

第 1 章 绪论

1.1 什么是人工神经网络

神经网络是由大量神经元互连而成的网络。通常来说，神经网络包括生物神经网络和人工神经网络。人工神经网络（Artificial Neural Network, ANN）是将人工神经元按照一定拓扑结构连接所形成的网络，用以模拟人类进行知识的表示与存储及利用知识进行推理的行为。简单地讲，人工神经网络是一个数学模型，可以用电子线路来实现，也可以用计算机程序来模拟，是人工智能研究的一种方法。

在 Simon Haykin 的《神经网络与机器学习》中，**神经网络定义**如下。

神经网络是由简单处理单元构成的大规模并行分布式处理器，天然地具有存储经验知识和使之可用的特性。神经网络在两方面与人类大脑相似。

(1) 神经网络是通过学习过程从外界环境中获取知识的。

(2) 互连神经元的连接强度，即突触权值，用于存储获取的知识。

人工神经网络模型的灵感来源于人脑。旨在理解人脑的功能，并朝着这一目标努力的认知科学家和神经学家构建了人脑的神经网络模型，并开展了模拟研究。然而在工程上，我们的目标是构建有用的机器，而不是理解人脑的本质。我们对人工神经网络感兴趣，相信它能帮助我们建立更好的计算机系统。

用于完成学习过程的程序称为学习算法，其功能是以有序的方式改变网络的突触权值，以获得想要的设计目标。对突触权值的修改提供了神经网络设计的传统方法，这种方法和现行自适应滤波器理论很接近，而滤波器理论已经很好地建立并成功应用于很多领域。但是，受大脑神经元会死亡及新的突触连接会生长的事实启发，神经网络修改它自身的拓扑结构是可能的。

神经网络的计算能力通过如下两点体现。

(1) 神经网络的大规模并行分布式结构。

(2) 神经网络的学习能力及由此而来的泛化能力，泛化（Generalization）是指神经网络对未在训练学习过程中遇到的数据可以得到合理的输出。

神经网络具有以下有用的性质和能力。

(1) 非线性（Nonlinearity）：人工神经元可以是线性的也可以是非线性的。非线性神经元互连而成的神经网络是非线性的，并且从某种意义上来说非线性是分布于整个网络的。

(2) 输入、输出映射（Input-Output Mapping）：从学习的角度来讲，又称为有教师学习或监督学习。它使用带标注的训练样例（Training Sample）或任务样例（Task Sample）对神经网络的突触权值进行修改。每个样例都由一个唯一的输入信号和对应的期望（目标）响应[Desired (Target) Response] 组成。在训练集中随机选取一个样例提供给网络，网络就会调整它的突触权值（自由参数），以最小化期望响应和由输入信号以适当的统计准则产生的网络实际响应之间的差别。使用训练集的很多样例重复训练神经网络，直到神经网络达到对突触权值没有显著修正的稳定状态。如此说来，对于当前问题，神经网络是通过建立输入、输出映射从样例中学习的。

(3) 自适应性 (Self Adaptivity): 神经网络具有调整自身突触权值以适应外界环境变化的固有能力。特别是, 一个在特定环境下接受训练的神经网络, 在环境条件变化不大的时候可以很容易重新训练。而且, 当神经网络在一个不稳定环境中运行时, 可以设计神经网络使其突触权值随时间实时变化。用于模式分类、信号处理和控制的神经网络与它的自适应性相耦合, 可以变成能进行自适应模式分类、自适应信号处理和自适应控制的有效工具。在系统保持稳定时, 一个系统的自适应性越好, 它被要求在一个不稳定环境中运行时的性能就越具有鲁棒性。但是, 自适应性不一定总能导致鲁棒性。

(4) 证据响应 (Evidential Response): 在模式分类问题中, 神经网络可以设计成不仅提供选择哪个特定模式的信息, 还能提供关于决策的置信度信息, 后者可以用来拒判那些可能出现的过于模糊的模式, 从而进一步改善神经网络的分类性能。

(5) 上下文信息 (Contextual Information): 神经网络的特定结构和激发状态代表知识。网络中的每个神经元都受网络中其他所有神经元全局活动的潜在影响。因此神经网络能够很自然地处理上下文信息。

(6) 容错性 (Fault Tolerance): 一个以硬件形式实现的神经网络具有天生的容错性, 或者说鲁棒性, 在这种意义上, 其性能在不利的运行条件下是逐渐下降的。原则上, 神经网络从性能上显示了一个缓慢恶化的过程, 而不是灾难性的失败。

(7) VLSI 实现 (VLSI Implement Ability): 神经网络的大规模并行性使它具有快速处理某些任务的潜在能力。这一能力使得神经网络很适合使用超大规模技术来实现。VLSI 的一个特殊优点是可以提供一个以高度分层的方式来捕捉真实复杂行为的方法。

(8) 分析和设计的一致性: 神经网络作为信息处理器具有通用性, 因为涉及神经网络应用的所有领域都使用同样的记号。这一性质以不同的方式体现。

① 神经元, 不管形式如何, 在所有的神经网络中都代表一种相同成分。

② 这种共性使得在不同应用中的神经网络共享相同的理论和学习算法成为可能。

③ 模块化网络可以用模块的无缝集成来实现。

(9) 神经生物类比: 神经网络的设计是由与人脑的类比引发的, 人脑是一个容错的并行处理的实例, 说明这种处理不仅在物理上是可实现的, 而且是快速高效的。神经生物学家将人工神经网络看作一个解释神经生物现象的研究工具。工程师对神经生物学的关注在于将其作为解决复杂问题的新思路。

人工神经网络力求从四个方面模拟人脑的智能行为: 物理结构、计算模拟、存储与操作训练。人工神经元是对生物神经元的物理模拟, 从结构上包括输入端、输出端和计算单元三部分。人工神经元是通过对生物神经元的高度简单抽象产生的, 这种由人工神经元构成的网络不具有人脑那样的能力, 但是它可以通过训练实现一些有用的功能。本书将讨论此类人工神经元, 以及由此类人工神经元构成的人工神经网络模型和相应的训练方法, 本书中将人工神经网络简称神经网络。

1.2 发展历史

本节将简单介绍神经网络的发展历史。神经网络的历史充满传奇色彩, 来自不同领域的充满创造力的先驱奋斗了数十年, 为我们探索了许多今天看来是理所当然的概念。这段历史在每本神经网络书中都有描述, 其中特别有趣的是由 John Anderson 和 Edward Rosenfeld 合著

的 *Neurocomputing: Foundations of Research* 《神经计算：研究基础》，该书收集了 43 篇具有历史意义的文章，感兴趣的读者也可以参阅该书。

下面我们简要阐述神经网络的主要发展历史，神经网络崎岖的发展历史可以用三起三落概括。

神经网络的一些基础性工作始于 19 世纪后期和 20 世纪初期。这些工作主要来自物理学、心理学、神经生物学等交叉领域的科学家，如 Hermann Von Helmholtz、Ernst Mach、Ivan Pavlov。这些早期工作致力于学习、视觉、条件反射等方面的理论研究，不包括神经元活动的数学模型。

现代神经网络源于 Warren McCulloch 和 Walter Pitts 在 20 世纪 40 年代的工作。1943 年，美国心理学家 Warren McCulloch 和数理逻辑学家 Walter Pitts 提出了第一个神经网络模型(MP 模型)，并给出了神经元的形式化描述及神经网络构建方法，证明了单个神经元能够执行逻辑运算功能，展示了由人工神经元组成的网络在原则上能完成任何算术或逻辑运算，这项工作通常被认为是现代神经网络的起源，从而开启了神经网络的新时代。

在此之后，Donald Hebb 提出了经典的条件反射源于个体神经元的性质，他提出了一套关于生物神经元学习机制的假说。

神经网络的第一个实际应用出现于 20 世纪 50 年代后期。1958 年，神经网络的研究取得了一个突破性进展。美国康奈尔大学的实验心理学家罗森布拉特（Rosenblatt）提出并实现了感知机这一神经网络模型，并展示了这种神经网络的模式识别能力。该模型能够完成一些简单的视觉处理工作，其研究热潮持续了十年。

几乎同时，Bernard Widrow 和 Ted Hoff 提出了一种新的学习算法用于训练自适应网络，这种网络在结构和能力上都类似 Rosenblatt 的感知机。Widrow-Hoff 学习算法直到今天还在使用。

不幸的是，Rosenblatt 和 Widrow 提出的网络都具有同样的内在局限性。这一局限性在 1969 年美国数学家、神经学家明斯基（Minsky）和佩珀特（Papert）出版的《感知机》一书中得以阐述和广泛传播。虽然 Rosenblatt 和 Widrow 当时也认识到了这种局限性，但是他们没能成功地改进感知机学习算法以训练更为复杂的网络。

