**机器学习**

机器学习定义：

机器学习是一类算法的总称，这些算法可以完成那些直接编程无法完成的功能，能从大量现有数据挖掘出其中暗含的规律，并用于预测或者分类，机器学习可以看作是寻找一个函数，其输入是样本数据，输出是期望的结果，只是这个函数过于复杂，以至于不太方便形式化表达。需要注意的是，机器学习的目标是使学到的函数很好地适用于“新样本”，而不仅仅是在训练样本上表现很好。学到的函数适用于新样本的能力，称为泛化能力。

机器学习的范围：语音

模式识别，统计学习，数据挖掘，计算机视觉，识别，自然语言处理等领域都与机器学习有着极深的联系。

从各自的范围上来说，机器学习与模式识别，统计学习，数据挖掘是类似的，同时，机器学习与其他领域的处理技术的结合，形成了计算机视觉、语音识别、自然语言处理等交叉学科。由此可见，一般说数据挖掘时，可以等同于说机器学习。同时，我们平常所说的机器学习应用，应该是通用的，不仅仅局限在结构化数据，还有图像，音频等应用。

模式识别 ：模式识别等于机器学习，区别在于发展来源的不同，前者是从工业界发展起来的，而后者主要源自计算机学科。在著名的《Pattern Recognition And Machine Learning》这本书中，Christopher M. Bishop在开头是这样说的“模式识别源自工业界，而机器学习来自于计算机学科。不过，它们中的活动可以被视为同一个领域的两个方面，同时在过去的10年间，它们都有了长足的发展”。

数据挖掘：数据挖掘是数据库与机器学习的结合，数据库提供数据管理技术，而机器学习提供数据分析技术。数据挖掘仅仅是一个思考的方式，让我们知道应该从数据中挖掘出有用的知识，但并不是所有的数据都是有效的，所以我们不应该太过于看中，相反更应该看中的是有数据挖掘思维的人才，并且还要对数据有更深的了解，这样才能从数据中挖掘出新的、准确的和有用的模式来改善功能。通过数据挖掘收集和处理的信息可以用来帮助机器学习。

统计学习：统计学习近似等于机器学习。机器学习中的大多数方法来自统计学，因此统计学习与机器学习高度重叠。但是在某种程度上两者是有区别的，统计学习是研究从一些样本出发得出不能通过原理分析得到的规律，利用这些规律去分析客观对象，对未来数据或无法观测的数据进行预测，而机器学习者更关注的是能够解决问题，因此机器学习研究者会注重研究学习算法在计算机上执行的效率与准确性的提升。  
　　　　  
计算机视觉：计算机视觉是图像处 理与机器学习的结合。图像处理技术用于将图像处理为适合进入机器学习模型中的输入，机器学习则负责从图像中识别出相关的模式。百度识图、手写字符识别、车牌识别等等应用都是利用计算机视觉。

语音识别：语音识别就是音频处理技术与机器学习的结合。[语音识别技术](https://baike.baidu.com/item/%E8%AF%AD%E9%9F%B3%E8%AF%86%E5%88%AB%E6%8A%80%E6%9C%AF" \t "https://baike.baidu.com/item/_blank)就是让机器通过识别和理解过程把语音信号转变为相应的文本或命令的高技术。　[语音识别技术](https://baike.baidu.com/item/%E8%AF%AD%E9%9F%B3%E8%AF%86%E5%88%AB%E6%8A%80%E6%9C%AF" \t "https://baike.baidu.com/item/_blank)主要包括特征提取技术、模式匹配准则及模型训练技术三个方面。生活中很多地方也是利用了语音识别左永刚，例如导航的语音助手和苹果的手机助手，siri。

