

第 1 章

CHAPTER 1

神经网络应用广泛的原因

神经网络是一门重要的机器学习技术，它是一种能够模拟人脑的神经网络，实现类人工智能的机器，是目前最为火热的研究方向。

1.1 人工神经网络的定义

人工神经网络（Artificial Neural Networks, ANNs）也简称为神经网络（NNs）或连接模型（connection model），它是一种模仿动物神经网络行为特征，进行分布式并行信息处理的算法数学模型。这种网络通过调整内部大量节点之间相互连接的关系，达到处理信息的目的。

1.1.1 神经网络基本概述

ANNs 是一种应用类似于大脑神经突触连接的结构进行信息处理的数学模型。神经网络是一种运算模型，由大量的节点（或称神经元）和节点之间的连接构成。每个节点代表一种特定的输出方，称为激励函数（activation function）。每两个节点间的连接都代表一个对于该连接信号的加权值，称为权重，这相当于神经网络的记忆。

ANNs 通常通过一个基于数学统计学的学习方法（learning method）得以优化，所以 ANNs 也是数学统计学的一种实际应用。另外，人工智能学的人工感知器通过数学统计学的应用可以解决人工感知方面的决定问题，这比正式的逻辑学推理演算更具有优势。

1.1.2 人工神经元的基本特征

人工神经网络是由大量处理单元互联组成的非线性、自适应信息处理系统，它具有以下 4 个基本特征。

（1）非线性。

非线性关系是自然界的普遍特性。大脑的智慧就是一种非线性现象。人工神经元处于激活或抑制两种不同的状态，具有阈值的神经元构成的网络具有更好的性能，可以提高容错性和存储容量。

（2）非局限性。

一个神经网络通常由多个神经元广泛连接而成。一个系统的整体行为不仅取决于单个

神经元的特征，而且可能主要由单元之间的相互作用、相互连接所决定。

(3) 非常定性。

神经网络可以处理的有各种变化的信息，而且在处理信息的同时，其本身也在不断变化。人工神经网络具有自适应、自组织、自学习能力。

(4) 非凸性。

一个系统的演化方向在一定条件下取决于某个特定的状态函数。在人工神经网络中，神经元处理可表示不同的对象，是一种非程序化、适应性、大脑风格的信息处理，其本质是通过网络的变换和动力学行为得到一种并行分布式的信息处理功能，并在不同程度和层次上模仿人脑神经系统的信息处理功能。

人工神经网络是并行分布式系统，采用了与传统人工智能和信息处理技术完全不同的机理，克服了传统的基于逻辑符号的人工智能在处理直觉、非结构化信息方面的缺陷，具有自适应、自组织和实时学习的特点。

1.1.3 人工神经元的特点与优越性

人工神经网络的结构如图 1-1 所示。

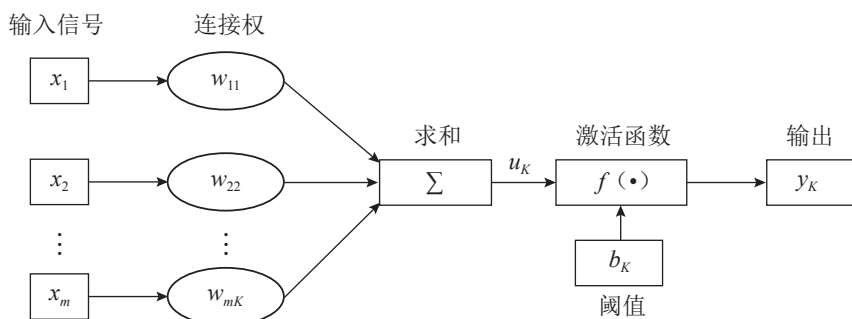


图 1-1 人工神经网络的结构

人工神经网络的特点和优越性主要表现在以下几方面。

(1) 具有自学习功能。例如，进行图像识别时，只要先把许多不同的图像样板和对应的识别结果输入人工神经网络，网络就会通过自学习功能，慢慢学会识别类似的图像。自学习功能对于预测有特别重要的意义，未来的人工神经网络计算机将可以为人类提供经济预测、市场预测、效益预测，其应用前景远大。

(2) 具有联想存储功能。用人工神经网络的反馈网络就可以实现这种联想。

(3) 具有高速寻找优化解的能力。寻找一个复杂问题的优化解往往需要很大的计算量，利用一个针对某问题而设计的反馈型人工神经网络，发挥计算机的高速运算能力，可能很快找到优化解。