Minsky 和 Papert 在书中证明感知机不能解决高阶谓词问题，指出感知机不能求解非线性分类问题，许多人认为进一步研究神经网络没有出路，加上当时没有足够计算能力的计算机帮助实验，许多人放弃了对神经网络的研究，导致神经网络的研究陷入十几年的低潮阶段。

虽然神经网络的研究陷入低潮阶段，但是 20 世纪 70 年代仍然有一些重要的研究工作值得提出来。1972 年，Teuvo Kohonen 和 James Anderson 独立发明了具有记忆功能的新型神经网络。Stephen Grossberg 在积极从事自组织神经网络的研究。20 世纪 80 年代，计算设备和研究路线这两个困难均被克服，人们对神经网络的研究兴趣显著增加。

有两个工作对神经网络的重新兴起起着重要作用。第一个是使用统计机制去解释一类回复神经网络的运行，这种网络可以用于联想记忆。这一重要工作是由 Hopfield 提出的，1982 年，美国加州工学院物理学院的 Hopfield 提出了 Hopfield 神经网络模型。第二个是用于训练多层感知机的反向传播算法的提出，1986 年，美国数学心理学家鲁姆哈特（Rumelhart）和麦克莱兰（McClelland）提出了反向传播（Back-Propagation, BP）算法，这个算法是对 20 世纪 60 年代 Minsky 和 Papert 对感知机批评的回答，这使得神经网络的研究再次兴起。

自 20 世纪 80 年代以来，人们发表了很多神经网络论文，开发了无数神经网络应用。

2006 年，深度神经网络得以提出，近年来，随着深度神经网络模型的巨大成功，神经网络的研究和应用得到了长足发展。

神经网络的许多进步都与新的概念息息相关，如新的结构和训练算法。同样重要的是新型计算机的出现，强大的计算能力能够测试新的概念。深度神经网络的巨大成功离不开新型计算机强大的计算能力。

神经网络取得了非常大的进步，但是作为一种数学或工程工具，神经网络不能解决所有问题，它只是在某些适当情况下的重要工具，它没有人脑的精妙，而且我们对人脑是如何工作的还研究得不够，神经网络的未来发展无疑是最为重要的。

1.3 人脑

本书所关注的神经网络与对应的生物神经网络的联系很少。本节我们简单阐述一些人脑的功能特征，其启发了神经网络的发展。

人脑是一种信息处理装置，具有非凡的能力，并在众多领域如视觉、语音识别和学习等超过了当前的工程产品。如果我们能够理解人脑是如何实现这些功能的，那么我们就可以用形式化算法定义这些任务的解并在计算机上实现它们。

人脑和计算机不同。计算机通常只有一个处理器，而人脑包含大量（100 亿个）并行操作的处理单元，称为神经元。这些神经元比计算机的处理器简单且慢很多。令人脑不同寻常且被认为提供了其计算能力的是连通性。人脑的神经元具有连接，称为突触，连接到大约 8000 个其他神经元，所有神经元都是并行操作的。人脑中的处理和存储都在网络上分布，处理由神经元来做，存储在神经元之间的突触中。

1) 神经系统框图

人脑，又称为人的神经系统，可分为三阶段，其框图如图 1.1 所示。系统的中央是人脑，由神经网络表示，它持续地接收信息，感知它并做出适当的响应。图中有两组箭头，从左到右的箭头表示携带信息的信号通过系统向前传播，从右到左的箭头表示系统中的反馈。感受器将来自人体或外界的刺激转换成电冲击，对神经网络传送信息。效应器将神经网络产生的电冲击转换为可识别的响应，从而作为系统的输出。

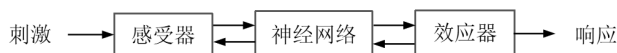


图 1.1 人的神经系统的框图

2) 生物神经元结构

神经元是人脑最基本的组织单位和工作单元。据估计，人的大脑皮层大约有 100 亿个神经元和 80 万亿个突触。从组织结构来看，神经元由三个主要部分构成：树突、细胞体和轴突。

树突是由细胞体向外延伸的除轴突以外的分支，用于接收电信号并传给细胞体的神经纤维接收网。

细胞体由细胞核、细胞质和细胞膜等组成，它是神经元的主体，内部是细胞核，外部是细胞膜，细胞膜的外面是许多向外延伸的纤维。细胞体有效地叠加这些传入的信息并用阈值控制电信号的输出。

轴突是一条长的神经纤维，用于向外传递神经网络产生的输出电信号。每个神经元都有

一条轴突，作为输出端与其他神经元的树突连接，实现神经元之间的信息传递。每条轴突大约由四部分组成：第一部分是由细胞体发起到开始被髓鞘包裹这一段，通常被称为始段；第二部分是从被髓鞘包裹开始到髓鞘消失这一段，通常被称为主枝；第三部分是髓鞘消失后形成的多条末梢神经纤维，通常被称为轴突末梢；最后一部分是在轴突末梢末端呈纽扣状的膨大体，称为突触。一个神经元的轴突和另一个神经元的树突的连接点称为突触或神经末梢。突触是调节神经元之间相互作用的基本结构和功能单位。

正是因为神经元的结构，以及由复杂化学过程决定的每个突触的连接强度，建立了神经网络的功能。图 1.2 所示为一个生物神经元的结构示意图。图 1.3 所示为生物神经元的信

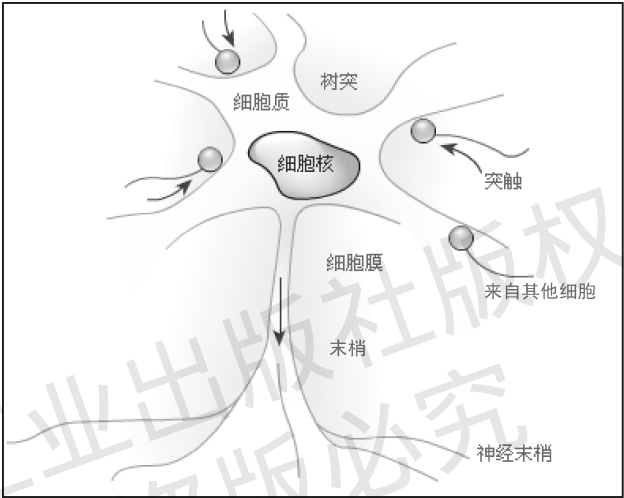


图 1.2 一个生物神经元的结构示意图

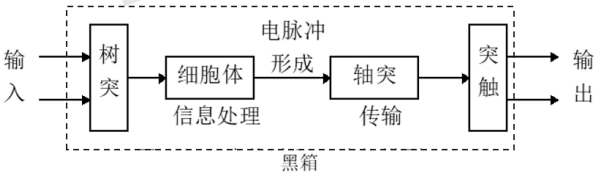


图 1.3 生物神经元的信处理过程

3) 生物神经元的基本功能

根据生物学的研究，生物神经元的主要功能为：神经元的抑制与兴奋；神经元内神经冲动的传导。

抑制与兴奋是生物神经元的两种常规工作状态。抑制状态是神经元没有产生冲动时的工作状态，兴奋状态是神经元产生冲动时的工作状态。通常情况下，在神经元没有受到任何外部刺激时，其膜电位约为 -70mV ，且膜内为负，膜外为正，神经元处于抑制状态。当神经元受到外部刺激时，其膜电位上升，上升到一定电位时，神经元会产生冲动，进入兴奋状态，该电位称为动作电位。

神经冲动在神经元内的传导过程是一种电传导过程，但其传导速度与电流在导线中的传导速度不一样。电流在导线内按光速运动，而神经冲动沿着神经纤维传导的速度为 $3.2\sim$

320km/s，其传导速度与纤维的粗细、髓鞘的有无有一定关系。

4) 突触的基本结构和突触传递

突触（Synapse）是调节神经元之间相互作用的基本结构和功能单位。它形成了神经元之间的联系，是构成神经系统最重要的组织基础。突触传递实现了神经元之间的信息交换，是神经系统最重要的工作基础。最普通的一类突触是化学突触，它是这样运行的：前突触过程释放发送器物质，扩散到神经元之间的突触，作用于后突触过程。这样突触就完成了突触前端的电信号向化学信号的转换，突触后端的化学信号向电信号的转换。用电学术语来说，这样的元素称为非互逆的两端口设备。在传统的神经组织描述中，仅假设突触是一个简单的连接，能施加兴奋或抑制，但不同时作用在接受神经元。