自然语言处理：自然语言处理是文本处理与机器学习的结合。自然语言处理技术主要是研制能有效地实现自然语言通信的[计算机系统](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%B3%BB%E7%BB%9F/7210959" \t "https://baike.baidu.com/item/_blank)。在自然语言处理技术中，大量使用了编译原理相关的技术，例如词法分析，语法分析等等，除此之外，在理解这个层面，则使用了语义理解，机器学习等技术。语言是人类所特有的东西，如何利用机器学习技术进行自然语言的深度理解，一直是工业和学术界关注的焦点。

**机器学习的方法：**

**机器学习算法大致可分为可分为三类：**

**监督学习算法**：在监督学习训练过程中，需要给出有正确标签的数据集，训练后能给新数据以正确的标签。例如将邮件进行是否垃圾邮件的分类，我们先把大量的邮件打好标签让进行训练，学习模型找出标签与邮件的联系进行完善和调整，最后训练出的模型能识别没有标签的邮件。主要算法包括神经网络、支持向量机、最近邻居法、朴素贝叶斯法、决策树等。主要包括：[线性回归](https://easyai.tech/ai-definition/linear-regression/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)、[逻辑回归](https://easyai.tech/ai-definition/logistic-regression/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)、[线性判别分、析](https://easyai.tech/ai-definition/linear-discriminant-analysis/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)、[决策树](https://easyai.tech/ai-definition/decision-tree/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)、[朴素贝叶斯](https://easyai.tech/ai-definition/naive-bayes-classifier/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)、[K邻近](https://easyai.tech/ai-definition/k-nearest-neighbors/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)、[学习向量量化](https://easyai.tech/ai-definition/learning-vector-quantization/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)、[支持向量机](https://easyai.tech/ai-definition/svm/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)、[随机森林](https://easyai.tech/ai-definition/random-forest/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)、[AdaBoost](https://easyai.tech/ai-definition/adaboost/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)。

**无监督的学习：**算法没有特定的输出目标，将数据集分为不同的组。主要包括：最大期望算法、[K-means 聚类](https://easyai.tech/ai-definition/k-means-clustering/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)、[限制波尔兹曼机](https://easyai.tech/ai-definition/restricted-boltzmann-machine/" \t "https://easyai.tech/ai-definition/machine-learning/_blank)、高斯混合模型。

**强化学习算法：**机器被放置在一个特定环境中，它可以根据输出结果的成功或错误来不停地自我训练，经过大量经验训练优化后的算法能够给出很好的预测。

1. 回归算法

回归算法比较简单，目的是了解两个或多个变量间是否相关、相关方向与强度，并建立数学模型以便观察特定变量来预测其它变量的变化情况。回归算法有两个重要的子类：线性回归和逻辑回归。线性回归算法的建模过程是使用数据点来寻找最佳拟合线，而逻辑回归是一个二分类问题，本质是线性回归，只是在计算结果加了Sigmoid函数来归一化因变量值，使其在(0,1)内，可以根据处理后的值进行预测。

1. 支持向量机算法

支持向量机/网络算法(SVM)属于分类型算法。SVM通过跟高斯“核”的结合，支持向量机可以表达出非常复杂的分类界线，从而达成很好的的分类效果。“核”事实上就是一种特殊的函数，最典型的特征就是可以将低维的空间映射到高维的空间。需要注意的是，支持向量机需要对输入数据进行完全标记，仅直接适用于两类任务，应用将多类任务需要减少到几个二元问题。

1. 深度学习

深度学习是指多层的人工神经网络和训练他的方法。一层神经网络会把大量矩阵数字作为输入，通过非线性激活方法取权重，再产生另一个集合作为输出。

深度学习的实质，是通过构建具有很多隐层的机器学习模型和海量的训练数据，来学习更有用的特征，从而最终提升分类或预测的准确性。因此，“深度模型”是手段，“特征学习”是目的。

