, object recognition, document analysis, environment modeling, content-based image retrieval and many more.

- Texture classification is a complex task that assigns unlabeled images or textures to the correct labeled class. Some key factors such as scaling and viewpoint variations and illumination changes make this task challenging.
- Almost all of the CNN model cases classify images based on global features that describe the image as a whole to generalize the entire object.
- The primary concept of using CNN features is its capability to capture the high-level features that are considered the key point to separate the texture image. Convolution Neural Network (CNN) captures low detail features from the first convolution layers and then generates high detail features in the last layers. Selecting the proper right set of features has always been a challenging task for the machine learning algorithm. CNN has numerous extensive applications in different fields. Whereas image classification and recognition are challenging tasks for machine learning algorithms, CNN is highly promising for accuracy.

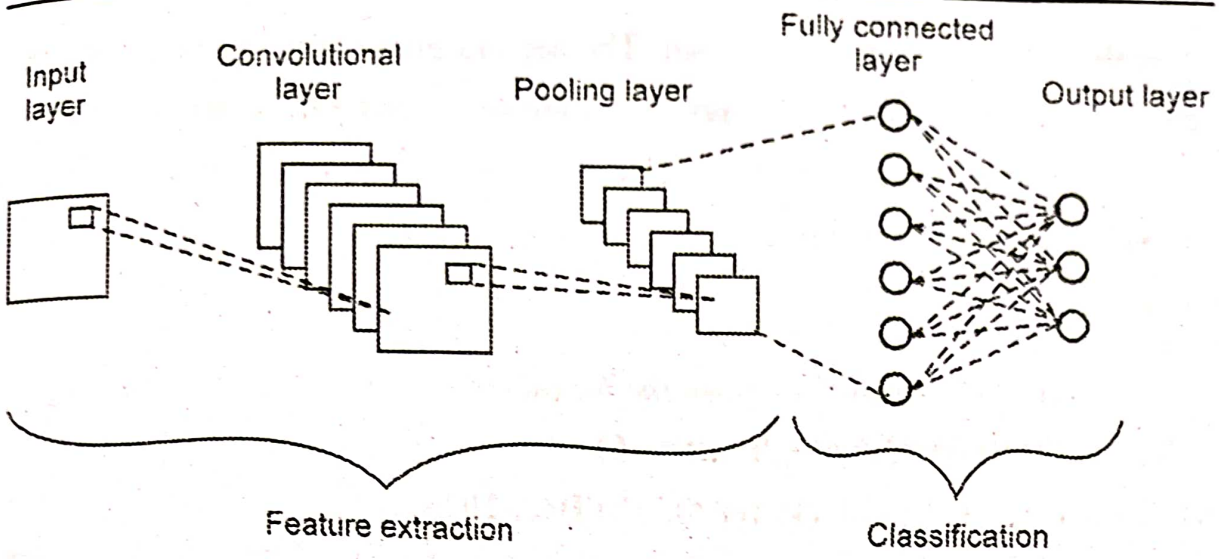


Fig. 1

As shown in above Fig. 1 feature extraction and classification involves different layers of network as discussed below.

- **Convolution layer :** It is used to apply filters to the input feature map and produce convolved features. The following two factors define the convolution layer.(1) The size of the block extracted from the input feature map.(2)The depth of convolved features.
- **Pooling layer :** Generally, applied after the convolution layer, it is a downsampling (Dimensional reduction) operation such as average pooling, min pooling and max pooling.
- **Fully connected layer :** It is typically found towards the end of the CNN architecture. It works on such a flattened input, in which each input is linked to all nodes.

Each model of CNN has its characteristics. Fig. Q.5.3 of Chapter - 5 summarizes the description of different CNN arch.

The motivation of the usage of CNN models as features descriptors is the ability of the deep neural network to capture the high-level features that can be a key point for the classification of the texture images. Texture plays a significant role in distinguishing objects in color images. Texture classification involves a two-phase process. The first phase is extracting the features, which provides a feature-based description for each texture type; this phase tends to select features unaffected by image transformation, such

as scaling, translation and rotation. The second phase tends to recognize the texture from the extracted features. Texture recognition is increasingly set as a critical issue in computer vision that has many applications such as biomedical image processing, object detection and remote sensing application fields.

c) *Write short notes on the following :*

i) NET talk **(Refer Q.5 of Chapter - 6)**

ii) Texture classification **(Refer Q.7(b) Dec.-2023)**

iii) Pattern classification **(Refer Q.1 of Chapter - 6).** **[5]**

OR

Q.8 **a)** *You have been asked to develop a model of recognizing hand written digits. What are the chosen steps for activity ? Explain each with detail.* **(Refer Q.3 of Chapter - 6)** **[7]**

b) *What is automatic translation ? How does it work ? What are its benefits ?* **[5]**

Ans. : Automatic translation refers to the process of replacing words from one language with their counterparts in another language. It involves the use of software that can **rapidly translate text** with minimal human intervention.

- Typically, automatic translation relies on corpora, which are collections of texts in multiple languages. Words are translated automatically by analyzing their context and proximity to other words. However, due to the inherent limitations of machines, automatic translation cannot provide a **flawless translation**. It lacks the ability to fully comprehend context and nuanced meanings.
- Neural Machine Translation (NMT) is typically software used to translate words from one language to another. Google Translate, Baidu Translate are well-known examples of NMT offered to the public via the Internet.
- The reason this NMT is important is because recent advancements in the technology have allowed an increasing number of multinational institutions to adopt NMT engines to aid in internal and external communications.

- Technically, NMTs encompass all types of machine translation where an artificial neural network is used to predict a sequence of numbers when provided with a sequence of numbers. In the case of translation, each word in the input sentence (e.g English) is encoded as a number to be translated by the neural network into a resulting sequence of numbers representing the translated target sentence (e.g. Chinese).

ANN benefits :

- Neural networks can have a large number of parameters with weights and biases between nodes to give them the flexibility to fit highly complex data and train complex models. Model complexity allows the model to generalize to the large volumes of examples it's trained on, such as digesting millions of language pairs.
- One way to understand neural networks is to think of the input as a signal with "information" in it. Some of this information is relevant for the task at hand (e.g. predicting the output). Think of the output as also a signal with a certain amount of "information". The neural network attempts to "repeatedly refine" and compress the input signal's information to match the desired output signal. Think of each hidden layer of the network as stripping out unimportant parts of the input information and keeping and/or transforming the output information along the way through the network. The fully-connected neural network will transform the input information into a form in the final hidden layer, such that it is separable by the output layer.

c) *What is neocognitron neural network and how it is trained ?*
(Refer Q.6 of Chapter - 6) **[5]**

END...

Unit III

3 Associative Learning

3.1 : Associative Learning, Hopfield Networks, Simulated Annealing

Q.1 Explain associative learning and associate neural network.

☞ [SPPU : 10 Marks]

Ans. : • Associative learning is **a form of conditioning.** It is a matter of **temporal relationship between a signal and a sequence** that can have positive or negative consequences for the organism. Neuronal connections in the brain are created through associative learning of these connections.

- The physiological basis for associative learning was explained and proven by the psychologist Donald Oldung Hebb in his work on the function of Neurons with common synapses. His Hebb's learning rule describes a mapping of learning into neural networks. The term is used to describe a process in which the frequent interaction of two neurons increases their action potentials in relation to each other.
- **People learn much faster with positive associations than with negative or neutral associations.** Thus, if someone evaluates the sequence of a signal as profitable for him, this leads more quickly to a learning success. The term "strength of association" is also used here, which can lie between zero and a finite value.
- In contrast to the approach of learning via linkages, the **non-associative learning** about information that stands alone. With this information, the organism does not find a connection to a subsequent event.
- From the point of view of psychology, learning is about enduring changes in behaviour that result from experience. Accordingly, it is a process that enables living beings to react to situations through previous experiences and by incorporating further experiences.

- Associative learning is classical conditioning. This type of learning **functions through a conditioned response triggered by a conditioned stimulus.** It goes back to the Russian Ivan Pavlov and his still famous discovery when feeding dogs.
- To support Ivan Pavlov's experiments, the success of this learning method was also confirmed by tests with sea snails and rabbits. Rodents, for example, can be conditioned to new situations with the help of maze or olfactory learning methods.
- **People also learn more easily when new information can be linked to existing personal impressions, such as places, memories or emotions.** This makes it easier to remember something than when new information occurs in isolation.
- An associative neural network (ASNN) is an ensemble-based method inspired by the function and structure of neural network correlations in brain. The method operates by simulating the short- and long-term memory of neural networks. The long-term memory is represented by ensemble of neural network weights, while the short-term memory is stored as a pool of internal neural network representations of the input pattern.
- An associative neural network (ASNN) is a combination of an ensemble of the feed-forward neural networks and the K-nearest neighbor technique.
- The introduced network uses correlation between ensemble responses as a measure of distance among the analyzed cases for the nearest neighbor technique and provides an improved prediction by the bias correction of the neural network ensemble both for function approximation and classification. Actually, the proposed method corrects a bias of a global model for a considered data case by analyzing the biases of its nearest neighbors determined in the space of calculated models. An associative neural network has a memory that can coincide with the training set. If new data become available the network can provide a reasonable approximation of such data without a need to retrain the neural network ensemble.

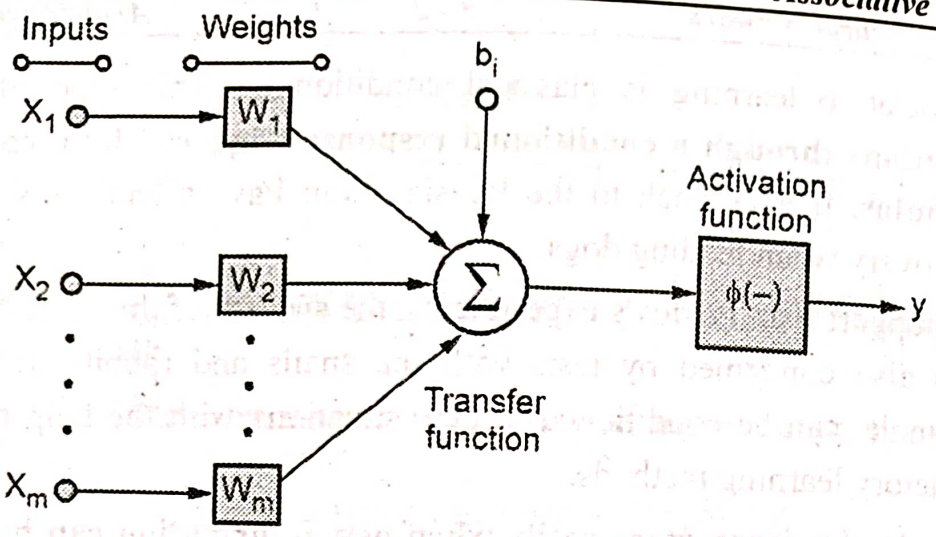


Fig. Q.1.1 Associate neural network

- The traditional multi-layer neural network (MLP) is a memory-less approach. This means that after training is complete all information about the input patterns is stored in the neural network weights and input data are no longer needed, that is there is no explicit storage of any presented example in the system complicated, there is no guarantee that all details of f, i.e. its fine structure, will be represented. Thus, the global model can be inadequate because it does not describe equally well the entire state space with poor performance of the method being mainly due to a high bias of the global model in some particular regions of space. The same problem of bias is also pertinent if neural networks are used for classification. The MLP variance can also contribute to poor performance of this method. However, the variance can be decreased by analyzing a large number of networks, that is using artificial neural network ensemble and taking, for example, a simple average of all networks as the final model. The problem of bias of MLP cannot be so easily addressed simply by using larger neural networks since such networks can fall in a local minimum and thus can still have a considerable bias.

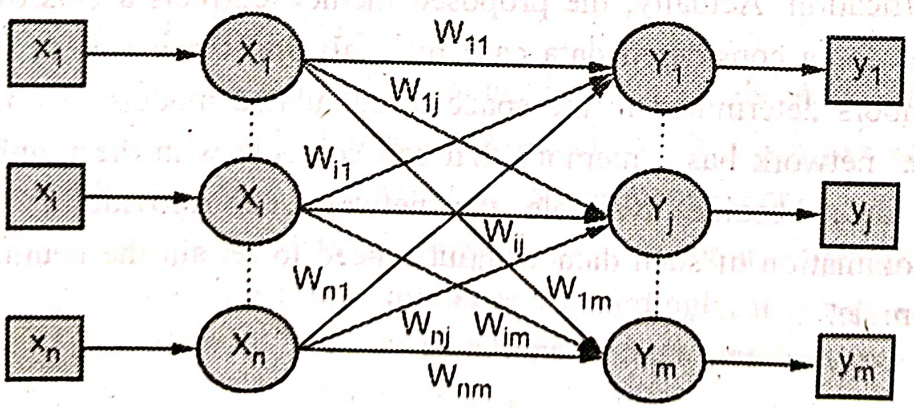


Fig. Q.1.2 Associative neural network

Q.2. What are Hopfield networks ? Give their characteristics.

☞ [SPPU : 8 Marks]

Ans. : Introduction

- Hopfield networks are a form of Recurrent Artificial Neural Networks (RNNs), first described by John Hopfield in his 1982 paper titled : "Neural networks and physical systems with emergent collective computational abilities.". Hopfield Networks were the first instance of associative neural networks : RNN architectures which are capable of producing an emergent associative memory.
- Associative memory, or content-addressable memory, is a system in which a memory recall is initiated by the associability of an input pattern to a memorized one. In other words, associative memory allows for the retrieval and completion of a memory using only an incomplete or noisy portion of it.
- As an example, a person might see a picture they like and be 'brought back' to the memory of their first time watching it. The context, people, surroundings, and emotions in that memory can be retrieved via subsequent exposure to only a portion of the original stimulus : the song alone. These features of Hopfield Networks (HNs) made them a good candidate for early computational models of human associative memory, and marked the beginning of a new era in neural computation and modeling.
- Hopfield's unique network architecture was based on the Ising model, a physics model that explains the emergent behavior of the magnetic fields produced by ferromagnetic materials. The model is usually described as a flat graph, where nodes represent magnetic dipole moments of regular repeating arrangements. Each node can occupy one of two states (i.e. spin up or spin down, + 1 or – 1), and the agreement of states between adjacent nodes is energetically favorable. As each dipole 'flips', or evolves to find local energetic minima, the whole material trends toward a steady-state, or global energy minimum. HNs can be thought of in a similar way where the network is represented as a 2D graph and each node (or neuron) occupies one of two states: active or inactive. Similar to Ising models, the dynamic behavior of a HN is ultimately determined according to a metaphorical notion of 'system energy', and the network converges to a

state of 'energetic minimum', which in the case of a learned network happens to be a memory.

Characteristics of Hopfield Network - Qualities and Attributes

- Each neuron in the network has three qualities namely,
  1. **Connections to other neurons** - Each neuron in the network is connected to all other neurons, and each connection has a unique strength, or weight, analogous to the strength of a synapse. These connection strengths are stored inside a matrix of weights.
  2. **Activation** - This is computed via the net input from other neurons and their respective connection weights, loosely analogous to the membrane potential of a neuron. The activation takes on a single scalar value.
  3. **Bipolar state** - This is the output of the neuron, computed using the neuron's activation and a thresholding function, analogous to a neuron's 'firing state.' In this case, – 1 and + 1.
- The *information* or *memories* of a Hopfield Network are stored in the strength of connections between neurons, much in the same way that information is thought to be stored in the brain according to models of long term memory. The connections, and their respective weights, directly affect the activity of the network with each generation, and ultimately determine the state to which the network converges. You can picture the weight between 2 neurons, neuron-a and neuron-b, as the extent to which the output of neuron-a will contribute to the activation of neuron-b, and vice versa. More on activation and its effect on neuronal state below.
- Importantly, the connections between neurons in a HN are symmetric. This means that if neuron-a is connected to neuron-b with a strength of + 1, neuron-b's connection to neuron-a is also + 1. One can store the weights of a network with n neurons in a square symmetric matrix of dimensions $n \times n$.
- Because neurons do not connect back to themselves, the weights on the matrix's diagonal are effectively null. It's important to note that the network structure, including the number of neurons and their connections in the network, is fixed.
- The *weights* of those connections are the tunable parameter. By 'network learning' it means it is the fine-tuning of each weight in the network in

order to achieve some desirable output. In the case of an HN, the initial state configuration can be thought of as an input, and its final state configuration as the output. Because each neuron is updated depending on linear combinations of its inputs, the entire network is really one massive mathematical function: a dynamical system, which, with each update generation, takes its past output as its current input. The parameters of this function, the weights, determine the way the network evolves over time.

Q.3 Write a note on activation function and thresholding function used in Hopfield networks. ☞ **[SPPU : 8 Marks]**

Ans. : • Any neuron's instantaneous activation can be calculated by taking the **weighted sum** of inputs from the neurons it's connected to :

$$y_i = \sum_j y_i w_{ij}$$

Equation 1 : The activation function of a neuron in a binary Hopfield Network,

Where y_i represents the activation of neuron-i in the network, y_j represents a vector of the respective outputs of all neurons inputting to neuron-i, and w_{ij} the symmetric weight of the connection between neurons i and j.

The activation of a neuron is used to determine the state or output, of the neuron according to a thresholding function :

$$s_i = \begin{cases} +1 & \text{if } y_i > 0 \\ -1 & \text{if } y_i < 0 \end{cases}$$

Equation 2 : The binary-threshold output function,

Where s_i represents a neuron-i's given state and output.

- As the state of each neuron in the network is updated, its contributions to the activities of other neurons change; this in turn feeds back and modulates more activity and so on, until the network reaches a stable formation.
- If a neuron's activation during a given generation is positive, its output will be + 1 and vice versa. Another way to think of this is that a given neuron is receiving a 'field' of inputs analogous to its activation. Each and every input the neuron receives is weighted, and summed, to yield a net activation, be it positive or negative. If the sign of that field differs from the sign of the neuron's current output, its state will flip to align itself. If

the sign of the field of input matches the sign of the neuron's current output, it will stay the same.

- If the behavior of the overall network is considered according to these rules, the quality of recurrence becomes clear; each network update, or output, becomes the input for the next timestep.

Translation to the distributed storage and representation of information in the network

- While each neuron can represent one of two states at a given time, the overall state of the network, termed *s*, can represent a string of binary information. For example consider the pattern,

$$\text{Pattern} = [0, 1, 0, 1, 0, 1, 0, 1, 0]$$

Fig. Q.3.1 A binary string of information

- This pattern is a 1×9 binary vector which can be reshaped to a 3×3 matrix as below,

Pattern.reshape (3, 3) = [[0, 1, 0], [1, 0, 1], [0, 1, 0]] → when drawn looks like :

0	1	0
1	0	1
0	1	0

Fig. Q.3.2 A binary string of information is reshaped and visualized as an image

- An image is just a matrix of numerical pixel values, so any image which can be represented with pixel values occupying binary states can be accurately represented by the states of a binary HN. There are many forms of information can be represented in a binary / bipolar fashion.
- If a pattern takes the form of an image, the pixels themselves are represented using individual neurons. In the example above there is a 3×3 matrix of pixels, so 9 neurons are required to fully represent the image. Another way to visualize this is to represent the network as a graph, as shown below,

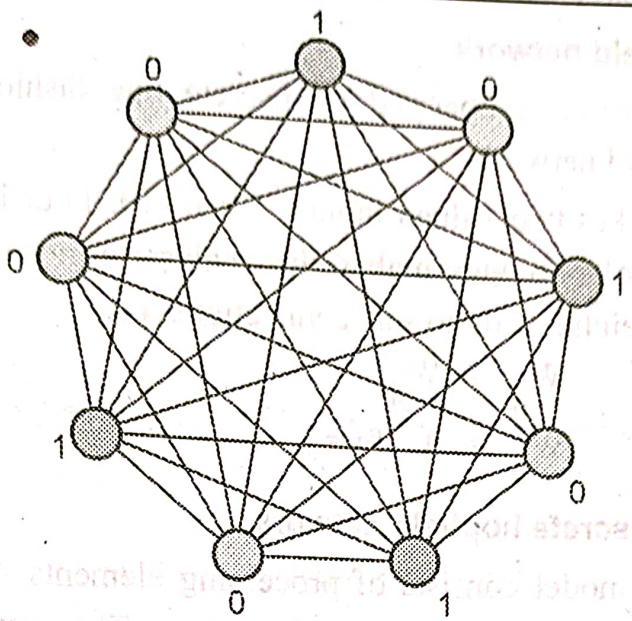


Fig. Q.3.3 Binary string representation using Hopfield Network

- In this network graph, the nodes represent neurons and the edges represent the connections between them. The black dot (outside the network image) indicates the neuron whose state represents the first element, 1, in the pattern vector. Following the state of the neurons in clockwise order yields the rest of the pattern.
- In a computer, the state of each neuron is represented as the individual elements in a 1×9 vector, S. Here the information to be stored is directly represented using the respective states of neurons in the network :

$$S = [0, 1, 0, 1, 0, 1, 0, 1, 0].$$

- Any arbitrary information string of n bits can be represented by a network of n neurons. It is the combined activity of the neurons in the network which collectively represent one's target information in a distributed fashion. In most HNs, the states of neurons are bipolar (– 1 or + 1). For the sake of simplicity, the example above uses binary 0 or 1, from here on out assume that the neurons occupy bipolar states.

Q.4 Discuss various types of Hopfield networks in detail.

☞ **[SPPU : 10 Marks]**

Ans. : The Hopfield network is of two types,

1. Discrete hopfield network
2. Continuous hopfield network

1. Discrete hopfield network

- When the network is operated in discrete line fashion it is called as discrete hopfield network.
- The network takes two-valued inputs : binary (0, 1) or bipolar (+ 1, – 1); the use of bipolar inputes makes the analysis easier. The network has symmetrical weights with no self-connections, i.e.,

$$W_{ij} = W_{ji};$$
$$W_{ij} = 0 \quad \text{if } i = j$$

Architecture of discrete hopfield network

- The hopfield's model consists of processing elements with two outputs, one inverting and the other non-inverting. The outputs from each processing element are fed back to the input of other processing elements but not to itself.

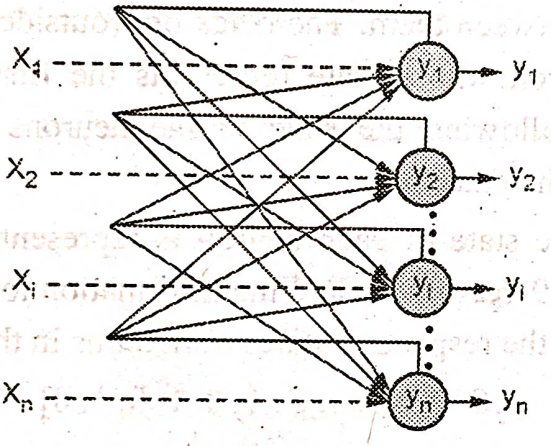


Fig. Q.4.1 Discrete Hopfield network

Training algorithm of discrete hopfield network

- During training of discrete hopfield network, weights will be updated. One can have the binary input vectors as well as bipolar input vectors.
- Let the input vectors be denoted by s(p), p = 1, ..., P. The weight matrix W is used to store a set of input vectors.
- In case of input vectors being binary, the weight matrix $W = \{w_{ij}\}$ is given by

$$w_{ij} = \sum_{p=1}^{P} [2s_i(p) - 1]\,[2s_j(p) - 1] \text{ for } i \neq j$$

- When the input vectors are bipolar, the weight matrix $W = \{w_{ij}\}$ can be defined as

$$w_{ij} = \sum p = 1P[s_i(p)]\ [s_j(p)] \text{ for } i \neq j$$

Testing algorithm of discrete hopfield net

Step 0 : Initialize the weights to store patterns, i.e., weights obtained from training algorithm using Hebb rule.

Step 1 : When the activations of the net are not converged, then perform steps 2 - 8.

Step 2 : Perform steps 3 - 7 for each input vector X.

Step 3 : Make the initial activations of the net equal to the external input vector X :

$$y_i = x_i \text{ for } i = 1 \text{ to } n$$

Step 4 : Perform steps 5 - 7 for each unit y_i. (Here, the units are updated in random order.)

Step 5 : Calculate the net input of the network :

$$y_i n_i = x_i + \sum j\, y_j w_{ji}$$

Step 6 : Apply the activations over the net input to calculate the output :

$$y_i = y_i 0 \text{ if } y_i n_i > \theta_i \cdot y_i n_i = \theta_i \text{ if } y_i n_i < \theta_i$$

where θ_i is the threshold and is normally taken as zero.

Step 7 : Now feedback the obtained output y_i to all other units. Thus, the activation vectors are updated.

Step 8 : Finally, test the network for convergence.

2. Continuous hopfield network

- Continuous network has time as a continuous variable and can be used for associative memory problems or optimization problems like traveling salesman problem. The nodes of this network have a continuous, graded output rather than a two state binary output. Thus, the energy of the network decreases continuously with time.
- Unlike the discrete hopfield networks, here the time parameter is treated as a continuous variable. So, instead of getting binary / bipolar outputs,

one can obtain values that lie between 0 and 1. It can be used to solve constrained optimization and associative memory problems. The output is defined as :

$$v_i = g(u_i)$$

where, v_i = Output from the continuous hopfield network

u_i = Internal activity of a node in continuous hopfield network

Q.5 What are energy functions in Hopfield networks ?

[SPPU : 5 Marks]

Ans. : • The hopfield networks have an energy function associated with them. It either diminishes or remains unchanged on update (feedback) after every iteration. The energy function for a continuous hopfield network is defined as :

$$E = 0.5 \sum_{i=1}^{n} \sum_{j=1}^{n} w_{ij} v_i w_j + \sum_{i=1}^{n} \theta_i v_i$$

- To determine if the network will converge to a stable configuration, one need to see if the energy function reaches its minimum by :

$$\frac{d}{dt} E \leq 0$$

- The network is bound to converge if the activity of each neuron with respect to time is given by the following differential equation :

$$\frac{d}{dt} u_i = \frac{-u_i}{\tau} + \sum_{j=1}^{n} w_{ij} v_j + \theta_i$$

Q.6 What are the various performance issues associated with Hopfield network ?

[SPPU : 8 Marks]

Ans. : • One of the critical shortcomings of Hopfield Neural Network (HNN) is that the network may not always converge to a fixed point. HNN, is limited to local optimization during training to achieve network stability. In the Hopfield network a solution of an optimization problem is obtained after the network is relaxed to an equilibrium state.

- Other major performance issues of Hopfield networks are as follows,

1. **Memory capacity :** The number m of training patterns should be about the number of neurons n or less (according to Hopfield, it should be less than 0.15 n ; according to some new results, m ε 0.5 n / log n). This means that the memorizing capacity of a Hopfield network is severely limited. Catastrophic "forgetting" may occur if we try to memorize more patterns than the network is supposed to handle.

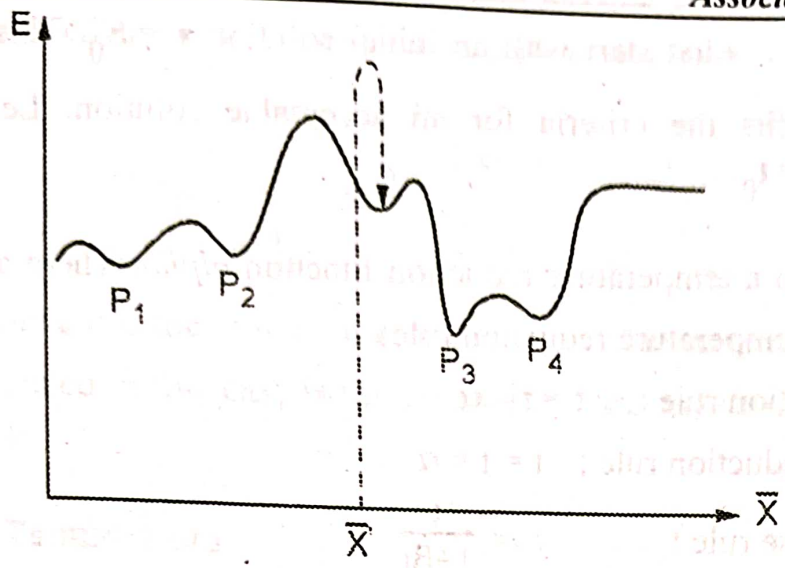


Fig. Q.6.1 A network may relax into a "spurious" state, which phenomenon is called the local minima problem

2. **Discrepancy limitation :** The new pattern to be recognized as one of the training patterns should not differ from any training pattern by more than about 25 %.
3. **Orthogonality between patterns :** The more orthogonal (dissimilar) the training patterns, the better the recognition.
4. **Spurious states of attraction :** Sometimes the network learns some patterns (creates basins of attraction) called spurious states, which are not presented in the set of training patterns. An example of such a state is shown in Fig. Q.6.1. In order to overcome this limitation, Hopfield introduced a "little bit of unlearning" for every learning pattern :

$$\Delta w_{ij} = \alpha x_i^{(p)} \cdot x_j^{(p)} \text{ for the } p^{th} \text{ pattern } x^{(p)}$$

Spurious states may be useful, if the Hopfield network is used for partial matching and approximate reasoning. The input values are between 0 and 1 represent the certainty of the facts or fuzzy membership degrees.

5. **Weight symmetry :** The weight matrix has to be symmetrical in order for the network to reach an equilibrium. The symmetrical synaptic weights are not at all biologically plausible, but they are a useful limitation here.

Q.7 Explain simulated annealing algorithm. ☞ **[SPPU : 10 Marks]**

Ans. : Step 1 : First start with an initial solution $s = S_0$. This can be any solution that fits the criteria for an acceptable solution. Let the initial temperature $t = t_0$.

Step 2 : Setup a temperature reduction function *alpha*. There are usually 3 main types of temperature reduction rules :

1. Linear reduction rule : $t = t - \alpha$
2. Geometric reduction rule : $t = t * \alpha$
3. Slow-decrease rule : $t = \frac{t}{1+\beta t}$

- Each reduction rule reduces the temperature at a different rate and each method is better at optimizing a different type of model. For the 3rd rule, beta is an arbitrary constant.

Step 3 : Starting at the initial temperature, loop through *n* iterations of step 4 and then decrease the temperature according to *alpha*. Stop this loop until the *termination conditions* are reached. The termination conditions could be reaching some end temperature, reaching some acceptable threshold of performance for a given set of parameters, etc. The mapping of time to temperature and how fast the temperature decreases is called the **Annealing Schedule**.

Step 4 : Given the neighbourhood of solutions N(s), pick one of the solutions and calculate the difference in cost between the old solution and the new neighbour solution. The neighbourhood of a solution are all solutions that are close to the solution. For example, the neighbourhood of a set of five parameters might be if one of the five parameters were to change but kept the remaining four the same.

Step 5 : If the difference in cost between the old and new solution is greater than 0 (the new solution is better), then accept the new solution. If the difference in cost is less than 0 (the old solution is better), then generate a random number between 0 and 1 and accept it if it's under the value calculated from the energy magnitude equation from before.

- In the simulated annealing case, the equation has been altered to the following :

$$P = \begin{cases} 1 & \text{if } \Delta c \leq 0 \\ e^{\frac{-\Delta c}{t}} & \text{if } \Delta c > 0 \end{cases}$$

Where the *delta c* is the change in cost and the *t* is the current temperature.

- The *P* calculated in this case is the probability that one should accept the new solution.

High vs. Low Temperature

- Due to the way the probability is calculated, when the temperature is higher, is it more likely that the algorithm accepts a worse solution. This promotes **Exploration** of the search space and allows the algorithm to more likely travel down a sub-optimal path to potentially find a global maximum.

Change	Temperature	Acceptance probability
0.2	0.9	0.8007
0.4	0.9	0.6412
0.6	0.9	0.5134
0.8	0.9	0.4111

- When the temperature is lower, the algorithm is less likely or will not to accept a worse solution. This promotes **Exploitation** which means that once the algorithm is in the right search space, there is no need to search other sections of the search space and should instead try to converge and find the global maximum.

Change	Temperature	Acceptance probability
0.2	0.1	0.1353
0.4	0.1	0.0183
0.6	0.1	0.0025
0.8	0.1	0.0003

Problems - to be optimized with simulated annealing

- Travelling Salesman Problem (TSP)
- Scheduling problems
- Task allocations
- Graph colouring and partitioning
- Non-linear function optimizations
- Consider an example of a difficult optimization task is the chip floor planning problem. Assume that an engineer at circuit manufacturing company has given a task to design the layout for an integrated circuit. There are set of modules of different shapes / sizes and a fixed area on which the modules can be placed. There are a number of objectives need to achieve: maximizing ability for wires to connect components, minimize net area, minimize chip cost, etc. With these in mind, engineer had to create a cost function, taking all, say, 1000 variable configurations and returning a single real value representing the 'cost' of the input configuration. This can be called as the objective function, since the goal is to minimize its value.
- A naive algorithm would be a complete space search - to search all possible configurations until one finds the minimum. This may suffice for functions of few variables, but the problem one has in mind would entail such a brute force algorithm to fun in O(n!).
- Due to the computational intractability of problems like these, and other NP-hard problems, many optimization heuristics have been developed in an attempt to yield a good, albeit potentially suboptimal, value. In current scenario one doesn't necessarily need to find a strictly optimal value - finding a near-optimal value would satisfy the goal. One widely used technique is simulated annealing, by which one can introduce a degree of stochasticity, potentially shifting from a better solution to a worse one, in an attempt to escape local minima and converge to a value closer to the global optimum.
- Simulated annealing is based on metallurgical practices by which a material is heated to a high temperature and cooled. At high temperatures, atoms may shift unpredictably, often eliminating impurities as the material cools into a pure crystal. This is replicated via the simulated annealing

optimization algorithm, with energy state corresponding to current solution.