可塑性允许神经系统进化以适应周边环境。在成年人的大脑中，可塑性可以解释两个机能：创建神经元间的新连接及修改已有的连接。

突触传递是由电变化和化学变化两个过程完成的，即先将由神经冲动引起的电脉冲传导转化为化学传导，然后将化学传导转换为电脉冲传导。

大多数神经元把它们的输出转化为一组简短的电压脉冲编码。这些脉冲编码一般称为动作电位或尖峰，产生于神经元细胞体或其附近，并以恒定的电压和振幅穿越个体神经元。

5) 人脑的分层结构

在人脑中，有小规模和大规模解剖组织之分，在底层和顶层会发生不同的机能。图 1.4 显示了人脑的分层结构。突触表示最基本的层次，其活动依赖分子和离子。其后的层次有神经微电路、树突树及神经元等。神经微电路是指突触集成，组成可以产生所需功能操作的连接模式。神经微电路被组织成属于个体神经元的树突树的树突子单元。整个神经元大约为 $100\mu\text{m}$ ，包含几个树突子单元（度量单位采用 μm 表示）。局部电路处在其次的复杂性水平，由具有相似或不同性质的神经元组成，这些神经元集成完成脑局部区域的特征操作。接下来是区域间电路，由通路、柱子和局部解剖图组成，牵涉人脑中不同部分的多个区域。

局部解剖图被组织成用来响应输入的感知信息，经常被组织成片束状。大脑皮层的细胞结构表明，不同的感知输入（运动、触觉、视觉、听觉等）被有序地映射到大脑皮层的相应位置。在复杂性的最后一级，局部解剖图和其他区域间电路成为中枢神经系统传递特定行为的媒介。

由上述内容可知，分层结构是人脑的独有特征，在计算机中我们找不到这种结构，在神经网络中也无法近似地重构它们，但是我们在向图 1.4 中描述的分层结构缓慢推进。用以构造神经网络的人工神经元和人脑中的神经元相比的确比较初级，但是我们目前能设计的神经网络和人脑中初级的局部电路和区域间电路相当，而且我们在许多前沿已经有了显著进步。以神经生物类比为灵感的源泉，加上当前理论和技术工具的日新月异，我们对神经网络及其应用的理解一定会越来越深入和宽广。

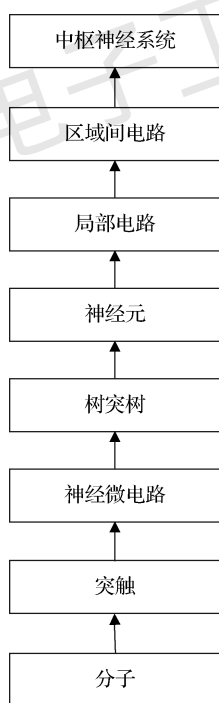


图 1.4 人脑的分层结构

1.4 Hebb 法则

Hebb 法则认为连接强度的变化与两个相连神经元激活的相关性成比例。如果两个神经元始终同时激活,那么它们之间的连接强度会变大。反之,如果两个神经元从来不同时激活,那么它们之间的连接会消失。这里的思想在于如果两个神经元都会对某件事做出反应,那么它们应该相连。我们看一个例子:假如你有一个能够辨识出你奶奶的神经元,你奶奶每次来看你时都会带给你颗水果糖,那么当辨识奶奶的神经元兴奋时,某些由于你喜爱水果糖的味道而开心的神经元同样会处于兴奋状态。这些神经元同时激活,它们之间就会相连,并且随着时间推移,连接强度会变得越来越来。巴普洛夫(Pavlov)使用这个被称为经典条件反射的思想来训练狗。每次给狗提供食物的同时发出铃声,这样分泌唾液的神经元和听到铃声的神经元就会同时激活,它们之间的连接强度变得很大。随着时间推移,对铃声做出反应的神经元及那些引起反射性分泌唾液的神经元之间的连接强度会变得足够大,以至于听到铃声就会激活分泌唾液的神经元。

这种当神经元同时激活,它们之间形成连接并且变得更强,从而形成神经元集合的思想还有其他名称,如长时程增强效应和神经可塑性,这似乎与实际人脑也有联系。

1.5 神经元模型

神经元是神经网络操作的基本信息处理单位。图 1.5 给出了神经元模型,它是本书其他章节将要讨论的神经网络模型、学习算法及其应用的基础。

在图 1.5 中, x_m 表示神经元的 m 个输入, w_{kj} 是权值, b_k 是外部偏置, y 为输出。人工神经元是一个具有多输入/单输出的非线性器件。我们在这里给出神经元模型的基本元素。

(1) 突触或连接链集,每个都有其权值或强度作为特征,第 k 个神经元的突触 j 上的输入 x_j 乘以 k 的权值 w_{kj} ,这里 w_{kj} 的第一个下标指的是当前神经元,第二个下标指权值所在的突触的输入端。人工神经元的突触权值有一个范围,可以取正值也可以取负值。

(2) 求和节点,用于求输入信号被神经元相应的突触加权的和,这个操作构成一个线性组合器。

(3) 激活函数,用于限制神经元输出振幅。由于它将输出信号压制(限制)到允许范围之间的一定值,因此激活函数也称为压制函数。通常一个神经元的输出的正常幅度范围在单位闭区间 $[0,1]$ 或 $[-1,+1]$ 上。

(4) 外部偏置,其作用在于根据其为正或负,相应地增加或降低激活函数的网络输入。

采用数学术语表示,我们可以用如下两个方程描述神经元:

$$u_k = \sum_{j=1}^m w_{kj} x_j \quad (1.1)$$

$$y_k = \phi(u_k + b_k) \quad (1.2)$$

式中, $x_j, j=1,2,\dots,m$ 是输入; w_{kj} 是神经元 k 的权值; u_k 是输入的线性组合器的输出; b_k 是外部偏置; $\phi(\cdot)$ 为激活函数; y_k 是神经元的输出。 b_k 的作用是对图 1.5 模型中的线性组合器的输出 u_k 做仿射变换 $v_k = u_k + b_k$ 。

偏置是人工神经元 k 的外部参数,我们在神经元 k 上加上一个新的突触,其输入是 $x_0 = +1$, 权值是 $w_{k0} = b_k$, 因此得到神经元 k 的新模型, 如图 1.6 所示, 采用数学术语表示, 我们可以用如下两个方程描述神经元:

$$v_k = \sum_{j=0}^m w_{kj} x_j \quad (1.3)$$

$$y_k = \phi(v_k) \quad (1.4)$$

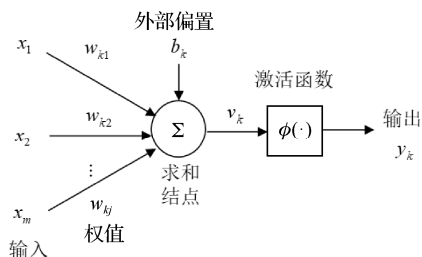


图 1.5 神经元模型

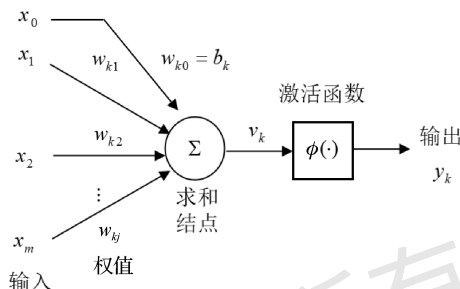


图 1.6 神经元的新模型

在图 1.6 中,偏置的作用为:添加新的固定的输入+1,添加新的等于 b_k 的突触权值。图 1.5 和图 1.6 的模型不同,但是在数学上它们是等价的。

激活函数,记为 $\phi(v)$,通过诱导局部域 v 定义神经元输出。激活函数有如下几种基本类型。

(1) 阈值函数。这种模型的神经元没有内部状态,激活函数是一个阶跃函数:

$$\phi(v) = \begin{cases} 1, & v \geq 0 \\ 0, & v < 0 \end{cases} \quad (1.5)$$

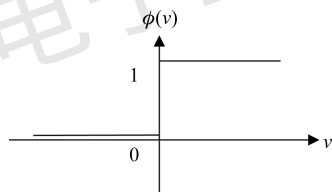


图 1.7 阈值函数

在神经计算中,这样的神经元称为 McCulloch-Pitts (MP) 模型,以纪念 McCulloch 和 Pitts 开拓性的工作。在 MP 模型中,若神经元的诱导局部域非负,则输出为 1,否则为 0,这描述了 MP 模型的皆有或皆无特性。阈值函数如图 1.7 所示。

(2) 分段线性型函数。这种模型又称为伪线性,其激活函数是一个分段线性函数:

$$\phi(v) = \begin{cases} 1, & v \geq \frac{1}{k} \\ kv, & 0 \leq v \leq \frac{1}{k} \\ 0, & v < 0 \end{cases} \quad (1.6)$$