深度学习的基本思想：

假设系统S有n层（S1，…,Sn），输入为I，输出为0，可表为：I=>S1=>S2=>.....=>Sn => O，若输出O等于输入I，则是输入I经过系统变化之后没有任何的信息损失，信息没发生变化，这意味着输入I经过每一层Si都不会有信息损失，即任意一层Si都是原有信息的另一种表示。那么深度学习，是自动地学习特征，当我们向系统S输入一堆I（如一堆图像或者文本），我么通过调整系统参数，使得它的输出仍是输入I，那么我们就可以自动地获取输入I的一系列层次特征，即S1，..., Sn。假如我们使输入与输出仅有细小的差别，这个条件的放松会导致另外一类不同的Deep Learning方法。

深度学习的训练过程：

　　1、使用自下上升非监督学习：

　　采用无标签数据（有标签数据也可）分层训练各层参数，这一步可以看作是一个无监督训练过程，是和传统神经网络区别最大的部分（这个过程可以看作是feature learning过程）：

　　实际中，先用无标签数据训练第一层，训练时先学习第一层的参数（这一层可以看作是得到一个使得输出和输入差别最小的三层神经网络的隐层），由于模型capacity的限制以及稀疏性约束，使得得到的模型能够学习到数据本身的结构，从而得到比输入更具有表示能力的特征；在学习得到第n-1层后，将n-1层的输出作为第n层的输入，训练第n层，由此分别得到各层的参数；

　　2、自顶向下的监督学习（就是通过带标签的数据去训练，误差自顶向下传输，对网络进行微调）：

　　基于第一步得到的各层参数进一步fine-tune整个多层模型的参数，这一步是一个有监督训练过程；第一步类似神经网络的随机初始化初值过程，由于DL的第一步不是随机初始化，而是通过学习输入数据的结构得到的，因而这个初值更接近全局最优，从而能够取得更好的效果；所以deep learning效果好很大程度上归功于第一步的feature learning过程。

四种经典的深度学习算法：

1、卷积神经网络 （CNN） ：能够将大数据量的图片有效的降维成小数据量(并不影响结果)能够保留图片的特征，类似人类的视觉原理

CNN包括：卷积层、池化层、全连接层，卷积层主要作用是保留图片的特征，池化层主要作用是把数据降维，可以有效的避免过拟合，全连接层根据不同任务输出我们想要的结果。

CNN 的实际应用：图片分类、检索，目标定位检测，目标分割，人脸识别，骨骼识别

1. 循环神经网络（RNN）：RNN 是一种能有效的处理序列数据的算法。比如：文章内容、语音音频、股票价格走势……之所以他能处理序列数据，是因为在序列中前面的输入也会影响到后面的输出，相当于有了“记忆功能”。但是 RNN 存在严重的短期记忆问题，长期的数据影响很小。

于是基于 RNN 出现了 LSTM 和 GRU 等变种算法。这些变种算法主要有几个特点：长期信息可以有效的保留，挑选重要信息保留，不重要的信息会选择“遗忘”。

## RNN 几个典型的应用如下：文本生成、语音识别、机器翻译、生成图像描述、视频标记。

## 3、生成对抗网络 (GANs)：[GANs](https://arxiv.org/abs/1406.2661)的核心思想源自于零和博弈，包括生成器和判别器两个部分。生成器接收随机变量并生成“假”样本，判别器则用于判断输入的样本是真实的还是合成的。两者通过相互对抗来获得彼此性能的提升。判别器所作的其实就是一个二分类任务，我们可以计算他的损失并进行反向传播求出梯度，从而进行参数更新。