- In this algorithm, an initial temperature is defined, often set as 1 and a minimum temperature, on the order of 10^{-4}. The current temperature is multiplied by some fraction alpha and thus decreased until it reaches the minimum temperature. For each distinct temperature value, the core optimization routine is run a fixed number of times. The optimization routine consists of finding a neighboring solution and accepting it with probability $e^{(f(c) - f(n))}$ where c is the current solution and n is the neighboring solution. A neighboring solution is found by applying a slight perturbation to the current solution. This randomness is useful to escape the common pitfall of optimization heuristics - getting trapped in local minima. By potentially accepting a less optimal solution than the current one, and accepting it with probability inverse to the increase in cost, the algorithm is more likely to converge near the global optimum. Designing a neighbor function is quite tricky and must be done on a case by case basis, but below are some ideas for finding neighbors in locational optimization problems,
    - Move all points 0 or 1 units in a random direction
    - Shift input elements randomly
    - Swap random elements in input sequence
    - Permute input sequence
    - Partition input sequence into a random number of segments and permute segments

Q.8 List advantages and disadvantages of simulated annealing.

[SPPU : 5 Marks]

Ans. : Advantages

- It is easy to implement and use.
- It provides optimal solutions to a wide range of problems.

Disadvantages

- It can take a long time to run if the annealing schedule is very long.
- In the algorithm there are a lot of parameters those need to be tuned for better performance.

3.2 : Boltzmann Machine and Boltzmann Learning

Q.9 Discuss in detail the architecture of Boltzmann machine.

☞ [SPPU : 10 Marks]

Ans. : • The main purpose of Boltzmann machine is to optimize the solution of a problem. It is the work of Boltzmann machine to optimize the weights and quantity related to that particular problem.

Architecture

- A Boltzmann machine has two kinds of nodes
  - Visible nodes : These are nodes that can be measured and are measured.
  - Hidden nodes : These are nodes that cannot be measured or are not measured.
- According to some experts, a Boltzmann machine can be called a stochastic Hopfield network which has hidden units. It has a network of units with an 'energy' defined for the overall network.
- Boltzmann machines seek to reach thermal equilibrium. It essentially looks to optimize global distribution of energy. But the temperature and energy of the system are relative to laws of thermodynamics and are not literal.
- A Boltzmann machine is made up of a learning algorithm that enables it to discover interesting features in datasets composed of binary vectors. The learning algorithm tends to be slow in networks that have many layers of feature detectors but it is possible to make it faster by implementing a learning layer of feature detectors.
- They use stochastic binary units to reach probability distribution equilibrium (to minimize energy). It is possible to get multiple Boltzmann machines to collaborate together to form far more sophisticated systems like deep belief networks.
- The following diagram shows the architecture of Boltzmann machine. It is clear from the diagram, that it is a two-dimensional array of units. Here, weights on interconnections between units are – **p** where **p > 0**. The weights of self-connections are given by **b** where **b > 0**.

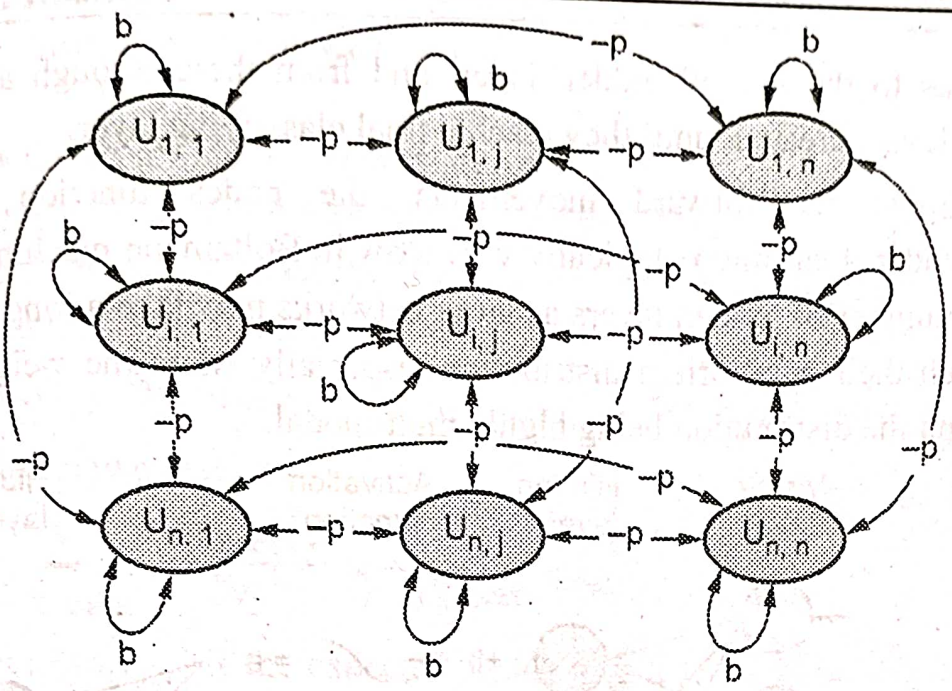


Fig. Q.9.1 Boltzmann machine architecture

- The architecture of the Boltzmann machine comprises a shallow, two-layer neural network that also constitutes the building blocks of the deep network. The first layer of this model is called the visible or input layer and the second is the hidden layer.
- They consist of neuron-like units called a node and nodes are the areas where calculations take place. These nodes are interconnected to each other across layers, but no two nodes of the same layer are linked.
- Therefore there is no intra-layer communication and hence being one of the restrictions in a Boltzmann machine. Each node through computation processes input, and makes stochastic decisions about whether to transmit that input or not. When data is fed as input, these nodes learn all the parameters, their patterns and correlation between them, on their own and form an efficient system. Hence a Boltzmann machine is also termed as an unsupervised deep learning model.
- This model can then be trained to get ready to monitor and study abnormal behaviour depending on what it has learnt. The coefficients that modify the inputs are randomly initialized. Each visible node takes a low-level feature from an item present in the dataset to be learned.
- The result of those two operations is fed into an activation function which in turn produces the node's output also known as the strength of the signal passing through it. The outputs of the first hidden layer would be passed

as inputs to the second hidden layer, and from there through as many hidden layers created, until they reach a final classifying layer.

- For simple feed-forward movements, the nodes function as an autoencoder. Learning is typically very slow in Boltzmann machines with a high number of hidden layers as large networks may take a long time to approach their equilibrium distribution, especially when the weights are large and the distribution being highly multimodal.

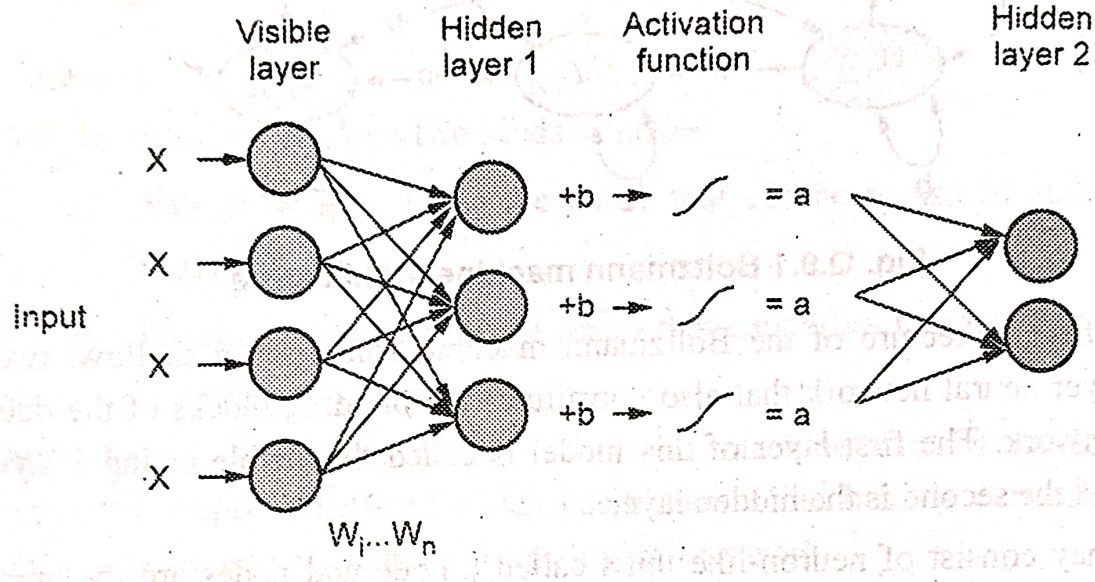


Fig. Q.9.2 Multiple hidden layers

- Boltzmann Machines consist of a learning algorithm that helps them to discover interesting features in datasets composed of binary vectors. The learning algorithm is generally slow in networks with many layers of feature detectors but can be made faster by implementing a learning layer of feature detectors.
- Boltzmann machines are typically used to solve different computational problems such as, for a search problem, the weights present on the connections can be fixed and are used to represent the cost function of the optimization problem. Similarly, for a learning problem, the Boltzmann machine can be presented with a set of binary data vectors from which it must find the weights on the connections so that the data vectors are good solutions to the optimization problem defined by those weights. Boltzmann machines make many small updates to their weights, and each update requires solving many different search problems.

Q.10 Explain the process of learning in Boltzmann machine.

☞ **[SPPU : 10 Marks]**

Ans. : • Given a training set of state vectors (the data), learning consists of finding weights and biases (the parameters) that make those state vectors good. More specifically, the aim is to find weights and biases that define a Boltzmann distribution in which the training vectors have high probability. By differentiating and using the fact that $\partial E(v)/\partial w_{ij} = s_i^v s_j^v$ it can be shown that

$$\sum_{v \in data} \frac{\partial \log P(v)}{\partial w_{ij}} = (s_i s_j)_{data} - (s_i s_j)_{model} \quad \text{... (Q.10.1)}$$

where $(s_i s_j)_{data}$ is the expected value of $s_i s_j$ in the data distribution and $(s_i s_j)_{model}$ is the excepted value when the Boltzmann machine is sampling state vectors from its equilibrium distribution at a temperature of 1. To perform gradient ascent in the log probability that the Boltzmann machine would generate the observed data when sampling from its equilibrium distribution w_{ij} is incremented by a small learning rate times the RHS of equation Q.10.1. The learning rule for the bias, b_i is the same as equation Q.10.1, but with s_j omitted.

- If the observed data specifies a binary state for every unit in the Boltzmann machine, the learning problem is convex : There are no non-global optima in the parameter space. Learning becomes much more interesting if the Boltzmann machine consists of some "visible" units, whose states can be observed data. The hidden units whose states are not specified by the observed data. The hidden units acts as latent variables (features) that allow the Boltzmann machine to model distributions over visible state vectors that cannot be modelled by direct pairwise interactions between the visible units. A surprising property of Boltzmann machines is that of Boltzmann machines is that, even with hidden units, the learning rule remains unchanged. This makes it possible to learn binary features that capture higher-order structure in the data. With hidden units, the expectation $(s_i s_j)_{data}$ is the average, over all data vectors, of the expected value of $s_i s_j$ when a data vector is clamped on the visible units and the hidden units are repeatedly updated until they reach equilibrium with the clamped data vector.

- It is surprising that the learning rule is so simple because $\partial \log P(v)/\partial w_{ij}$ depends on all the other weights in the network. Fortunately, the difference in the two correlations in equation (Q.10.1) tells w_{ij} everything it needs to know about the other weights. This makes it unnecessary to explicitly propagate error derivatives, as in the backpropagation algorithm.

Q.11 List the uses of Boltzmann machine. ☞ [SPPU : 5 Marks]

Ans. : • The main purpose of the Boltzmann machine is to optimize the solution of a problem. It optimizes the weights and quantities related to the particular problem assigned to it. This method is used when the main objective is to create mapping and learn from the attributes and target variables in the data. When the objective is to identify an underlying structure or the pattern within the data, unsupervised learning methods for this model are considered to be more useful. Some of the most popular unsupervised learning methods are clustering, dimensionality reduction, anomaly detection and creating generative models.

- Each of these techniques has a different objective of detecting patterns such as identifying latent grouping, finding irregularities in the data, or generating new samples from the available data. These networks can also be stacked layer-wise to build deep neural networks that capture highly complicated statistics. The use of restricted Boltzmann machines has gained popularity in the domain of imaging and image processing as well since they are capable of modelling continuous data that are common to natural images. They also are being used to solve complicated quantum mechanical many-particle problems or classical statistical physics problems like the Ising and Potts classes of models.

Q.12 Write a note on restricted Boltzmann machines. ☞ [SPPU : 10 Marks]

Ans. : Boltzmann machine : • In a full Boltzmann machine, each node is connected to every other node and hence the connections grow **exponentially.** This is the reason RBMs are used. The restrictions in the node connections in RBMs are as follows -

- Hidden nodes cannot be connected to one another.
- Visible nodes connected to one another.

- A restricted term means that one is not permitted to connect two types of layers that are of the same type to one another. In other words, the two

hidden layers or input layers of neurons are unable to form connections with one another. However, there may be connections between the apparent and hidden layers.

- Since there is no output layer in the machine, it is unclear how the weights would be detected and modified, and determine whether or not the prediction was right. **One response fits all the questions : Restricted Boltzmann Machine.**
- The neural network that is a part of the energy-based model is called RBM. It is a generative, unsupervised, probabilistic deep learning algorithm. Finding the joint probability distribution that maximizes the log-likelihood function is the goal of RBM. RBM only has two layers : the input layer and the hidden layer and it is undirected. All of the hidden nodes are linked to all of the visible nodes. RBM is also referred to as an asymmetrical bipartite graph since it has two layers : a visible or input layer and a hidden layer. The visible nodes don't have any connections inside the same layer. The concealed nodes are not connected intralayer either. Only the input and hiding nodes have connections.
- All of the nodes in the original Boltzmann machine are connected. RBM is referred to as a Restricted Boltzmann Machine since it restricts intralayer connectivity.
- RBMs do not modify their weights through backpropagation and gradient descent since they are undirected. They change their weights using a technique known as contrastive divergence. The visible nodes' weights are initially created at random and utilized to create the hidden nodes. Then, these concealed nodes recreate exposed nodes using the same weights. All throughout, the same weights were utilized to reconstruct the visible nodes. Due to their lack of connectivity, the created nodes are different from one another.
- Some key characteristics of the Restricted Boltzmann machine are :
    - There are no connections between the layers.
    - They employ symmetric and recurring structures.
    - It is an algorithm for unsupervised learning, meaning that it draws conclusions from the input data without labeled replies.
    - In their learning process, RBMs attempt to link low energy states with high probability ones and vice versa.

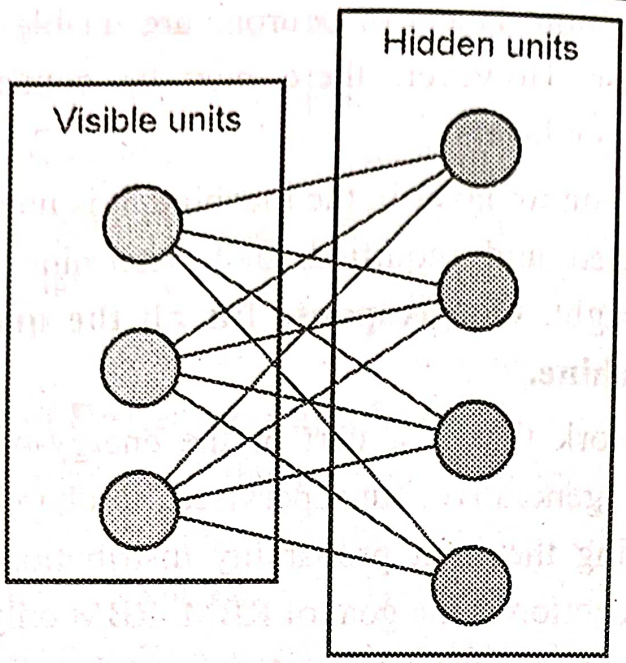


Fig. Q.12.1 RBMs

Working of RBM

- A low-level feature from a learning target item in the dataset is used by each visible node. The hidden layer's node 1 multiplies x by weight and adds it to a bias. These two procedures' outcomes are fed into an activation function, which, given an input of x, creates the output of the node, or the signal strength traveling through it.
- One can examine how many inputs would mix at a single hidden node. The output of the node is created by multiplying each x by a distinct weight, summing the products, adding the sum to a bias and then passing the final result once again via an activation function.
- Each input x is multiplied by its corresponding weight w at each buried node. In other words, a single input x would have three weights in this situation, totaling 12 weights (4 input nodes x 3 hidden nodes). The weights between the two layers will always create a matrix with input nodes in the rows and output nodes in the columns.
- The four inputs are sent to each hidden node, multiplied by each weight. Each hidden node receives one output as a result of the activation algorithm after the sum of these products is once more added to a bias (which compels at least some activations to occur).

Training of RBM

- Two methods - Gibbs sampling and Contrastive divergence are used to train RBM.

- When direct sampling is challenging, the Markov chain Monte Carlo method known as Gibbs sampling is used to get a series of observations that are roughly drawn from a given multivariate probability distribution.
- The prediction is the hidden value by h and p(h|v) if the input is represented by v. P(v|h) is utilized for the regenerated input values' prediction when the hidden values are known. Let's say that after k rounds, v k is acquired from input value v 0 after this process has been performed k times.
- In order to approximate the graph slope, a graphical slope showing the relationship between a network's errors and its weights is called the gradient in contrastive divergence. Contrastive divergence is a rough maximum-likelihood learning approach and is employed when one needs to approximate the learning gradient of the algorithm and choose which direction to go in because one cannot directly evaluate a set of probabilities or a function.
- Weights are updated on CD. The gradient is first determined from the reconstructed input, and the old weights are updated by adding the delta.

Q.13 List advantages, disadvantages and applications of restricted Boltzmann machines. ☞ **[SPPU : 8 Marks]**

Ans. : Advantages of RBM

- The hidden layer's activations can be included in other models as valuable features to boost performance.
- Due to the limitations on connections between nodes, it is faster than a standard Boltzmann machine.
- Efficiently computed and expressive enough to encode any distribution.

Disadvantages of RBM

- The backpropagation algorithm is more well known than the CD-k algorithm, which is utilized in RBMs.
- Because it is challenging to calculate the energy gradient function, training is more challenging.
- Weight modification.

Applications of RBMs

- Restricted Boltzmann machines are the most successful type of Boltzmann machines. They have been used in a wide range of applications.

i. Dimensionality reduction

- The RBM's architecture is convenient for such type of problems since their hidden nodes are of lower dimension than their visible nodes, hence they have a reduced representation of the data.

ii. Data reconstruction

- RBM is an undirected graphical model. However, it can be shown to be equivalent to a directed graphical model with infinite number of layers.

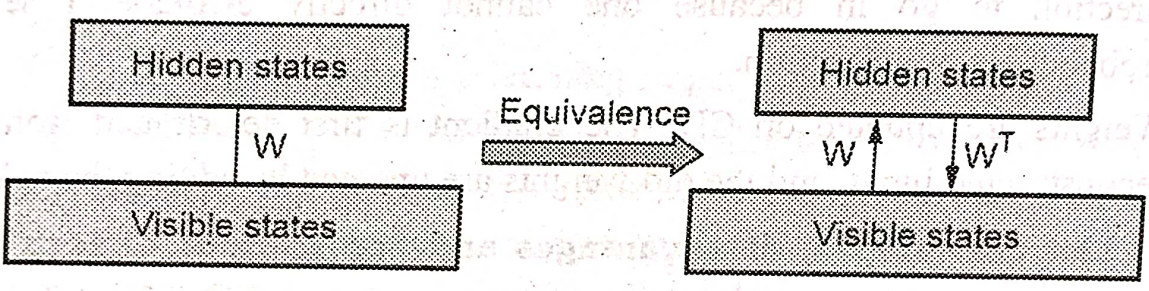


Fig. Q.13.1 Equivalence between undirected and directed RBM graph

- With this idea in mind, and with the idea that Auto-encoders (AE) are used to reconstruct data, one can unfold an RBM to approximate the AE architecture to perform the same task.

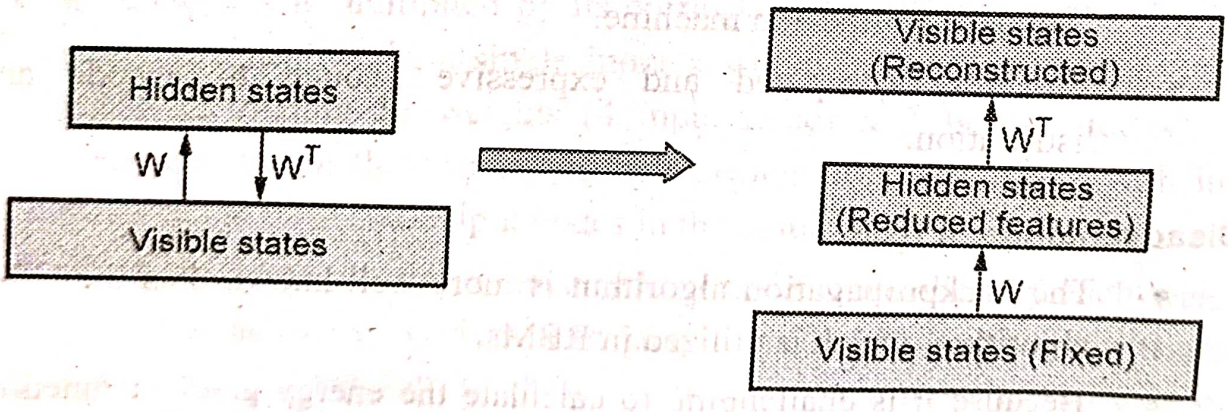


Fig. Q.13.2 Using RBM to approximate auto-encoder

iii. Recommendation engines

- One of the most known applications for RBM is collaborative filtering where the network should provide a recommendation to the end user.
- The basic idea behind recommender systems is to create a different training instance and a different RBM for each user, depending on the ratings provided by the users. All RBMs share weights.
- It is also important to notice that the ratings range from 1 to 5, hence one should use softmax nodes instead of sigmoid nodes, in order to correspond to the rating values.

Q.14 Write a note on Deep Belief Networks. ☞[SPPU : 5 Marks]

Ans. : • Consider stacking numerous RBMs so that the outputs of the first RBM serve as the input for the second RBM, and so forth. Deep Belief Networks are the name given to these networks. Each layer's connections are undirected (as each layer is an RBM). Those between the strata are simultaneously directed (except for the top two layers – whose connections are undirected). The DBNs can be trained in two different ways :

- **Greedy layer-wise training algorithm :** RBMs are trained using a greedy layer-by-layer training algorithm. The orientation between the DBN layers is established as soon as the individual RBMs have been trained (i.e., the parameters, weights, and biases, have been defined).
- **Wake-sleep algorithm :** The DBN is trained from the bottom up using a wake-sleep algorithm (connections going up indicate wake), and then from the bottom up using connections indicating sleep.

- Deep Belief Networks are pre-trained using a greedy algorithm like all other networks. The algorithm applies a layer-by-layer approach to learn the top-down weights, and these weights determine the dependencies between each layer. In this network, numerous steps of Gibbs sampling run on the top two hidden layers. This step essentially creates a sample from the Restricted Boltzmann Machine defined by the top two hidden layers. Later, a single pass of the previous sampling is used to find a piece from the visible layer throughout the rest of the model.

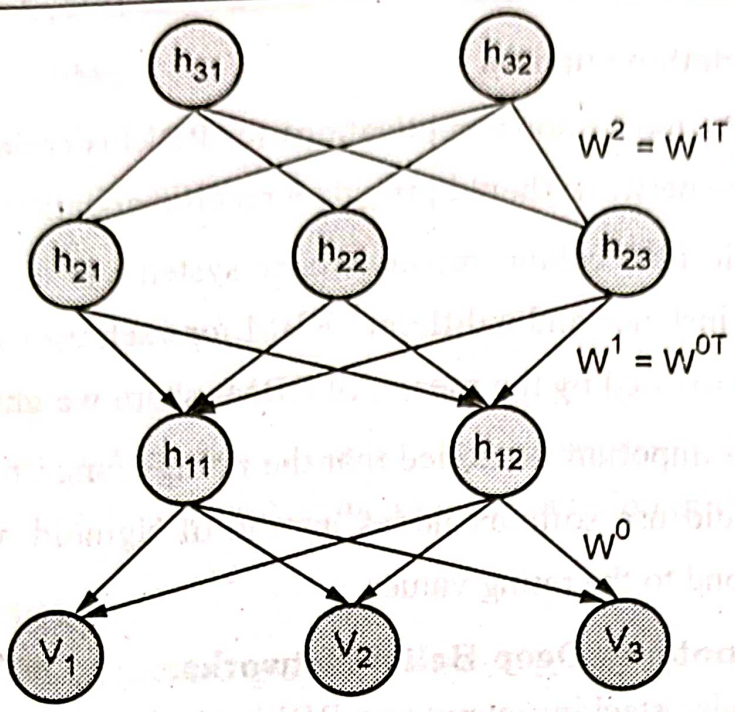


Fig. Q.14.1 DBNs

- In order to ensure that the layer connections only work downwards, the RBMs can be stacked, trained, and then do so (except for the top two layers).

Q.15 Write a note on Deep Boltzmann Machines. ☞ **[SPPU : 5 Marks]**

Ans. : • Similar to DBNs, DBMs also have undirected connections between the layers in addition to the connections inside the levels (unlike DBN, in which the layer connections are directed). DBMs can be utilized for more challenging jobs since they can extract more sophisticated or complex features.

- The Deep Boltzmann Machine works by greedy layer-by-layer training. It depends on learning stacks of restricted Boltzmann machines. In layer-wise training, increase the input twice for lower-level and top-level Restricted Boltzmann Machine. The lower level Restricted Boltzmann Machine inputs are doubled to compensate for the deficiency of top-down information into the first hidden layer. Likewise, the hidden units are doubled for the top-level Restricted Boltzmann Machine to pay for the lack of bottom-up input.

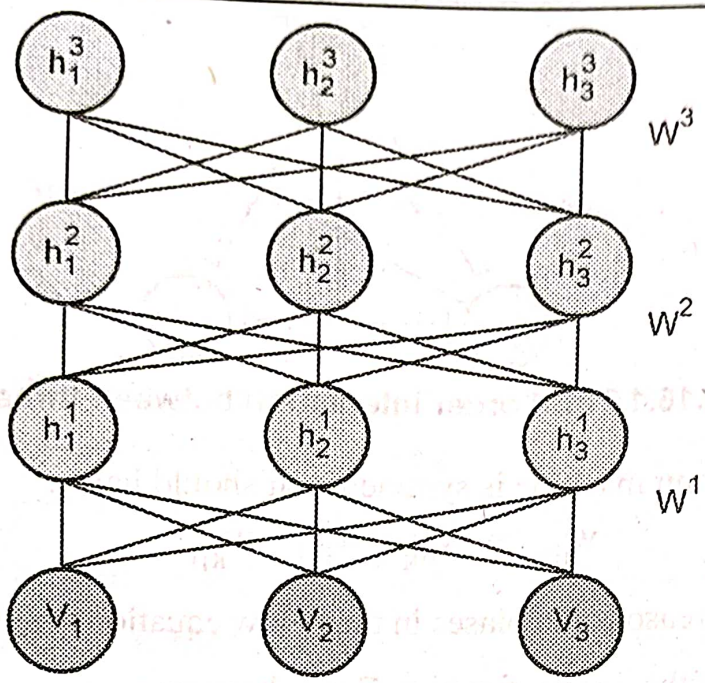


Fig. Q.15.1 DBMs

Q.16 Write a note on conditional Boltzmann machines and higher-order Boltzmann machines. ☞ **[SPPU : 5 Marks]**

Anms. : • Boltzmann machines are used to model distributions of data vectors. In order to do so they learn automatically the existing patterns in the given data which makes them more suitable for unsupervised learning tasks. However, they can also be used in **supervised learning** tasks where the goal is to predict the output that is conditioned on the input.

- The equations will be the same, the only difference is in the learning process. When generating the **model-centric samples,** instead of randomly initializing the visible and the hidden nodes, a **subset** from the **visible** nodes will be **clamped.** The latter will act as the inputs and the remaining visible nodes will act as outputs.
- Now the network will be maximizing the log probability of the observed output conditioned on the input vectors (the clamped visible nodes).

Higher-order Boltzmann Machines

- Boltzmann machine is a non-linear network that models interactions between pairwise stochastic binary nodes. However, the learning algorithm of a BM can be extended to higher order interaction. This type of networks is used to faster the learning process. For example for order $l = 3$, there is a weight w_{ijk} that is shared between three nodes as shown in the Fig. Q.16.1 below.

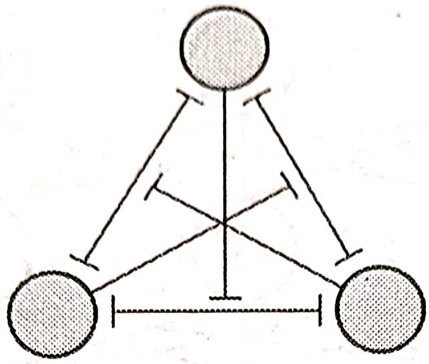


Fig. Q.16.1 Third order interaction between three nodes

Since a Boltzmann machine is symmetric, it should have :

$$w_{ijk} = w_{jik} = w_{ikj} = w_{kji}$$

For simplicity reasons the biases in the below equations are ignored.

The equation of the energy function **E** will become :

$$E = -\frac{1}{3}\sum_i\sum_j\sum_k w_{ijk} s_i s_j s_k$$

In Gibbs sampling, the conditional probability will be computed just like in standard BM, by applying the **sigmoid** function on the energy gap for node **i.** However the equation of the latter will be modified like the following :

$$\Delta E_i = \sum_j\sum_k w_{ijk} s_j s_k$$

Finally, the update rule will be the same except for the term $s_i s_j$ that will be replaced by $s_i s_j s_k$.

Q.17 List limitations of Boltzmann machines. ☞ **[SPPU : 5 Marks]**

Ans. : • Boltzmann machines suffer from many limitations that make them unsuitable for practical use.

- The learning process is very slow especially when the weights are large and the equilibrium distribution is multimodal.
- The generation of data using Boltzmann machine is challenging compared to other generative models, because of the cyclic dependency between the nodes.
- Boltzmann machine suffer from the **variance-trap** that causes the activations to saturate. This is harmful for the network because the nodes no longer outputs values between **0** and **1** .

3.3 : ANN for Pattern Recognition

Q.18 What is pattern recognition ? What are features of pattern recognition ? ☞ [SPPU : 8 Marks]

Ans. :

- Human problem solving is basically a pattern processing problem and not a data processing problem. In any pattern recognition task humans perceive patterns in the input data and manipulate the pattern directly.
- Pattern recognition is a process of finding regularities and similarities in data using machine learning data. These similarities can be found based on statistical analysis, historical data, or the already gained knowledge by the machine itself.
- A pattern is a regularity in the world or in abstract notions. If music is being discussed, a description of a type would be a pattern. If a person keeps watching music videos, Video playing website wouldn't recommend the person sports videos.
- The act of recognition can be divided into two broad categories : recognizing concrete items and recognizing abstract items. The recognition of concrete items involves the recognition of spatial and temporal items. Examples of spatial items are fingerprints, weather maps, pictures and physical objects. Examples of temporal items are waveforms and signatures. Recognition of abstract items involves the recognition of a solution to a problem, an old conversation or argument, etc. In other words, recognizing items that do not exist physically.

Features of pattern recognition

- Pattern recognition system should recognize familiar patterns quickly and accurate
- Recognize and classify unfamiliar objects
- Accurately recognize shapes and objects from different angles
- Identify patterns and objects even when partly hidden

- Recognize patterns quickly with ease and with automaticity.

Q.19 List down and explain various pattern recognition tasks.

Ans. : • The inherent differences in information handling by human beings and machines in the form of patterns and data and in their functions in the form of understanding and recognition. Below are pattern recognition tasks.

1. **Pattern association -** Pattern association problem involves storing a set of patterns or a set of input-output pattern pairs in such a way that when test data are presented, the pattern or pattern pair corresponding to the data is recalled. This is purely a memory function to be performed for patterns and pattern pairs. Typically, it is desirable to recall the correct pattern even though the test data are noisy or incomplete. The problem of storage and recall of patterns is called autoassociation. Since this is a content addressable memory function, the system should display accretive behaviour, that is, should recall the stored pattern closest to the given input. It is also necessary to store as many patterns or pattern pairs as possible in a given system. Printed characters or any set of fixed symbols could be considered as examples of patterns for these tasks. Note that the test patterns are the same as the training patterns, but with some noise added or some portions missing. In other words, the test data are generated from the same source in an identical manner as the training data.