式中, k 是放大系数。该函数的输入、输出在一定范围内满足线性关系,一直延续到输出最大值为 1。到达最大值后,输出就不再增大。分段线性型函数如图 1.8 所示。

(3) Sigmoid 函数。此函数的图形是“S”形的,因此又称为 S 形函数,其在构造神经网络时是最常用的激活函数。Sigmoid 函数是严格的递增函数,是一个连续的神经元模型,在线性和非线性行为之间显现出较好的平衡。这种模型常取指数、对数或双曲正切等 Sigmoid 函数。Sigmoid 函数如图 1.9 所示。

(4) 子阈累积型函数。这是一个非线性函数,当产生的激活值超过 T 时,该神经元被激活产生反响。在线性范围内,系统的反响是线性的。子阈累积型函数如图 1.10 所示。

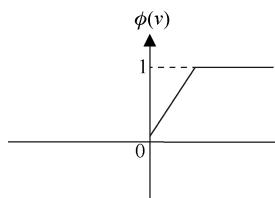


图 1.8 分段线性型函数

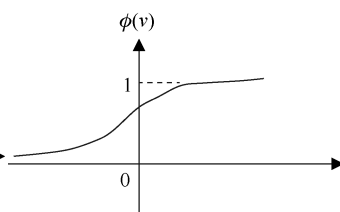


图 1.9 Sigmoid 函数

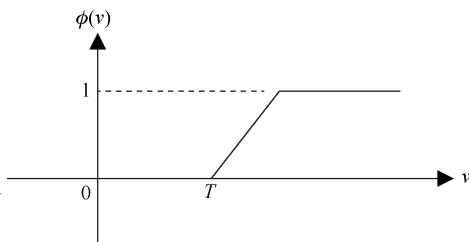


图 1.10 子阈累积型函数

1.6 神经网络的拓扑结构

神经网络里的神经元的构造方式与用于训练网络的学习算法有着紧密联系,因此可以说,用于神经网络设计的学习算法(规则)是被构造的,本节将介绍神经网络的体系结构(又称为拓扑结构或互连结构)。在分层神经网络中,神经元以层的形式组织,通常我们将多个神经元以并行方式运算,这些神经元称为一个“层”。

神经网络的拓扑结构是指单个神经元之间及层与层之间的连接模式,是构造神经网络的基础,也是神经网络诱发偏差的主要来源。从拓扑结构的角度来看,神经网络可分为前馈神经网络和反馈神经网络(又称为递归神经网络)两种。

1) 前馈神经网络

前馈神经网络是指只包含前向连接的神经网络。前馈连接是指从上一层所有神经元到下一层所有神经元的连接方式。根据神经网络中拥有计算节点(拥有权值的神经元)的层数,前馈神经网络分为单层前馈神经网络、多层前馈神经网络、输出到输入具有反馈的前馈神经网络和层内互连前馈神经网络等类型。

(1) 单层前馈神经网络。

单层前馈神经网络是指只拥有单层计算节点的前馈神经网络,仅含输入层和输出层,且只有输出层的神经元是可计算节点,其结构如图 1.11 所示,其中输入向量 $\mathbf{X} = (x_1, x_1, \dots, x_n)$, 输出向量 $\mathbf{Y} = (y_1, y_2, \dots, y_n)$, 输入层第 i 个神经元和输出层第 j 个神经元之间的权值是 $w_{ij} (i=1, 2, \dots, n, j=1, 2, \dots, m)$, 假设第 j 个神经元的阈值为 $b_j (j=1, 2, \dots, m)$, 激活函数为 $\phi(\cdot)$, 则各神经元的输出为

$$y_j = \phi \left(\sum_{i=1}^n w_{ij} x_i - b_j \right), j=1, 2, \dots, m \quad (1.7)$$

其中,由所有的权值 $w_{ij} (i=1, 2, \dots, n, j=1, 2, \dots, m)$ 构成的权值矩阵为

$$\mathbf{W} = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1m} \\ w_{21} & w_{22} & \cdots & w_{2m} \\ \vdots & \vdots & & \vdots \\ w_{n1} & w_{n2} & \cdots & w_{nm} \end{bmatrix}$$

在实际应用中,该权值矩阵是利用某种学习算法对训练样本进行学习获得的。

(2) 多层前馈神经网络。

多层前馈神经网络是指除输入层、输出层以外,还至少包含一个隐含层的前馈神经网络。所谓隐含层是指由那些既不属于输入层又不属于输出层的神经元构成的处理层。由于隐含层

仅与周围输入层、输出层连接，不直接与外部输入层、输出层打交道，因此又被称为中间层。隐含层的作用是通过输入层信号的加工处理，将其转化为更能被输出层接受的形式。隐含层使得神经网络的非线性处理能力得到提升，隐含层越多，神经网络的非线性处理能力越强，但是隐含层的加入也增加了神经网络的复杂度。

多层前馈神经网络的结构如图 1.12 所示，其中输入层的输出是第一隐含层的输入，第一隐含层的输出是第二隐含层的输入，以此类推，直至输出层。多层前馈神经网络的典型代表有 BP 神经网络和 RBF 神经网络等。

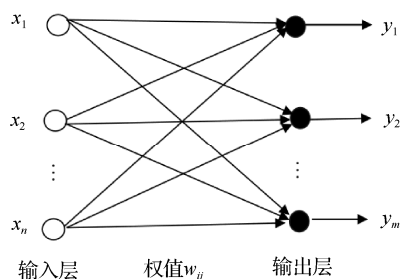


图 1.11 单层前馈神经网络的结构

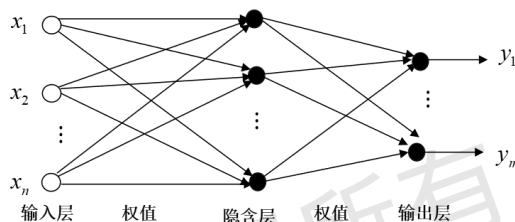


图 1.12 多层前馈神经网络的结构

(3) 输出层到输入层具有反馈的前馈神经网络。

图 1.13 所示为输出层到输入层具有反馈的前馈神经网络的结构，其中输出层上存在一个反馈回路，将信号反馈到输入层，而网络本身还是前馈型的。

(4) 层内互连前馈神经网络。

图 1.14 所示为层内互连前馈神经网络的结构，外部看是一个前馈神经网络，内部有很多自组织网络在层内互连，从而形成反馈环。

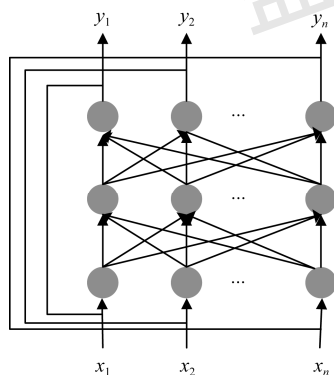


图 1.13 输出层到输入层具有反馈的前馈神经网络的结构

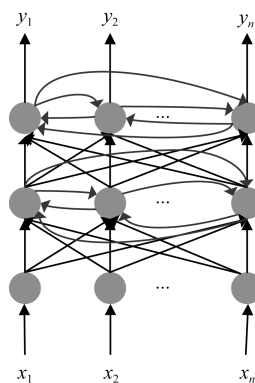


图 1.14 层内互连前馈神经网络的结构

2) 反馈神经网络

反馈神经网络是指允许使用反馈连接方式形成的神经网络。反馈神经网络在有些参考书中又叫作递归神经网络或回复神经网络。反馈连接方式是指神经网络的输出可以被反馈至同层或前层神经元重新作为输入。通常把那些引出有反馈连接弧的神经元称为隐神经元，其输出称为内部输出。由于反馈连接方式的存在，一个反馈神经网络中至少含有一条反馈回路，这些反馈回路实际上是一条封闭环路。反馈神经网络又分为如下两种形式。

(1) 反馈型全互连网络。

在这种神经网络中，所有计算单元之间都有连接，如 Hopfield 神经网络，图 1.15 所示为离散 Hopfield 神经网络的结构。

(2) 反馈型局部连接网络。

在这种神经网络中，每个神经元的输出只与其周围的神经元相连，形成反馈神经网络，图 1.16 所示为反馈型局部连接网络的结构。

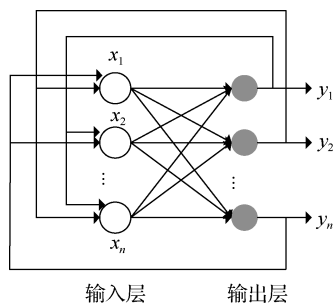


图 1.15 离散 Hopfield 神经网络的结构

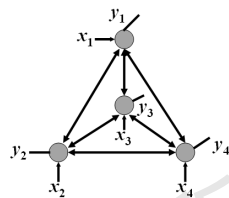


图 1.16 反馈型局部连接网络的结构

无论是哪种反馈神经网络，反馈环的存在都对网络的学习能力和它的性能有深刻的影响，并且由于反馈环涉及使用单位时间延迟元素构成的特殊分支，因此，假设神经网络包含非线性单元时，将导致非线性的动态行为。