1.2 人工神经网络的类型

神经网络中神经元的连接方式与用于训练网络的学习算法是紧密结合的，可以认为应用于神经网络设计中的学习算法是被结构化了的。可以从以下不同角度对人工神经网络进

行分类。

(1) 从网络性能角度可分为连续型网络和离散型网络，以及确定性网络和随机性网络。

(2) 从网络结构角度可分为前向网络和反馈网络。

(3) 从学习方式角度可分为有导师学习网络和无导师学习网络。

(4) 从连续突触性质角度可分为一阶线性关联网络和高阶非线性关联网络。

本书将网络结构和学习算法相结合，对人工神经网络进行分类。

1.2.1 单层前向网络

单层前向网络是指拥有的计算节点（神经元）是单层的，如图 1-2 所示。这里把表示源节点个数的输入层看作一层神经元，因为该输入层不具有执行计算的功能。

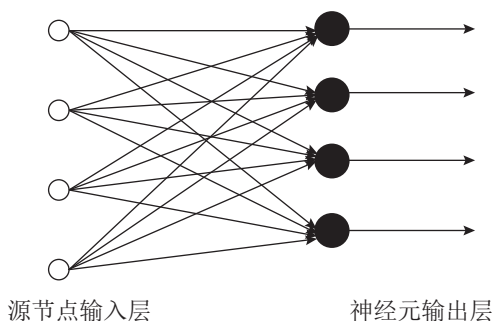


图 1-2 单层前向网络

1.2.2 多层前向网络

多层前向网络与单层前向网络的区别在于：多层前向网络含有一个或更多的隐含层，其中计算节点被相应地称为隐含神经元或隐含单元，如图 1-3 所示。

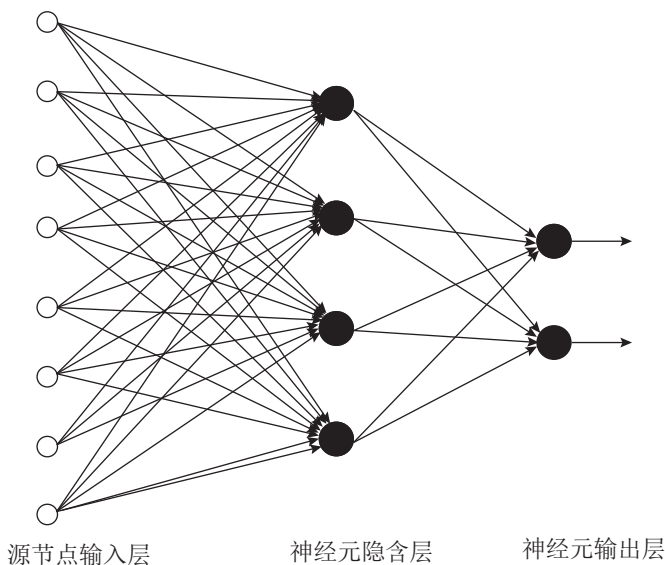


图 1-3 多层前向网络

图 1-3 所示的多层前向网络由含有 8 个神经元的输入层、含有 4 个神经元的隐含层和含有 2 个神经元的输出层组成。

网络输入层中的每个源节点的激励模式（输入向量）单元组成了应用于第二层（如第一隐含层）神经元（计算节点）的输入信号，第二层的输出信号成为第三层的输入信号，其余层类似。网络每一层的神经元只含有作为它们输入前一层的输出信号，网络输入层（终止层）神经元的输出信号组成了对网络中输入层（起始层）源节点产生的激励模式的全部响应。即信号从输入层输入，经隐含层传给输出层，由输出层得到输出信号。

通过加入一个或更多的隐含层，网络能提取出更高维的统计，尤其当输入层规模庞大时，隐神经元提高高维统计数据的能力便显得格外重要。

1.2.3 反馈网络

反馈网络是指在网络中至少含有一个反馈回路的神经网络。反馈网络可以包含一个单层神经元，其中每个神经元都将自身的输出信号反馈给其他所有神经元的输入，如图 1-4 所示，图 1-4 中所示的网络即为著名的 Hopfield 网络。