2. **Pattern mapping -** In pattern mapping, given a set of input patterns and the corresponding output pattern or class label, the objective is to capture the implicit relationship between the patterns and the output, so that when a test input is given, the corresponding output pattern or the class label is retrieved. Note that the system should perform some kind of generalization as opposed to memorizing the information. This can also be viewed as a pattern classification problem belonging to supervised learning category. Typically, in this case the test patterns belonging to a class are not the same as the training patterns, although they may originate from the same source. Speech spectra of steady vowels generated by a person or hand-printed characters, could be considered as examples of patterns for pattern mapping problems. Pattern mapping generally displays interpolative behaviour, whereas pattern classification displays accretive behaviour.

3. **Pattern grouping** - In this case, given a set of patterns, the problem is to identify the subset of patterns possessing similar distinct features and group them together. Since the number of groups and the features of each group are not explicitly stated, this problem belongs to the category of unsupervised learning or pattern clustering. Note that this is possible only when the features are unambiguous as in the case of hand-printed characters or steady vowels. In the pattern mapping problem the patterns for each group are given separately, and the implicit, although distinct, features have to be captured through the mapping. In pattern grouping on the other hand, patterns belonging to several groups are given, and the system has to resolve the groups.
4. **Feature mapping** - In several patterns the features are not unambiguous. In fact the features vary over a continuum, and hence it is difficult to form groups of patterns having some distinct features. In such cases, it is desirable to display the feature changes in the patterns directly. This again belongs to the unsupervised learning category. In this case what is learnt is the feature map of a pattern and not the group or class to which the pattern may belong. This occurs, for example, in the speech spectra for vowels in continuous speech. Due to changes in the vocal tract shape for the same vowel occurring in different contexts, the features (formants or resonances of the vocal tract in this case) vary over overlapping regions for different vowels.
5. **Pattern variability** - There are many situations when the features in the pattern undergo unspecified distortions each time the pattern is generated by the system. This can be easily seen in the normal handwritten cursive script. Human beings are able to recognize them due to some implicit interrelations among the features, which themselves cannot be articulated precisely. Classification of such patterns falls into the category of pattern variability task.
6. **Temporal patterns** - Human beings are able to capture effortlessly the dynamic features present in a sequence of patterns. This is true, for example, in speech where the changes in the resonance characteristics of the vocal tract system (e.g. formant contours) capture the significant information about the speech message. This is also true in any dynamic scene situation. All such situations require handling sequences of static patterns simultaneously, looking for changes in the

features in the subpatterns in adjacent pattern pairs.

7. **Stability-plasticity dilemma** - In any pattern recognition task the input patterns keep changing. Therefore it is difficult to freeze the categorization task based on a set of patterns used in the training set. If it is frozen, then the system cannot learn the category that a new pattern may suggest. In other words, the system lacks its plasticity. On the other hand, if the system is allowed to change its categorization continuously, based on new input patterns, it cannot be used for any application such as pattern classification or clustering, as it is not stable. This is called stability-plasticity dilemma in pattern recognition.

Q.20 What are the steps taken for pattern recognition input processing ? ☞ **[SPPU : 8 Marks]**

Ans. : • Recognition of an item involves three levels of processing : input filtering, feature extraction and classification

- **Filtering** is removing unwanted information or data from input. Depending on the application, the filter algorithm or method will change. For example, consider finger print identification. Each time one scans the fingerprints through a (non-ink) fingerprint device, the scanned output may be different. The difference may be due to a change in contrast or brightness or in the background of the image. There could be some distortion. In order to process the input, one may need only lines in the fingerprints and one may not need the other parts or background of the fingerprint. In order to filter out the unwanted portion of the image and replace it with a white background, one needs a filter mechanism. Once the image is filtered through the filter mechanism, one will get standard clean finger prints only with lines, which in turn helps with the process of feature extraction.
- **Feature extraction** is a process of studying and deriving useful information from the filtered input patterns. The derived information may be general features, which are evaluated to ease further processing. For example, in image recognition, the extracted features will contain information about gray shade, texture, shape or context of the image. This is the main information used in image processing. The methods of feature extraction and the extracted features are application dependent.

- **Classification** is the final stage of the pattern recognition. This is the stage where an automated system declares that the inputted object belongs to a particular category. There are many classification methods in the field. Classification method designs are based on the following concepts.

  i. **Member-roster concept -** Under this template-matching concept, a set of patterns belonging to a same pattern is stored in a classification system. When an unknown pattern is given as input, it is compared with existing patterns and placed under the matching pattern class.

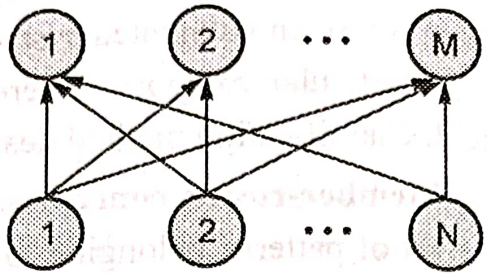
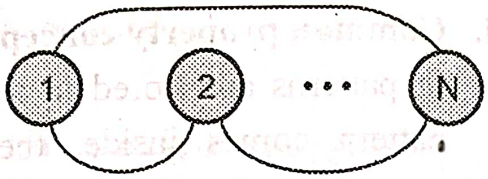
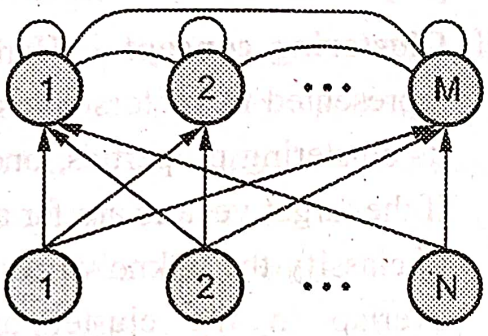
  ii. **Common property concept -** In this concept, the common properties of patterns are stored in a classification system. When an unknown pattern comes inside, the system checks its extracted common property against the common properties of existing classes and places the pattern/object under a class, which has similar, common properties.

  iii. **Clustering concept -** Here, the patterns of the targeted classes are represented in vectors whose components are real numbers. So, using its clustering properties, one can easily classify the unknown pattern. If the target vectors are far apart in geometrical arrangement, it is easy to classify the unknown patterns. If they are nearby or if there is any overlap in the cluster arrangement, one needs more complex algorithms to classify the unknown patterns. One simple algorithm based on the clustering concept is minimum distance classification. This method computes the distance between the unknown pattern and the desired set of known patterns and determines which known pattern is closest to the unknown and, finally, the unknown pattern is placed under the known pattern to which it has minimum distance. This algorithm works well when the target patterns are far apart.

Q.21 What are functional units of pattern recognition ? How ANN helps in pattern recognition ? ☞ **[SPPU : 8 Marks]**

Ans. : • Pattern recognition systems consist of four functional units - A feature extractor (to select and measure the representative properties of raw input data in a reduced form), a pattern matcher (to compare an input pattern to reference patterns using a distance measure), a reference templates memory (against which the input pattern is compared), and a decision maker (to make the final decision as to which reference template is the closest to the input pattern).

- Below are ANN that are used in pattern recognition

1. Feedforward ANN a) Pattern association b) Pattern classification c) Pattern mapping / classification	
2. Feedback ANN a) Auto association b) Pattern storage (LTM) c) Pattern environment storage (LTM)	
3. Feedforward and Feedback ANN a) Pattern storage (STM) b) Pattern clustering c) Features map	

Q.22 Explain pattern association task carried out by feedforward ANN in pattern recognition. ☞ **[SPPU : 8 Marks]**

Ans. : Pattern association - The objective is to design a linear network that can capture the association in the pairs of vectors (a~,bz), l = 1, 2... L, through a set of weights to be determined by a learning or training law. The input data used in training are typically generated synthetically, like machine printed characters. The input data used for recall may be corrupted by external noise.

- The network consists of a set of weights connecting the two layers of processing units, the output function of each unit being linear. Such a network is called a linear associator network. Due to linearity of the output function of each unit, the activation values and the output signals

of the units in the input layer are same as the input data values. The activation value of the ith unit in the output layer is given by,

$$y_i = \sum_{j=1}^{N} w_{ij} a_{ij}$$

- The output of the ith unit is the same as its activation value y_i, since the output function of the unit is linear. The objective is to determine a set of weights w_{ij} in such a way that the actual output b'_{ii} is equal to the desired output b_{ii} for all the L pattern pairs.
- If the input L pattern vectors $\{a_l\}$ are all orthogonal, then it is possible to use Hebb's learning law to determine the optimal weights of the network. It should be noted that a learning law enables updating of weights as patterns are applied one by one to the network. The optimality of the weights is determined by minimizing the mean squared error between the desired and the actual output values. The optimal weights after I pattern pairs are fed to the network are given by,

$$w_{ij}^{(l)} = w_{ij}^{l-1} + b_{li} a_{lj}, \quad w_{ij}^{0} = 0.$$

- The final optimal weights for pattern association task are given by,

$$w_{ij} = w_{ij}^{L}$$

- If the input vectors {as} are only linearly independent, but not necessarily orthogonal, then the optimal weights that minimize the mean squared error can be obtained using the LMS learning law.
- Once the network is trained, for any given input pattern a_l, the associated pattern b_l can be recalled using the equations,

$$y_i = \sum_{j=1}^{N} w_{ij} a_{lj} \quad \text{and} \quad b_{li} = y_i$$

- When noisy input patterns are used during recall, i.e., $\{a_{li}\}$, then the recalled pattern $\{b'_{li}\}$ will also be noisy. Since the given set of input pattern $\{a_l\}$, $l = 1 \ldots L$, is assumed to be linearly independent, the number of patterns in the input set is limited to the dimensionality of the input vector, namely, N. Therefore, it is not possible to store more than N pattern pairs in a linear associative network. If the number of input pattern are more than its dimension (N) or if the input set (even for L < N) are not

linearly independent, then the resulting weight vectors are not optimal any more. In such a case the recall of the associative pattern for a given input pattern may not be correct always.

- Even if the input patterns are linearly independent and optimal weights are used, the recall may be in error if a noisy input pattern is presented to recall the associated pattern.

Q.23 Explain pattern classification task carried out by feedforward ANN in pattern recognition. ☞ [SPPU : 8 Marks]

Ans. : Pattern classification : In an N-dimensional space if a set points could be considered as input patterns without restriction on their number, and if an output pattern, not necessarily distinct, is assigned to each of the input patterns, then the number of distinct output patterns can be viewed as distinct classes or class labels for the input patterns. Since there is no restriction on the type and number of input patterns, the input-output pattern pairs (a_l, b_l), $l = 1, 2, \ldots L$ in this case can be considered as a training set for a pattern classification problem. Typically for pattern classification problems the output patterns are points in a discrete (normally binary) M-dimensional space. The input patterns are usually from natural sources like speech and hand-printed characters. The input patterns may be corrupted by external noise at the time of recall.

- A two layer network with non-linear (threshold or hard limiting) output function for the units in the output layer, can be used to perform the task of pattern classification. This may also be identified as a single layer perceptron network.
- The network can be trained (i.e. weights can be adjusted) for the given set of input-output patterns using a delta rule.
- The corresponding learning is also called perceptron learning law.
- The training patterns are applied several times, if needed, until the weights do not change appreciably. But there is no guarantee that the weights converge to some stable values. Convergence of the weights depends on whether the problem specified by the input-output pattern pairs is representable or not by a network of this type. For all representable problems the learning law converges.

- During recall, a pattern generated from one of the same sources is given as input. By direct computation of the weighted sum of the input, the network determines the pattern class to which the input belongs. The network thus exhibits accretive behaviour. Even when the input pattern is noisy, the output class may still be correct, provided the noise has not significantly altered the input pattern.

Q.24 Explain pattern mapping task carried out by feedforward ANN in pattern recognition.

☞ [SPPU : 8 Marks]

Ans. : Pattern mapping : For a pattern mapping problem input and output patterns are points in the N- and M-dimensional continuous spaces, respectively. The objective is to capture the implied functional relationship or mapping function between the input and output by training a feedforward neural network. This is also called the generalization problem. Once the network generalized by capturing the mapping function through its weights, then during recall from an input pattern the network produces an output which is an interpolated version of the outputs of the training input patterns near the current input pattern. The input patterns are generally naturally occurring patterns as in speech and hand printed characters.

- A multilayer feedforward network with at least two intermediate layers in addition to the input and output layers can perform a pattern mapping task. The number of units in the input and output layers correspond to the dimensions of the input and output patterns, respectively. The additional layers are called hidden layers and the number of units in a hidden layer is determined depending on the problem, usually by trial and error. The network can be trained (i.e. weights at different layers can be adjusted) for a given set of input-output pattern pairs using a generalized delta rule or backpropagation law.
- It is derived using the principle of gradient descent along the error surface in the weight space. The given patterns are applied in some random one by one, and the weights are adjusted using the backpropagation law. The pattern pairs may have to be applied several times till the output error is reduced to an acceptable value.
- Once the network is trained, it can be used to recall the appropriate pattern (in this case some interpolated) for a new input pattern. The computation is straight forward in the sense that the weights and the output functions of

the units at different layers are used to compute the activation values and output signals. The signals from the output layer correspond to the output.

Q.25 Explain pattern recognition tasks by feedback ANN.

☞ [SPPU : 10 Marks]

Ans. : Auto association (Pattern Srograge) : • Arch : Single layer with feedback, linear processing units

- Learning : Hebb (orthogonal inputs), Delta (linearly independent inputs)
- Recall : Direct
- Limitation : Linear independence of patterns, # of patterns limited to dimensionality
- To overcome : Non-linear processing units, becomes a pattern storage problem.

Pattern storage

- Arch : FBNN, non-linear processing units, states, Hopfield energy analysis
- Learning : Not important
- Recall : Activation dynamics until stable states are reached
- Limitation : False minima, hard problems, limited # patterns
- To overcome : Stochastic update, hidden units.

Pattern environment storage

- Arch : Boltzmann machine, nonlinear processing units, hidden units, stochastic update
- Learning : BM learning law, simulated annealing
- Recall : Activation dynamics, simulated annealing
- Limitation : Slow learning
- To overcome : Different architecture

i. **Auto association -** auto association is the task where in the input and output patterns in each pair are the same i.e., $a_l = b_l$, $l = 1, 2, \ldots, l$. The objective in an auto association task is to design a network that can recall a stored pattern given a corrupted (noisy or partial) version of the pattern. A feedback network with N linear processing units can perform the task of auto association. Such a network can be trained (i.e., the weights can

be determined) using either Hebb's law or delta rule. Hebb's learning law leads to a set of optimal weights when the given patterns are orthogonal. Delta rule leads to set of optimal weights when the given patterns are linearly independent. Pattern recall will be exact when the test pattern is same as one of the stored ones, represented by the weights. If the test pattern is a noisy version of the stored pattern, the recalled pattern is also a noisy version of the stored pattern. In fact the network recalls the input pattern itself, as every vector is associated with itself, thus completely eliminating any accretive behavior.

- Thus auto association by a feedback network with linear units is not going to serve any purpose. Moreover, the number of patterns is limited to the dimensionality of the pattern. Although there is no simple learning law, it can be shown that the weights of such a network can be determined to store any L <= N patterns, without any error in recall, where N is the dimension of the input pattern space. The auto association task by a feedback network with linear units has, any input pattern comes out as itself if it is one of the stored ones and a noise input comes out as a noisy pattern, not as the nearest stored pattern. To overcome this limitation due to the absence of accretive behaviour, the linear units are replaced with units having nonlinear output functions. The resulting feedback network can then perform pattern storage task.

ii. **Pattern storage :** The objective is to store a given set of patterns so that any one of the patterns can be recalled exactly when an approximate (corrupted) version of the pattern is presented to the network. What is needed is the storage of features and their spatial relations in the patterns and the pattern recall should take place even when the features and their relations are slightly modified due to noise and distortion. The approximation of pattern refers to the closeness of the features and their spatial relations in the pattern when compared to the original stored pattern. What is actually stored in practice is the information in the pattern data itself. The approximation is measured in terms of some distance, like Hamming distance (in case of binary patterns.) The distance

features is automatically realized through the threshold (binary) features of the output function of a processing unit. The pattern storage is accomplished by a feedback network consisting of nonlinear processing units.

- For the simplest case, the weights on the connecting links between units are assumed to be symmetric, i.e. $w_{ij} = w_{ji}$ and that there is no self feed back, i.e. $w_{ii} = 0$. The output signals of all units at any instant of time define the state of the network at that instant. Each state of the network can be assumed to correspond to some energy the instant. Each state of the network can be assumed to correspond to some energy which is defined in terms of the output state $\{s_i\}$ and weights $[w_{ij}]$ of the network as

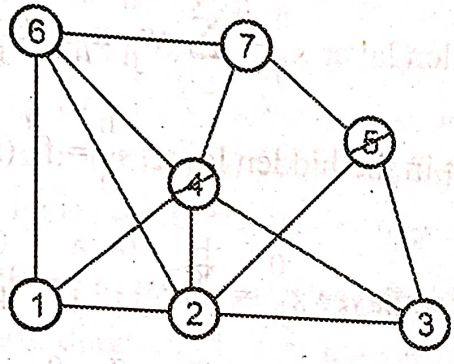
$$E = -\frac{1}{2}\sum_{i}\sum_{j \neq 1} s_i w_{ij} s_j - \sum_{i} I_i s_i + \sum_{i} \theta_i s_i$$

where I_i is an external input and θ_i is the threshold of the unit. The energy as a function of the output state can be viewed as something like an energy landscape. The shape of the landscape is dictated by the network units and their interconnection strengths (weights). The feedback and the non-linear processing units of the network create *basins of attraction* in the energy landscape. The basins tend to be region of equilibrium states. If there is a fixed state (point in the output state space) in each of these basins where the energy is minimum, these states corresponds to fixed points of equilibrium. There could also be periodic (or oscillating) regions or chaotic regions of equilibrium.

- It is the existence of the basins of attraction that is exploited to store the desired patterns and recall them even with approximate inputs as keys. Each pattern is stored at a fixed point of equilibrium of the energy minimum. An erroneous or distorted pattern is more likely to be closer to the corresponding true pattern than to the other stored patterns. Each input pattern results in a state of the network that may be closer to the desired state, in the sense that it may lie near the basin of attraction corresponding to the true state. Since an arbitrary state need not correspond to a stable state, the activation dynamics of the network may eventually lead to a stable state from which the desired pattern may be read or derived.

- Hopfield Net algorithm to store and recall a set of bipolar patterns.

iii. Pattern environment storage : A pattern environment is described by the set of desired patterns together with their probability distribution. The objective is to store a pattern environment in a network in such a way that the average probability of error in recall is minimized. This is achieved if the energy landscape is designed in such a way that the desired patterns are stored at the stable states corresponding to the lowest minima, with the higher probability patterns at lower energy minima points. Boltzmann machine architecture together with the Boltzmann learning law can achieve an optimal storage of pattern environment.



Visible units : 1,2,3 are input units, 4, 5 are output units

Hidden units (4 and 5)

Fig. Q.25.1 Boltzmann architecture

- Each unit is connected to every other unit, although only a few connections are shown in the figure. Some of the visible units can be identified as input units and others as output units if the machine is to be used for pattern mapping.
- The architecture consists of a number of processing units with each unit connecting to all the other units. The number of units is typically larger than the dimension of the input pattern. The additional units are called hidden units. Use of hidden units helps in overcoming the limitation of the hard problems of pattern storage by a fully connected network. The patterns are applied to the so-called visible units, the number of visible units being equal to the dimension of the input patterns.

Q.26 Write a note backpropagation algorithm. ☞ **[SPPU : 5 Marks]**

Ans. : Given a set of input-output patterns a_l, b_l = 1, 2, ..., L

l^{th} input vector $a_l = (a_{l1}, a_{l2}, \ldots, a_{lN})^T$ and output vector $b_l = (b_{l1}, b_{l2}, \ldots, b_{lN})^T$

Assume only one hidden layer and initial setting of weights to be arbitrary

Assume input layer with only linear units. Then output signal = input activation value η is the learning rate parameter.

Activation of unit i in the input layer $x_{li} = a_{li}$

Activation of unit j in the hidden layer $x_{lj}^h = \sum_{i=l}^{N} w_{ji}^h x_{li} + \theta_j^h$

Output signal from the jth unit in the hidden layer, $s_{lj}^h = f_j^h (x_{lj}^h)$

Activation of unit k in the output layer $x_{lk}^0 = \sum_{j=1}^{H} w_{kj}^0 s_{lj}^h + \theta_k^0$

Output signal from unit k in the output layer $s_{lk}^0 = f_k^0 (x_{lk}^0)$

Error term for the kth output unit $\delta_k^0 = (b_{lk}^0 - s_{lk}^0) f_k^0 (x_{lk}^0)$

Update the weights on the output layer $w_{kj}^0 (t+1) = w_{kj}^0(t) + \eta \delta_{lk}^0 s_{lj}^h$

Error term for the jth hidden unit $\delta_{lj}^h = f_j^{h'} (x_{lj}^h) \sum_{k=1}^{M} \delta_{lk}^0 w_{kj}^0$

Update the weights on the hidden layer $w_{ji}^h (t+1) = w_{ji}^h(t) + \eta \delta_{lj}^h a_{li}$

Calculate the error for the lth pattern $E_l = \frac{1}{2} \sum_{k=1}^{M} \delta_{lk}^2$

Total error for all patterns $E = \sum_{l=1}^{L} E$

Apply the given patterns, may be several times, in some random order and update the weighs until the total error reduces to an acceptable value.

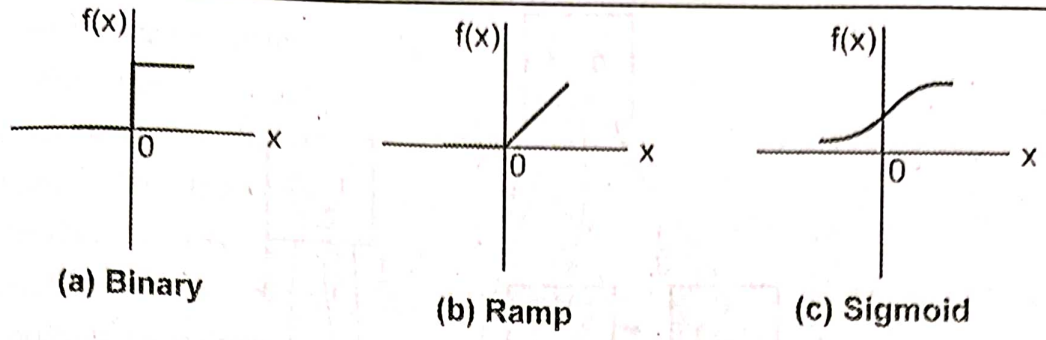


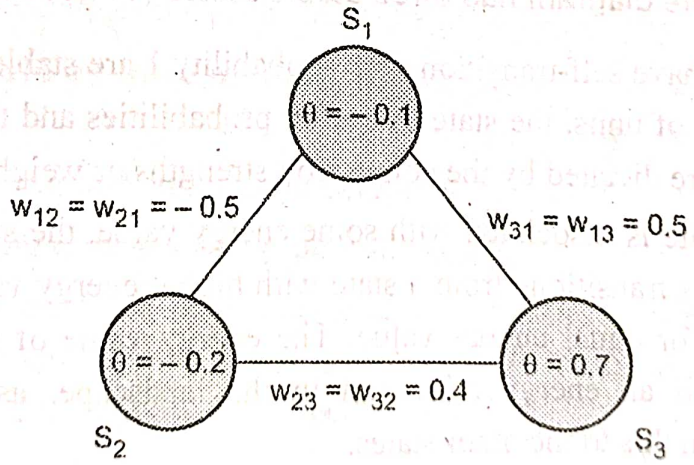
Fig. Q.26.1 Some nonlinear functions

- If the nonlinear output function of each unit is a binary threshold function (curve a in above figure), then the stable stables of the network would lie at the corners of the binary hypercube in the N-dimensional discrete binary space. On the other hand, if the output function is a semilinear function (curve C in above figure), then the points corresponding to these states may move closer to each other within the unit hypercube. If the output function is a horizontal line, then almost all states remain close to each other, and hence there will be only one state for the network.

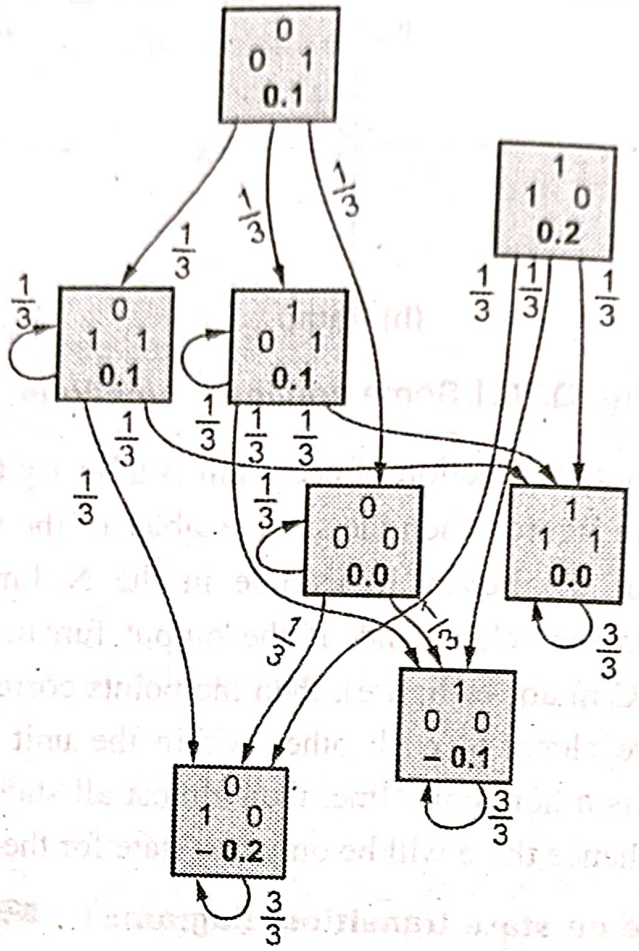
Q.27 Write a note on state transition diagram. ☞ **[SPPU : 5 Marks]**

Ans. : • A transition diagram or state transition diagram is a directed graph, **used to represent a finite state machine.** These are used to model objects which have a finite number of possible states and whose interaction with the outside world can be described by its state changes in response to a finite number of events.

- Given a network, it is possible to determine the state transition diagram. Fig. Q.27.1 below shows the state transition diagram for a 3-unit network.
- The diagram illustrates the different states of the network and their transition probabilities.



(a)



(b)

Fig. Q.27.1 (a) A 3-unit feedback network with symmetric weights and binary threshold units. Activation dynamics $x_j = \sum_j w_{ji} s_i - \theta_j$, $s_j = f(s_j)$; Energy $E = -\frac{1}{2}\sum_i \sum_j w_{ij} s_i s_j + \sum_i s_i \theta_i$. (b) State transition diagram for the 3-unit network of Fig. (a). Each block represents a state given by sequence s_1, s_2, s_3. There are eight blocks for eight states. The energy for each state is indicated by the bold numbers with each block. Note that the state diagram has three stable states (111,100 and 010)

- States which have self-transition with probability 1 are stable states. For a given number of units, the state transition probabilities and the number or stable states are dictated by the connection strengths or weights.
- Since each state is associated with some energy value, the state transition diagram shows transitions from a state with higher energy value to a state having lower or equal energy value. The energy value of a stable state corresponds to an energy minimum in the landscape, as there is no transition from this to the other states.

- The number of basins of attraction in the energy landscape depends only on the network, i.e., the number of processing units and their interconnection strengths (weights). When the number of patterns to be stored is less than the number of basins of attraction, i.e., stable states, then there will be spurious stable states, which do not correspond to any desired patterns. In such a case, when the network is presented with an approximate pattern for recall, the activation dynamics may eventually lead to a stable state which may correspond to one of the spurious states or a false energy minimum, or to one of the stable states corresponding to some other pattern.
- In the latter case there will be an undetected error in the recall. The average probability of error depends on the energy values of the stable states corresponding to the desired patterns, and the relative locations of these states in the state space, measured in terms of some distance criterion.
- If the number of desired patterns to be stored is more than the number of basins of attraction in the energy landscape, then the problem becomes a hard problem, in the sense that the given patterns cannot be stored in the network.
- For a given network it is not normally possible to determine exactly the number of basins of attraction as well as their relative spacing's and depths in the state space of the network. It is possible to estimate the capacity (number of patterns that can be stored) of the network and also the average probability of error in recall. The probability of error in recall can be reduced by adjusting the weights in such a way that the resulting energy landscape is matched to the probability distribution of the input patterns. This becomes the problem of storing a pattern environment.

Q.28 Write a note on false minima and stochastic update.

☞ **[SPPU : 10 Marks]**

Ans. : False Minima and Stochastic Update

Stochastic Update concept and gradient descent

- **Gradient descent** is an optimization algorithm that finds the set of input variables for a target function that results in a minimum value of the target function, called the minimum of the function.

- As its name suggests, gradient descent involves calculating the gradient of the target function.
- From calculus theory and first-order derivative of a function one can calculate the slope or curvature of a function at a given point. Read left to right, a positive derivative suggests the target function is sloping uphill and a negative derivative suggests the target function is sloping downhill.
- **Derivative :** Slope or curvature of a target function with respect to specific input values to the function.
- If the target function takes multiple input variables, they can be taken together as a vector of variables. Working with vectors and matrices is referred to linear algebra and doing calculus with structures from linear algebra is called matrix calculus or vector calculus. In vector calculus, the vector of first-order derivatives (partial derivatives) is generally referred to as the gradient of the target function.
- **Gradient :** Vector of partial derivatives of a target function with respect to input variables.
- The gradient descent algorithm requires the calculation of the gradient of the target function with respect to the specific values of the input values. The gradient points uphill, therefore the negative of the gradient of each input variable is followed downhill to result in new values for each variable that results in a lower evaluation of the target function.
- A step size is used to scale the gradient and control how much to change each input variable with respect to the gradient.
- **Step size :** Learning rate or alpha, a hyperparameter used to control how much to change each input variable with respect to the gradient.
- This process is repeated until the minimum of the target function is located, a maximum number of candidate solutions are evaluated or some other stop condition.
- Gradient descent can be adapted to minimize the loss function of a predictive model on a training dataset, such as a classification or regression model. This adaptation is called stochastic gradient descent.
- **Stochastic gradient descent :** Extension of the gradient descent optimization algorithm for minimizing a loss function of a predictive model on a training dataset.

- The target function is taken as the loss or error function on the dataset, such as mean squared error for regression or cross-entropy for classification. The parameters of the model are taken as the input variables for the target function.
- **Loss function :** Target function that is being minimized.
- **Model parameters :** Input parameters to the loss function that are being optimized.
- The algorithm is referred to as "stochastic" because the gradients of the target function with respect to the input variables are noisy (e.g. a probabilistic approximation). This means that the evaluation of the gradient may have statistical noise that may obscure the true underlying gradient signal, caused because of the sparseness and noise in the training dataset.
- Stochastic gradient descent can be used to train (optimize) many different model types, like linear regression and logistic regression, although often more efficient optimization algorithms have been discovered and should probably be used instead.

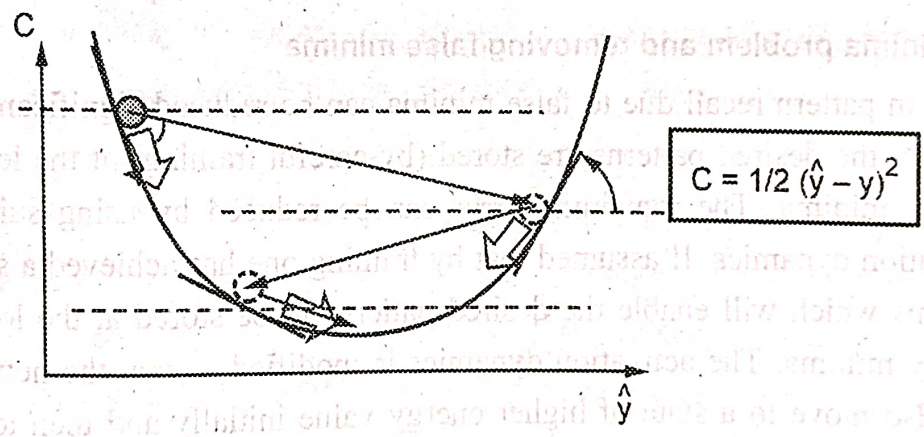


Fig. Q.28.1 Stochastic gradient descent

- Gradient descent is a **time-saving method** with which one is able to leapfrog large chunks of unusable weights by leaping down and across the U-shape on the graph.
- This is great if the weights fit cleanly into this U-shape seen in above figure. This happens when there is one global minimum, the single lowest point of all the weights. However, depending on the cost function used, the graph will not always plot out so tidily.

The difference between Local and Global

- If the aforementioned gradient descent method is used here, it may very well end up with what is called a **local minimum** of the cost function. What one wants is the **global minimum.** The black dot in below figure is the local minimum. It is a low point on the gradient. But not the lowest. That would be the purple dot, further down.