1.7 知识表示

首先给出知识的一般性定义：知识就是人或机器存储起来以备使用的信息或模型，用来对外部世界做出解释、预测和适当的反应。

知识表示的主要特征有两个方面：①什么信息是明确表述的；②物理上信息是如何被编码和使用的。按照知识表示的本性，它是目标导向的。在智能机器的现实应用中，可以说好的方案取决于好的知识表示。代表一类特殊智能机器的神经网络也是如此。但是，典型地从输入到内部网络参数的可能表现形式是高度多样性的，这就导致基于神经网络的对满意解的求解成为一个具有挑战性的设计。

神经网络的一个主要任务是学习它所依存的外部世界（环境）模型，并且保持该模型和真实世界足够兼容，使之能够实现感兴趣应用的特定目标。有关世界的知识由两类信息组成。

(1) 已知世界的状态，由“什么是”事实和“什么是已知道的”事实表示，这种形式的知识称为先验信息（Prior Information）。

(2) 对世界的观察（测量），由神经网络中被设计用于探测环境的传感器获得。一般来说，这些观察是带有固定噪声的，这是由于传感器的噪声和系统的不完善产生的误差。不管怎样，这样得到的观察会提供一个信息池，从中提取样例来训练神经网络。

样例可以是有标号的，也可以是无标号的。对于有标号的样例，每个样例的输入信号都有相应的与之配对的期望响应（目标输出）。无标号的样例包括输入信号自身的不同实现。不管怎样，一组样例，无论有无标号，都代表神经网络通过训练可以学习的环境知识。但是要说明的是，有标号的样例的采集代价较高，因为它们需要“教师”来对每个有标号的样例提

供需要的期望响应。与之相反，通常无标号的样例的数目是足够的，因为对于无标号的样例，不需要“教师”。

一组由输入信号和相应的期望响应组成的输入、输出对，称为训练数据集或训练样本。为了说明怎样使用这样的数据集，我们以手写数字识别问题为例。在这个问题中，输入信号是一幅黑白图像，每幅图像代表可以从背景中明显区分出的 10 个数字之一。期望响应就是“确定”网络的输入信号代表哪个数字。通常训练样本是手写数字的大量变形，这代表真实世界的情形。有了这些样本，可以用如下的办法设计神经网络。

(1) 为神经网络选择一个合适的结构，输入层的源节点数和输入图像的像素数一样，而输出层包含 10 个神经元（每个数字对应一个神经元）。利用合适的算法，用样本的一个子集来训练网络，这个网络设计阶段称为学习。

(2) 用陌生样本来测试已训练网络的识别性能。具体来说，呈现给网络一幅输入图像时并不告诉它这幅图像属于哪个数字。网络的性能就用网络报告的数字类别和输入图像的实际类别的差异来衡量。网络运行的这个阶段叫作测试，对测试模式而言的成功性叫作泛化，这借用了心理学的术语。

这里神经网络的设计与传统信息处理对应部分（模式分类器）的设计有着根本区别。对后一种情况来说，我们通常先设计一个观测环境的数学模型，并利用真实数据来验证这个模型，再以此模型为基础来设计。相反，神经网络的设计直接基于真实数据，“让数据自己说话”。因此神经网络不但提供了其内嵌于环境的隐含模型，也实现了感兴趣的信息处理功能。

用于训练神经网络的例子可以由正例和反例组成。例如，在被动声呐探测问题上，正例是包括感兴趣的目标（如潜艇）的输入训练数据。在被动声呐环境下，测试数据中可能存在的海洋生物经常造成虚警。为了缓解这个问题，可以把反例（如海洋生物的回声）包括在训练集中，从而教会网络不要混淆海洋生物和目标。

在神经网络的独特结构中，周围环境的知识表示是由网络的自由参数（突触权值和偏置）的取值定义的。这种知识表示的形式构成神经网络的设计，因此也是网络性能的关键。

在神经网络中，知识表示是非常复杂的，这里给出有关知识表示的 4 条通用规则。

规则 1 相似类别中的相似输入通常应产生网络中相似的表示，因此可以归入同一类。

测量输入相似性的方法很多，常用的测量方法是利用欧几里得距离的概念，具体来说，令 $\mathbf{x}_i$ 定义一个 $m \times 1$ 的向量，即

$$\mathbf{x}_i = [x_{i1}, x_{i2}, \dots, x_{im}]^T$$

所有的元素都是实值；上标 T 表示矩阵转置。向量 $\mathbf{x}_i$ 就是 m 维欧几里得空间的一个点，记为 R^m 。两个 $m \times 1$ 的向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 之间的欧几里得距离定义为

$$d(\mathbf{x}_i, \mathbf{x}_j) = \|\mathbf{x}_i - \mathbf{x}_j\| = \left[\sum_{k=1}^m (x_{ik} - x_{jk})^2 \right]^{\frac{1}{2}}$$

式中， x_{ik} 和 x_{jk} 分别是向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 的第 k 个分量。相应地，由向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 表示的两个输入的相似性就定义为欧几里得距离 $d(\mathbf{x}_i, \mathbf{x}_j)$ 。向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 相距越近，欧几里得距离就越小，相似性就越大。**规则 1** 说明，如果两个向量是相似的，就将它们归入同一类。

另一个测量相似性方法基于点积或内积，它也借用了矩阵代数的概念。给定一对相同维数的向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ ，它们的内积是 $\mathbf{x}_i^T \mathbf{x}_j$ ，定义为向量 $\mathbf{x}_i$ 对向量 $\mathbf{x}_j$ 的投影，可展开如下

$$\langle \mathbf{x}_i, \mathbf{x}_j \rangle = \mathbf{x}_i^T \mathbf{x}_j = \sum_{k=1}^m x_{ik} x_{jk}$$

内积 $\langle \mathbf{x}_i, \mathbf{x}_j \rangle$ 除以范数积 $\|\mathbf{x}_i\| \cdot \|\mathbf{x}_j\|$ ，就是两个向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 的夹角的余弦。

这里定义两种相似性度量有密切的关系，如图 1.17 所示，该图清晰地展示了欧几里得距离越小，向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 越相似，内积 $\langle \mathbf{x}_i, \mathbf{x}_j \rangle$ 越大。

为了把这种关系置于形式化基础之上，首先将向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 归一化，即 $\|\mathbf{x}_i\| = \|\mathbf{x}_j\| = 1$ ，我们可以将欧几里得距离定义写成

$$d^2(\mathbf{x}_i, \mathbf{x}_j) = (\mathbf{x}_i - \mathbf{x}_j)^T (\mathbf{x}_i - \mathbf{x}_j) = 2 - 2\mathbf{x}_i^T \mathbf{x}_j$$

上式表明，最小化欧几里得距离 $d(\mathbf{x}_i, \mathbf{x}_j)$ 对应最大化

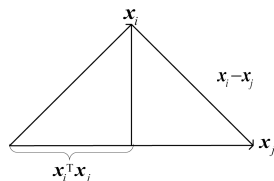


图 1.17 两种相似性度量的密切关系

内积 $\langle \mathbf{x}_i, \mathbf{x}_j \rangle$ ，因此，也对应最大化向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 之间的相似性。

这里的欧几里得距离和内积的定义都是用确定性的术语定义的。如果向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 是“随机的”，是从不同数据群体或集合中得来的，那么又该如何定义相似性呢？具体来说，假设两个群体的差异仅在于它们的均值向量。令 μ_i 和 μ_j 分别表示向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 的均值，即

$$\mu_i = E[\mathbf{x}_i]$$

式中， E 是向量 $\mathbf{x}_i$ 的集合体的统计期望算子。用同样的方法定义均值向量 μ_j 。为了度量这两个群体的距离，可以用 Mahalanobis 距离来衡量，记为 d_{ij} 。从 $\mathbf{x}_i$ 到 $\mathbf{x}_j$ 的距离的平方值定义为

$$d_{ij}^2(\mathbf{x}_i, \mathbf{x}_j) = (\mathbf{x}_i - \mu_j)^T \mathbf{C}^{-1} (\mathbf{x}_i - \mu_j)$$

式中， $\mathbf{C}^{-1}$ 是协方差矩阵 $\mathbf{C}$ 的逆矩阵。假设两个群体的协方差矩阵是一样的，表示如下：

$$\mathbf{C} = E[(\mathbf{x}_i - \mu_i)(\mathbf{x}_j - \mu_j)^T] = E[(\mathbf{x}_j - \mu_j)(\mathbf{x}_j - \mu_j)^T]$$