图 1-5 所示是另一种类型的含有隐含层的反馈网络，图中的反馈连接起始于隐神经元和输出神经元。图 1-4 和图 1-5 所示的网络结构中没有自反馈回路。自反馈回路是指一个神经元的输出反馈至其输入，含有自反馈的网络也属于反馈网络。

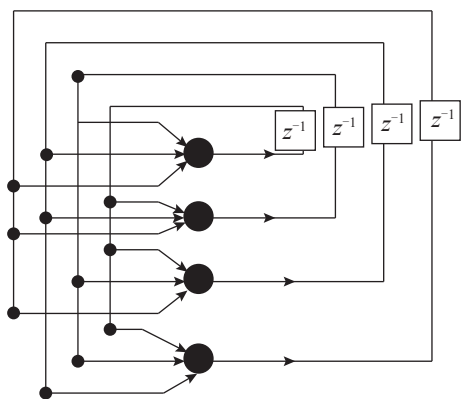


图 1-4 无自反馈回路和隐含层的反馈网络

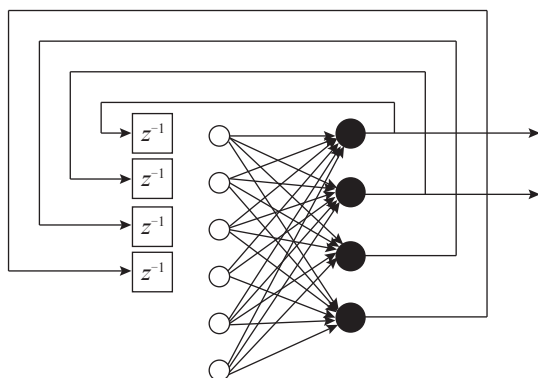


图 1-5 含有隐含层的反馈网络

1.2.4 竞争型神经网络

竞争型神经网络的显著特点是它的输出神经元相互竞争以确定胜者，胜者指出哪一种原形模式最能代表输入模式。

Hamming 网络是一个最简单的竞争型神经网络，如图 1-6 所示。神经网络有一个单层的输出神经元，每个输出神经元都与输入节点全相连，输出神经元之间全互联。从源节点到神经元之间是兴奋性连接，输出神经元之间横向侧抑制。

1.2.5 深度神经网络

深度神经网络是一个由多个层组成的递归函数，如图 1-7 所示。网络中每一层由多个

神经元组成，每个神经元都接收前一层所有神经元的输出，根据输入数据对输出进行计算并传递给下一层神经网络，最终完成预测或分类任务。

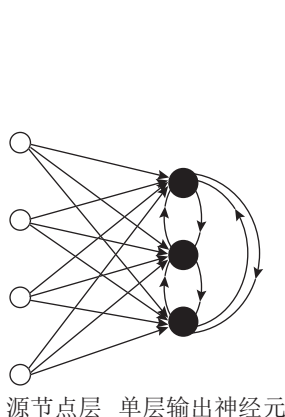


图 1-6 最简单的竞争型神经网络

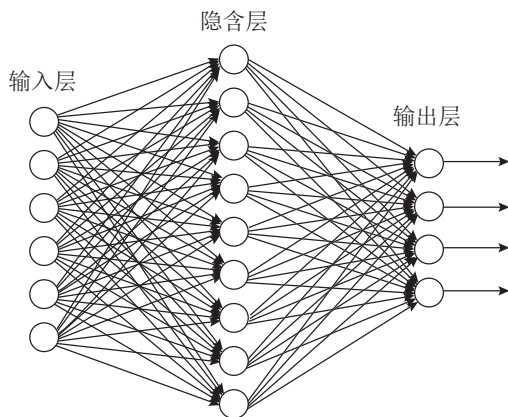


图 1-7 深度神经网络

1.3 人工神经网络的应用

在网络模型与算法研究的基础上，利用人工神经网络可以组成实际的应用系统，例如，完成某种信号处理或模式识别的功能、构建专家系统、制成机器人、进行复杂系统控制等。

纵观当代新兴科学技术的发展史，人类在征服宇宙空间、基本粒子、生命声源等科学技术领域的进程中历经了崎岖不平的道路。探索人脑功能和神经网络的研究也是伴随着重重困难的克服而日新月异。