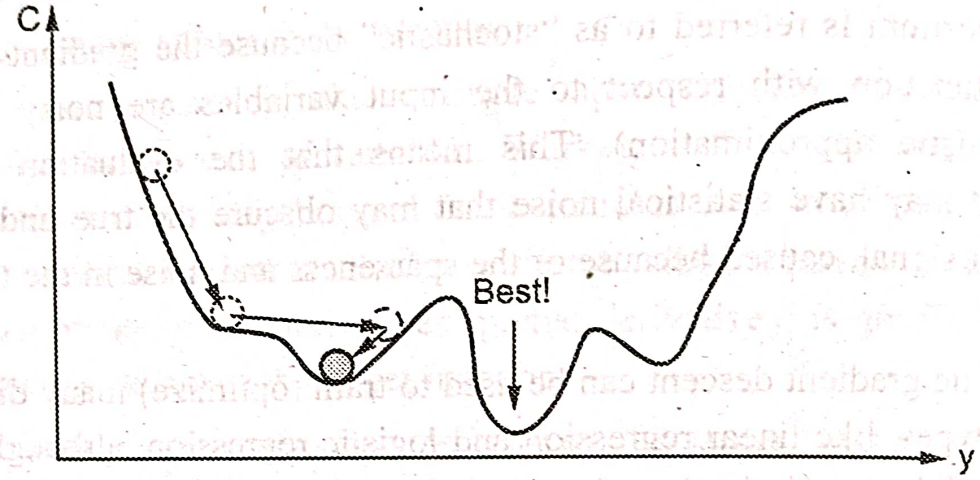


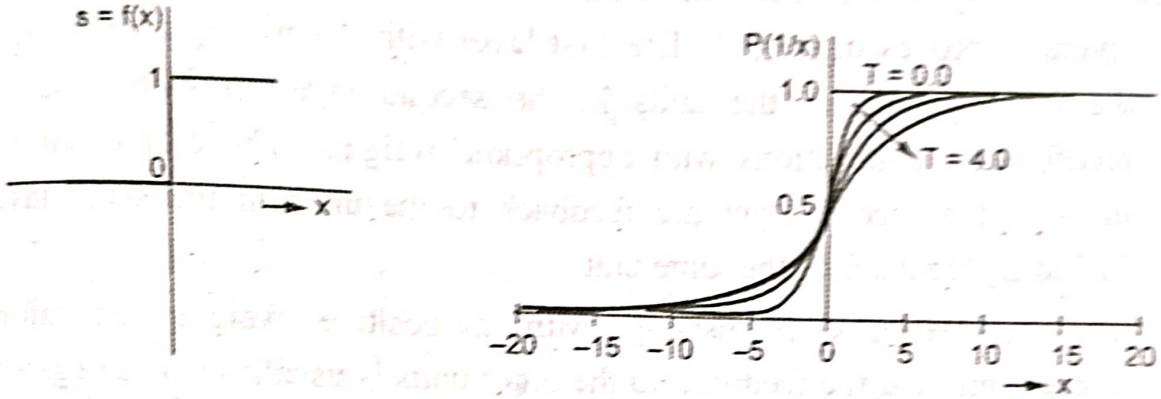
Fig. Q.28.2

False minima problem and removing false minima

- Error in pattern recall due to false minima can be reduced significantly if initially the desired patterns are stored (by careful training) at the lowest energy minima. The remaining error can be reduced by using suitable activation dynamics. If assumed that by training one has achieved a set of weights which will enable the desired patterns to be stored at the lowest energy minima. The activation dynamics is modified so that the network can also move to a state of higher energy value initially and then to the nearest deep energy minimum. It is possible to realize this by using a stochastic update in each unit instead of the deterministic update of the output function.
- Stochastic update means that the activation value or the net input to a unit need not decide the next output state of the unit in a deterministic manner as in the case of Hopfield backpropagation algorithm mentioned above. The update is expressed in probabilistic terms, like the probability of firing the unit being greater than 0.5 if the net input exceeds a threshold and less than 0.5 if the net input is less than the threshold for the unit. Note that the output function could still be a threshold logic (hardlimiter), but it is applied in a stochastic manner. With the new activation dynamics,

the state transition diagram shows transitions from a lower energy state to a higher energy state as well, the probability of such a transition is dictated by the probability function used in determining the firing of a unit in the stochastic update.

- The probability function (in below figure) can in turn be defined in terms of a parameter, called temperature (T). As the temperature is increased, the uncertainty in the update increases, giving the network a greater chance to go to a higher energy level state.



(a) Binary output function

(b) Probability function for stochastic update

Fig. Q.28.3 Stochastic update of a unit using probability law.

Probability of firing P(1/x) = 1/[1 + exp (– x/T)]

Since eventually there is a need of the activation dynamics to lead the network to a stable state corresponding to the pattern closest to the given input pattern, one needs to provide greater mobility for transition to higher states only initially. The mobility is slowly decreased by reducing the temperature, eventually to T = 0. At the lowest temperature the network settles down to a fixed point state corresponding to the desired pattern. At each temperature the network dynamics is allowed to settle to some equilibrium situation, called thermal equilibrium. At thermal equilibrium the average probability of visiting the states of the networks will not change further. The temperature parameter is reduced in a predetermined manner (called annealing schedule), making sure that at each temperature the network is allowed to reach thermal equilibrium before the next change in temperature is made. This process is called simulated annealing as described in below algorithm. It should be noted that at each temperature the state update

dynamics is fixed, as the probability of transition from one state to another depends only on the temperature. The update dynamics is however altered when the temperature is changed, and it results in a new state transition diagram.

Q.29 Explain the tasks in pattern recognition that are carried out by feedforward and feedback ANN. ☞ **[SPPU : 10 Marks]**

Ans. : • There are tasks that can be performed by a network consisting of two layers of processing units : The first layer with linear output units feeds the input pattern to the units in the second layer through a set of feedforward connections with appropriate weights. The outputs of the units in the second layer are feedback to the units in the same layer including feedback to the same unit.

- The self-feedback is usually with a positive weight (excitatory connection) and the feedback to the other units is usually with a negative weight (inhibitory connection). The weights on the feedback connections in the second layer are usually fixed. The first layer of units is called input layer and the second layer is called competitive layer. Different choices of output functions and methods of learning lead to networks for different types of competition tasks. There are three such tasks. Assuming fixed weights in the feedforward connections from the input to the competitive layer and in the feedback connections in the competitive layer, one can study the behaviour of the network for different types of output functions of the units in the competition layer.

  i. **Pattern storage (short term memory) -** Consider the output functions to be linear. When an input pattern is applied, the units in the competition layer settle to a steady activation state which will remain there even after the input pattern is removed. The activation pattern will remain as long as the network is not given a different input pattern. Another input pattern will erase the previous activation state. Hence this is called short-term memory. The pattern is stored only temporarily. This pattern storage representation is only of theoretical interest. There is no application for such a short-term memory function. However, by using a nonlinear output function for the units in the competition layer one could show that the network can perform a pattern clustering task.

ii. **Pattern clustering** - Given a set of patterns, the objective is to design a competition network which groups the patterns into subgroups of patterns based on similarity of features in the patterns. A two layer network with input and competition layers and with nonlinear units in the competition layer can perform the task of pattern clustering or grouping. If a nonlinear output function of the type $f(x) = x^2$ is used for the units in the competitive layer, then it can be shown that the activation dynamics leads to a steady state situation where the network tends to enhance the activity of the unit with the largest activity. When the input pattern is removed, the activities of all units except the largest one will decay to zero. Thus only one of the units in the competitive layer will win.

- The weights leading to the winning unit j are adjusted to respond more to the input pattern a. This weight adjustment is repeated for all the input patterns several times. For input patterns belonging to different groups, different units in the competition layer will win. When the weight vector for each output unit reaches an average position within the cluster, it will stay generally within a small region around that average position. Each unit in the competitive layer refers to a different group or category of patterns.

When an unknown input pattern is given, the activation dynamics leads to a steady state situation where only one unit in the competitive layer is active. That unit gives the category to which the input pattern belongs.

It should be noted that in a competitive network the physical location of the units does not reflect any relation between categories. But there are many situations where the patterns do not fall into fixed categories. There may be a gradual change of features from one pattern to another. This change of features can be captured by a self-organisation network which performs the task of feature mapping.

iii. **Feature map** - Given a set of patterns, the objective is to design a network that would organise the patterns in accordance with similarity of features among them in such a way that by looking at the output of the network one can visually obtain an idea of how different patterns are related. The display of signals from the output layer (typically in 2-dimension) of units is called a feature map.

To accomplish the task of feature mapping, a competitive network is modified into one called a self-organising network as shown below.

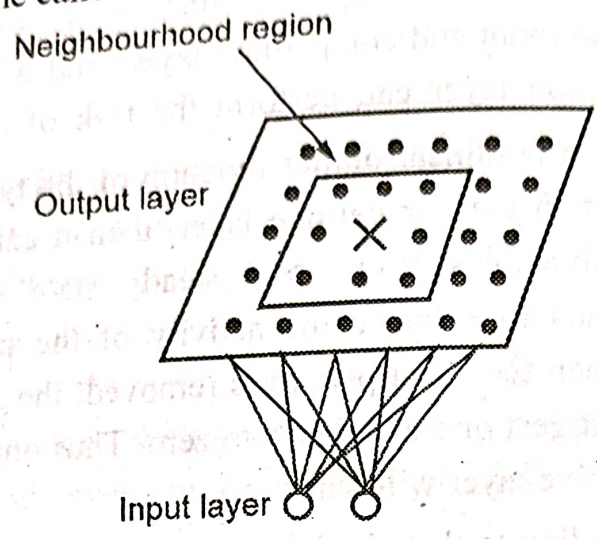


Fig. Q.29.1 A feature mapping architecture. Each input unit is connected to all the units of the output layer

The modification consists of creating a neighbourhood region around the winning unit in the competitive layer, so that during training all the feedforward weights leading to the units in this region are adjusted to favour the input pattern. The weight adjustment is similar to the case of a competitive network. The neighbourhood region around a winning unit is gradually reduced for each application of the given set of patterns as describe in below algorithm.

Algorithm for self-organizing feature map

1. Initialize the weights from N inputs to the M output units to small random values. Initialize the size of the neighbourhood region R(0).
2. Present a new input **a**
3. Compute the distance d_i between input and the weight on each output unit i :

$$d_i = \sum_{j=1}^{N} [a_j(t) - w_{ij}(t)]^2 \quad , \text{for } i = 1, 2, \ldots, M$$

where $a_j(t)$ is the input to the jth input unit at time t and $w_{ij}(t)$ is the weight from the jth input unit to the ith output unit.

4. Select the output unit i^* with minimum distance

$$i^* = \text{index of } [\min_i d_i]$$

5. Update weight to node i^* and its neighbours

$$w_{ij}(t+1) = w_{ij}(t) + \eta(t)(a_i(t) - w_{ij}(t)), \text{ for } i \in R_i^*(t), \text{ and } i = 1, 2, \ldots, N,$$

where $\eta(t)$ is the learning rate parameter $(0 < \eta(t) < 1)$ that decreases with time $R_i^*(t)$ gives the neighbourhood region around the node i^*, at time t.

6. Repeat steps 2 through 5 for all inputs several times.

- For recall, when an unknown input is applied, the activation dynamics determines the winning unit whose location would determine its features relative to the features represented by the other units in its neighbourhood. While a feature map produces a more realistic arrangement of patterns, the output is useful only for visual observation. Since it is difficult to categorize a feature map, it is difficult to use it for applications such as pattern classification. A more complex architecture is needed to exploit the advantages of a feature map for pattern classification purposes.

END...

Unit IV

4 Competitive Learning Neural Network

4.1 : Competitive Learning and ART

Q.1 Discuss competitive learning networks and components of competitive learning network ? ☞ [SPPU : 8 Marks]

Ans. : Introduction to Competitive Learning

- Competitive learning is a type of unsupervised learning model used in machine learning and artificial intelligence systems.
- In this unsupervised training model output units are said to be in competition for input patterns. During training, the output unit that provides the highest activation to a given input pattern is declared the weights of the winner and is moved closer to the input pattern, whereas the rest of the neurons are left unchanged.
- This strategy is also called winner-take-all since only the winning neuron is updated. Output units may have lateral inhibitory connections so that a winner neuron can inhibit others by an amount proportional to its activation level.
- The winner-take-all networks are the networks that are based on the competitive learning rule and will use the strategy where it chooses the neuron with the greatest total inputs as a winner. The connections between the output neurons show the competition between them and one of them would be 'ON' which means it would be the winner and others would be 'OFF'.

Components of CL network

- CL network is similar to a single layer feed-forward network having feedback connection between the outputs. The connections between the outputs are inhibitory type, which means the competitors never support themselves.

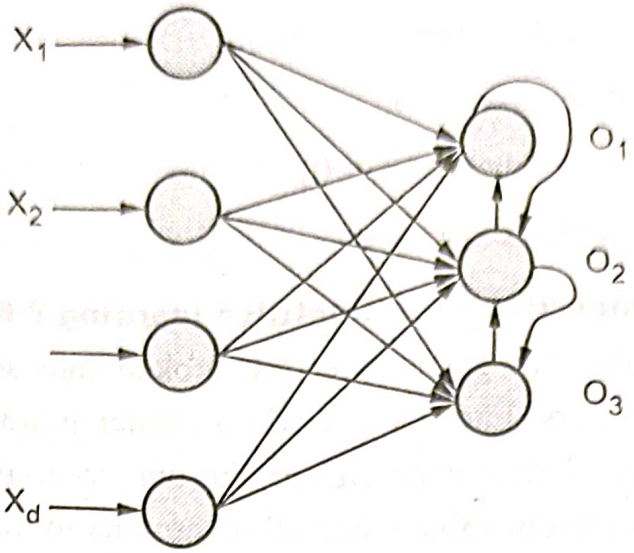


Fig. Q.1.1 Single layer network

- A simple competitive network is basically composed of two networks namely, each of them specializes in a different function.

  1) Hamming net - The Hamming net measures how much the input vector resembles the weight vector of each perceptron.

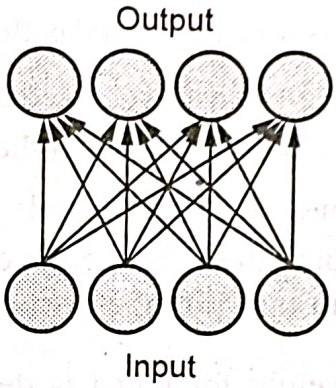


Fig. Q.1.2 Hamming net

  2) Maxnet (Mexican Hat Output) - The Maxnet finds the perceptron with the maximum value.

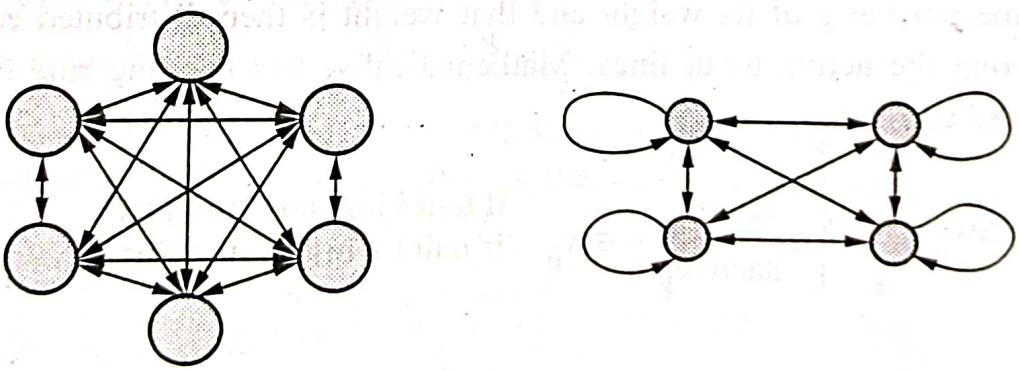


Fig. Q.1.3 Maxnet perceptrons

Here the computations are done as follows,

- Close neighbors : (w > 0)
- Not so close neighbors : (w < 0)
- Distance neighbors : (w = 0)

Q.2 What are properties of competitive learning ? ☞ **[SPPU : 5 Marks]**

Ans. : • The units in a given layer are broken into several sets of non-overlapping clusters. Each unit within a cluster inhibits every other unit within a cluster. Within each cluster, the unit receiving the largest input achieves its maximum value while all other units in the cluster are pushed to their minimum value. One can arbitrarily set the maximum value to 1 and the minimum value to 0.

- Every unit in every cluster receives inputs from all members of the same set of input units.
- A unit learns if and only if it wins the competition with other units in its cluster.
- A stimulus pattern S_j consists of a binary pattern in which each element of the pattern is either active or inactive. An active element is assigned the value 1 and an inactive element is assigned the value 0.
- Each unit has a fixed amount of weight (all weights are positive) that is distributed among its input lines. The weight on the line connecting to unit i on the upper layer from unit j on the lower layer is designated w_{ij}. The fixed total amount of weight for unit j is designated $\sum_j w_{ij} = 1$. A unit learns by shifting weight from its inactive to its active input lines. If a unit does not respond to a particular pattern, no learning takes place in that unit. If a unit wins the competition, then each of its input lines gives up some portion ϵ of its weight and that weight is then distributed equally among the active input lines. Mathematically, this learning rule can be stated as,

$$\Delta w_{ij} = \begin{cases} 0 & \text{if unit i loses on stimulus k} \\ \epsilon \dfrac{active_{ik}}{nactive_k} - \epsilon w_{ij} & \text{if unit i wins on stimulus k} \end{cases}$$

- where $active_{jk}$ is equal to 1 if in stimulus pattern S_k unit j in the lower layer is active and is zero otherwise and $nactive_k$ is the number of active units in pattern S_k (thus $nactive_k = \sum_j active_{jk}$)

Q.3 How competitive networks are built ? [SPPU : 10 Marks]

Ans. : Following are the important factors of competitive learning rule,

i. Condition to be a winner : Suppose if a neuron y_k wants to be the winner, then there would be the following condition

$$y_k = \begin{cases} 1 & \text{if } v_k > v_j \text{ for all } j, j \neq k \\ 0 & \text{otherwise} \end{cases}$$

This indicates that any neuron say y_k wants to win, then its induced local field (output_of_summation_units) say v_k should be the largest among all the other neurons in the network.

ii. Condition of sum total of weight : Next constraint over the competitive learning rule is the sum total of weights to a particular output neuron is going to be 1. For example, consider a neuron k then

$$\sum_k w_{kj} = 1 \text{ for all } k$$

iii. Change of weight for the winner : When a neuron does not respond to the input pattern, then no learning takes place in that neuron. Also a particular neuron wins, then the corresponding weights are adjusted as follows,

$$\Delta w_{kj} = \begin{cases} -\alpha (x_j - w_{kj}), & \text{if neuron k wins} \\ 0 & \text{if neuron k losses} \end{cases}$$

Where α is a learning rule here.

Below is the summary of above constraints,

- With normalized vectors, the activation function of the ith unit can be computed as the inner product of the unit's weight vector w_1 and a particular input pattern $x^{(n)}$

$$g_i(x^{(n)}) = w_i^T x^{(n)}$$

- Note : the inner product of two normal vectors is the cosine of the angle between them
- The neuron with largest activation is then adapted to be more like the input that caused the excitation

$$w_i(t+1) = w_i(t) + \eta x^{(n)}$$

- Following update, the weight vector is renormalized ($\|w\| = 1$)

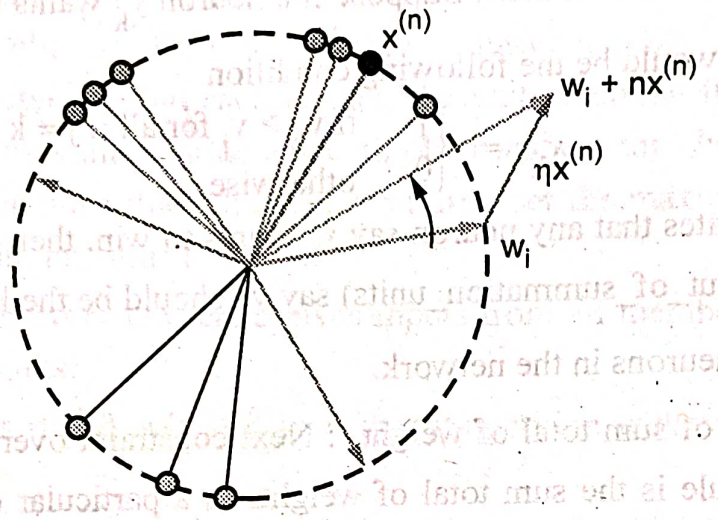


Fig. Q.3.1 Building competitive learning rule

If weights and input patters are un-normalized, the activation function becomes the Euclidean distance

$$g_i(x^{(n)}) = \sqrt{\sum_i (w_i - x_i^{(n)})^2}$$

- The learning rule then become

$$w_i(t+1) = w_i(t) + \eta(x^{(n)} - w_i(t))$$

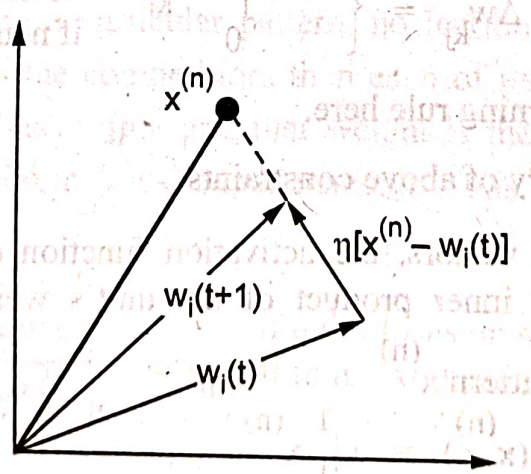


Fig. Q.3.2 Building competitive learning rule

Competitive learning algorithm :

1. Normalize all input patterns
2. Randomly select a pattern $x^{(n)}$

   2a. Find the winner neuron

$$i = [w_i^{(n)}]$$

   2b. Update the winner neuron

$$w_i = w_i + \eta x^{(n)}$$

   2c. Normalize the winner neuron

$$w_i = \frac{w_i}{\|w_i\|}$$

3. Go to step 2 until no changes occur in N_{EX} runs

Q.4 What are features of competitive learning ? ☞ **[SPPU : 5 Marks]**

Ans. : Features of competitive learning

- Each cluster classifies the stimulus set into M groups, one for each unit in the cluster. Every single unit captures roughly an equal number of stimulus patterns. It is possible to consider a cluster as forming an M-valued feature in which every stimulus pattern is classified as having exactly one of the M possible values of this feature. Thus, a cluster containing two units acts as a binary feature detector. One element of the cluster responds when a particular feature is present in the stimulus pattern, otherwise the other element responds.
- If there is structure in the stimulus patterns, the units will break up the patterns along structurally relevant lines. Roughly speaking, this means that the system will find clusters if they are there.
- If the stimuli are highly structured, the classifications are highly stable. If the stimuli are less well structured, the classifications are more variable and a given stimulus pattern will be responded to first by one and then by another member of the cluster. These configurations can be more or less stable. For example, if the stimulus points do not actually fall into good clusters, then the configurations will be relatively unstable and the presentation of each stimulus will modify the pattern of responding so that the system will undergo continual evolution. On the other hand, if the stimulus patterns fall in the best way into clusters, then the system will

become very stable in the sense that the same units will always respond to the same stimuli.

- The particular grouping done by a particular cluster depends on the starting value of the weights and the sequence of stimulus patterns actually presented. A large number of clusters, each receiving inputs from the same input lines can, in general, classify the inputs into a large number of different groupings or, alternatively, discover a variety of independent features present in the stimulus population. This can provide a kind of distributed representation of the stimulus patterns.
- To a first approximation, the system develops clusters that minimize within - cluster distance, maximize between - cluster distance and balance the number of patterns captured by each cluster. In general, tradeoffs must be made among these various forces and the system selects one of these tradeoffs.

Q.5 List competitive learning advantages, limitations and applications. ☞ [SPPU : 8 Marks]

Ans. : Competitive learning advantages

1. Similar to Instar weight update and hence stable.
2. Won't result in excessive positive or negative weights.
3. Ideal when one wants to analyze raw data of which there is no prior knowledge.
4. Idea of completion can be applied to different types of networks (Hebbian, Kohonen networks, etc.).
5. It can be used for Vector quantization.
6. It can be used for clustering – competitive rule allows a single layer network to group data that lies in a neighborhood of the input space

Competitive learning limitations

1. If a PE weight vector is far away from any of the data clusters, it may never win competition.
2. One is not sure about what it has learnt.
3. If used for clustering, number of clusters have to be decided in advance.

4. Inner product takes account of both direction and magnitude of vector. If vectors are not normalized, may select wrong weight vector after competition.

Applications of competitive networks

1. Vector quantization
2. Analyze raw data
3. Bibliographic classification
4. Image browsing systems
5. Medical diagnosis (visualization of data and
6. Speech recognition
7. Data compression
8. Separating sound sources
9. Environmental modeling
10. Feature extraction
11. Dimensionality reduction
12. Optimization

Q.6 Discuss ART networks. ☞ **[SPPU : 8 Marks]**

Ans. : • The Adaptive Resonance Theory (ART) was incorporated as a hypothesis for human cognitive data handling. The hypothesis has prompted neural models for pattern recognition and unsupervised learning. ART system has been utilized to clarify different types of cognitive and brain data.

- This network was developed by Stephen Grossberg and Gail Carpenter in 1987. It is based on competition and uses unsupervised learning model. Adaptive Resonance Theory ART networks, is always open to new learning adaptive without losing the old patterns *resonance*. Fundamentally, ART network is a vector classifier which accepts an input vector and classifies it into one of the categories depending upon which of the stored pattern it resembles the most.
- The Adaptive Resonance Theory addresses the **stability-plasticity** (stability can be defined as the nature of memorizing the learning and plasticity refers to the fact that they are flexible to gain new information) dilemma of a system that asks how learning can proceed in response to huge input patterns and simultaneously not to lose the stability for irrelevant patterns.
- Other than **stability-plasticity**, the stability-elasticity dilemma is concerned about how a system can adapt new data while keeping what was learned before. For such a task, a feedback mechanism is included

among the ART neural network layers. In this neural network, the data in the form of processing elements output reflects back and ahead among layers. If an appropriate pattern is build-up, the resonance is reached, then adaption can occur during this period.

- This formal analysis of how to overcome the learning instability accomplished by a competitive learning model, result into an expended hypothesis, called **Adaptive Resonance Theory** (ART).

Q.7 What are features of ART networks ? ☞ [SPPU : 10 Marks]

Ans. : The main operation of ART classification can be divided into the following phases,

- **Recognition phase -** The input vector is compared with the classification presented at every node in the output layer. The output of the neuron becomes "1" if it best matches with the classification applied, otherwise it becomes "0".
- **Comparison phase -** In this phase, a comparison of the input vector to the comparison layer vector is done. The condition for reset is that the degree of similarity would be less than vigilance parameter.
- **Search phase -** In this phase, the network will search for reset as well as the match done in the above phases. Hence, if there would be no reset and the match is quite good, then the classification is over. Otherwise, the process would be repeated and the other stored pattern must be sent to find the correct match.

Working of ART and ART 1

1. ART1 is an unsupervised learning model primarily designed for recognizing binary patterns.
2. It comprises an attentional subsystem, an orienting subsystem, a vigilance parameter and a reset module.
3. The vigilance parameter has a huge effect on the system. High vigilance produces higher detailed memories.
4. The ART1 comprises of two competitive networks, comparison field layer L_1 and the recognition field layer F_2, two control gains, Gain1 and Gain2 and two Short-Term Memory (STM) stages S_1 and S_2.

5. Long Term Memory (LTM) follows somewhere in the range of S_1 and S_2 multiply the signal in these pathways. It gains control and empowers L_1 and L_2 to recognize the current stages of the running cycle.
6. STM reset wave prevents active L_2 cells when mismatches between bottom-up and top-down signals happen at L_1. The comparison layer gets the binary external input passing it to the recognition layer liable for coordinating it to a classification category. This outcome is given back to the comparison layer to find out when the category coordinates the input vector. If there is a match, then a new input vector is read and the cycle begins once again. If there is a mismatch, then the orienting system is in charge of preventing the previous category from getting a new category match in the recognition layer. The given two gains control the activity of the recognition and the comparison layer, respectively. The reset wave specifically and enduringly prevents active L_2 cell until the current is stopped. The offset of the input pattern ends its processing L_1 and triggers the offset of Gain2. Gain2 offset causes consistent decay of STM at L_2 and thereby prepares L_2 to encode the next input pattern without bais.
7. Processing of ART 1
   a. ART1 is a self-organizing neural network having input and output neurons mutually couple using bottom-up and top-down adaptive weights that perform recognition.
   b. The system is first trained as per the adaptive resonance theory by inputting reference pattern data under the type of 5 * 5 matrix into the neurons for clustering within the output neurons.
   c. Further, the maximum number of nodes in L_2 is defined following by the vigilance parameter. The inputted pattern enrolled itself as short term memory activity over a field of nodes L_1.
   d. Combining and separating pathways from L_1 to coding field L_2, each weighted by an adaptive long - term memory track, transform into a net signal vector T. Internal competitive dynamics at L_2 further transform T, creating a compressed code or content addressable memory.

e. With strong competition, activation is concentrated at the L_2 node that gets the maximal $L_1 \rightarrow L_2$ signal.

f. Thus the overall processing is divided into four phases comparision, recognition, search and learning.

ART model is unsupervised in nature and consists of,

1. Input unit layer - L_1 layer or the comparison field where in the inputs are processed.

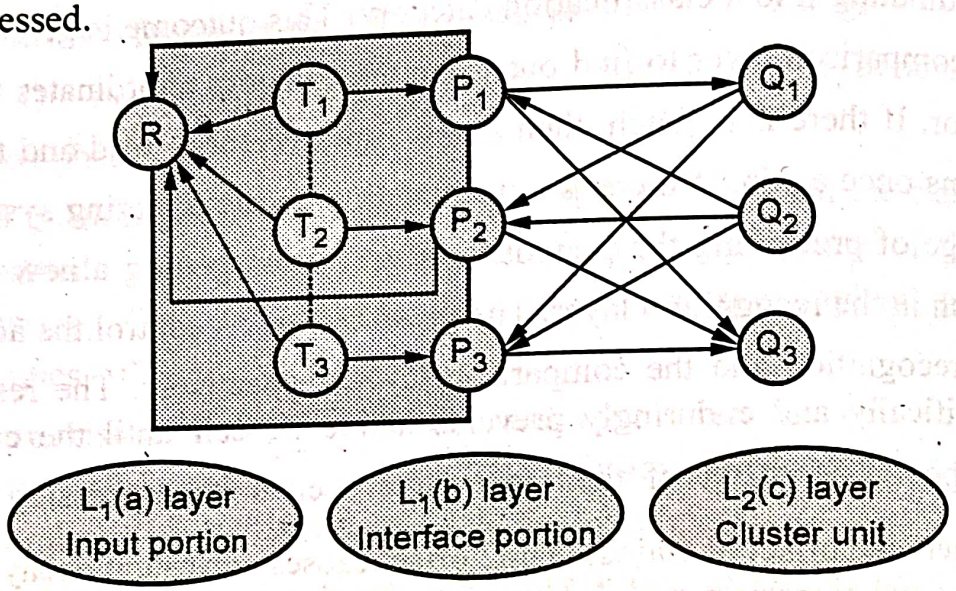


Fig. Q.7.1 ART1 - Layer 1

L_1a layer Input portion – In ART1, there would be no processing in this portion rather than having the input vectors only. It is connected to F_1b layer *interface portion.*

L_1b layer Interface portion – This portion combines the signal from the input portion with that of F_2 layer. F_1b layer is connected to F_2 layer through bottom up weights $\mathbf{b_{ij}}$ and F_2 layer is connected to F_1b layer through top down weights $\mathbf{t_{ji}}$.

2. Layer 2 - F_2 layer or the recognition field which consists of the clustering units. This is a competitive layer. The unit having the largest net input is selected to learn the input pattern. The activation of all other cluster unit are set to 0.

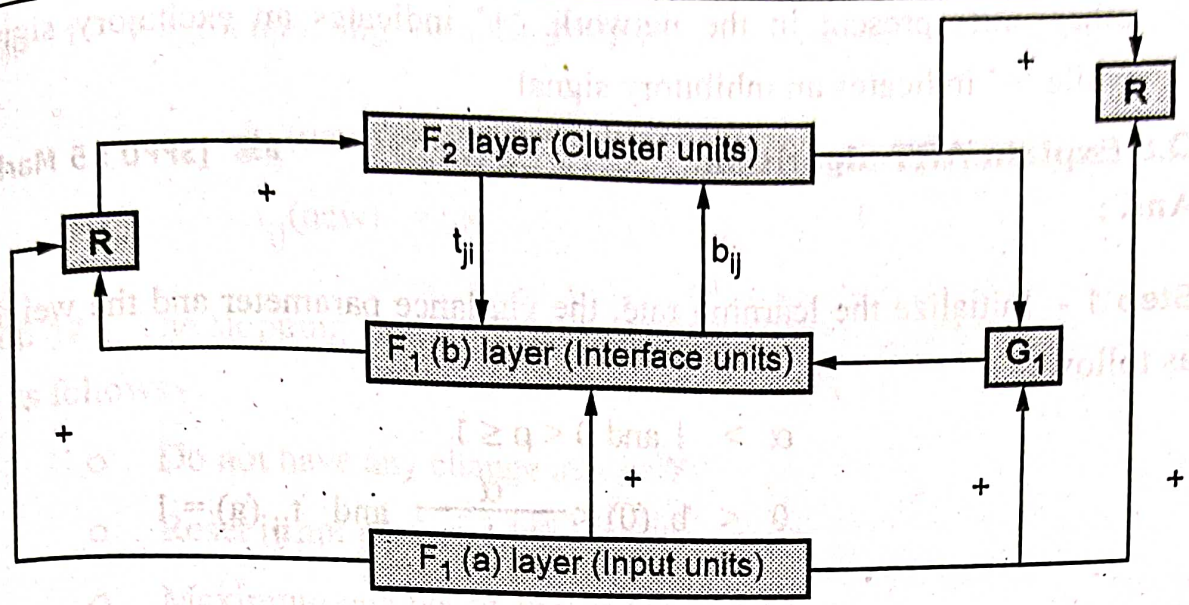


Fig. Q.7.2 Art 1 – Layer 2

Parameters used

Following parameters are used -

n - Number of components in the input vector

m - Maximum number of clusters that can be formed

b_{ij} - Weight from F_1b to F_2 layer, i.e. bottom-up weights

t_{ji} - Weight from F_2 to F_1b layer, i.e. top-down weights

p - Vigilance parameter

$||x||$ - Norm of vector x

3. The Reset Module acts as a control mechanism - The **reset unit** makes the decision whether or not the cluster unit is allowed to learn the input pattern depending on how similar its top-down weight vector is to the input vector and to the decision. This is called the vigilance test.