则对于给定的 $\mathbf{C}$ ， d_{ij} 越小，向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 越相似。

当 $\mathbf{x}_i = \mathbf{x}_j$ ， $\mu_i = \mu_j = \mu$ 且 $\mathbf{C} = \mathbf{I}$ ($\mathbf{I}$ 为单位矩阵) 时， d_{ij} 变为向量 $\mathbf{x}_i$ 和均值向量 μ 之间的欧几里得距离。

无论向量 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 是确定的还是随机的，规则 1 都讨论了这两个向量之间是如何彼此相关的。相关性不仅在人脑中起着关键作用，对多种信号处理系统来说也是如此。

规则 2 网络对可分离为不同类的输入向量给出了差别很大的表示。

根据规则 1，一方面，从一个特定的类中获取的模式之间有一个很小的代数测量值（如欧几里得距离）。另一方面，从不同类中获取的模式之间的代数测量值必须很大。因而，我们说规则 2 和规则 1 正好相反。

规则 3 如果某个特征很重要，那么网络表示这个向量将涉及大量神经元。

规则 4 如果存在先验信息和不变性，那么应该将其附加在网络设计中，这样就不必因学习这些信息而简化网络设计。

规则 4 很重要，因为坚持这一规则会使网络具有特定结构，这一点是我们所需要的，原因如下。

(1) 已知生物视觉和听觉网络是非常特别的。

(2) 相对全连接网络，特定网络用于调节的自由参数是较少的，因此特定网络所需的训练数据更少、学习更快、泛化性能更强。

(3) 能够加快通过特定网络的信息传输率（网络的吞吐量）。

(4) 和全连接网络相比，特定网络的建设成本较低，因为其规模小。

然而，需要说明的是，将先验信息结合神经网络的设计会限制神经网络，使其仅能应用于根据某些感兴趣的知识来解决特定问题。

怎样在神经网络设计中加入先验信息，以此建立一种特定的网络结构，是必须考虑的重要问题。遗憾的是，目前还没有一种有效的规则来实现这一目的。目前，我们更多的是通过某些特别的过程来实现，并已知可以产生一些有用的结果。特别是下面两种方法的结合。

(1) 通过使用称为接收域的局部连接，限制网络结构。

(2) 通过使用权值共享，限制权值的选择。

这两种方法，特别是后一种，有很好的附带效益，使得网络自由参数的数量显著减少。

卷积网络就是一种典型的使用局部连接和权值共享的前馈网络。在第 8 章中我们将重点介绍，此处不深入讨论。

在神经网络设计中加入先验信息是**规则 4**的一部分，该规则的剩余部分涉及不变性问题，下面进一步讨论。

考虑以下物理现象。

(1) 当感兴趣的目标旋转时，观察者感知到的目标图像通常会产生相应的变化。

(2) 在一个提供它周围环境的幅度和相位信息的相干雷达中，由于目标相对雷达射线运动造成的多普勒效应，活动目标的回声在频率上会产生偏移。

(3) 人说话的语调会有高低快慢的变化。

为了建立一个对象识别系统、一个雷达目标识别系统和一个语音识别系统来处理这些现象，系统必须应付一定范围内观察信号的变换。相应地，一个模式识别问题的主要任务就是设计对这些变换不变的分类器。也就是说，分类器输出的类别估计不受分类器输入观察信号变换的影响。

至少可以用三种技术使分类器类型的神经网络对变换不变。

(1) 结构不变性。适当地组织神经网络的设计，在神经网络设计中建立不变性。具体来说，在建立网络的神经元突触连接时，要求同一输入变换后必须得到同样的输出。例如，考虑利用神经网络对输入图像的分类问题，要求神经网络不受图像关于中心的平面旋转的影响。我们可以在网络中强制加上旋转不变性：让 w_{ij} 表示神经元 j 和输入图像的像素 i 的权值。如果对所有两个到图像中心距离相等的像素 i 和 k 强制 $w_{ij} = w_{jk}$ ，那么神经网络对平面内的旋转不变。但是为了保护旋转不变性，对从原点出发的相同半径距离上输入图像的每个像素必须复制 w_{ij} 。这说明了结构不变性的一个缺点：神经网络即使在处理中等大小的图像时，其连接数目也会变得很大。

(2) 训练不变性。神经网络具有天生的模式分类能力。利用这种能力可以直接得到下面的变换不变性：用一些来自同一目标的不同样本来训练网络，这些样本代表目标的不同变换（目标的不同方面）。假设样本足够大且训练后的网络已经学会分辨目标的不同变换，我们可以期望训练后的网络能对已出现目标的不同变换做出正确的泛化。但是从工程的角度来看，训练不变性有两方面不足：第一，即使一个神经网络训练后对已知变换具有不变性，也不一定能保证它对其他类型目标的变换具有不变性。第二，网络的计算要求可能很难达到，特别是在高维特征空间。

(3) 不变特征空间。不变特征空间类型系统框图如图 1.18 所示。它依赖这样的前提条件, 即能提取表示输入数据本质信息内容的特征, 且这些特征对输入的变换保持不变。如果使用这样的特征, 那么分类神经网络可以从刻画具有复杂决策边界的目标变换范围的负担中解脱出来。确实, 同一目标的不同事例的差异仅在于噪声和偶发事件等不可避免的因素。不变特征空间提供了三个明显的好处: 第一, 适用于网络的特征数可以降低到理想的水平。第二, 网络设计的要求放宽了。第三, 所有目标已知变换的不变性都得到了满足。

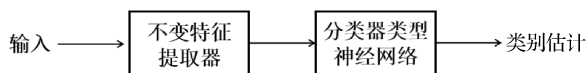


图 1.18 不变特征空间类型系统框图

神经网络中的知识表示和网络结构有着直接关系。遗憾的是, 还没有成功的理论可以根据环境来优化网络结构, 或者评价修改网络结构对网络内部知识表示的影响。实际上, 对这些问题的满意结果要通过经常对感兴趣的具体应用进行彻底的实验研究才能得到, 而神经网络的设计者也成为结构学习环的关键部分。

1.8 神经网络的学习算法

神经网络有多种学习算法, 通过学习算法, 神经网络可以从周围环境中学习。通常来说, 可以通过神经网络的功能将神经网络的学习算法分为如下两类: 有教师学习 (又称为监督学习) 和无教师学习。按照同样的标准, 无教师学习又分为强化学习和无监督学习。这些神经网络的不同学习算法跟人类学习的形式相似。

1) 有教师学习

图 1.19 说明了有教师学习的框图。从概念上讲, 我们可以认为教师具有对周围环境的知识, 这些知识被表达为一系列输入、输出样本。然而神经网络对环境却一无所知。假设给教师和神经网络提供从同样环境中提取出来的样例 (训练向量), 教师可以根据自身掌握的一些知识为神经网络提供对训练向量的期望响应。事实上, 期望响应一般代表神经网络完成的最优动作。神经网络的参数可以在样例和误差信号的综合影响下进行调整。误差信号可以定义为神经网络的实际响应和期望响应之差。这种调整可以逐步又反复地进行, 其最终目的是让神经网络模拟教师, 在某种统计的意义下, 可以认为这种模拟是最优的。利用这种手段, 教师所掌握的关于环境的知识可以通过训练过程最大限度地传授给神经网络。当条件成熟时, 可以将教师排除在外, 让神经网络完全自主地应对环境。

上述监督学习形式是误差-修正学习的基础。由图 1.19 可知, 监督学习系统构成一个闭环反馈系统, 但未知的环境不包含在循环中。我们可以采用计算训练样本的均方误差和或平方误差和作为系统性能的测试手段, 它可以定义为系统的一个关于突触权值的函数。该函数可以看作一个多维误差-性能曲面, 简称误差曲面, 其中突触权值作为坐标轴。实际误差曲面是在所有可能的输入、输出样例上的平均。任何一个在教师监督下的系统给定的操作都表示误差曲面上的一个点。该系统要随时间提高性能, 就必须向教师学习, 操作点必须向误差曲面的最小点逐渐下降, 误差极小点可能是局部最小, 也可能是全局最小。监督学习系统可以根据系统当前的行为计算误差曲面的梯度, 然后利用梯度这一有用信息求得误差极小点。误差曲面上任何一点的梯度都是指向最快速下降方向的向量。实际上, 通过样本进行监督学习,

系统可以采用梯度向量的“瞬时估计”，这时将样例的索引假定为访问的时间。采取这种方法一般会导致在误差曲面上操作点的运动轨迹经常以“随机行走”的形式出现。然而，如果我们能给定一个设计好的算法来使代价函数最小，而且有足够的输入、输出样本集和充裕的训练时间，那么监督学习系统就能较好地逼近一个未知的输入、输出映射。