神经网络的研究内容相当广泛，是多学科交叉的技术领域，其主要研究工作集中在以下几方面。

1. 生物原型

从生理学、心理学、解剖学、脑科学、病理学等方面研究神经细胞、神经网络、神经系统的生物原型结构及其功能机理。

2. 建立模型

根据生物原型的研究，建立神经元、神经网络的理论模型，其中包括概念模型、知识模型、物理化学模型、数学模型等。

3. 算法

在理论模型研究的基础上构建具体的神经网络模型，以实现计算机模拟或准备制作硬件，包括网络学习算法的研究。这方面的工作也称为技术模型研究。

神经网络用到的算法就是向量乘法，并且广泛采用符号函数及其各种逼近。并行、容错、可以硬件实现以及自我学习，是神经网络的几个基本优点，也是神经网络计算方法与传统方法的区别所在。

1.4 神经网络的发展史

神经网络的发展起伏不平，经历了以下几个历程。

1.4.1 模型提出

1. 第一个神经元模型

1943年，麦卡洛克（McCulloch）和皮茨（Pitts）为单个神经元建立了第一个数学模型，称为MP模型，从而开创了研究人工神经网络的时代。

2. 感知机模型

1958年，罗森·布拉特正式把算法取名为Perceptron（感知机），感知机是二类分类的线性分类模型，其输入为实例的特征向量，输出为实例的类别。

假设输入空间（特征空间）是 $X \subseteq \mathbf{R}^n$ ，输出空间是 $y = \{+1, -1\}$ 。输入 $x \in X$ 表示实例的特征向量，对应输入空间（特征空间）的点；输出 $y \in Y$ 表示实例的类别。由输入空间到输出空间的函数

$$f(x) = \text{sign}(w \cdot x + b)$$

称为感知机。其中 w 和 b 为感知机模型参数， $w \in \mathbf{R}^n$ 叫作权值或权值向量， $b \in \mathbf{R}$ 叫作偏置， $w \cdot x$ 表示 w 和 x 的内积。 sign 为符号函数，即

$$\text{sign}(x) = \begin{cases} +1, & x \geq 0 \\ -1, & x < 0 \end{cases}$$

1.4.2 冰河期

1. XOR 异或问题

马文·明斯基在1969年指出了神经网络的两个缺陷：第一，感知器无法处理异或问题；第二，当时的计算机不具备大型神经网络所需要的算力。

2. BP 反向传播

反向传播（Back Propagation，BP）是“误差反向传播”的简称，是一种与最优方法（如梯度下降法）结合使用的、用来训练人工神经网络的常见方法。BP算法对网络中所有权重计算损失函数的梯度，这个梯度会反馈给最优化方法，用来更新权值以最小化损失函数。BP算法会先按前向传播方式计算（并缓存）每个节点的输出值，然后按反向传播遍历图的方式计算损失函数值相对于每个参数的偏导数。

3. 新识别机的提出

福岛邦彦（Fukushima）于1979年提出了神经认知机（Neocognitron，新识别机）模型，这是一个使用无监督学习训练的神经网络模型，也是卷积神经网络的雏形。

1.4.3 反向传播引起的复兴

1. Hopfield 网络

约翰·霍普菲尔德于1982年发明了一种递归神经网络——Hopfield神经网络。Hopfield网络是一种结合存储系统和二元系统的神经网络。它保证了向局部极小值的收敛，但收敛到错误的局部极小值而非全局极小值的情况也可能发生。Hopfield网络也提供了模拟人类记忆的模式。

2. 玻尔兹曼机

玻尔兹曼机（Boltzmann machine）是一种随机神经网络和递归神经网络，于1985年

由杰弗里·辛顿（Geoffrey Hinton）和特里·谢泽诺斯基（Terry Sejnowski）发明。

玻尔兹曼机可被视作随机过程，可生成相应的 Hopfield 神经网络。它是最早能够学习内部表达，并能表达和解决复杂的组合优化问题的神经网络。但目前并没有证据证明没有特定限制连接方式的玻尔兹曼机对机器学习的实际问题起作用，所以它目前只有理论意义。然而，由于局部性和训练算法的赫布性质，以及它们和简单物理过程相似的并行性，如果连接方式是受约束的（即约束玻尔兹曼机），那么它在解决实际问题时将会足够高效。

3. RNN (1986 年)

循环神经网络（Recurrent Neural Network, RNN）是一类以序列（sequence）数据为输入，在序列的演进方向进行递归，且所有节点（循环单元）按链式连接的递归神经网络（Recursive Neural Network）。