   The **vigilance parameter** helps to incorporate new memories or new information. Higher vigilance produces more detailed memories, lower vigilance produces more general memories.

   Supplement unit - The major issue with Reset mechanism is that the layer F_2 must have to be inhibited under certain conditions and must also be available when some learning happens. That is why two supplemental units namely, G_1 and G_2 is added along with reset unit, **R**. They are called **gain control units**. These units receive and send signals to the

other units present in the network. '+' indicates an excitatory signal, while '–' indicates an inhibitory signal.

Q.8 Explain ART algorithm. [SPPU : 5 Marks]

Ans. :

Step 1 - Initialize the learning rate, the vigilance parameter and the weights as follows -

$$\alpha > 1 \text{ and } 0 < \rho \leq 1$$

$$0 < b_{ij}(0) < \frac{\alpha}{\alpha - 1 + n} \text{ and } t_{ij}(a) = 1$$

Step 2 - Continue step 3 - 9, when the stopping condition is not true.

Step 3 - Continue step 4 - 6 for every training input.

Step 4 - Set activations of all F_1a and F_1 units are follows

$$F_2 = 0 \text{ and } F_1\alpha = \text{Input vectors}$$

Step 5 - Input signal from F_1 a to F_1b layer must be sent like

$$s_i = x_i$$

Step 6 - For every inhibited F_2 node

$$y_j = \sum_i b_{ij} x_i \quad \text{The condition is } y_j \neq -1$$

Step 7 - Perform step 8 - 10, when the reset is true

Step 8 - Find **J** for $y_J \geq y_j$ for all nodes **j**

Step 9 - Again calculate the activation on F_1b as follows

$$x_i = \text{sit } J_i$$

Step 10 - Now, after calculating the norm of vector **x** and vector **s**, we need to check the reset condition as follows -

If $\|x\|/\|s\| <$ vigilance parameter ρ, then inhibit node **J** and go to step 7

Else If $\|x\|/\|s\| \geq$ vigilance parameter p, then proceed further.

Step 11 - Weight updating for node J can be done as follows -

$$b_{ij}(new) = \frac{ax_i}{\alpha - 1 + \|x\|}$$

$$t_{ij}(new) = x_i$$

Step 12 - The stopping condition for algorithm must be checked and it may be as follows -

- Do not have any change in weight.
- Reset is not performed for units.
- Maximum number of epochs reached.

- Generally **two types of learning** exists, slow learning and fast learning. In fast learning, weight update during resonance occurs rapidly. It is used in ART1. In slow learning, the weight change occurs slowly relative to the duration of the learning trial. It is used in ART2.

Q.9 Discuss various types of ART. ☞ **[SPPU : 5 Marks]**

Ans. : The ARTs can be classified as follows :

- **ART1 -** It is the simplest and the basic ART architecture. It is capable of clustering binary input values.
- **ART2 -** It is extension of ART1 that is capable of clustering continuous - valued input data.
- **Fuzzy ART -** It is the augmentation of fuzzy logic and ART.
- **ARTMAP -** It is a supervised form of ART learning where one ART learns based on the previous ART module. It is also known as predictive ART.
- **FARTMAP -** This is a supervised ART architecture with Fuzzy logic included.

Q.10 List advantages of ART. ☞ **[SPPU : 5 Marks]**

Ans. : Advantages of Adaptive Learning Theory (ART)

1. It can be utilized with different techniques to give more precise outcomes.
2. It is stable and is not disturbed by a wide variety of inputs provided to its network.

3. It doesn't ensure any stability in forming clusters.
4. It can be used in variety fields such as face recognition, embedded system and robotics, target recognition, medical diagnosis, signature verification, etc.
5. It has benefit over competitive learning that the competitive learning can not include new clusters when considered necessary but ART can.

Advantages and Limitations of Adaptive Resonance Theory

All the ART networks are not consistent (like the Fuzzy ART and ART1) as they depend upon the order in which training data, or upon the learning rate.

Q.11 Discuss ART application in character recognition.

[SPPU : 10 Marks]

Ans. : There are varied ART applications including character and target recognition, face recognition, medical diagnosis, signature verification, mobile control robot.

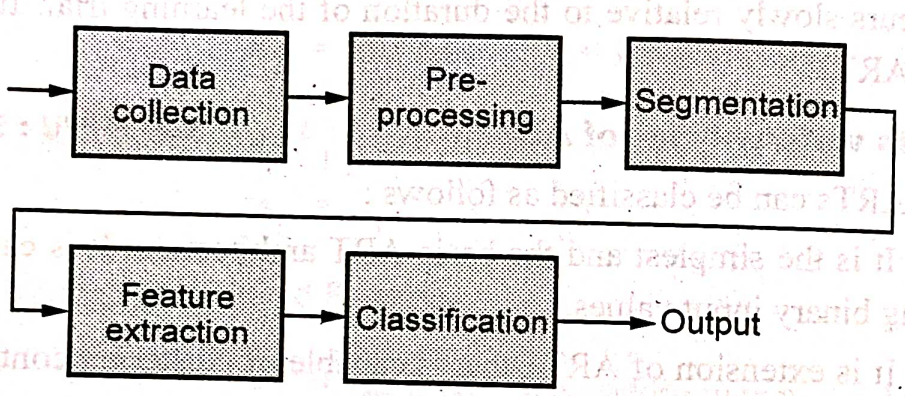


Fig. Q.11.1 Character recognition process

- A typical character recognition system consists of stages given in above figure. The recognition process starts with data collection stage. Data is collected in the form of images of different machine printed alphabets.
- Next the data is converted into binary form. The images are noise free so no need to do extra preprocessing for removing noise.
- Segmentation is the most important part of character recognition systems. This step involves localization of the limits of each character and to isolate them properly. In this the identification of the boundaries of the character and separating them for further processing.
- After segmentation a set of features are required for each character. In feature extraction stage each character is represented as a feature vector,

which becomes its identity. This vector is used to distinguish the character from other characters. The features extracted from the images will be the inputs given Back Propagation algorithm for classification.

- There are two main methods for extracting features in character recognition
  1. In the first method, the algorithm for feature detection defines a character by evaluating its lines and strokes.
  2. In the second method, pattern recognition works by identifying the entire character.
- In the ART algorithm, a backward network is adopted for vigilance test in addition to the conventional forward networks between the input neurons and output neurons, two widely used versions of ART algorithms are : ART-1 for binary-valued patterns and ART-2 for continuous - valued patterns.
- It can adaptively create a new neuron for an incoming input pattern if it is determined (by a vigilance test) to be sufficiently different from the existing clusters. Such a vigilance test is incorporated into the adaptive backward network.
- Suppose that w_{ij} and t_{ij} are the forward and backward weights between neuron j and input i, respectively. Note that x_i's and t_{ij}'s binary-valued while w_{ij}'s are real. The weight adjustments are applied to both the feed-forward weights w_{ij} and the feedback weight t_{ij}^* from winning neuron j^*.

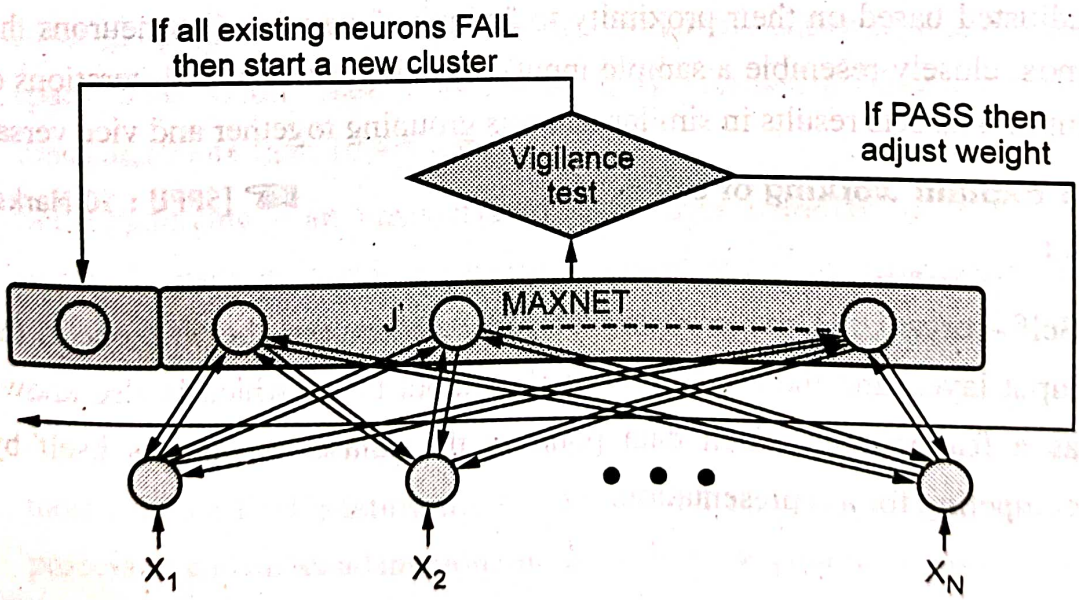


Fig. Q.11.2 ART structure

4.2 : Self-Organization Maps

Q.12 What are self-organization maps ? ☞ [SPPU : 8 Marks]

Ans. : • A **Self-Organizing Map (SOM)** is a type of Artificial Neural Network (ANN) that is trained using unsupervised learning to produce a low-dimensional (typically two - dimensional), discretized representation of the input space of the training samples, called a **map** and is therefore a method to do dimensionality reduction.

- **SOM** was introduced by Finnish professor Teuvo Kohonen in the 1980s is sometimes called a **Kohonen map.**
- Self-organizing maps differ from other artificial neural networks as they apply competitive learning as opposed to error - correction learning (such as backpropagation with gradient descent) and in the sense that they use a neighborhood function to preserve the topological properties of the input space.
- A Self-organizing Map is a data visualization technique. SOMs map multidimensional data onto lower dimensional subspaces where geometric relationships between points indicate their similarity. The reduction in dimensionality that SOMs provide allows people to visualize and interpret what would otherwise be, for all intents and purposes, indecipherable data.
- SOMs generate subspaces with an unsupervised learning neural network trained with a competitive learning algorithm. Neuron weights are adjusted based on their proximity to "winning" neurons (i.e. neurons that most closely resemble a sample input). Training over several iterations of input data sets results in similar neurons grouping together and vice versa.

Q.13 Explain working of SOM. ☞ [SPPU : 10 Marks]

Ans. :

1. Self - organizing maps consist of two basic layers, the first one is the input layer, and the second one is the output layer, which is also known as a feature map. Each data point in the dataset recognizes itself by competing for a representation.

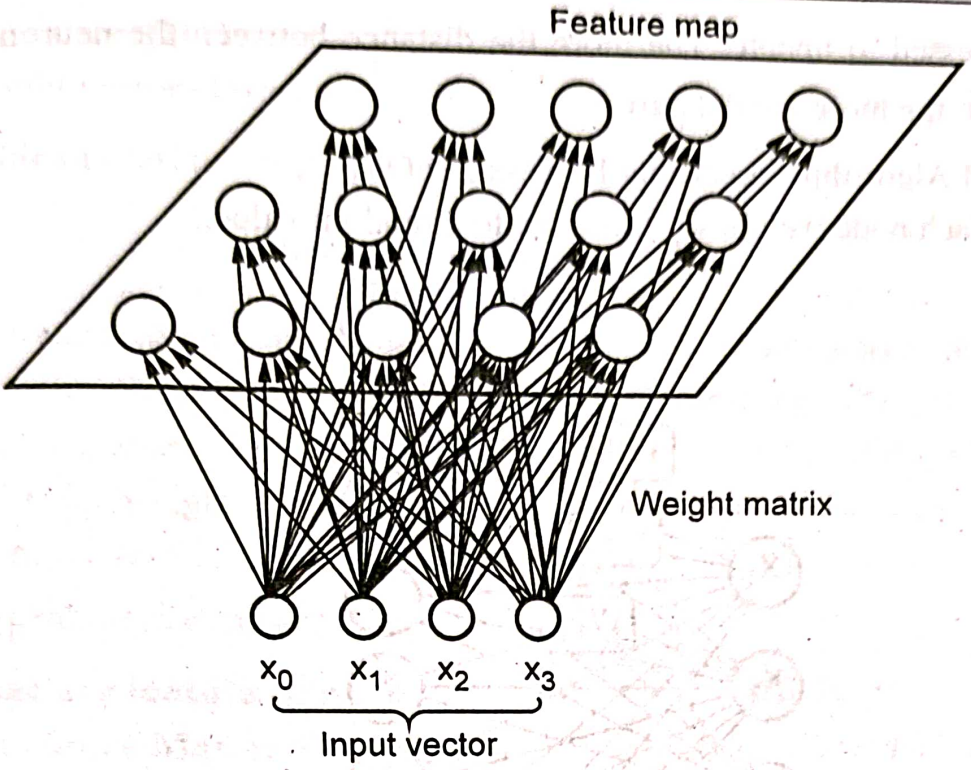


Fig. Q.13.1 Self organizing map

2. The Self-Organizing Maps' mapping steps start from initializing the weight to vectors. After this, a random vector as the sample is selected and the mapped vectors are searched to find which weight best represents the chosen sample.
3. Each weighted vector has neighboring weights present that are close to it. The chosen weight is then rewarded by being able to become a random sample vector. This helps the map to grow and form different shapes.
4. Most generally, they form square or hexagonal shapes in a 2D feature space. This whole process is repeatedly performed a large number of times and more than 1000 times.
5. Self-Organizing - an unsupervised ANN uses competitive learning to update its weights that is competition, cooperation and adaptation. Each neuron of the output layer is present with a vector with dimension n. The distance between each neuron present at the output layer and the input data is computed. The neuron with the lowest distance is termed as the most suitable fit. Updating the vector of the suitable neuron in the final process is known as adaptation, along with its neighbour in cooperation. After selecting the suitable neuron and its neighbours, the neurons are

processed to update. The more the distance between the neuron and the input, the more the data grows.

6. SOM Algorithm - Learning Process in SOM

i. Each node weight w_{ij} initialize to a random value.

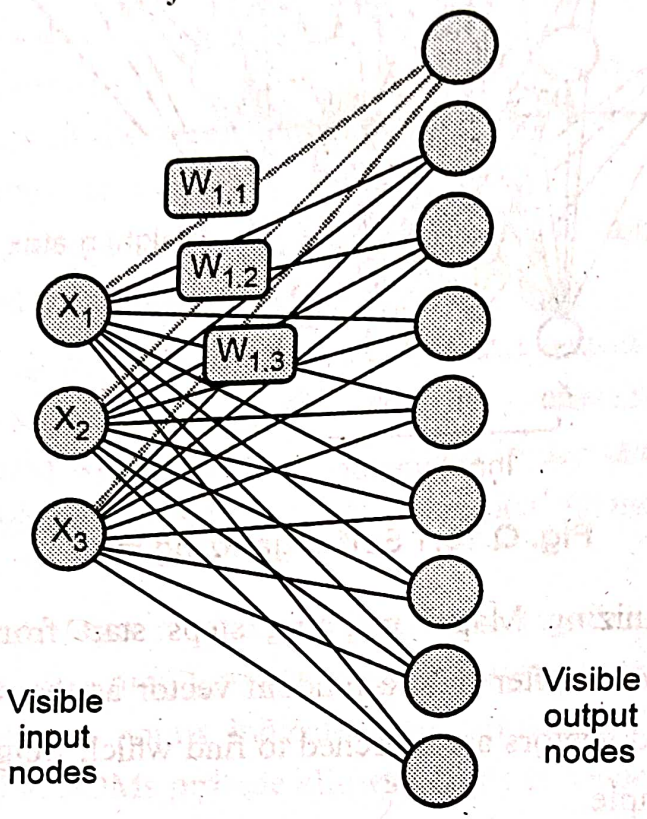


Fig. Q.13.2

ii. Choose a random input vector x_k. Repeat step iii to v till the nodes are on map.

iii. Every node is examined to calculate which suitable weights are similar to the input vector. The suitable node is commonly known as the Best Matching Unit. Calculate the Euclidean distance between weight vector w_{ij} and the input vector x(t) connected with the first node, where t, i, j = 0.

The neighbourhood value of the Best Matching Unit is then calculated. The number of neighbours tends to decrease over time. **Best Matching Unit** is a technique which calculates the distance from each weight to the sample vector, by running through all weight vectors. The weight with the shortest distance is the winner.

To determine the best matching unit, one method is to iterate through all the nodes and calculate the Euclidean distance between each

node's weight vector and the current input vector. The node with a weight vector closest to the input vector is tagged as the BMU.

The Euclidean distance is given as :

$$\text{Distance} = \sqrt{\sum_{i=0}^{i=n} (X_i - W_i)^2}$$

iv. The suitable weight is further rewarded with transitioning into more like the sample vector. The neighbours transition like the sample vector chosen. The closer a node is to the Best Matching Unit, the more its weights get altered and the farther away the neighbour is from the node, the less it learns.

v. Repeat the second step for N iterations.

Q.14 What are feature maps ? ☞ **[SPPU : 10 Marks]**

Ans. : • **Feature Map** is also called as Activation map. Once the filters are extracted from the Image. And these filters are small sections of the image which will be having different features.

- Number of filters used on the input should be created the same number amount of feature maps. So an input image with 6 filters will have 6 feature maps. Central goal of SOM is to generate and learn the feature map.
- The aim is to learn a **feature map** from the spatially **continuous input space**, in which our input vectors live, to the low dimensional spatially **discrete output space**, which is formed by arranging the computational neurons into a grid.
- The stages of the SOM algorithm that achieves this can be summarised as follows :

1. **Initialization** - Choose random values for the initial weight vectors w_j.
2. **Sampling** - Draw a sample training input vector x from the input space.
3. **Matching** - Find the winning neuron I(x) that has weight vector closest to the input vector, i.e. the minimum value of $d_j(x) = \sum_{i=1}^{D} (x_i - w_{ji})^2$.

4. **Updating** - Apply the weight update equation $\Delta w_{ji} = \eta(t)\, T_{j,I(x)}(t)\, (x_i - w_{ji})$ where $T_{j,I(x)}(t)$ is a Gaussian neighbourhood and $\eta(t)$ is the learning rate.
5. **Cotinuation** - Keep returning to step 2 until the feature map stops changing.

Properties of the feature map

- Once the SOM algorithm has converged, the feature map displays important statistical characteristics of the input space. Given an input vector x, the feature map Φ provides a winning neuron I(x) in the output space and the weight vector $\mathbf{w}_{I(x)}$ provides the coordinates of the image of that neuron in the input space.

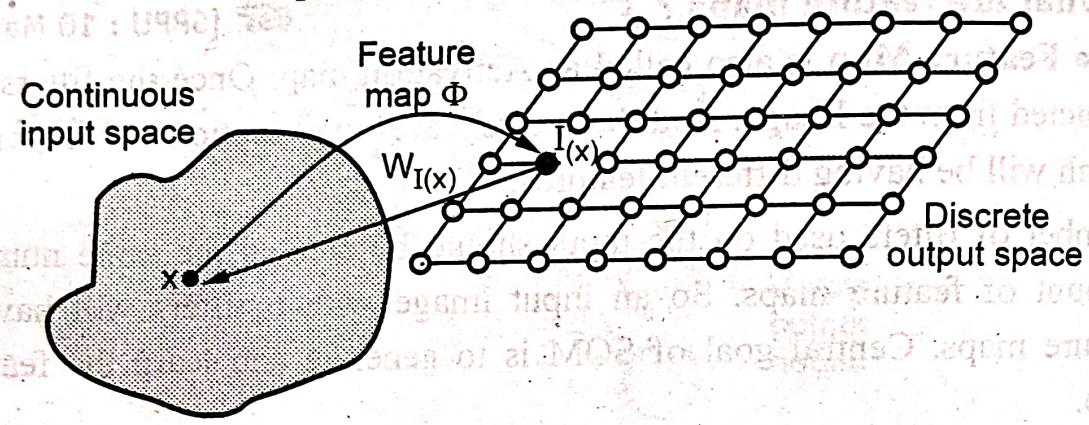


Fig. Q.14.1

Properties of feature map

1. Approximation of the input space - The feature map is represented by the set of weight vectors $\{w_i\}$ in the output space, provides a good approximation to the input space. The aim of the SOM as storing a large set of input vectors $\{x\}$ by finding a smaller set of prototypes $\{w_i\}$ so as to provide a good approximation to the original input space. The theoretical basis of this idea is rooted in vector quantization theory, the motivation of which is dimensionality reduction or data compression.

   In effect, the goodness of the approximation is given by the total squared distance,

$$D = \sum_x \|x - w_{I(x)}\|^2$$

which to minimize. Gradient descent method is followed in SOM in weight update algorithm, which confirms that it is generating a good approximation to the input space.

2. Topological ordering - The feature map computed by the SOM algorithm is topologically ordered that is the spatial location of a neuron in the output lattice/grid corresponds to a particular domain or feature of the input patterns. The topological ordering property is a direct consequence of the weight update equation that forces the weight vector $w_{I(x)}$ of the winning neuron I(x) to move toward the input vector x. The crucial factor is that the weight updates also move the weight vectors w_j of the closest neighbouring neurons j along with the winning neuron I(x). Together these weight changes cause the whole output space to become appropriately ordered.

   The feature map can be visualized as an elastic or virtual net with a grid like topology. Each output node can be represented in the input space at coordinates given by their weights. Then if the neighbouring nodes in output space have their corresponding points in input space connected together, the resulting image of the output grid reveals directly the topological ordering at each stage of the network training.

3. Density matching - The feature map reflects variations in the statistics of the input distribution - regions in the input space from which the sample training vectors x are drawn with high probability of occurrence are mapped onto larger domains of the output space and therefore with better resolution than regions of input space from which training vectors are drawn with low probability.

   There is a need to relate the input vector probability distribution p(x) to the magnification factor m(x) of the feature map. Generally, for two dimensional feature maps the relation cannot be expressed as a simple function, but in one dimension one can show that,

$$m(x) \propto p^{2/3}(x)$$

So the SOM algorithm doesn't match the input density exactly, because of the power of 2/3 rather than 1. Computer simulations indicate similar approximate density matching in general, always with the low density regions slightly over-represented.

4. Feature selection - Given data from an input space with a non-linear distribution, the self organizing map is able to select a set of best features for approximating the underlying distribution.

This property is a natural deducible from properties 1 through 3. SOM overcomes the approximation problem by virtue of its topological ordering property. The SOM provides a discrete approximation of finding so-called principal curves or principal surfaces and may therefore be viewed as a non-linear generalization of PCA.

Q.15 List advantages and disadvantages of SOMs.

☞ **[SPPU : 8 Marks]**

Ans. : Advantages

- Data can be easily interpreted and understood with the help of techniques like reduction of dimensionality and grid clustering.
- Self-organizing maps are capable of handling several types of classification problems while providing a useful and intelligent summary from the data at the same time.

Disadvantages

- It does not create a generative model for the data and therefore the model does not understand how data is being created.
- Self-organizing maps are not good choice to perform well while working with categorical data and even worse for mixed types of data.
- The model preparation time is comparatively very slow and hard to train against the slowly evolving data.

Q.16 Write a note on Learning vector quantization.

☞ **[SPPU : 10 Marks]**

Ans. : • The Learning Vector Quantization Algorithm (or LVQ for short) is an artificial neural network algorithm that allows to choose the number of training instances to suspend and know exactly what these examples should look like.

- The representation of LVQ is a collection of codebook vectors. These are randomly selected at the beginning and are suitable for optimally summarizing the training data set in multiple iterations of the learning algorithm. After learning, one can use the codebook vector to K-nearest neighbors (A similar forecast).
- The most similar neighbor (best matching codebook vector) is found by calculating the distance between each codebook vector and the new data instance. Then return the class value of the best matching unit or (actual value in the case of regression) as a prediction. The best results are obtained if the data is rescaled to the same range (for example between 0 and 1).
- A Kohonen SOM is a clustering technique, which can be used to provide insight into the nature of data. One can transform this unsupervised neural network into a supervised LVQ neural network.
- The network architecture is just like a SOM, but without a topological structure.
- Each output neuron represents a known category (e.g. apple, pear, orange).

Input vecto $\underline{x} = (x_1, x_2, x_3, \ldots, x_n)$

Weight vector for the jth output neuron $\underline{w}_j = (w_{1j}, w_{2j}, w_{3j}, \ldots, w_{nj})$

C_j = Category represented by the jth neuron.

This is pre-assigned.

T = Correct category for input $\underline{x}$

Define **Euclidean** distance between the input vector and the weight vector of the jth neuron as :

$$D(j) = \sqrt{\sum_{i=1}^{n} (x_i - w_{ij})^2}$$

- Training algorithm

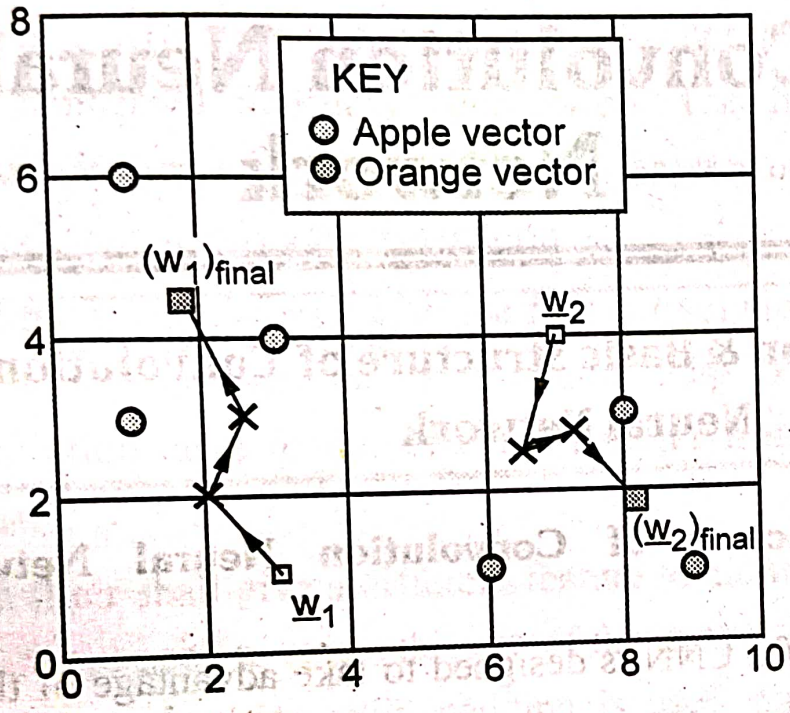
STEP	
0	Initialize weight vectors to the first m training vectors, where m is the number of different categories and set $\alpha(0)$. This weight initialization techniques is presented here is only one of many different methods.
1	While stopping condition false, do steps 2 to 6.
2	For each training input vector $\underline{x}$, do steps 3 to 4.
3	Find J so that D(J) is a minimum

4	Update the weights of the J neuron as follows :
	IF $T = C_J$ THEN
	$\underline{w}_J(new) = \underline{w}_J(old) + \alpha(\underline{x} - \underline{w}_J(old))$
	(i.e. move the weight vector $\underline{w}$ toward the input vector $\underline{x}$)
	IF $T \neq C_J$ THEN
	$\underline{w}_J(new) = \underline{w}_J(old) - \alpha(\underline{x} - \underline{w}_J(old))$
	(i.e. move $\underline{w}$ away from $\underline{x}$)

5	Reduce learning rate is α
6	Test stopping condition : This may be a fixed number of iterations or the learning rate reaching a sufficiently small value.

- Example - Measure the weight and height of three apples and three oranges.
- The input vector $\underline{x} = (x_1, x_2, x_3, \ldots, x_n)$ in this case would be $\underline{x}$ = (height, weight). These input vectors are shown in the graph below.
- Using only two neurons in the output layer, let the initial weight vectors of the first and second neuron be $\underline{w}_1 = (3,1)$ and $w_2 = (7,4)$ respectively.
- Using a learning rate of 0.5, the graph below shows how the weight vectors of the two neurons change as the LVQ network is presented with

input vectors. The order of presentation of the input vector is (1,3), (3,4), (6,1), ..., (1,6).



$$x = \begin{bmatrix} x_1 & x_2 & T \\ 1 & 3 & 1 \\ 3 & 4 & 1 \\ 6 & 1 & -1 \\ 8 & 3 & -1 \\ 9 & 1 & -1 \\ 1 & 6 & 1 \end{bmatrix}$$

$\alpha = 0.5$

Fig. Q.16.1

END...

Unit V

5 Convolution Neural Network

5.1 : Introduction & Basic Structure of Convolution Neural Network

Q.1 Explain architecture of Convolution Neural Networks (ConvNet).

Ans. : • The architecture of a CNN is designed to take advantage of the 2D structure of an input image.

- CNN consists of a number of convolutional and sub-sampling layers optionally followed by fully connected layers.
- The input to a convolutional layer is **"m × m × r"** image where m is the height and width of the image and r is the number of channels.
- Fig. Q.1.1 shows architecture of convolution neural network.

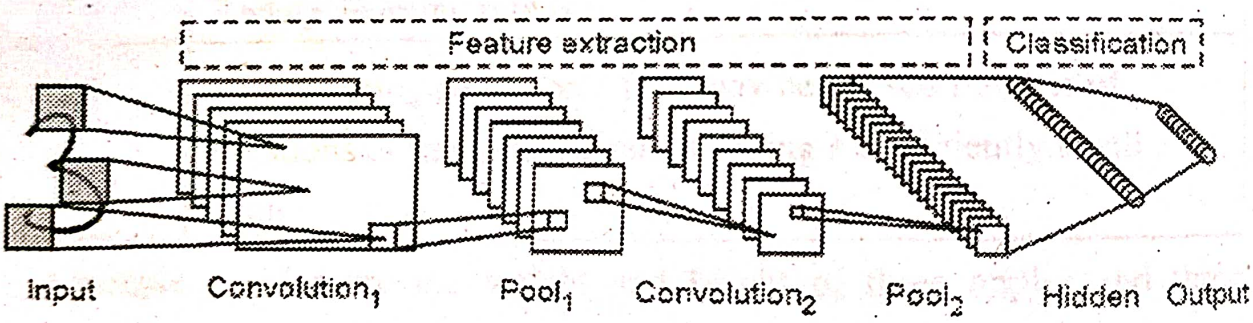


Fig. Q.1.1 Architecture of convolution neural network

- CNN architecture is made up of several layers that implement feature extraction, and then classification.
- The image is divided into receptive fields that feed into a convolutional layer, which then extracts features from the input image.

- The next step is pooling, which reduces the dimensionality of the extracted features (through down-sampling) while retaining the most important information (typically through max pooling).
- Another convolution and pooling step is then performed that feeds into a fully connected multilayer perceptron. The final output layer of this network is a set of nodes that identify features of the image. You train the network by using back-propagation.
- An input image is passed to the first convolutional layer. The convoluted output is obtained as an activation map. The filters applied in the convolution layer extract relevant features from the input image to pass further.
- Each filter shall give a different feature to aid the correct class prediction. In case we need to retain the size of the image, we use same padding (zero padding), otherwise valid padding is used since it helps to reduce the number of features.
- Pooling layers are then added to further reduce the number of parameters.
- Several convolution and pooling layers are added before the prediction is made. Convolutional layer help in extracting features.
- As we go deeper in the network more specific features are extracted as compared to a shallow network where the features extracted are more generic.
- The output layer in a CNN as mentioned previously is a fully connected layer, where the input from the other layers is flattened and sent so as the transform the output into the number of classes as desired by the network.
- The output is then generated through the output layer and is compared to the output layer for error generation.
- A loss function is defined in the fully connected output layer to compute the mean square loss. The gradient of error is then calculated.
- The error is then backpropagated to update the filter (weights) and bias values. One training cycle is completed in a single forward and backward pass..

Q.2 Explain applications of convolutional neural network.

Ans. : • **Computer vision :** CNN are employed to identify the hierarchy or conceptual structure of an image. Instead of feeding each image into the neural network as one grid of numbers, the image is broken down into overlapping image tiles that are each fed into a small neural network.