4、深度强化学习

人工神经网络

人工神经网络有着重要的三个基础的知识点：一是神经元模型；二是神经网络结构；三是学习算法。

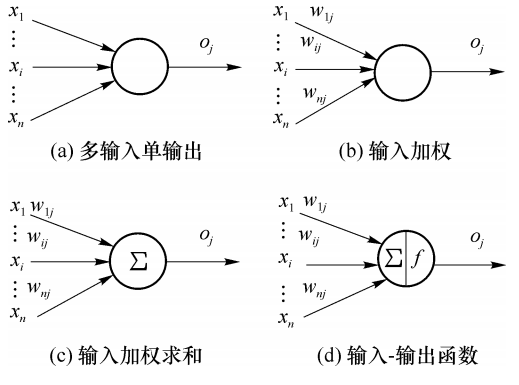
神经元模型：

人工神经网络实在现代神经生物学研究基础上提出的模拟生物过程，它反映了人类某些特性的一种算法，是对人脑神系统的一柱抽象、简化和模拟。在生物神经网络中神经元与突触是神经网络的基本单元。所以在模拟神经网络结构之前应先模拟神经元，在人工神经网络中，神经元常被称为“处理单元”，从网络的结构来看也可以叫做“节点”。人工神经元是用数学语来抽象生物神经元的信息处理过程。

1. 神经元建模：M-P模型经过不断改善后，形成了摸钱广泛应用的形式神经元模型。关羽神经元的信息处理机制，该模型再简化的基础上提出了6点假定进行描述：

（１） 每个神经元都是一个多输入单输出的信息处理单元 ；  
（２） 神经元输入分兴奋性输入和抑制性输入两种类型 ；  
（３） 神经元具有空间整合特性和阈值特性 ；  
（４） 神经元输入与输出间有固定的时滞 ，主要取决于突触延搁 ；  
（５） 忽略时间整合作用和不应期 ；  
（６） 神经元本身是非时变的 ， 即其突触时延和突触强度均为常数 。

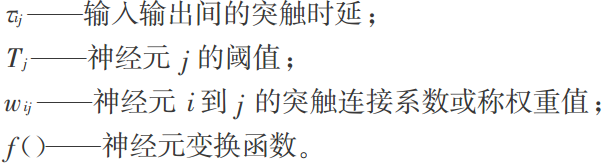
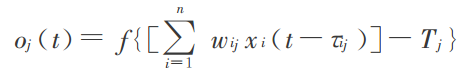
基于上面的6条假设，神经元建模图示如下：



实际上表达就是一个整合∑、映射F的数学建模。

1. 神经元的数学模型

由神经元模型示意图，可以得到神经元的数学模型如下：



若将阈值参数作为输入端与w0权值整合到∑当中，就可以得到如下的简化形式：

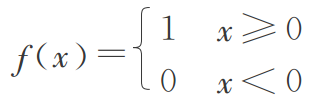
IMG_258

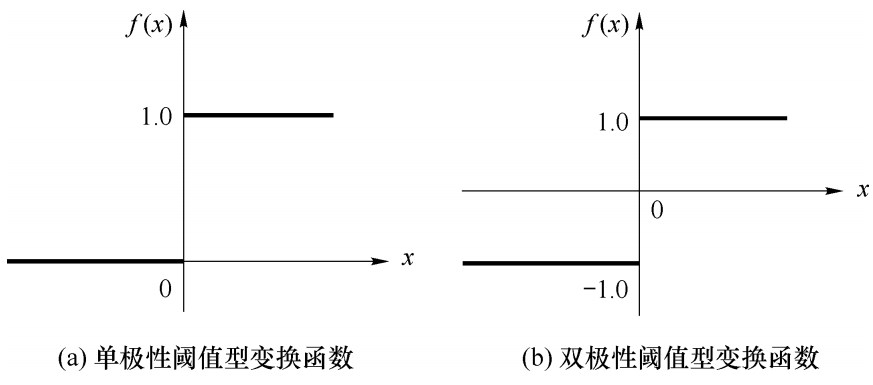
3. 神经元的激活函数（映射F）

神经元的不同数学模型主要的区别在于采用了不同的变化函数，从而使神经元具有不同的信息处理特性。神经元的信息处理特性决定着人工神经网络整体性能的三大要素之一 ，因此变换函数是非常的重要。最常用的变换函数有以下四种形式。