4. LeNet (1990 年)

LeNet 是一个 7 层的神经网络，包含 3 个输入层、2 个池化层、2 个全连接层。其中所有卷积层的所有卷积核都为 5×5 ，步长 $\text{strid}=1$ ，池化方法都为全局 pooling，激活函数为 Sigmoid，其网络结构如图 1-8 所示。

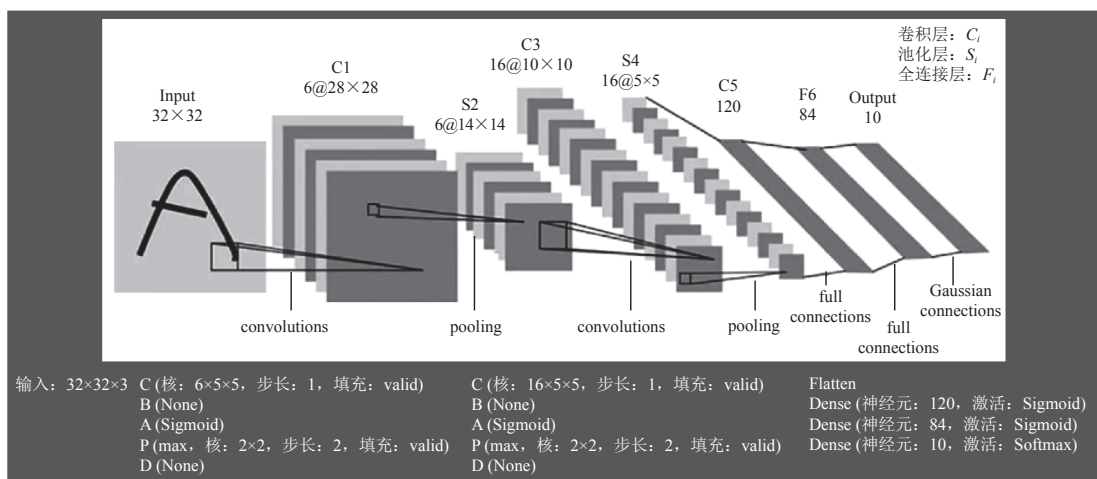


图 1-8 LeNet 网络结构

1.4.4 第二次低潮

这一阶段，机器学习的一些策略的流行度超过了深度学习，如 1997 年的 LSTM、双向 RNN。

1.4.5 深度学习的崛起

1. DBN 深度置信网络

深度置信网络是深度学习方法中的一种神经网络模型，如图 1-9 所示。该模型以限制玻尔兹曼机为基础，运用多 RBM 的方式实现概率生成，其概率生成方式主要是构造联合分布函数，函数用于针对输入数据与样本之间的标签。

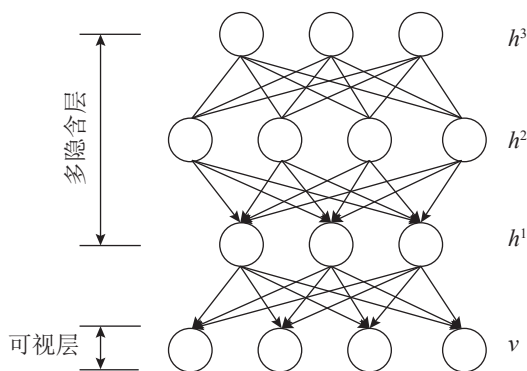


图 1-9 深度置信网络结构

2. ImageNet

ImageNet 是一个用于视觉对象识别软件研究的大型可视化数据库。超过 1400 万幅图像 URL 被 ImageNet 手动注释，以指示图像中的对象；其在至少 100 万幅图像中提供了边界框。ImageNet 包含 2 万多个类别，一个典型的类别，如“气球”或“草莓”，包含数百幅图像。第三方图像 URL 的注释数据库可以直接从 ImageNet 免费获得，但实际的图像不属于 ImageNet。2012 年，研究人员在解决 ImageNet 问题方面获得了巨大的突破，被广泛认为是“深度学习革命”的开始。

3. AlexNet

AlexNet 是于 2012 年设计的，同年更多更深的神经网络被提出，如优秀的 VGGNet、GoogLeNet。它们相对于传统的机器学习分类算法而言，已经相当地出色。