- Speech recognition : CNN have been used recently in speech recognition and has given better results over deep neural networks. Robustness of CNN is enhanced when pooling is done at a local frequency region and over-fitting is avoided by using fewer parameters to extract low-level features.
- CNNs use relatively little pre-processing compared to other image classification algorithms. This means that the network learns the filters that in traditional algorithms were hand-engineered. This independence from prior knowledge and human effort in feature design is a major advantage.
- They have applications in image and video recognition, recommender systems, image classification, medical image analysis and natural language processing.
- Video analysis : Compared to image data domains, there is relatively little work on applying CNNs to video classification. Video is more complex than images since it has another (temporal) dimension. However, some extensions of CNNs into the video domain have been explored. One approach is to treat space and time as equivalent dimensions of the input and perform convolutions in both time and space.
- Drug discovery : CNNs have been used in drug discovery. Predicting the interaction between molecules and biological proteins can identify potential treatments.
- Natural language processing : CNNs have also explored natural language processing. CNN models are effective for various NLP problems and achieved excellent results in semantic parsing, search query retrieval, sentence modeling, classification, prediction and other traditional NLP tasks.

Q.3 Explain advantages and disadvantages of CNN.

Ans. : 1. Advantages :

- CNN automatically detects the important features without any human supervision.
- CNN is also computationally efficient
- Higher accuracy
- Weight sharing is another major advantage of CNNs.
- Convolutional neural networks also minimize computation in comparison with a regular neural network.
- CNNs make use of the same knowledge across all image locations.

2. Disadvantages :

- Adversarial attacks are cases of feeding the network 'bad' examples to cause misclassification.
- CNN requires lot of training data.
- CNNs tend to be much slower because of operations like maxpool.

5.2 : Convolution Operation and Pooling

Q.4 What is convolutional layers ?

Ans. : • A convolutional layer is the main building block of a CNN. It contains a set of filters parameters of which are to be learned throughout the training. The size of the filters is usually smaller than the actual image. Each filter convolves with the image and creates an activation map.

- Components of convolutional layers are as follows :

  a) Filters b) Activation maps

  c) Parameter sharing d) Layer-specific hyper-parameters

- Filters are a function that has a width and height smaller than the width and height of the input volume. The filters are tensors, and they are used to convolve the input tensor when the tensor is passed to the layer instance. The random values inside the filter tensors are the weights of the convolutional layer.

- Sliding each filter across the spatial dimensions (width, height) of the input volume during the forward pass of information through the CNN. This produces a two dimensional output called an activation map for that specific filter.

Q.5 Discuss briefly convolution operation with example.

Ans. : • Convolution operation focuses on extracting/preserving important features from the input. Convolution operation allows the network to detect horizontal and vertical edges of an image and then based on those edges build high-level features in the following layers of neural network.

- In general form, convolution is an operation on two functions of a real valued argument. To motivate the definition of convolution, we start with examples of two functions we might use.
- Suppose we are tracking the location of a spaceship with a laser sensor. Laser sensor provides a single output x(t), the position of the spaceship at time t. Both "x" and "t" are real-valued, i.e., we can get a different reading from the laser sensor at any instant in time.
- Now suppose that our laser sensor is somewhat noisy. To obtain a less noisy estimate of the spaceship's position, we would like to average together several measurements. Of course, more recent measurements are more relevant, so we will want this to be a weighted average that gives more weight to recent measurements.
- We can do this with a weighting function w(a), where "a" is the age of a measurement. If we apply such a weighted average operation at every moment, we obtain a new function providing a smoothed estimate of the position "s" of the spaceship.
- Convolution operation uses three parameters : Input image, Feature detector and Feature map.
- Convolution operation involves an input matrix and a filter, also known as the kernel. Input matrix can be pixel values of a grayscale image whereas a filter is a relatively small matrix that detects edges by darkening areas of input image where there are transitions from brighter to darker areas.

There can be different types of filters depending upon what type of features we want to detect, e.g. vertical, horizontal, or diagonal, etc.

- Input image is converted into binary 1 and 0. The convolution operation, shown in Fig. Q.5.1 is known as the feature detector of a CNN. The input to a convolution can be raw data or a feature map output from another convolution. It is often interpreted as a filter in which the kernel filters input data for certain kinds of information.
- Sometimes a 5 × 5 or a 7 × 7 matrix is used as a feature detector. The feature detector is often referred to as a "kernel" or a "filter,". At each step, the kernel is multiplied by the input data values within its bounds, creating a single entry in the output feature map.
- Generally, an image can be considered as a matrix whose elements are numbers between 0 and 255. The size of image matrix is : $image\ height * image\ width * number\ of\ image\ channels$

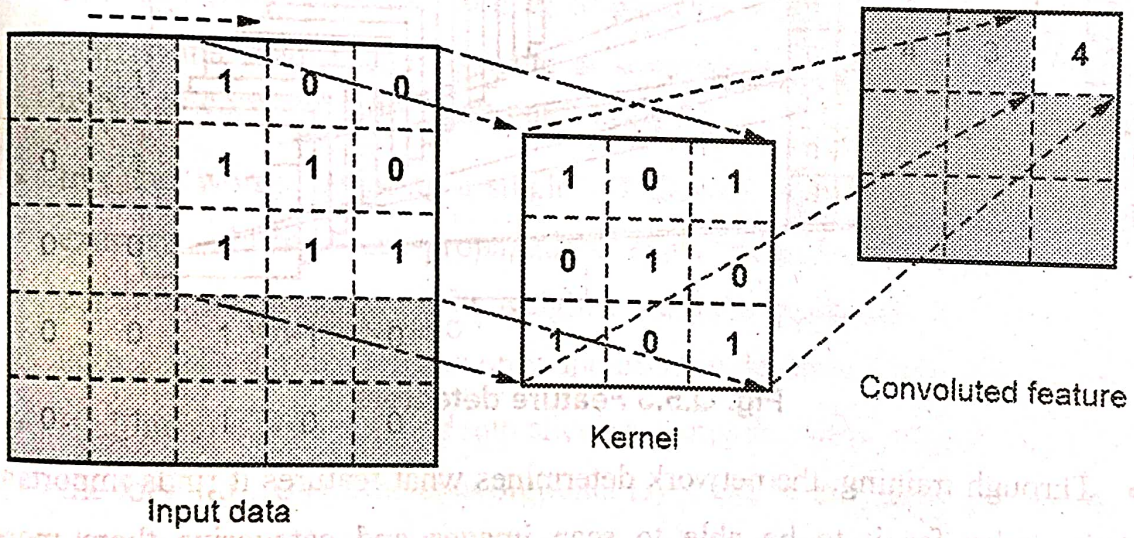


Fig. Q.5.1 Convolution operation

- A grayscale image has 1 channel, where a colour image has 3 channels.
- Kernel : A kernel is a small matrix of numbers that is used in image convolutions. Differently sized kernels containing different patterns of numbers produce different results under convolution. The size of a kernel is arbitrary but 3 × 3 is often used. Fig. Q.5.2 shows example of kernel.

0	1	0
1	1	1
0	1	0

Fig. Q.5.2 Example of kernel

- Convolutional layers perform transformations on the input data volume that are a function of the activations in the input volume and the parameters.
- In reality, convolutional neural networks develop multiple feature detectors and use them to develop several feature maps which are referred to as convolutional layers and it is shown in Fig. Q.5.3.

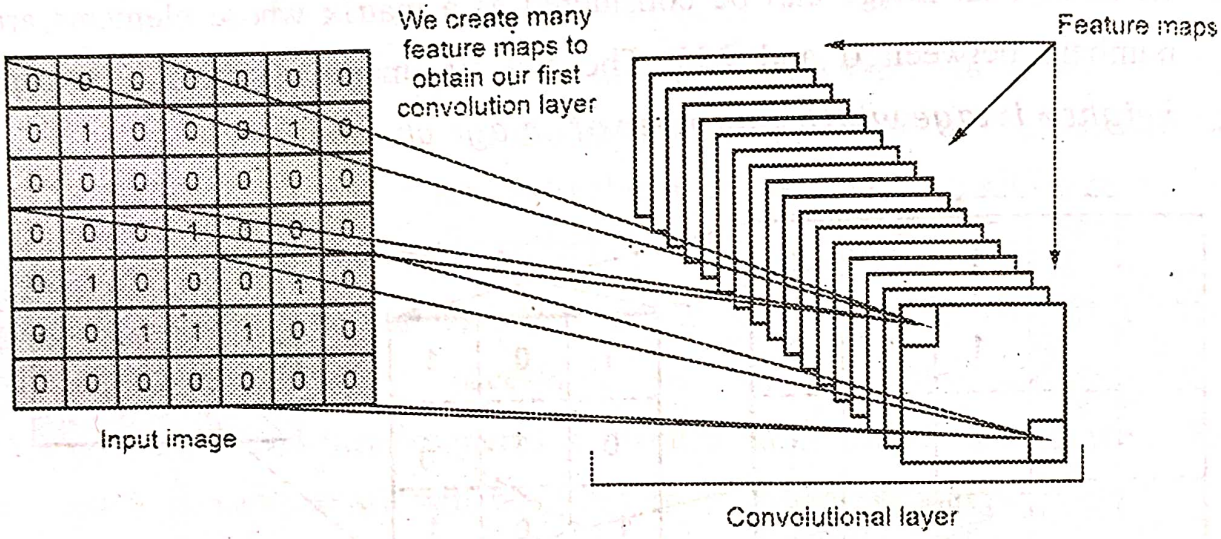


Fig. Q.5.3 Feature detectors

- Through training, the network determines what features it finds important in order for it to be able to scan images and categorize them more accurately.
- Convolutional layers have parameters for the layer and additional hyper-parameters. Gradient descent is used to train the parameters in this layer such that the class scores are consistent with the labels in the training set.
- Components of convolutional layers are as follows :
  a) Filters
  b) Activation maps
  c) Parameter sharing
  d) Layer-specific hyper-parameters

- Filters are a function that has a width and height smaller than the width and height of the input volume. The filters are tensors, and they are used to convolve the input tensor when the tensor is passed to the layer instance. The random values inside the filter tensors are the weights of the convolutional layer.
- Sliding each filter across the spatial dimensions (width, height) of the input volume during the forward pass of information through the CNN. This produces a two dimensional output called an activation map for that specific filter.

Q.6 How parameter sharing is used in CNN to control the total parameter count ?

Ans. : • Parameter sharing is used in CNN to control the total parameter count. Convolutional layers reduce the parameter count further by using a technique called parameter sharing.

- The user can reduce the number of parameters by making an assumption that if one feature can compute at some spatial position $(x,)$, then it is useful to compute a different place (x_2,y_2).
- In other words, denoting a single 2D slice of depth as a depth slice. For example, during back-propagation, every neuron in the network will compute the gradient for its weights, but these gradients will be added up across each depth slice and only update a single set of weights per slice.
- If all neurons in a single depth slice are using the same weight vector, then the forward pass of the convolutional layer can be computed in each depth slice as a convolution of the neuron's weights with the input volume. This is the reason why it is common to refer to the sets of weights as a filter (or a kernel), that is convolved with the input.
- Fig. Q.6.1 shows convolution shares the same parameters across all spatial locations.

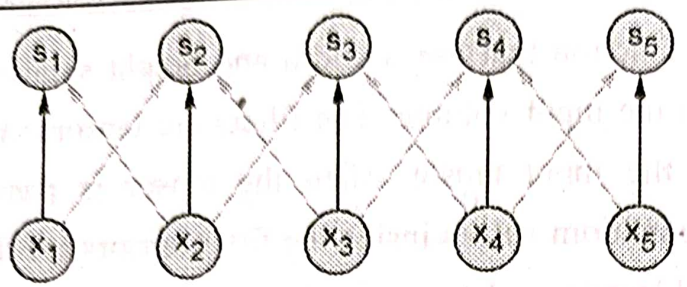


Fig. Q.6.1 Convolution shares the same parameters across all spatial locations

Q.7 Write short note on Pooling layer.

Ans. : • Pooling layers were developed to reduce the number of parameters needed to describe layers deeper in the network.

- Pooling also reduces the number of computations required for training the network, or for simply running it forward during a classification task.
- Fig. Q.7.1 shows pooling layer.

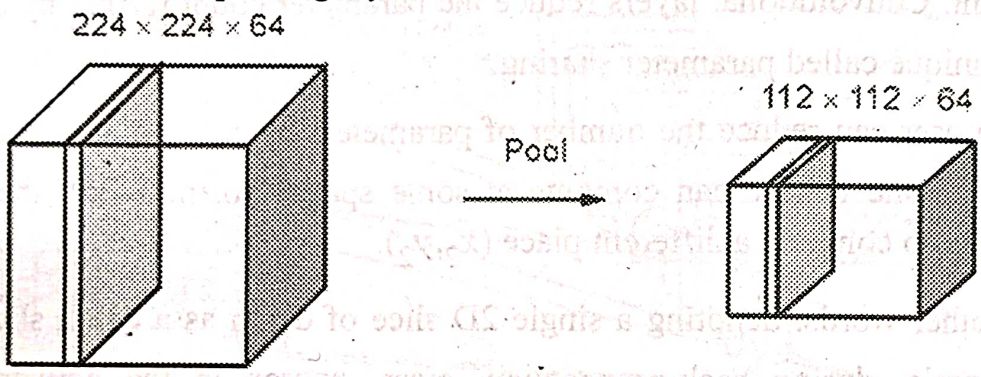


Fig. Q.7.1 Pooling layer

- Pooling layers provide some limited amount of translational and rotational invariance. However, it will not account for large translational or rotational perturbations, such as a face flipped by 180.
- Perturbations like these could only be detected if images of faces, rotated by 180, were present in the original training set.
- Accounting for all possible orientations of an object would require more filters and therefore more weight parameters would be required.
- Its function is to progressively reduce the spatial size of the representation to reduce the amount of parameters and computation in the network. Pooling layer operates on each feature map independently.
- The most common approach used in pooling is max pooling.

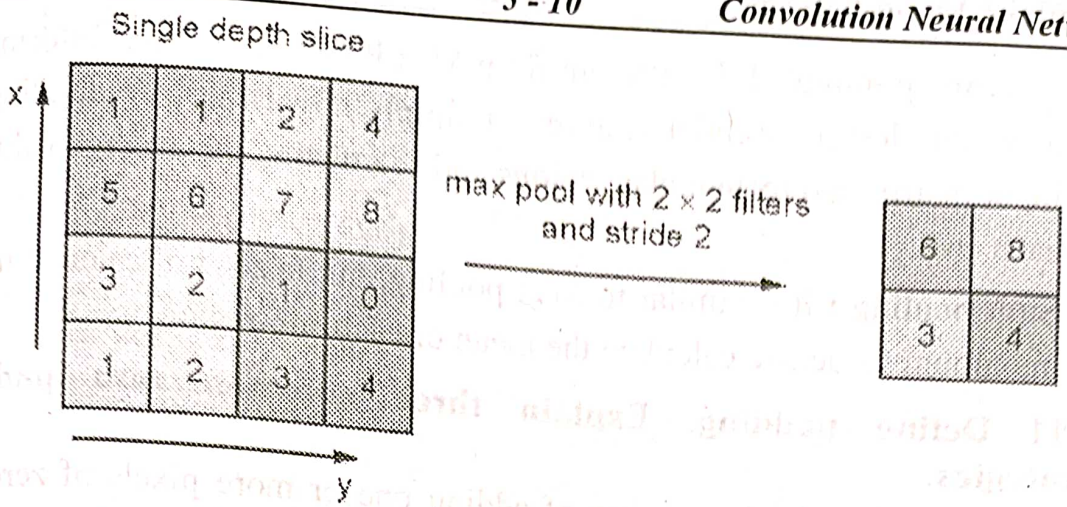


Fig. Q.7.2 Max pooling

- The pooling function replaces the output of the net at a certain location with a summary statistic of the nearby outputs. Max pooling reports the maximum output within a rectangular neighborhood. Average pooling reports the average output.
- Pooling helps make the representation approximately invariant to small input translations.

Q.8 What are dropouts ?

Ans. : A dropout is an approach where randomly selected neurons are ignored during training; they are dropped out randomly. In other words, their contribution to the activation of downstream neurons is temporarily removed on the forward pass and any weight updates are not applied to the neuron on the backward pass

Q.9 How is convolution different from pooling ?

Ans. : The significant difference is that a convolution layer extracts features from the data matrix, whereas the pooling layer only down samples the data matrix.

Q.10 Define the Max, sum and average pooling.

Ans. : • **Max pooling** is a rule to take the maximum of a region and help to proceed with the most crucial features from the image. It is a sample-based process that transfers continuous functions into discrete counterparts. Its primary objective is to downscale an input by reducing its dimensionality and making assumptions about features contained in the sub-region that were rejected.

- **Average pooling :** It is different from Max Pooling; it retains information about the lesser essential features. It simply downscales by dividing the input matrix into rectangular regions and calculating the average values of each area.
- **Sum pooling :** It is similar to Max pooling, but instead of calculating the maximum value, we calculate the mean of each sub-region.

Q.11 Define padding. Explain three common zero padding strategies.

Ans. : • **Padding** is the process of adding one or more pixels of zeros all around the boundaries of an image, in order to increase its effective size. Zero padding helps to make output dimensions and kernel size independent.

- One observation is that the convolution operation reduces the size of the $(q + 1)^{th}$ layer in comparison with the size of the qth layer. This type of reduction in size is not desirable in general, because it tends to lose some information along the borders of the image. This problem can be resolved by using padding.
- Three common zero padding strategies are :

  a) **Valid convolution :** Extreme case in which no zero-padding is used whatsoever, and the convolution kernel is only allowed to visit positions where the entire kernel is contained entirely within the input. For a kernel of size k in any dimension, the input shape of m in the direction will become m – k+1 in the output. This shrinkage restricts architecture depth

  b) **Same convolution :** Just enough zero-padding is added to keep the size of the output equal to the size of the input. Essentially, for a dimension where kernel size is k, the input is padded by k-1 zeros in that dimension

  c) **Full convolution :** Other extreme case where enough zeroes are added for every pixel to be visited k times in each direction, resulting an output image of width m + k – 1.

Q.12 List the various types of convolution function.

Ans. : Various types of convolution functions are as follows :

1. Stride
2. Zero padding
3. Unshared convolution
4. Partial connectivity between channels
5. Tiled

Q.13 Explain stride convolution functions.

Ans. : • The stride indicates the pace by which the filter moves horizontally and vertically over the pixels of the input image during convolution.

• Fig. Q.13.1 Shows stride during convolution.

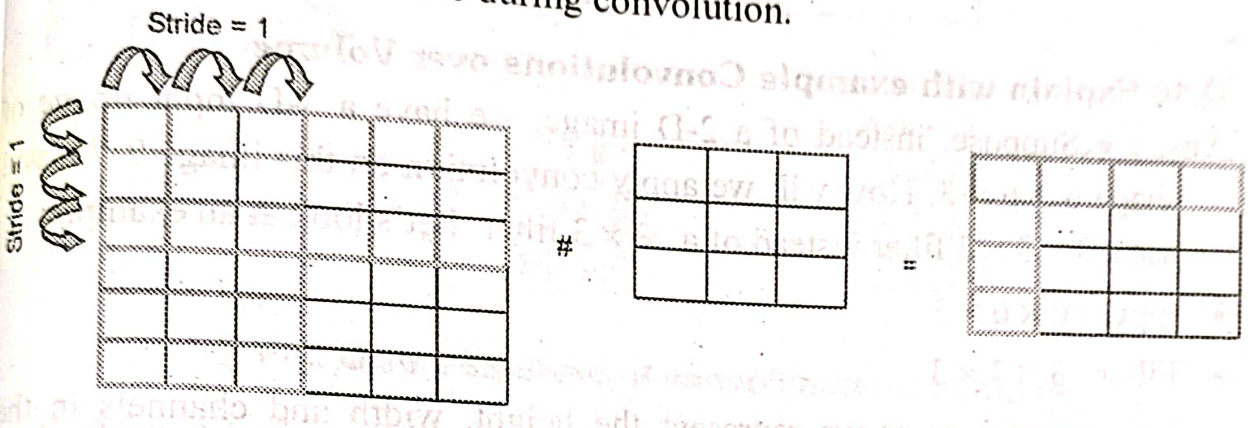


Fig. Q.13.1 Stride during convolution

• Stride is a parameter of the neural network's filter that modifies the amount of movement over the image or video. Stride is a component for the compression of images and video data. For example, if a neural network's stride is set to 1, the filter will move one pixel, or unit, at a time. If stride = 1, the filter will move one pixel.

• Stride depends on what we expect in our output image. We prefer a smaller stride size if we expect several fine-grained features to reflect in our output. On the other hand, if we are only interested in the macro-level of features, we choose a larger stride size.

Q.14 How many filters must a CNN have ?

Ans. : CNN does not learn with a single filter; they know through multiple features in parallel for a given input. For example, it is usual for a convolution layer to learn from 32 to 512 filters in parallel for a piece of shared information.

Q.15 What is tiled convolution ?

Ans. : • Tiled convolution learn a set of kernels that is rotated through as we move through space, rather than learning a separate set of weights at every spatial location as in locally connected layer.

• It offers a compromise between a convolutional layer and a locally connected layer.

- Memory requirements for storing the parameters will increase only by a factor of the size of this set of kernels.

5.3 : 6 Convolutions Over Volume

Q.16 Explain with example Convolutions over Volume.

Ans. : • Suppose, instead of a 2-D image, we have a 3-D input image of shape $6 \times 6 \times 3$. How will we apply convolution on this image ? We will use a $3 \times 3 \times 3$ filter instead of a 3×3 filter. Let's look at an example:

- Input : $6 \times 6 \times 3$
- Filter : $3 \times 3 \times 3$
- The dimensions above represent the height, width and channels in the input and filter. Keep in mind that the number of channels in the input and filter should be same. This will result in an output of 4×4. Fig. Q.16.1 shows convolution image.

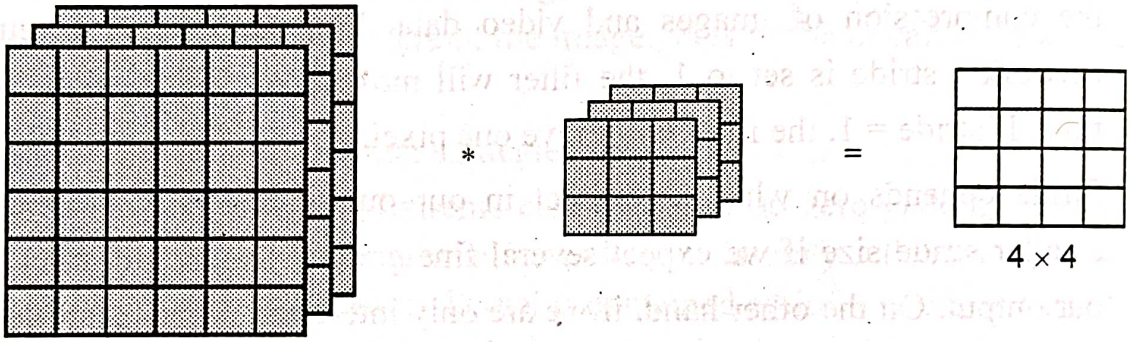


Fig. Q.16.1 Convolution image

- Since there are three channels in the input, the filter will consequently also have three channels. After convolution, the output shape is a 4×4 matrix. So, the first element of the output is the sum of the element-wise product of the first 27 values from the input (9 values from each channel) and the 27 values from the filter. After that we convolve over the entire image.
- Instead of using just a single filter, we can use multiple filters as well. How do we do that ? Let's say the first filter will detect vertical edges and the second filter will detect horizontal edges from the image. If we use multiple filters, the output dimension will change. So, instead of having a 4×4 output as in the above example, we would have a $4 \times 4 \times 2$ output (if we have used 2 filters) :

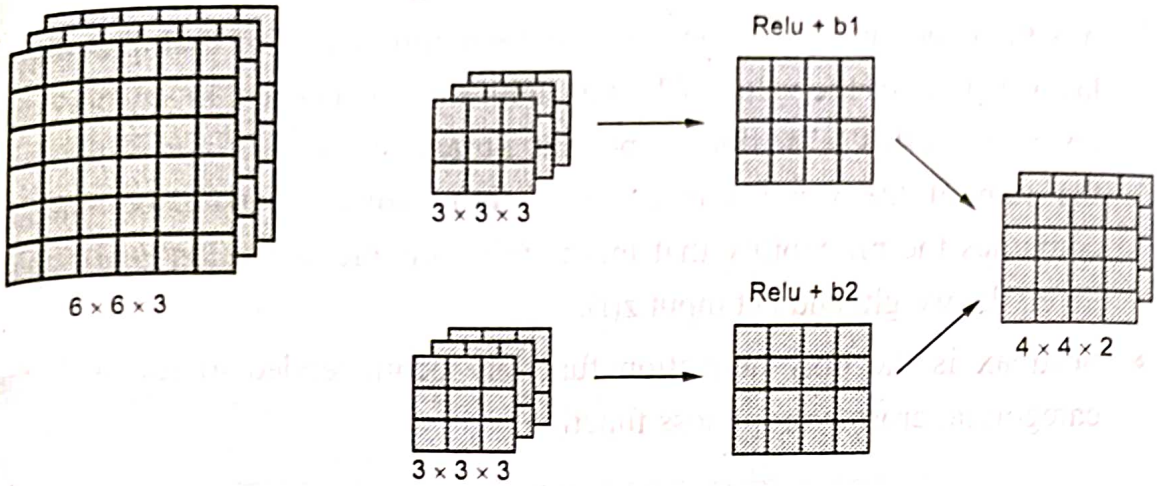


Fig. Q.16.2 Example of convolution over volume

- After a series of 3D convolutional layers, we need to 'flatten' the 3D tensor to a 1D tensor and add one or several dense layers to connect the output to the response variable.

5.4 : SoftMax Regression

Q.17 Write short note on SoftMax regression.

Ans. : • The softmax function is nothing but a generalization of the sigmoid. The Softmax regression is a form of logistic regression that normalizes an input value into a vector of values that follows a probability distribution whose total sums up to 1. The output values are between the range [0, 1].

- When we have to deal with a classification with more than 2 possible levels, we use a generalization of the logistic regression function called softmax regression; a logistic regression class for multi-class classification tasks. In Softmax regression, we replace the sigmoid logistic function by the so-called softmax function.

$$P(y = j \mid z^{(i)}) = \phi_{softmax}(z^{(i)}) = \frac{e^{z^{(i)}}}{\sum_{j=0}^{k} e^{z_k^{(i)}}}$$

where we define the net input z as

$$z = w_1 x_1 + \ldots + w_m x_m + b = \sum_{l=1}^{m} w_1 x_1 + b$$
$$= w^T x + b$$

- The w is the weight vector, x is the feature vector of 1 training sample and b is the bias unit. A bias unit is an extra neuron added to each pre-output layer that stores the value of 1. Bias units aren't connected to any previous layer and in this sense don't represent a true activity. It is used in the case the sum of the weights is equal to zero. Now, this softmax function computes the probability that this training sample x(i) belongs to class j given the weight and net input z(i).
- Softmax is the only activation function recommended to use with the categorical cross-entropy loss function.

5.5 : Deep Learning Frameworks

Q.18 What is Deep Learning? Explain Deep learning (DL) frameworks. Why Use a Deep Learning Framework ?

Ans. : • The term "deep" usually refers to the number of hidden layers in the neural network.

- Deep learning is a subset of machine learning, which is predicated on idea of learning from example. In machine learning, instead of teaching a computer a massive list of rules to solve the problem, we give it a model with which it can evaluate examples, and a small set of instructions to modify the model when it makes a mistake.
- The basic idea of deep learning is that repeated composition of functions can often reduce the requirements on the number of base functions (computational units) by a factor that is exponentially related to the number of layers in the network.
- Deep learning eliminates some of data pre-processing that is typically involved with machine learning.

Deep learning (DL) frameworks :

- A deep learning framework is a software package used by researchers and data scientists to design and train deep learning models. The idea with these frameworks is to allow people to train their models without digging into the algorithms underlying deep learning, neural networks, and machine learning.

- **Deep learning (DL) frameworks** offer building blocks for designing, training, and validating deep neural networks through a high-level programming interface.
- Widely used deep learning frameworks such as PyTorch, TensorFlow, MXNet and others can also use GPU-accelerated libraries such as cuDNN and NCCL to deliver high-performance multi-GPU accelerated training.

Why Use a Deep Learning Framework?

- They supply readily available libraries for defining layers, network types (CNNs, RNNs) and common model architectures
- They can support computer vision applications; image, speech and natural language processing
- They have familiar interfaces via popular programming languages such as Python, C, C++ and Scala
- Many deep learning frameworks are accelerated by NVIDIA deep learning libraries such as cuDNN, NCCl and cuBLAS for GPU accelerated deep learning training.

Q.19 What is TensorFLow? Why it is popular? List the Features of Tensorflow.

Ans. : • TensorFlow is an end-to-end open source platform for Deep learning. It was developed by the Google Brain team and released in November 2015.

- It uses Python or JavaScript to provide a convenient front-end API for building applications, while executing those applications in high-performance C++.
- TensorFlow is popular for its TensorFlow Core programs where it has two main actions.
  1. Building the computational graph in the construction phase
  2. Running the computational graph in the execution phase
- A tensor is a mathematical object and a generalization of scalars, vectors, and matrices. A tensor can be represented as a multidimensional array. Let's understand how TensorFlow works.
  1. Its programs are usually structured into a construction phase and an execution phase.
  2. The construction phase assembles a graph that has nodes (ops/operations) and edges (tensors).

3. The execution phase uses a session to execute ops (operations) in the graph.

- Features of Tensorflow are as follows :
  1. Faster debugging with Python tools
  2. Dynamic models with Python control flow
  3. Support for custom and higher-order gradients
  4. TensorFlow offers multiple levels of abstraction, which helps to build and train models.
  5. TensorFlow provides the flexibility and control with features like the Keras Functional API and Model
  6. Well-documented so easy to understand
  7. Probably the most popular easy to use with Python.

Q.20 Write about data structure of TensorFlow.

Ans. : • TensorFlow programs use a tensor data structure to represent all data, only tensors are passed between operations in the computation graph. TensorFlow allows developers to create dataflow graphs, structures that describe how data moves through a graph, or a series of processing nodes.

- Each node in the graph represents a mathematical operation and each connection or edge between nodes is a multidimensional data array, or tensor.
- TensorFlow applications can be run on most any target that's convenient: a local machine, a cluster in the cloud, iOS and Android devices, CPUs or GPUs. If you use Google's own cloud, you can run TensorFlow on Google's custom TensorFlow Processing Unit (TPU) silicon for further acceleration. The resulting models created by TensorFlow, though, can be deployed on most any device where they will be used to serve predictions.
- Tesorflow supports three main type of data types : Constants, Variables and Placeholders.
- Constant in TensorFlow : tf.constant() function is used to create constant in TensorFlow. Here, it will always create host/CPU tensor. Syntax is as follows :

tf.constant (value, dtype=None, shape=Name, name='Constant')

where

a) Value : A constant value or list. This value is the constant value that is passed to the function.

b) Dtype : It is the data type of the element. dtype is passed to the specify the datatype of the value which is passed as constant. If dtype is not mentioned, then it concludes the type from value, by default.

c) Shape: It is optional dimensions given to the value.

d) Name : Another optional attribute which assigns name for the tensor, which contains the constant value.

e) Verify_shape : It is a boolean value that helps enabling of verification of the shape of values.

Q.21 What is Keras? Explain salient feature of keras. What are the limitations of Keras?

Ans. : • Keras is a high-level neural networks API, capable of running on top of Tensorflow, Theano, and CNTK. It enables fast experimentation through a high level, userfriendly, modular and extensible API. Keras can also be run on both CPU and GPU.

- Keras is written in Python and supports multiple back-end neural network computation engines.
- Keras provides seven different datasets, which can be loaded in using Keras directly. These include image datasets as well as a house price and a movie review datasets.
- Salient Features of Keras

1. Keras is a high-level interface and uses Theano or Tensorflow for its backend.
2. It runs smoothly on both CPU and GPU.
3. Keras supports almost all the models of a neural network – fully connected, convolutional, pooling, recurrent, embedding, etc. Furthermore, these models can be combined to build more complex models.
4. Keras, being modular in nature, is incredibly expressive, flexible, and apt for innovative research.
5. Keras is a completely Python-based framework, which makes it easy to debug and explore.

- The Model is the core Keras data structure. There are two main types of models available in Keras : the Sequential model, and the Model class used with the functional API.
- The easiest way of creating a model in Keras is by using the sequential API, which lets we stack one layer after the other. The problem with the sequential API is that it doesn't allow models to have multiple inputs or outputs, which are needed for some problems.
- The functional API allows user to create the same models but offers more flexibility at the cost of simplicity and readability. It can be used with multiple input and output layers and shared layers, which enables to build complex network structures. When using the functional API, we always need to pass the previous layer to the current layer. It also requires the use of an input layer. The functional API is also often used for transfer learning.
- Keras provides seven different datasets, which can be loaded using Keras directly. These include image datasets, a house price and a movie review dataset. Keras is a high-level neural networks API running on top of Tensorflow.
- Demerits of Keras :
  1 Restricted to use only on smaller datasets.
  2 Slower performance since it is completely written in Python.
  3 The project repository is not as huge compared to TensorFlow.

Q.22 What are the difference between Keras and Tensorflow ?

Ans. :

Keras	Tensorflow
Keras is a high-level API which is running on top of TensorFlow.	TensorFlow is a framework that offers both high and low-level APIs.
Keras is used for small datasets as it is slower.	TensorFlow is used for high-performance models and massive datasets that require execution fast.
It can be used for low-performance models.	It is used for high-performance models.