2) 无教师学习

在监督学习中，学习过程是在教师的监督下进行的。而在无教师学习中，没有教师监督学习过程，也就是没有任何有标注的样例可以供神经网络学习使用。在无教师学习中，有如下两个子类。

(1) 强化学习。

在强化学习中，输入、输出映射的学习是通过与环境的不断交互完成的，目的是使一个标量性能指标达到最小。图 1.20 所示为强化学习系统的框图。这种学习系统建立在一个评价的基础上，评价将从周围环境中接收到的原始强化信号转换成一种称为启迪强化信号的高质量强化信号，二者都是标量输入。设计该系统的目的是适应延迟强化情况的学习，意味着系统观察从环境接收的一个时序刺激，最终产生启迪强化信号。

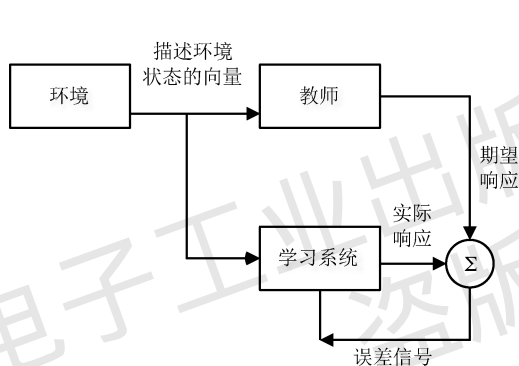


图 1.19 有教师学习的框图

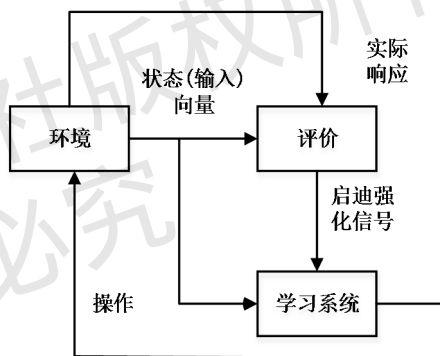


图 1.20 强化学习系统的框图

强化学习的目的是将 Cost-To-Go 函数最小化，Cost-To-Go 函数定义为采取一系列动作的代价累计期望值，而不是简单的直接代价。可以证明：在时间序列上，早期采取的动作事实上是整个系统最好的决定。学习系统的功能是用来发现这些动作并将它们反馈给环境。

基于如下两个原因，延迟强化学习系统很难完成。

① 在学习过程中的每个步骤都没有教师提供一个期望响应。

② 生成原始强化信号的延迟意味着学习机必须解决时间信任赋值问题，即对将导致最终结果的时间序列步中的每个动作，学习机必须各自独立地对信任和责任赋值，而原始强化可能仅评价最终结果。

尽管存在这些困难，但延迟强化学习还是非常有吸引力的，它提供系统与周围环境交互的基础，因此可以在这种仅与环境交互获得经验结果的基础上，发展学习能力来完成指定任务。

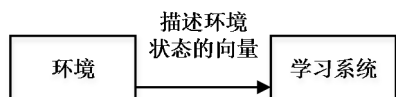


图 1.21 无监督学习的框图

(2) 无监督学习。

图 1.21 所示为无监督学习的框图。在无监督或自组织学习系统中，没有外部的教师或评价来监督学习过程。而且必须提供任务独立度量来度量网络的表达质量，让

网络学习该度量,并根据这个度量来最优化网络自由参数。对一个特定的任务独立度量来说,一旦神经网络能够和输入数据的统计规律一致,那么网络将发展其形成输入数据编码特征的内部表示的能力,从而自动创造新的类别。

为了完成无监督学习,我们可以使用竞争性学习规则。例如,可以采用包含两层的神经网络:输入层和竞争层。输入层接收有效数据,竞争层由相互竞争(根据一定的学习规则)的神经元组成,它们力图获得响应包含在输入数据中的特征的“机会”。最简单的形式就是神经网络采用“胜者全得”的策略。在这种策略中,具有最大总输入的神经元赢得竞争而被激活,其他神经元被关掉。

1.9 神经网络的学习任务

前面讨论了一些不同的学习范例,本节将讨论一些基本的学习任务。对特定学习规则的选择与神经网络需要完成的学习任务密切相关,而学习任务的多样性正是神经网络通用性的证明。

1) 模式联想

联想记忆是与人脑相似的依靠联想学习的分布式记忆。从亚里士多德时代起,联想就被视为人类记忆的一个显著特征,而且认知的所有模型都以各种形式使用联想作为其基本行为。

联想有两种方式:自联想和异联想。在自联想方式中,神经网络被要求通过不断出示一系列模式(向量)给网络而存储这些模式。其后将某已存模式的部分描述或畸变(噪声)形式出示给网络,网络的任务是检索(回忆)已存储的该模式。异联想与自联想的不同之处在于一个任意的输入模式集合与另一个输出模式集合配对。自联想需要使用无监督学习,而异联想采用监督学习。

假设 $\mathbf{x}_k$ 表示在联想记忆中的关键模式, $\mathbf{y}_k$ 表示存储模式。网络完成的模式联想为

$$\mathbf{x}_k \rightarrow \mathbf{y}_k, k=1, \dots, q \quad (1.8)$$

式中, q 是存储在网络中的模式数。 $\mathbf{x}_k$ 作为输入,不仅决定 $\mathbf{y}_k$ 的存储位置,而且拥有恢复该模式的键码。

在自联想方式中, $\mathbf{y}_k = \mathbf{x}_k$, 所以输入、输出数据的空间维数相同。在异联想方式中, $\mathbf{y}_k \neq \mathbf{x}_k$, 因此输入、输出数据的空间维数可能相同,也可能不同。

模式联想器输入、输出关系如图 1.22 所示。

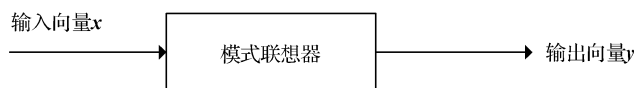


图 1.22 模式联想器输入、输出关系

联想记忆模式的操作一般包括两个阶段。

(1) 存储阶段,这阶段根据式(1.8)对网络进行训练。

(2) 回忆阶段,网络根据呈现的有噪声的或畸变的关键模式恢复对应的存储模式。

令刺激(输入) $\mathbf{x}$ 表示关键模式 $\mathbf{x}_j$ 的有噪声或畸变形式。如图 1.22 所示,这个刺激产生响应(输出) $\mathbf{y}$ 。对理想的回忆来说,我们有 $\mathbf{y} = \mathbf{y}_j$, 其中 $\mathbf{y}_j$ 为由 $\mathbf{x}_j$ 联想的记忆模式。如果对 $\mathbf{x} = \mathbf{x}_j$ 来说有 $\mathbf{y} \neq \mathbf{y}_j$, 那么表示联想记忆有回忆错误。

联想记忆中存储的模式数 q 提供网络存储能力的一个直接度量。在设计联想记忆时,关

键是使存储能力 q （表示与构建网络的神经元总数 N 的百分比）尽量大，并且保持记忆中的大部分模式能被正确回忆。

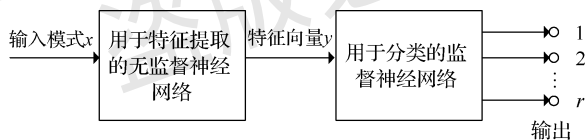
2) 模式识别

人类是通过学习过程来成功地实现模式识别的，神经网络也是如此。

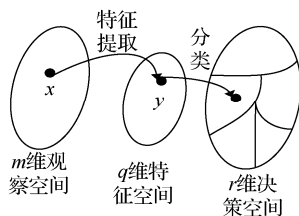
模式识别被形式地定义为一个过程，由这个过程接收到的模式或信号确定为一些指定类中的一个类。神经网络要实现模式识别首先需要通过训练过程，在此过程中，网络会不断地接受一个模式集合及每个特定模式所属的类；然后把一个以前没有见过但属于用于训练网络的同一模式总体的新模式呈现给神经网络。神经网络能根据从训练数据中提取的信息识别特定模式的类。神经网络的模式识别本质上是基于统计特性的，各个模式可表示成多维决策空间的一些点。决策空间被划分为不同的区域，每个区域都对应一个模式类。决策边界由训练过程决定。我们可以根据各个模式类内部及它们之间的固有可变性统计方式来确定边界。

模式识别是神经网络诞生时就应用的领域之一。最开始的感知器可以用于求解线性分类问题，后来的 BP 神经网络能求解非线性分类问题。神经网络应用于模式识别时，可以将神经网络作为单独的分类器使用，也可以将神经网络作为特征提取器和模式分类器一起使用。一般来说，采用神经网络的模式识别机分为如下两种形式。