1. 阈值型变换函数

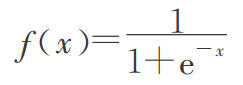
采用单位阶跃响应函数，如图

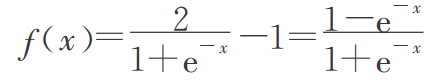


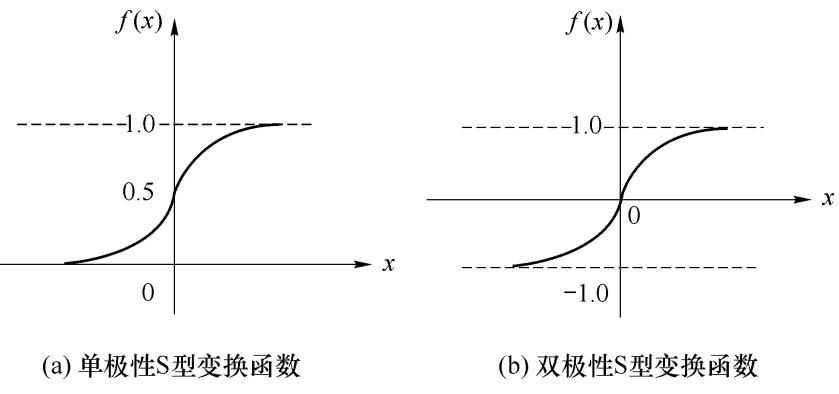


### 非线性变换函数

非线性变换函数为实数域R到[0,1]闭集的非减连续函数，代表状态连续型神经元模型，常用Sigmoid 函数曲线，也称S型函数。单极性以及双极型S型函数公式及图示如图：

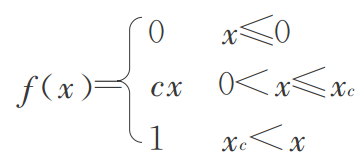


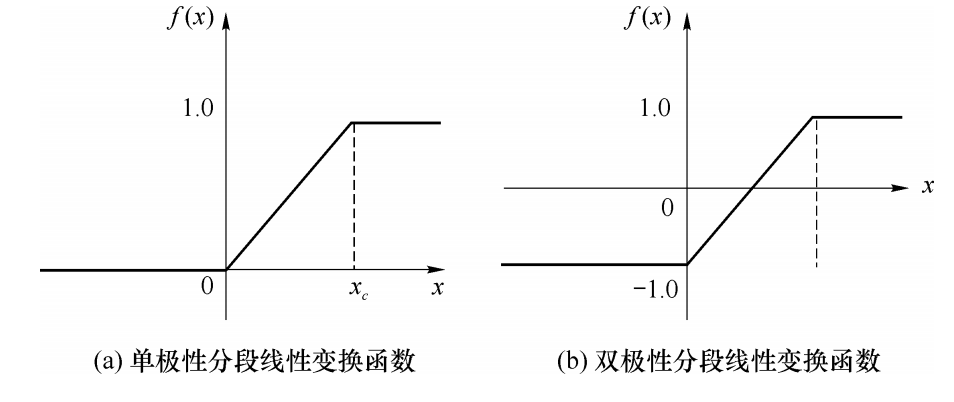




1. 分段线性变换函数

该函数的特点是神经元的输入与输出在一定区间内满足线性关系。单极性分段线性变换函数如图：





1. 概率型变换函数

采用该函数的神经元模型其输入与输出之间的关系使不确定的，需要一个随机函数来描述其输出的状态为1或为0 的概率。

神经网络结构：

庞大的神经网络是由大量的神经元组成，能实现对复杂信息的处理与储存，并表现出表现出各种优越的特性。神经网络有如此强大功能与其的结构有很大的关系，神经元按照特定的一定的规则连在一起形成神经网络。人工神经网络中的神经元都具有相同的结构，其动作在时间和空间上均同步。