Working with beginner-friendly projects with small datasets.	Rendering heavy projects with ease.
Readable and concise architecture.	Comparatively complex architecture.
Community support is minimal but growing.	Being one of the first deep learning frameworks that were developed, it has an extensive community and a rich reserve of readable material.

Q.23 Write short note on following :
a) PyTorch b) Caffe c) Shogun

Ans. : a) PyTorch : • PyTorch is an open source machine learning library for Python and is completely based on torch. It is primarily used for applications such as natural language processing. It was developed by Facebook's AI research lab.

- PyTorch uses dynamic computation, which allows greater flexibility in building complex architectures. PyTorch uses core Python concepts like classes, structures and conditional loops.
- PyTorch has a very simple interface like Python. It provides an easy way to use API.
- It allows developers to train a neural network model in a distributed manner. It provides optimized performance in both research and production with the help of native support for peer to peer communication and asynchronous execution of collective operation from Python and C++.
- The PyTorch core is used to implement tensor data structure, CPU and GPU operators, basic parallel primitives and automatic differentiation calculations.
- PyTorch is supported by many major cloud platforms such as AWS. With the help of prebuilt images, large scale training on GPU's and ability to run models in a production scale environment etc.; it provides frictionless development and easy scaling.

b) Caffe : • Convolutional Architecture for Fast Feature Embedding (Caffe) is a deep learning framework made with expression, speed and modularity in mind. It is developed by Berkeley AI Research (BAIR) and by community contributors.

- Caffe is primarily a C++ library and exposes a modular development interface. Caffe offers interfaces for daily use by way of the command line, Python and MATLAB.
- Caffe processes data in the form of Blobs which are N-dimensional arrays stored in a C-contiguous fashion. Data is stored both as data we pass along the model and as diff, which is a gradient computed by the network.
- Data layers handle how the data is processed in and out of the caffe model. Pre-processing and transformation like random cropping, mirroring, scaling and mean subtraction can be done by configuring the data layer. Furthermore, pre-fetching and multiple-input configurations are also possible.

c) Shogun : • Shogun is an open source machine learning software library built in C++. Shogun was developed in 1999 by Soeren Sonnenburg and Gunnar Raetsch.

- It offers numerous algorithms and data structures for machine learning problems. The focus of Shogun is on kernel machines such as support vector machines for regression and classification problems. Shogun also offers a full implementation of hidden Markov models.
- Shogun is a community learning platform in every sense, anyone can use the toolbox to learn about ML and apply it to solve problems.
- Shogun is community-based and non-commercial. It is currently released under the GPLv3. It is also moving towards BSD compatibility with optional GPL (General Public License) parts. This means companies can use the code without having to turn their code-base to GPL.

5.6 : Bias and Variance with Mismatched Data Distributions

Q.24 Explain briefly bias-variance trade off.

Ans. : • In the experimental practice we observe an important phenomenon called the bias variance dilemma.

- In supervised learning, the class value assigned by the learning model built based on the training data may differ from the actual class value. This error in learning can be of two types, errors due to 'bias' and error due to 'variance'.

Fig. Q.24.1 shows bias-variance trade off.

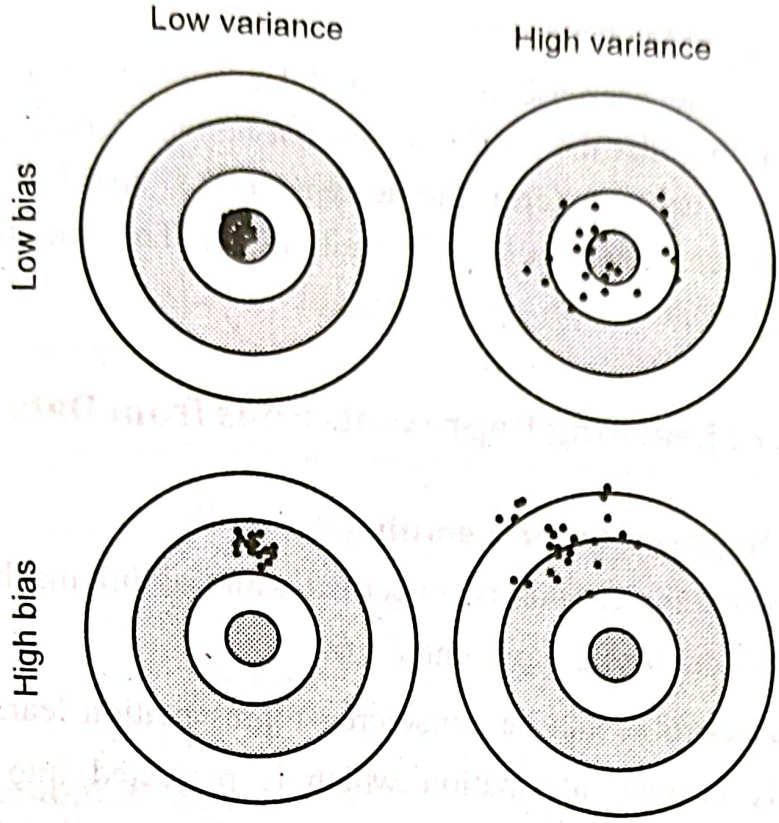


Fig. Q.24.1 Bias-variance trade off

Give two classes of hypothesis (e.g. linear models and k-NNs) to fit to some training data set, we observe that the more flexible hypothesis class has a low bias term but a higher variance term. If we have parametric family of hypothesis, then we can increases the flexibility of the hypothesis but we still observe the increase of variance.

The bias-variance-dilemma is the problem of simultaneously minimizing two sources of error that prevent supervised learning algorithm from generalizing beyond their training set :

1. The bias is error from erroneous assumptions in the learning algorithm. High bias can cause an algorithm to miss the relevant relations between features and target outputs.
2. The variance is error from sensitivity to small fluctuations in the training set. High variance can cause overfitting : Modeling the random noise in the training data, rather than the intended outputs.

- In order to reduce the model error, the designer can aim at reducing either the bias or the variance, as the noise components is irreducible.
- As the model increases in complexity, its bias is likely to diminish. However, as the number of training examples is kept fixed, the parametric

identification of the model may strongly vary from one DN to another. This will increase the variance term.

- At one stage, the decrease in bias will be inferior to the increase in variance, warning that the model should not be too complex. Conversely, to decrease the variance term, the designer has to simplify its model so that it is less sensitive to a specific training set. This simplification will lead to a higher bias.

5.7 : Learning Representations from Data

Q.25 What is Representation Learning ?

Ans. : • Representation learning is concerned with training machine learning algorithms to learn useful representations.

- Deep neural networks can be considered representation learning models that typically encode information which is projected into a different subspace. These representations are then usually passed on to a linear classifier to, for instance, train a classifier.
- Representation learning can be divided into :
  a) Supervised representation learning : Learning representations on task A using annotated data and used to solve task B
  b) Unsupervised representation learning : Learning representations on a task in an unsupervised way. These are then used to address downstream tasks and reducing the need for annotated data when learning news tasks.

Q.26 What is Greedy Algorithm ?

Ans. : Greedy algorithms break a problem into many components, then solve for the optimal version of each component in isolation. Unfortunately, combining the individually optimal components is not guaranteed to yield an optimal complete solution.

Q.27 Write and explain an algorithm for Gready Layer-Wise Unsupervised Pretraining.

Ans. : • Greedy Layer - Wise Unsupervised Pretraining relies on single-layer representation learning algorithm. Each layer is pretrained using

unsupervised learning, taking the output of previous layer and producing as output a new representation of the data, whose distribution is hopefully simpler.

- Unsupervised feature learning algorithm L, which takes a training set of examples and returns an encoder or feature function f. The X is raw input data.

$$F \leftarrow \text{Identify function}$$

$$\tilde{X} = X$$

$$\text{for } k = 1 \ldots m \text{ do}$$

$$f^{(k)} = L(\tilde{X})$$

$$f \leftarrow f^{(k)} \circ f$$

$$\tilde{X} \leftarrow f^{(k)}(\tilde{X})$$

$$\text{end for}$$

$$\text{if fine-tuning then}$$

$$f \leftarrow T(f \cdot X \cdot Y)$$

$$\text{end if}$$

$$\text{Return } f$$

- Gready : Optimize each piece of the solution independently, on piece at a time.
- Layer-Wise : The independent pieces are the layer of the network. Training proceeds once layer at a time, training the kth layer while keeping the previous ones fixed.
- Unsupervised : Each layer is trained with an unsupervised representation learning algorithm

Q.28 When and why does unsupervised pretraining ideas work ?

Ans. :

1. Idea1 : Choice of initial parameters for a deep NN can have a significant regularizing effect on the model.
   - It remains possible that pretraining initializes the model in a location that would otherwise be inaccessible. For example : a region surrounded by areas where the cost function varies so much from

one example to another that mini-batches give only a very noisy estimate of the gradient a region surrounded by areas where the Hessian matrix is so pooly conditioned that gradient descent methods must use very small steps.

- We cannot characterize the exactly what aspects of the pretrained parameters are retained during the supervised training stages.

2. Idea2 : Learning about the input distribution can help with learning about the mapping from input to output.
   - Some features that are useful for the unsupervised task may also be useful for supervised task. This is not yet understood at a mathematical, theoretical level. Many aspects of this approach are highly dependent on the specific models used.
   - For example, if we wish to add a linear classifier on top of pretrained features, the features must make the underlying classes linearly separable. This is another reason that simultaneous supervised and unsupervised learning can be preferable.

Q.29 Why it is called Greedy layer-wise pretraining ?

Ans. : • Greedy because, it is a greedy algorithm that optimizes each piece of the solution independently

- Layer-wise because, independent pieces are the layers of the network and training proceeds one layer at a time.
- Pretraining because, it is only a first step before applying a joint training algorithm is applied to fine-tune all layers together.

Q.30 Explain disadvantage of Unsupervised Pretraining.

Ans. :

1. Unsupervsied pretraining does not offer a clear way to adjust the strength of the regularization arising from the unsupervised stage. When we perform unsupervised and supervised learning simultaneously, instead of using the pretraining strategy, there is a single hyperparameter, usually a coefficient attatched to the unsupervised cost, that determine hows strongly supervised objective will regularize the supervised model.
2. Two separate training phases has its own hyperparameters. The performance of the second phase cannot be predicted during the first

phase, so there is a long delay between proposing hyperparameters for the first phase and being able to update them using feedback from the second phase. Most principled approach : use validation set error in the supervised phase to select hyperparameters of the pretraining phase.

Q.31 Define Transfer learning and domain adaptation.

Ans. : Transfer learning and domain adaptation refer to situation where what has been learned in one setting is exploited to improve generalization in another settings.

Q.32 What is transfer learning ? Explain its types.

Ans. : • Transfer learning, multitask learning and domain adaptation can be achieved via representation learning when there exist features that are useful for different settings or tasks, corresponding to underlying factors that appear in more than one setting.

- Two extreme form of transfer learning :
  1. One-shot learning : Only one example of transfer task is given for one-shot learning. It is possible because the representation learns cleanly separate the underlying classes during first stage. During the transfer learning stage, only one labeled example is needed to infer the label of many possible test examples that all cluster around the same point in representation space.
  2. Zero-shot learning : No labeled examples are given at all. It is only possible because additional information has been exploited during training.

5.8 : Multi-task Learning

Q.33 What is multitasking? What are the advantages of multitasking?

Ans. : • Multi-Task learning is a sub-field of Machine Learning that aims to solve multiple different tasks at the same time, by taking advantage of the similarities between different tasks.

- Multitask learning is a way to improve generalization by pooling the examples arising out of several tasks.

- Different supervised task shared the same input and some intermediate-level representation.
- We can view multi-task learning as a form of inductive transfer. Inductive transfer can help improve a model by introducing an inductive bias, which causes a model to prefer some hypotheses over others.
- For instance, a common form of inductive bias is ℓ_1 regularization, which leads to a preference for sparse solutions.

Advantages of Multi-task Learning:

- Reduce overfitting
- Implicit data augmentation
- Regularization : MTL acts as a regularizer by introducing an inductive bias
- Focus on relevant features : If a task is very noisy or data is limited and high-dimensional, it can be difficult for a model to differentiate between relevant and irrelevant features

Q.34 Explain the types of multitasking.

Ans. : • Multi-tasking learning are of two types : hard or soft parameter sharing of hidden layers.

- **Hard parameter :** It is generally applied by sharing the hidden layers between all tasks, while keeping several task-specific output layers. Hard parameter sharing greatly reduces the risk of overfitting.
- Fig. Q.34.1 shows hard sharing of hidden layers.

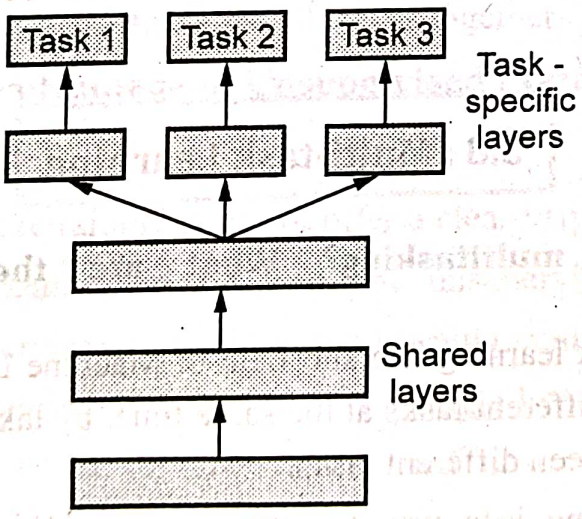


Fig. Q.34.1 Hard sharing of hidden layers

- **Soft parameter** sharing adds a constraint to achieve similarity among related parameters rather than sharing the same value. Furthermore, we penalize the difference in parameters across the models that we train for each task. By loosely connecting the shared space representations, this method, in contrast to rigid sharing, allows activities greater flexibility.
- Fig. Q.34.2 shows soft parameter sharing multi-tasking.

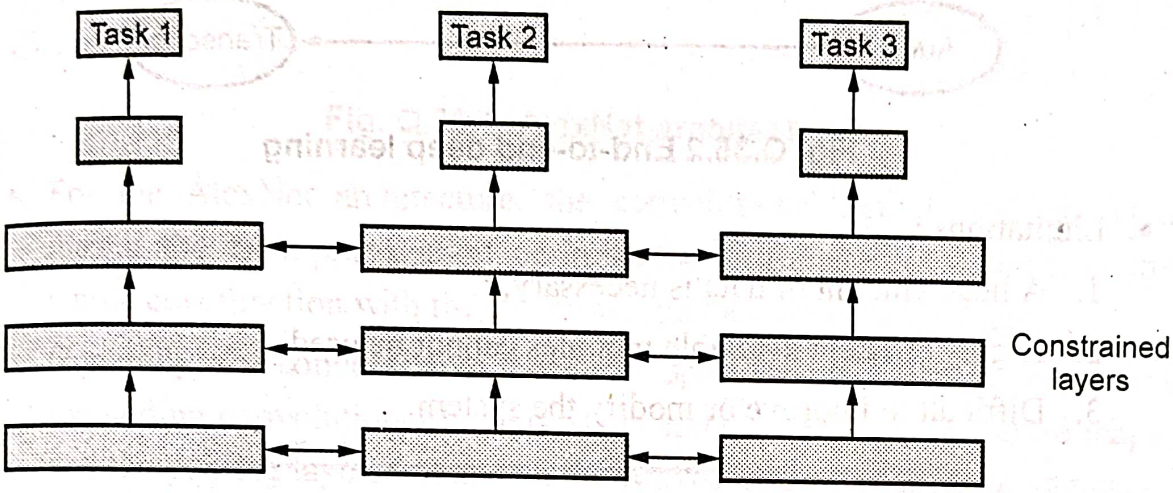


Fig. Q.34.2 Soft parameter sharing multi-tasking

- In soft parameter sharing on the other hand, each task has its own model with its own parameters. The distance between the parameters of the model is then regularized in order to encourage the parameters to be similar.

5.9 : End-to-End Deep Learning

Q.35 Explain briefly End-to-end deep learning.

Ans. : • End-to-end (E2E) learning refers to training a possibly complex learning system represented by a single model that represents the complete target system, bypassing the intermediate layers usually present in traditional pipeline designs.

- End-to-end deep learning is the simplification of a processing or learning system into one neural network. Example is speech recognition model. It requires small data set.

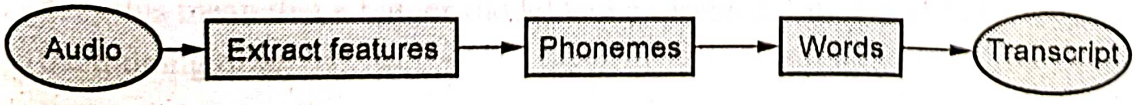


Fig. Q.35.1 Traditional way

- End-to-end deep learning cannot be used for every problem since it needs a lot of labeled data.
- It is used mainly in audio transcripts, image captures, image synthesis, machine translation, steering in self-driving cars, etc. The End-to-End deep learning way -large data set.
- Fig. Q.35.2 shows end-to-end deep learning.

Fig. Q.35.2 End-to-end deep learning

- Limitations :
  1. A huge amount of data is necessary.
  2. Highly efficient available modules cannot be used.
  3. Difficult to improve or modify the system.

5.10 : Introduction to CNN Models

Q.36 Write short note on : AlexNet.

Ans. : • Alexnet is a Deep Convolutional Neural Network for image classification.

- AlexNet is composed of 5 convolutional layers with a combination of max-pooling layers, 3 fully connected layers, and 2 dropout layers. The activation function used in all layers is Relu. The activation function used in the output layer is Softmax. The total number of parameters in this architecture is around 60 million.
- The AlexNet architecture was created with large-scale image datasets in mind, and it produced state-of-the-art results when it was first released. It has 60 million characteristics in all.
- Fig. Q.36.1 shows AlexNet architecture.

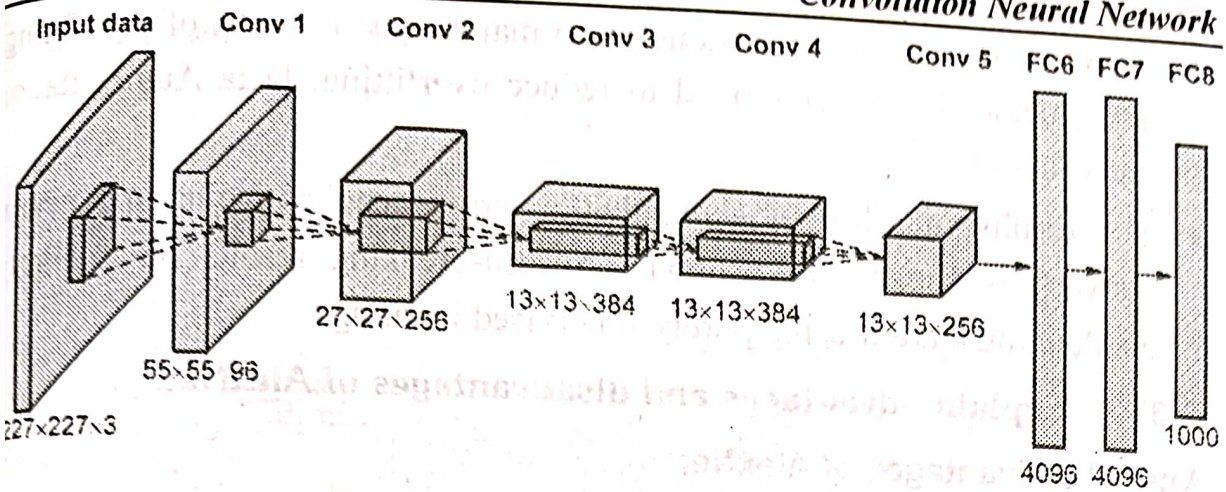


Fig. Q.36.1 AlexNet architecture

- For the AlexNet architecture, the convolutional kernels are extracted during the back-propagation optimization procedure by optimizing the whole cost function with the stochastic gradient descent algorithm.
- Generally, the convolutional layers act upon the input feature maps with the sliding convolutional kernels to generate the convolved feature maps, and the pooling layers operate on the convolved feature maps to aggregate the information within the given neighborhood window with a max pooling operation or average pooling operation.
- Max pooling is applied between every two conv layers. After the tensors are flattened, two fully-connected (dense) layers are used. The output layer is a softmax layer to compute the softmax loss function for learning
- AlexNet uses Rectified Linear Units (ReLU) instead of the tanh function, which was standard at the time. ReLU's advantage is in training time; a CNN using ReLU was able to reach a 25 % error on the CIFAR-10 dataset six times faster than a CNN using tanh.
- Use of multiple GPUs and parallel computing is highlighted in the training of AlexNet. The use of ReLU as the activation function for image classification by CNN.
- Multiple GPUs : GPUs were still rolling around with 3 gigabytes of memory. This was especially bad because the training set had 1.2 million images. AlexNet allows for multi-GPU training by putting half of the model's neurons on one GPU and the other half on another GPU. Not only does this mean that a bigger model can be trained, but it also cuts down on the training time.
- Overlapping Pooling : CNNs traditionally "pool" outputs of neighboring groups of neurons with no overlapping.

- AlexNet had 60 million parameters, a major issue in terms of overfitting. Two methods were employed to reduce overfitting: Data Augmentation and dropout.
- The results of AlexNet show that a large, deep convolutional neural network is capable of achieving record-breaking results on a highly challenging dataset using purely supervised learning.

Q.37 Explain advantages and disadvantages of AlexNet.

Ans. : 1. Advantages of AlexNet

- AlexNet is considered as the milestone of CNN for image classification
- Many methods such as the conv and pooling design, dropout, GPU, parallel computing, ReLU is still the industrial standard for computer vision.
- The unique advantage of AlexNet is the directly image input to the classification model.
- The convolution layers can automatically extract the edges of the images and fully connected layers learning these features.
- Theoretically the complexity of visual patterns can be effective extracted by adding more conv layers.

2. Disadvantages of AlexNet

- AlexNet is NOT deep enough compared to the later model such as VGG Net, GoogLENet, and ResNet.
- The use of large convolution filters (5 * 5) is not encouraged.
- Use normal distribution to initiate the weights in the neural networks cannot effective solve the problem of gradient vanishing, replaced by the Xavier method later.
- The performance is surpassed by more complex models such as GoogLENet and ResNet.

Q.38 Write short note on: LeNet – 5.

Ans. : • LeNet-5 is a convolutional neural network architecture that was created by Yann LeCunn in 1998. It includes 7 layers, excluding the input layer, which contains the trainable parameters called weights.

- **LeNet-5** consists of two parts : i) A convolutional encoder consisting of two convolutional layers; and ii) A dense block consisting of three fully connected layers.
- Fig. Q.38.1 shows architecture of LaNet-5.

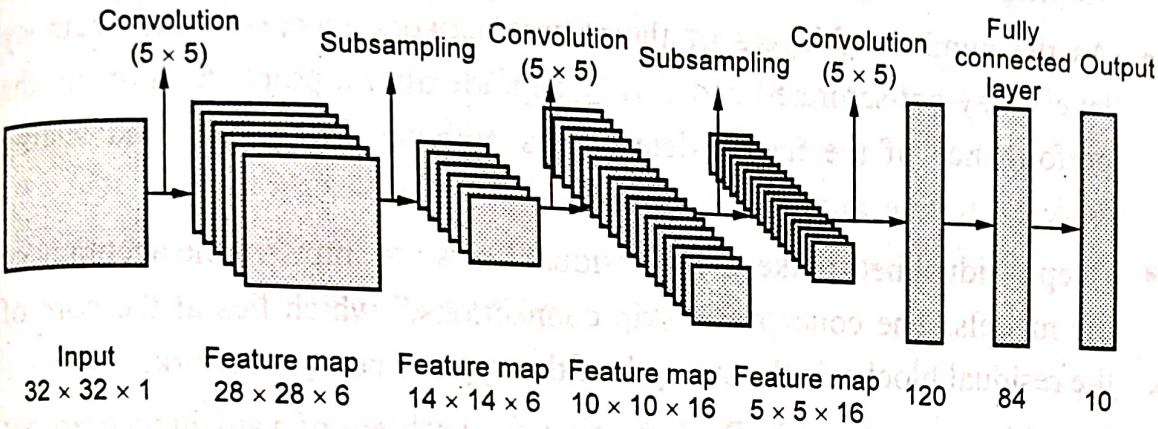


Fig. Q.38.1 LaNet-5 architecture

- Layer C1 is a convolutional layer with six feature maps where the size of the feature maps is 28 × 28;
- Layer S2 is a sub-sampling layer with six feature maps where the size of the feature maps is 14 × 14;
- Layer C3 is a convolutional layer with sixteen feature maps where the size of the feature maps is 10 × 10;
- Layer S4 is s sub-sampling layer with sixteen feature maps where the size of feature maps is 5 × 5;
- Layer C5 is a convolutional layer with 120 feature maps where the size of the feature maps is 1 × 1;
- Layer F6 contains 84 units and is fully connected to the C5 convolutional layer.
- The ability to process higher resolution images requires larger and more convolutional layers, so this technique is constrained by the availability of computing resources.

Q.39 What is residual networks? Explain with neat diagram of residual networks.

Ans. : • Residual network is a specific type of neural network that was introduced in 2015 by Kaiming He, Xiangyu Zhang, Shaoqing Ren and Jian Sun. ResNet has many variants that run on the same concept but have different numbers of layers. Resnet50 is used to denote the variant that can work with 50 neural network layers.

- When working with deep convolutional neural networks to solve a problem related to computer vision, machine learning experts engage in stacking more layers. These additional layers help solve complex problems more efficiently as the different layers could be trained for varying tasks to get highly accurate results.
- As the number of layers of the neural network increases, the accuracy levels may get saturated and slowly degrade after a point. As a result, the performance of the model deteriorates both on the training and testing data.
- Deep residual nets make use of residual blocks to improve the accuracy of the models. The concept of "skip connections," which lies at the core of the residual blocks, is the strength of this type of neural network.
- The skip connections in ResNet solve the problem of vanishing gradient in deep neural networks by allowing this alternate shortcut path for the gradient to flow through.
- **Residual Block :** Resnets are made up of smaller sections called residual blocks. Each residual block consists of 2 or 3 layers of neural network where we have an incoming activation to the first residual block. This activation is taken by the first layer and is also passed on to the next layer or layer further down in the resnet.
- Fig. Q.39.1 shows residual block.

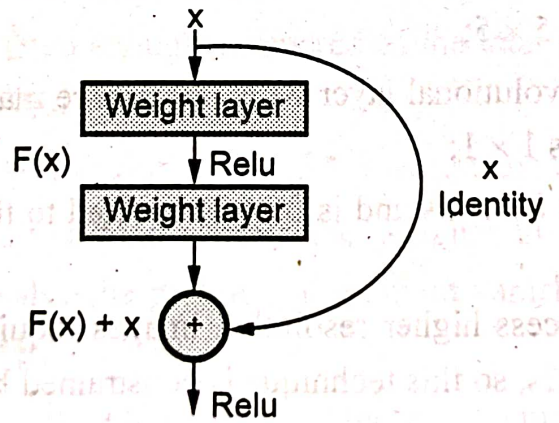


Fig. Q.39.1 Residual block

- In a residual network, each layer feeds to its next layer and directly to the 2-3 layers below it. The residual block consists of two 3 × 3 convolution layers and an identity mapping also called a shortcut connection. Each convolution layer is followed by a batch normalization layer and a ReLU

activation function. An element-wise addition is performed between the identity mapping with the output of the last batch normalization.

- It provides an alternative path for the better flow of gradients during the backpropagation. It helps the earlier layers to learn better, which helps to improve the performance of the network.
- The identity mapping learns an identity function that ensures that the residual block performs as good as the lower layer.
- The residual network uses a 34-layer plain network architecture inspired by VGG-19 in which then the shortcut connections are added and thus forming a residual network with 34-layers.

END...

Unit VI

6 Applications of ANN

6.1 : Applications of ANN in Symbol Recognition

Q.1 What is the central concept of pattern recognition ? How ANN plays role in pattern recognition ? ☞ [SPPU : 5 Marks]

Ans. : • Neural networks is a best choice for pattern classification due to its ability of a multilayer feedforward neural network to form complex decision regions in the pattern space for classification.

- Many pattern recognition problems, especially character or other symbol recognition and vowel recognition, have been implemented using a multilayer neural network. It should be well noted that multilayer neural networks are not directly applicable for situations where the patterns are deformed or modified due to transformations such as translation, rotation and scale change, although some of them may work well even with large additive uncorrelated noise in the data.
- When the data is directly presentable to the classification network, the direct applications are highly successful.
- When the data is clean and ready to input then it is easy to process for multilayer neural network. Limits of classification performance will be reached if the symbols are degraded due to 'deformations', in the case of Olympic symbols or if the input corresponds to casually 'handwritten'.
- Characters in the case of character recognition, or if the 'knowledge' of the bidding sequence and the 'reasoning' power of human players have to be used in the bridge bidding problem.

Q.2 Explain recognition of Olympic games symbols using ANN. ☞ [SPPU : 10 Marks]

Ans. : Recognition of Olympic games symbols :

The problem - Recognition of Olympic games symbols.

The data -

- All the symbols are represented as black and white pixels on a 128×128 points grid. Although the symbols appear complex in terms of detail, each symbol represents a rigid-object-like behaviour. This behaviour ensures that the relative pixel positions of a symbol do not change even under severe degradation, such as translation, rotation and scaling.
- From above 128×128 points images set, a 16×16 element array is reconstructed as shown below.

Pattern Classification Process

1. Here, Hamming network which performs template matching using neural principles is suitable for classification. The Hamming network is a maximum likelihood classifier for binary inputs and it performs correlation matching between the input and the stored templates.
2. It consists of two subnets as shown in below Fig. Q.2.1. The lower subnet consists of M(128×128) input units, each corresponding to a pixel in the given pattern and N output units corresponding to the N pattern classes, which in this case is 20.
3. In the lower subnet the connection weights between the input and output units are fixed in such a way that the network calculates the distance from the input pattern to each of the N stored pattern classes. The weights are given by below equation,

$$w_{ij} = \alpha_{ij}/2, \theta_i = M/2, 1 < j \leq M, i \leq I \leq N \quad \text{...(Q.2.1)}$$

where w_{ij} is the connection weight from the input unit j to the output unit i in the lower subnet, θ_i is the threshold for the ith output unit and a_{ij}, is the element j of the pattern for the ith symbol. The values of a_{ij} are – 1 or 1.

4. In the upper subnet, the weights are fixed in such a way that the output units inhibit each other. That is,

$$v_{kl} = 1, \quad \text{for } k = l$$
$$= -E, \text{ for } k \neq l \qquad \ldots(Q.2.2)$$

where v_{kl} is the connection weight between the units K and l in the upper net and E is a small positive number, say E = 0.1.

5. When a bipolar pattern is presented for classification, the lower subnet calculates its matching score (si) with the stored pattern for the ith class as shown below,

$$s_i = s_i(0) = f\left(\sum_j w_{ij} x_j - \theta_i\right) \qquad \ldots(Q.2.3)$$

where f (.) is the output function, x_j is the jth element of the input pattern and θ_i is the threshold value for the ith unit.

6. The output of the lower subnet is presented to the upper subnet, where a competitive interaction takes place among the units. The dynamics of the upper subnet is given by,

$$s_i(t+1) = f\left(s_i(t) - \varepsilon \sum_{k \neq i} s_k(t)\right), i = 1, 2, \ldots, N \qquad \ldots(Q.2.4)$$

7. The competition continues until the output of only one unit remains positive and the outputs of all other units become negative. The positive unit corresponds to the class of the input pattern.

8. For the set of degraded symbols given in Fig. Q.2.1, the correct classification performance is 100 % which is highly impressive, since it is difficult even for human to identify visually the discriminating features in many of these images. When the degradation is increased by reducing the resolution using an array of 8 × 8 elements, the recognition performance is only 13 out of 20.

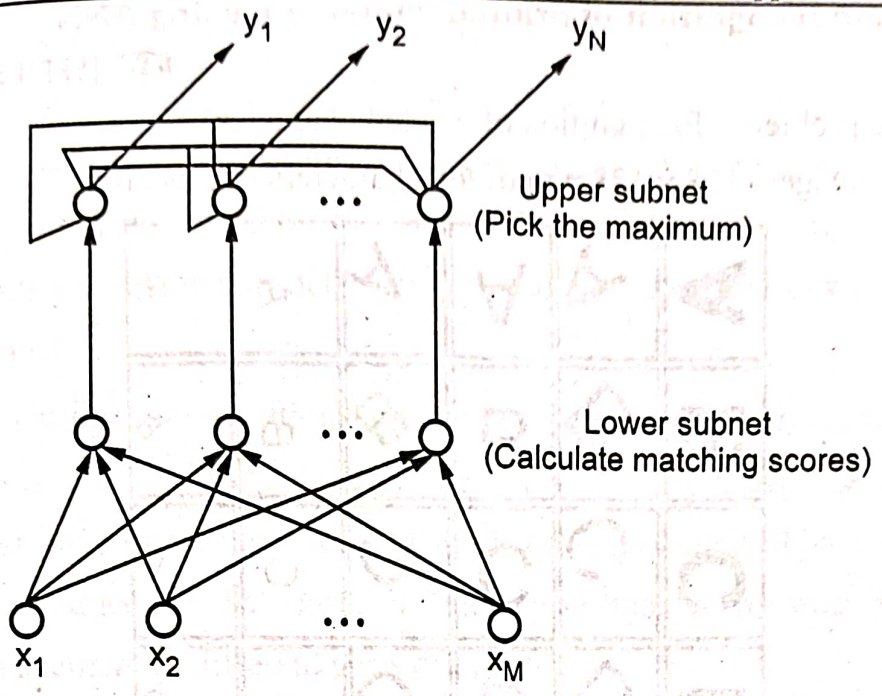


Fig. Q.2.1 The Hamming network. The input and output units are represented by x and y vectors, respectively.