AlexNet 有以下亮点。

- （1）首次利用 GPU 进行网络加速训练。
- （2）使用了 ReLU 激活函数，而不是传统的 Sigmoid 激活函数或 Tanh 激活函数。
- （3）使用了 LRN 局部响应归一化。
- （4）在全连接层的前两层中使用了 Dropout 随机失活神经元操作，减少了过拟合。

4. VGGNet、GoogLeNet

牛津大学计算机视觉组和 Google DeepMind 公司一起研发了新的卷积神经网络——VGGNet，它是比 AlexNet 更深的深度卷积神经网络。

GoogLeNet 是 2014 年提出的一种全新的深度学习结构，之前的 AlexNet、VGGNet 等结构都是通过增大网络的深度（层数）来获得更好的训练效果，但层数的增加会带来很多负面的作用，如过拟合、梯度消失、梯度爆炸等。

5. 残差网络

残差网络是由来自 Microsoft Research 的 4 位学者提出的卷积神经网络，它的特点是容易优化，并且能通过增加深度来提高准确率。其内部的残差块使用了跳跃连接，缓解了深度神经网络中增加深度带来的梯度消失问题。



1.5 神经网络学习

学习是神经网络研究的一个重要内容，神经网络的适应性是通过学习实现的——根据

环境的变化,对权值进行调整,改善系统的行为。

由 Hebb 提出的 Hebbian 学习规则为神经网络的学习算法奠定了基础。Hebbian 规则认为学习过程最终发生在神经元之间的突触部位,突触的联系强度随着突触前后神经元的活动而变化。

在此基础上,人们提出了各种学习规则和算法,以适应不同网络模型的需要。有效的学习算法使神经网络能够通过连接权值的调整,构造客观世界的内在表示,形成具有特色的信息处理方法,信息存储和处理体现在网络的连接中。

根据学习环境不同,神经网络的学习方式可分为监督学习和非监督学习。在监督学习中,将训练样本的数据加到网络输入端,同时将相应的期望输出与网络输出相比较,得到误差信号,以此调整连接权值,多次训练后收敛到一个确定的权值。当样本情况发生变化时,经学习可以修改权值以适应新的环境。使用监督学习的神经网络模型有反传网络、感知器等。

非监督学习时,事先不给定标准样本,直接将网络置于环境之中,学习阶段与工作阶段是一体的。此时,学习规律的变化服从连接权值的演变方程。非监督学习最简单的实例是 Hebbian 学习规则。竞争学习是一个更复杂的非监督学习的实例,它根据已建立的聚类进行权值调整。下面对神经网络常用的几种学习规则进行介绍。

1. Hebbian 学习规则

Hebbian 学习规则是一种参数更新的方式。该学习规则将一个神经元的输入与输出信息进行对比,对该神经元的输入权重参数进行更新。该学习规则使每个神经元独自作战。一个神经元的参数更新,仅与它自己的输入与输出数据有关,不考虑整个网络的情况。

Hebbian 学习规则通常使用双极性激活函数,即激活函数的取值范围是 $[-1, 1]$,其作用是当输入与输出同号 (+ 或 -) 时加大权重,否则降低权重。

因此,通常 Hebbian 学习规则用当前神经元的输入与输出的乘积更新自己的权重。

$$\Delta w_{ij} = \eta o_j x_i$$

式中, o_j 是第 j 个神经元的输出, x_i 是神经元的第 i 个输入, w_{ij} 是神经元 j 与第 i 个输入数据 x_i 之间的权重。

2. 感知器学习规则

感知器的学习规则规定,学习信号等于神经元期望输出(教师信号)与实际输出之差。

对样本输入 x ,假定神经元的期望输出为 d ,当前输出为 y ,而神经元的传递函数取符号函数,则在感知器学习规则中,权值调整量为

$$\Delta w(t) = e(t) \cdot x$$

其中,误差信号为

$$e(t) = d - y = d - \text{sgn}(w^T x)$$

3. δ (Delta) 学习规则

δ 学习规则也称梯度法或最速下降法,是最常用的神经网络学习算法。

4. Widrow-Hoff 学习规则

Widrow-Hoff(简称 W-H)学习规则又称最小均方规则(LMS)。W-H 学习规则与 δ 学习规则的推导类似,该学习规则也可用于神经元传递函数取符号函数的情形。