(1) 如图 1.23 (a) 的混合系统所示，模式识别机分为两部分：用作特征提取的无监督神经网络和作为分类的监督网络。这种方法遵循传统的统计特性模式识别方法。用概念术语表示，一个模式是一个 m 维的可观察数据，即 m 维观察空间中的一个点 x 。如图 1.23 (b) 所示，特征提取被描述成一个变换，它将点 x 映射成一个 q 维特征空间对应的中间点 y ($q < m$)。这种变换可视为维数缩减（数据压缩），这种做法主要是为了简化分类任务。分类本身可描述为一个变换，它将中间点 y 映射成 r 维决策空间上的一个类，其中 r 是要区分的类别数。



(a) 混合系统



(b) 空间映射

图 1.23 模式分类的两种方法

(2) 设计一个采用监督学习算法的前馈神经网络，在这种方法中，特征提取由网络的隐含层的计算单元执行。

3) 函数逼近

函数逼近是一个令人感兴趣的学习任务。考虑由函数关系 $d = f(x)$ 描述的一个非线性输入、输出映射，其中向量 x 是输入，向量 d 是输出。向量值函数 $f(\cdot)$ 假定为未知。为了弥补

函数 $f(\cdot)$ 知识的缺乏, 我们假定有如下的有标号的样例集合 $\Gamma = \{\mathbf{x}_i, \mathbf{d}_i\}_{i=1}^N$, 要求设计一个神经网络用于逼近未知函数 $f(\cdot)$, 使由网络实际实现的描述输入、输出映射的函数 $F(\cdot)$ 在欧几里得距离的意义下与 $f(\cdot)$ 足够接近, 即

$$\|F(\mathbf{x}) - f(\mathbf{x})\| < \varepsilon, \text{ 对于所有的 } \mathbf{x} \quad (1.9)$$

式中, ε 是一个很小的正数。假定 Γ 的样本数 N 足够大, 神经网络也有适当数目的权值, 那么对于特定的任务, 逼近误差 ε 应该是足够小的。

本质上来说, 函数逼近问题其实是一个很完整的监督学习, 其中 $\mathbf{x}_i$ 是输入向量, $\mathbf{d}_i$ 是期望响应。我们也可以将监督学习看作一个逼近问题。神经网络逼近一个未知输入、输出映射的能力可以从两个重要途径加以利用: 系统辨识和逆模型。

4) 控制

神经网络的一个重要学习任务是对设备进行控制操作。这里的设备是指一个过程或在被控条件下维持运转的系统的一个关键部分。人脑就是一个计算机(信息处理器), 作为整个系统的输出是实际的动作, 也就是控制。在控制的这种意义下, 人脑是一个生动的例子, 它证明可以建立一个广义控制器, 充分利用并行分布式硬件, 能够并行控制多个制动器(如肌肉神经纤维), 处理非线性和噪声, 并且可以在长期计划水平上进行优化。

图 1.24 所示为反馈控制系统的框图。该系统涉及利用被控设备的单元反馈, 即设备的输出直接反馈给输入。因此设备输出 $\mathbf{y}$ 减去从外部信息源提供的参考信号 $\mathbf{d}$, 产生误差信号 $\mathbf{e}$, 并将其应用到控制器, 以便调节它的权值。控制器的主要功能是为设备提供相应的输入, 从而使设备输出 $\mathbf{y}$ 跟踪参考信号 $\mathbf{d}$ 。也就是说, 控制器不得不对设备的输入、输出行为进行转换。

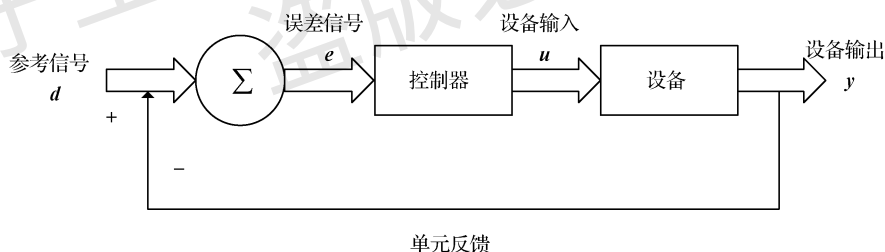


图 1.24 反馈控制系统的框图

在图 1.24 中, 误差信号 $\mathbf{e}$ 在到达设备之前先通过控制器。结果, 根据误差-修正学习算法, 为了实现对设备权值的调节, 我们必须知道如下 Jacobi 矩阵

$$\mathbf{J} = \left\{ \frac{\partial y_k}{\partial u_j} \right\}_{j,k} \quad (1.10)$$

式中, y_k 是设备输出 $\mathbf{y}$ 的一个元素; u_j 是设备输入 $\mathbf{u}$ 的一个元素。令人遗憾的是, 偏导数 $\partial y_k / \partial u_j$ 对于不同的 k, j 依赖设备的运行点, 因而是未知的。可以采用如下两种方法来近似计算该偏导数。

(1) 间接学习。利用设备的实际输入、输出测量值, 首先构造神经网络模型, 产生一个它的复制品。然后利用这个复制品提供矩阵 $\mathbf{J}$ 的一个估计值。随后把构成矩阵 $\mathbf{J}$ 的偏导数用于误差-修正学习算法, 以便计算对控制器的突触权值的调节。

(2) 直接学习。偏导数的符号通常是已知的，且在设备的动态区域内一般是不变的。这表明我们可以通过各自的符号来逼近这些偏导数。它们的绝对值由控制器突触权值的一种分布式表示给出。因此神经控制能够直接从设备中学习如何调节它的突触权值。

5) 波束形成

波束形成是用来区分目标信号和背景噪声之间的空间性质的。用于实现波束形成的设备称为波束形成器。波束形成适合应用于如蝙蝠回声定位听觉定位系统的特征映射这样的任务。蝙蝠的回声定位根据发送短时频率调制声呐信号来了解周围环境，然后利用它的听觉系统集中注意于它的猎物（如飞行的昆虫）。蝙蝠的耳朵提供波束形成能力，听觉系统利用它产生注意选择性。

波束形成通常用于雷达和声呐系统，它们的基本任务是在接收器噪声和干扰信号出现的情况下探测和跟踪感兴趣的目标。

此处仅简单介绍波束形成的基本概念，更多信息请参考相关资料。

1.10 小结

本章介绍了神经网络的基本知识，给出了神经网络的概念，介绍了神经网络的生物学机理，探讨了人工神经元模型，重点阐述了神经网络的不同结构：前馈神经网络和反馈型神经网络，重点介绍了神经网络学习算法，最后总结了神经网络多种不同的学习任务。

神经网络是以生物神经网络为基础，模拟人脑的结构和功能建立的一种数学模型。神经网络首先需要构建其网络结构，其生命周期大体上可以分为训练阶段和测试阶段，其中更重要的是训练阶段。在训练阶段，利用某种学习算法或规则将神经网络的连接权值训练调整好，供测试阶段使用。所以神经网络最重要的是网络拓扑结构和训练阶段中的学习算法。神经网络的学习算法主要分为如下三种不同类型。

(1) 监督学习，通过最小化感兴趣的误差函数来实现特定的输入、输出映射，其中需要提供期望响应，属于有教师学习。

(2) 强化学习，其执行依赖提供网络在自组织方式下学习所需要的表示质量的任务独立度量。

(3) 无监督学习，学习系统通过持续地与环境交互来最小化一个标量性能指标，从而实现输入、输出映射。

监督学习依赖有标号的样例的训练样本，每个样例都由一个输入信号和对应的期望响应构成。但是在实际中，人工收集有标号的样例费时而昂贵，而且很多实际领域无法收集到大量标号。因此很多时候有标号的样例是短缺的。此外，无监督学习仅依赖无标号的样例，样例仅由输入信号或刺激构成，因而通常无标号的样例的供应很充分。在这种形势下，半监督学习研究引起了业界的高度关注。半监督学习的训练数据包括有标号和无标号的样例。半监督学习的最大挑战在于当处理大规模模式分类问题时如何设计学习系统，使其运行过程实际可行。

强化学习介于监督学习和无监督学习之间。它通过学习系统和环境之间的持续交互而工作。学习系统提供行动并从环境对该行动的反应中学习。

参考文献

- [1] SIMON H. 神经网络与机器学习[M]. 申富饶, 徐烨, 郑俊, 等译. 北京: 机械工业出版社, 2011.
- [2] MARTIN T H, HOWARD B D, MARK H B. 神经网络设计[M]. 章毅, 译. 北京: 机械工业出版社, 2017.
- [3] 王万森. 人工智能原理及其应用[M]. 北京: 电子工业出版社, 2018.
- [4] 埃塞姆·阿培丁. 机器学习导论[M]. 范明, 译. 北京: 机械工业出版社, 2016.

电子工业出版社版权所有
盗版必究