9. **Avoiding effects of object transformations -**

(i) If the images are clean and noise-free, then there exist methods to overcome the effects of metric transformations of the objects. Several neural network models have been proposed for invariant pattern recognition.

(ii) The networks which achieve invariance by structure, the structure of the network is designed such that the output is invariant to the transformations of interest. In the case of invariance by training, representative samples of various transformations are presented during training so that the network learns equivalent transformations.

Invariance by structure or by training assumes the existence of a fixed set of weights which provide invariance over the continuum of transformations.

(iii) It also assumes that a network can be trained to estimate this set of weights from examples. But invariances cannot be built as static functions in the structure. They have to be dynamically estimated from the data. Alternatively, one can first address the transformation invariance by feature extraction and then use these features as input to a classifier.

Q.3 Explain recognition of printed characters using ANN.

☞ [SPPU : 8 Marks]

Ans. : The problem - Recognition of printed characters.

The data - images (128 × 128 pts) of ten characters of alphabet.

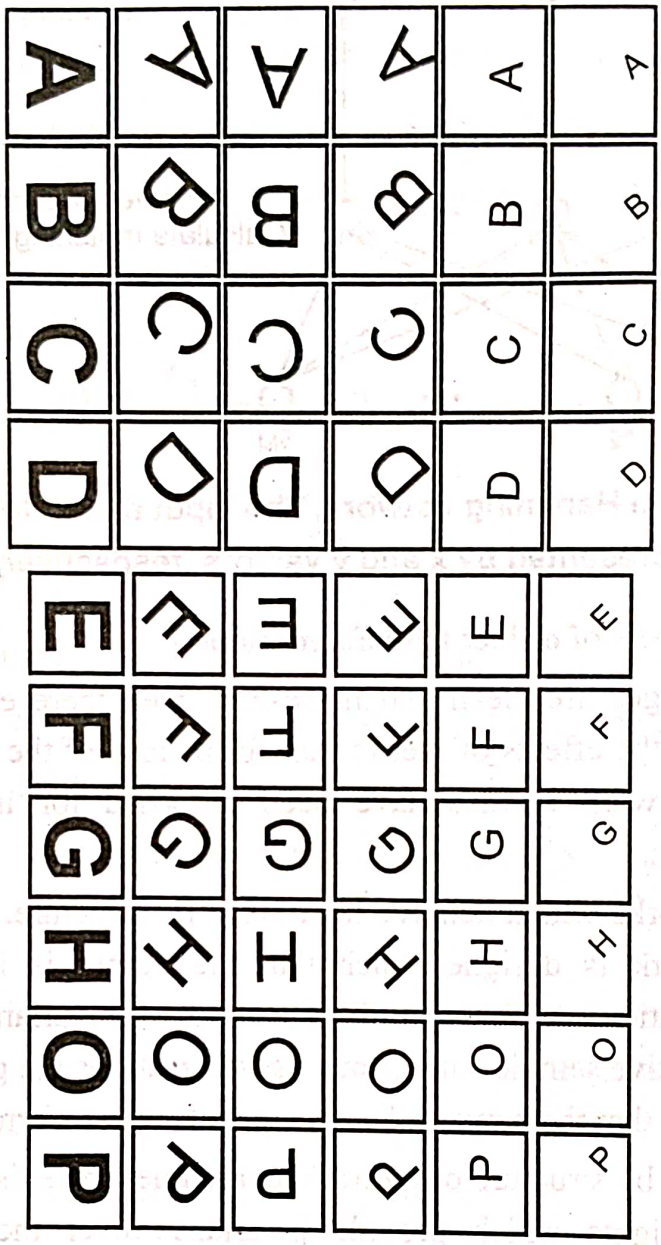


Fig. Q.3.1 Rotated, scaled and translated images of characters used for translation invariant recognition

Pattern recognition process

1. The ten characters and some transformed versions of these characters used in the current pattern recognition are shown in Fig. Q.3.1. In this case 100 % classification accuracies could be obtained for all the test data

upto a scale reduction of 1/12 of the linear dimension of the original, that is, the reduced image is about 10×10 points.

2. Here the feature approach gives better transformation invariant recognition than in the case of the Olympic games symbols, since the objects are simpler in detail in the case of the printed characters of the alphabet.
3. The pattern classifications can be accomplished using neural network models for objects whose images are severely degraded by transformations and noise. But in all these cases the objects considered are assumed to be rigid, in the sense that there was no relative displacement in different parts of the object.
4. It should be noted that the above illustrations differ from the handwritten characters in which different parts of a character are deformed differently in each sample.
5. Thus the classification methods based on correlation matching or training a feedforward network using moment features are not useful for problems such as recognition of handwritten characters.

Q.4 Explain Neocognitron application used for hand written character recognition. ☞ [SPPU : 8 Marks]

Ans. :

1. The neocognitron is a **hierarchical multilayered neural network** proposed by Professor Kunihiko Fukushima for **handwritten character recognition.**
2. There are various different versions of the neocognitron. Two original basic versions proposed by Professor Fukushima differ in used **learning** principle namely,
   - Learning without a teacher
   - Learning with a teacher.
3. The first version of the neocognitron was based on the **learning without a teacher.** This version is often called **self-organized** neocognitron.

4. The **main advantage** of neocognitron is its ability to recognize correctly not only learned patterns but also patterns which are produced from them by using of partial shift, rotation or another type of distortion.
5. **Feature extraction in neocognitron - Hierarchical feature extraction** is the basic principle of the neocognitron. Hierarchical feature extraction consists in **distribution of extracted features to several stages**. The simplest features (usually only rotated lines) are extracted in the first stage and in each of the following stages the more complex features are extracted. In this process it is important fact that only informations obtained in the previous stage are used for feature extraction in the certain stage.

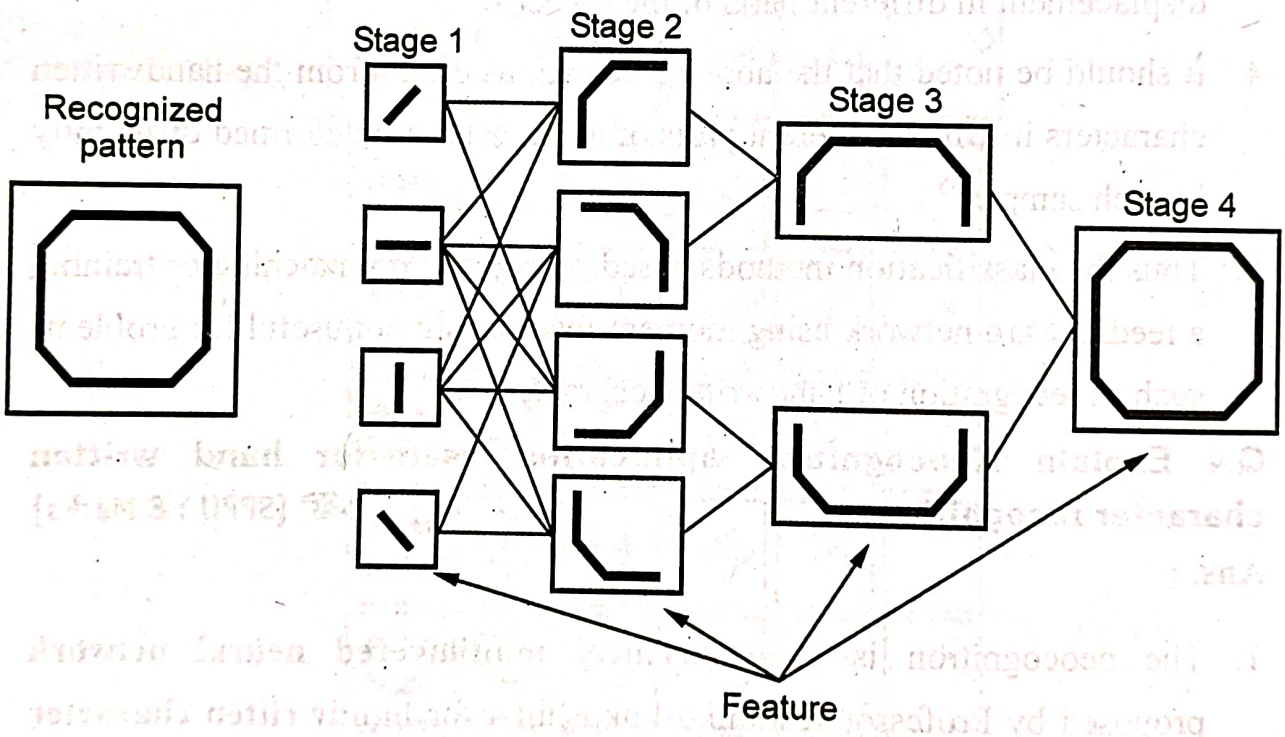


Fig. Q.4.1 Hierarchical feature extraction

6. Neocognitron architecture

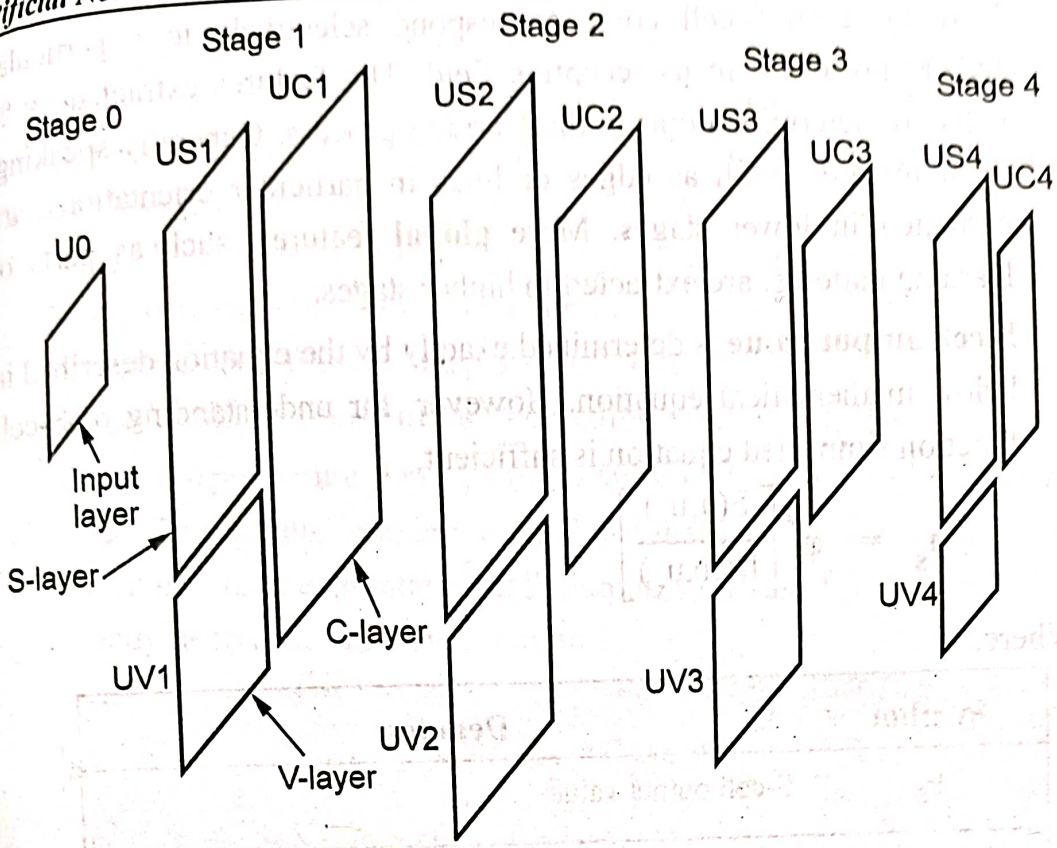


Fig. Q.4.2 Neocognitron network structure

Symbol	Denotes
U0	Input layer
USl	S-layer in the l-th stage of the network
UVl	V-layer in the l-th stage of the network
UCl	C-layer in the l-th stage of the network

i) A typical architecture of the network has the lowest stage which is the input layer consisting of two-dimensional array of cells, which correspond to photoreceptors of the retina. There are retinotopically ordered connections between cells of adjoining layers. Each cell receives input connections that lead from cells situated in a limited area on the preceding layer. Layers of "S-cells" and "C-cells" are arranged alternately in the hierarchical network. In the above figure the contrast-extracting layer is inserted between the input layer and the S-cell layer of the first stage.

ii) **S-cells** work as feature-extracting cells. They resemble simple cells of the primary visual cortex in their response. Their input connections are variable and are modified through learning. After having finished

learning, each S-cell come to respond selectively to a particular feature presented in its receptive field. The features extracted by S-cells are determined during the learning process. Generally speaking, local features, such as edges or lines in particular orientations, are extracted in lower stages. More **global** features, such as parts of learning patterns, are extracted in higher stages.

S-cell output value is determined exactly by the equation described in below mathematical equation. However, for understanding of S-cell function simplified equation is sufficient,

$$u_s = \varphi^* \left[\frac{E(a,u_c)}{I(r,b,u_v)} \right]$$

Where,

Symbol	Denotes
u_s	S-cell output value
φ^*	Non-linear function
E	Excitatory part
a	a-weights
u_c	Output values of C-cells from connection areas
I	Inhibitory part
r	Selectivity
b	b-weight
u_v	V-cell output value

The S-cells ability to extract not only learned features but also deformed representations of these features is influenced by the choice of parameter denoted as **selectivity** to a great extent.

iii) **C-cells**, which resembles complex cells in the visual cortex, are inserted in the network to allow for positional errors in the features of the stimulus. The input connections of C-cells, which come from S-cells of the preceding layer, are fixed and invariable. Each C-cell receives excitatory input connections from a group of S-cells that

extract the same feature, but from slightly different positions. The C-cell responds if at least one of these S-cells yield an output. Even if the stimulus feature shifts in position and another S-cell comes to respond instead of the first one, the same C-cell keeps responding. Thus, the C-cell's response is less sensitive to shift in position of the input pattern. One can also express that C-cells make a blurring operation, because the response of a layer of S-cells is spatially blurred in the response of the succeeding layer of C-cells.

C-cell output value depends on activity of **S-cells** from **connection area**. The greater number of active S-cells is or the greater their activities are the greater C-cell output value is. C-cell function is exactly described in below equation.

$$u_{cl}(n, k) = \Psi\left[\sum_{k=1}^{k_{Sl}} J_l(K, k) \cdot \sum_{v \in Dl} d_l(v) \cdot u_{Sl}(n + v, K)\right]$$

l	Serial number of the stage
n	**Cell** position
k	Serial number of the cell plane
K_{Sl}	Number of cell planes in the previous **S-layer**
J_l	Connection factor
v	Position in the **connection area**
D_t	Connection area of the **C-cell**
d_t	d-weights (> = 0)

$$\Psi[x] = \frac{\varphi[x]}{1 + \varphi[x]}$$

$$\varphi[x] = \begin{cases} x \\ 0 \end{cases}$$

For C-cell to be active it is sufficient that at least one active S-cell is present in its connection area. With regard to overlapping of neighbouring C-cell connection areas activity of one S-cell affects activity of greater number of C-cells. In consequence of that C-plane contains a **blurred** representation of S-plane content. This is obvious from Fig. Q.4.2 as well where one active S-cell and all C-cells influenced by it are marked.

Ability of C-cell to **compress** content of connection area in the certain

way is the next consequence of C-cell function. Hence one can decrease the density of cells in C-layer to the half of density of cells in previous S-layer in some cases.

iv) Each layer of S-cells or C-cells is divided into sub-layers, called **"cell-planes"**, according to the features to which the cells responds. The cells in each cell-plane are arranged in a two-dimensional array. A cell-plane is a group of cells that are arranged retinotopically and share the same set of input connections. That is the connections to a cell-plane have a translational symmetry. As a result, all the cells in a cell-plane have receptive fields of an identical characteristic, but the locations of the receptive fields differ from cell to cell. The modification of variable connections during the learning progresses also under the restriction of shared connections.

v) V-cell function - Each **V-cell** in the neocognitron **evaluates outputs of C-cells** (or receptor cells) from the certain connection areas from previous C-layer (or input layer). **Size of connection areas** is the same for all V-cells and S-cells in one stage of the network and it is determined at construction of the network. **V-cell output value** represents average activity of cells from connection areas and it is used for inhibition of corresponding S-cell activity. Exact specification of V-cell function is described in mathematical description of its behaviour.

7. Weights and connections

i) The neocognitron is characteristic not only by large number of **cells** but also by large number of **connections**. These connections serve for **transfer of information** between cells in adjoining layers. Particular cell obtains by means of connections information from all cells which are located in its connection areas.

For each connection there is a **weight** by means of it one can affect amount of transferred information. If a connection is thought of as a pipeline with a valve it can be compare with weight assigned to the connection to a degree of opening of this valve.

ii) **Four types of weights** (a-weights, b-weights, c-weights and d-weights) exist in the neocognitron. Each of these types of weights is used for connections between two layers of different types. It is shown schematically.

iii) **Weight sharing** is the next term being connected with weights. By this term one can designate the fact that all cells in one cell plane use the same weights for connections leading from cells in their connection areas. By the means of weight sharing it is guaranteed that all cells from one cell plane always extract the same feature.

One can split the weights according to the way which they are adjusted,

- Weights modified by learning
  - **a-weights**
  - **b-weights**
- Fixed weights
  - **c-weights**
  - **d-weights**

a-weights

The a-weights are the first type of weights **modified by learning**. These weights are used for connections **between S-cells and C-cells** which belong to their **connection areas. Features** extracted by S-cells are encoded in these a-weights. Adjusting of a-weights is performed during **learning** of the network according to the presented **training patterns.**

b-weights

- The b-weights are the second type of weights **modified by learning**. These weights are used for connections between **S-cells and corresponding V-cells.** Adjusting of b-weights is performed during **learning** of the network according to the presented **training patterns** as well.

c-weights

- **Fixed** c-weights are used for connections **between V - cells and C - cells** which belong to their **connection areas.** Values of c-weights are determined at construction of the network. These weights are most often set up in such a way that they mostly reduce transfer of information from the periphery of connection area and towards to the center of area the degree of reduction decreases.

d-weights

- **Fixed** d-weights are used for connections **between C - cells and S - cells** which belong to their **connection areas.**
- As well as c-weights also d-weights are determined at construction of the network and again in such a way so as to reduce transfer of information from periphery of connection areas mostly.

8. Learning in neocognitron - Learning in this version of the network is controlled by a **teacher**. His task is to determine what features shall be extracted in particular stages of the network and to prepare corresponding training patterns before beginning of learning.

   Learning of the neocognitron proceeds stage by stage from the lowest stage of the network and it inheres in **adjusting of modifiable weights** (i.e. a-weights and b-weights) according to the response of already learned parts of the network to presented training patterns. For each S-plane in the network one training pattern is usually used and this pattern is usually necessary to present to the network only once.

   On the beginning of learning teacher have to set all **a-weights** and **b-weights** in the network to zero. Then he selects S-plane from layer US1 and in this cell plane he selects one of cells, so-called **seed cell.** Presentation of training pattern given for this S-plane into the **input layer** U0 is the next step. Finally teacher adjusts weights of the seed cell according to the equations mentioned in mathematical description of learning as shown below.

$$\Delta a_l(v,K,\hat{k}) = q_l \cdot c_l(v) \cdot u_{cl-1}(\hat{n}+v,K)$$

$$\Delta a_l(\hat{k}) = q_l : u_{vl}(\hat{n})$$

l	Serial number of the stage
a_l	a-weights (>=0)
b_l	b-weights (>=0)
c_l	c-weights (>=0)
q_l	Learning coefficient (>>0)

$\hat{n}$ **Seed cell** position

$\hat{k}$ Serial number of the cell plane with seed cell

Since **weight sharing** is used in the neocognitron adjusting of weights of all the other S-cells in the cell plane occurs simultaneously. If more training patterns for the selected S-plane exist then they are presented subsequently and process repeats. In opposite case it is moved to learning of the next S-plane.

9. **Recall** in the neocognitron inheres in evaluation of output values of all **cells** stage by stage. The result of this process is a decision to which of **learned** categories presented pattern belongs.

   The process of recall begins with presentation of pattern intended for recognition to the **input layer** U0. Then output values of **V-cells** in the layer UV1 are evaluated. **S-cells** from the layer US1 can **extract** the simplest **features** and **C-cells** from layer UC1 ensure decreasing of effect of extracted **features** shifts. The whole process repeats analogically for all the following layers of the network. After completion of recall output values of C-cells from the highest layer of the network correspond to measures of belonging presented pattern to categories which the particular C-cells represent.

10. Types of neocognitron - Various modifications of the neocognitron have been proposed to improve the recognition rate or to make biologically more natural. If backward (i.e., top-down) connections are added to the conventional neocognitron, for example, the network come to have an ability to recognize occluded patterns correctly and can restore the occluded parts of the patterns. Even if many patterns are presented simultaneously, it focuses **attention** to individual patterns one by one and recognizes them correctly.

6.2 : Applications of ANN in Speech Recognition

Q.5 How ANN can be used for English text conversion to speech application?

OR Write a note on NETTalk application. ☞ **[SPPU : 10 Marks]**

Ans. :

1. Speech Signal - Speech signal is the output of a time - varying vocal tract system excited by a time-varying excitation signal. The vocal tract system, including the coupling of the nasal tract, can be accurately described in terms of the positions of the articulators such as tongue, lips, jaw, velum, etc.
2. Usually, the vocal tract system is approximately described in terms of the acoustic features such as the frequency response or the resonances (formants) and anti - resonances (anti-formants) of the system. These features are easier to extract from the signal than the articulatory parameters.
3. The excitation of the vocal tract system consists of broadly three categories,

   i) Voiced source (the quasiperiodic excitation due to the vibrating vocal folds).

   ii) Unvoiced source (the turbulent flow of air at a narrow constriction created in the vocal tract during production)

   iii) Plosive source (the abrupt release of the pressure built up behind a closure in the vocal tract system). The voiced source is characterized by the periodicity (pitch period) and the change of the pitch period with time (intonation).
4. The short -time characteristics of the speech signal are represented by the short- time (10-20 ms) spectral features of the vocal tract system as well as the nature of excitation in the short-time segment. These are called **segmental features**. Supra- segmental features of speech are represented by the variation of the pitch period (intonation), the durations of different sound units, and the coarticulation reflecting the dependence of

characteristics of one sound unit on the neighbouring sound units during speech production.

5. Speech is a sequence of sound units corresponding to a linguistic message. Below are important applications in speech area,
   a) **Speech recognition** - The objective is to determine the sequence of sound units from the speech signal so that the linguistic message in the form of text can be decoded from the speech signal.
   b) **Speech synthesis** - The objective is to determine the sequence of sound units corresponding to a text so that the given text message can be encoded into a speech signal.
   c) **Speaker identification** - The objective is to determine the identity of the speaker from the speech signal.
6. Problems in speech recognition problems -
   i) The main challenge and problem in the speech applications is processing of the speech signal in a manner similar to human auditory processing mechanism, so that features relevant to a particular task can be extracted.
   ii) The speech problem is further complicated by the fact that the message is conveyed not only through the segmental features but also by the suprasegmental features. It is the lack of understanding of these segmental and suprasegmental features and their extraction mechanism that makes the speech tasks extremely difficult for implementation by machines.
7. The NETtalk working
   i) It is a multilayer feedforward neural network (Fig. Q.5.1) developed to generate pronunciation units or phoneme code from an input text. The phoneme code is presented as input to a speech synthesizer to produce speech corresponding to the text.
   ii) The network consists of an input layer of 7 * 29 binary units, corresponding to 7 input text characters including punctuation, one hidden layer with 80 units and one output layer with 26 units corresponding to 26 different phonetic units.

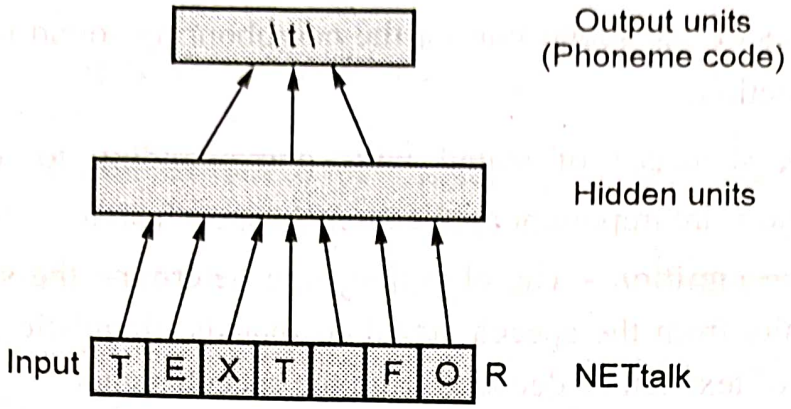


Fig. Q.5.1 NETtalk - feedforward network to convert English text to speech

iii) The network takes as input 7 consecutive characters at a time and produces the phoneme corresponding to the pronunciation of the letter at the centre of the input string. Each character of the input is represented as a 29-bit string. The network was trained on 1024 words from a set of English phoneme exemplars giving the pronunciation of words, m d was tested using different text sentences. The system produces a string of phonemes for a given input text. The speech produced by a synthesizer using these strings of phonemes as input was intelligible, although the quality was poor.

iv) The network was capable of distinguishing between vowels and consonants. On a new text the network achieved a generalization accuracy of 78 % in phonetic transcription. The system merely demonstrated the ability of a neural network to capture the letter to sound rules from input-output data. The quality will be obviously poor, as it cannot capture the significant supresegmental features which are essential for producing natural sounding synthetic speech.

Q.6 Brief on vowel and consonants segment recognition, texture classification.

OR How ANN is used in recognition of consonants, vowels, texture classification and segmentation ? ☞ **[SPPU : 8 Marks]**

Ans. :

1. Consonant-Vowel (CV) utterance typically forms a production unit (syllable) in speech and hence several attempts have been reported for recognition of CV utterances. Since these are dynamic sounds, the spectral patterns change with time. Each utterance of a CV unit is

represented as a temporal sequence of spectral vectors. Each spectral vector corresponding to a fixed 10 ms segment may be represented using 16 log spectral coefficients on a mel-frequency scale or using the corresponding mel-scale cepstral coefficients.

2. The number of spectral vectors per CV utterance generally varies. But usually a fixed duration (50-200 ma) segment of CV enclosing the vowel onset, the transition to vowel and some steady part of the vowel, is used to represent a CV unit. The CV units are thus temporal sequence patterns and hence static pattern recognition networks like Multilayer Feedforward Neural Network (MLFFNN) are not suitable for recognition of these units.

3. Moreover, discriminability among these CV units is low due to domination of the vowel context. Straight forward method to perform sequence recognition is to view the temporal sequence of the spectral vectors as a two-dimensional spatial input pattern for a MLFTNN. The conventional backpropagation learning can then be used to train the network. A better approach for CV recognition is through Time Delay Neural Networks (TDNN). TDNN is a MLFFNN with its input consisting of time-delayed input frames of data. The input to the intermediate hidden layers also consists of time-delayed outputs of the preceding layer. Below figure illustrates the idea of a time-delay,

(See Fig. Q.6.1 on next page)

In the Fig. Q.6.1 the neural network is applied for classification of three CV units lbl, Id and Igl. The time sequence is reflected in, the computation of block of three frames of data at a time, with two frames overlapping for successive blocks. The Fig. Q.6.1 shows multiple copies of the TDNN aligned with adjacent input spectral vectors. The first TDNN is shown in the boxes marked by thick lines. In this case each utterance has 15 frames of data, each frame consisting of 16 spectral components. For this, 13 different copies of TDNN are created. These include 13 copies of the input layer, nine copies of the first hidden layer,

and only one second hidden layer and one output layer. The output layer has three units corresponding to the three classes Ibl, ldl, and Igl. For each TDNN, each unit in a layer is connected to all the units in the layer below it. For each TDNN there are 16 × 3 units in the input layer, 8 × 5 units in the first hidden layer and 9 × 3 units in the second hidden layer and 3 units in the output layer. Multiple copies of the TDNN as shown in the Fig. Q.6.1 enable the entire history of the network activity to be present at the same time. This allows the use of the backpropagation learning algorithm to train the network.

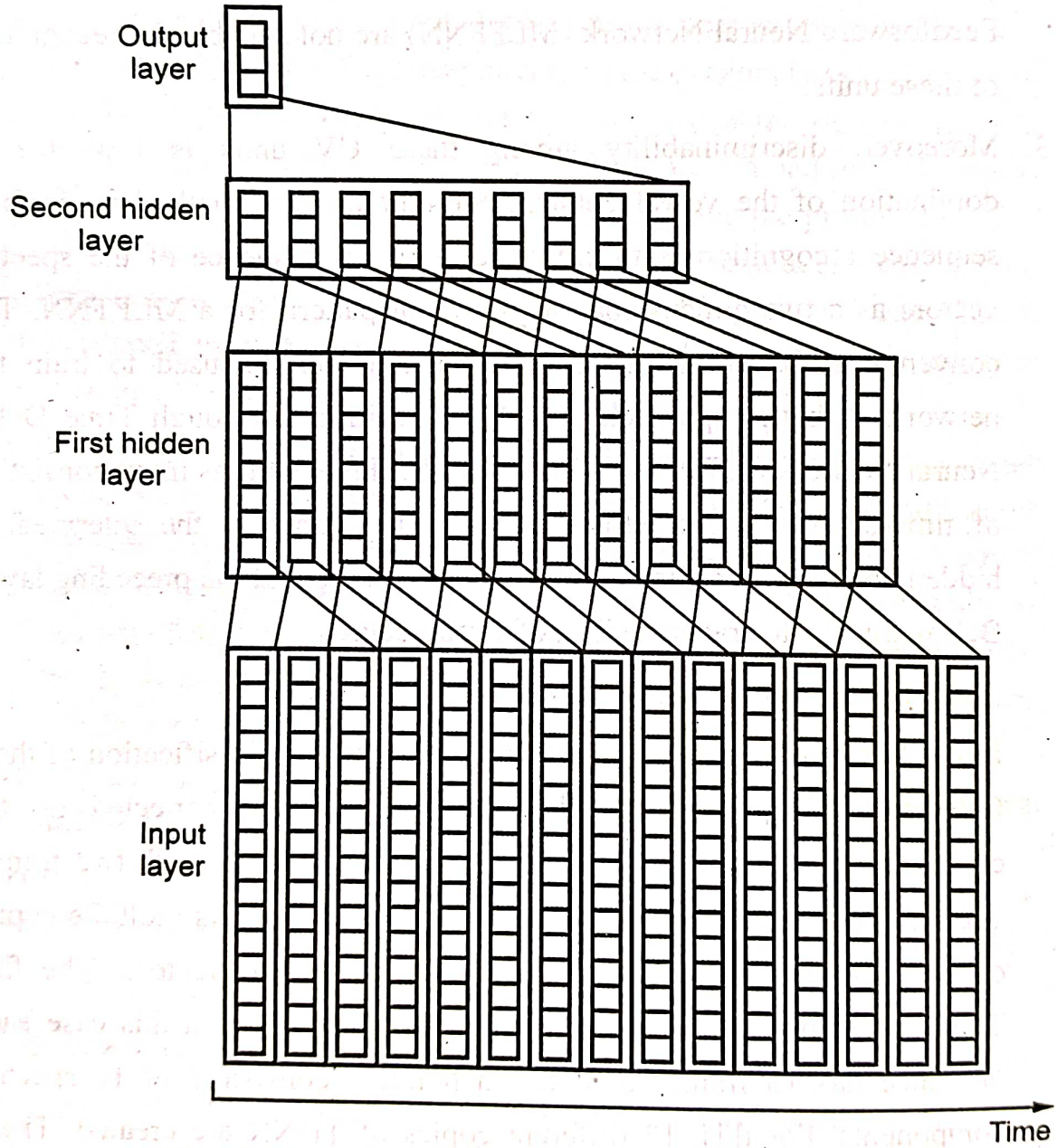


Fig. Q.6.1 Time delay neural network architecture

4. The 16 log spectral coefficients for each 10 ms frame are normalized using the average of each coefficient for an the 15 frames in the utterance and the coefficients are mapped into the range [– 1, 1]. The normalized values are given as input to the TDNN network. The speech data for the three classes was excised from continuous speech in Japanese and a database of about 800 CV units was collected for a given speaker. The TDNN was able to discriminate the three classes with an accuracy of 98.5 %. Considering the fact that the data for each class has significant variation due to contextual effects, this result is impressive. Extending this network model for large number of CV classes requires modular approach, where it is necessary to distinguish the groups of CV classes first before the individual classes can be identified. Additionally, because of the large size of the network, the training of the network will be slow. It will also be difficult to collect sufficient data to obtain good generalization performance from such a type of large networks.

END...