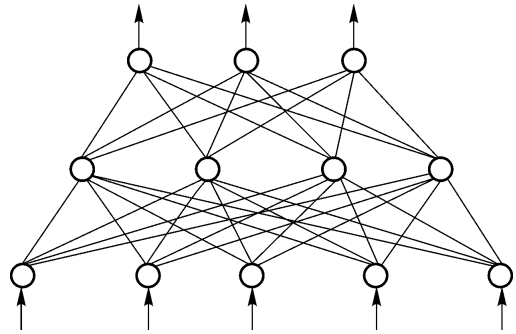
人工神经网络模型常见的两种分类方法：按网络连接的拓扑结构分类和按网络内部的信息流向分类。

1、网络拓扑结构类型

神经元之间的连接方式不同，网络的拓朴结构也不同。根据神经元之间连接方式，可将神经网络结构分为两大类。

（1）层次型

具有层次型结构的神经网络将神经元按功能分成若干层，如输入层、中间层（也称为隐层）和输出层，各层顺序相连，如图：

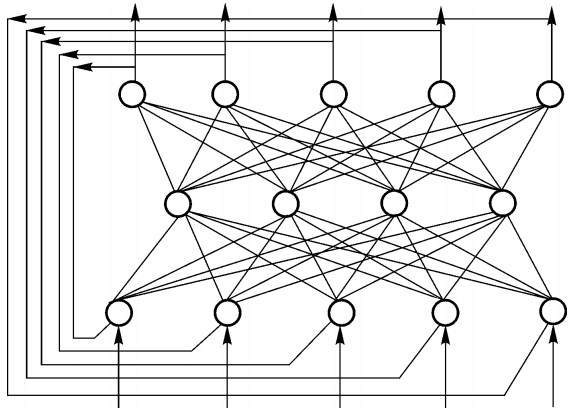


输入层各神经元负责接收来自外界的输入信息，并传递给中间各隐层神经元；隐层是神经网络的内部信息处理层，负责信息变换，根据信息变换能力的需要，隐层可设计为一层或多层；最后一个隐层传递到输出层各神经元的信息经进一步处理后即完成一次信息处理，由输出层向外界输出信息处理结果。层次型网络结构有３种典型的结合方式。

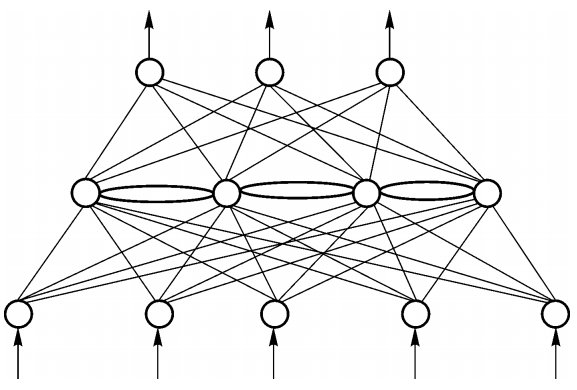
(A) 单纯型层次网络结构

神经元分层排列，各层神经元接收前一层输入并输出到下一层，层内神经元自身以及神经元之间不存在连接通路。

(B) 输出层到输入层有连接的层次网络结构，输入层神经元既可接收输入，也具有信息处理功能，如图：



(C) 层内有互连的层次网络结构，这种结构的特点是在同一层内引入神经元间的侧向作用，使得能同时激活的神经元个数可控，以实现各层神经元的自组织，如图：

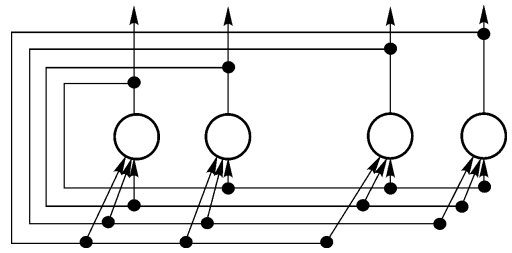


（2）互连型结构

对于互连型网络结构，网络中任意两个节点之间都可能存在连接路径，因此可以根据网络中节点的互连程度将互连型网络结构细分为３种情况。

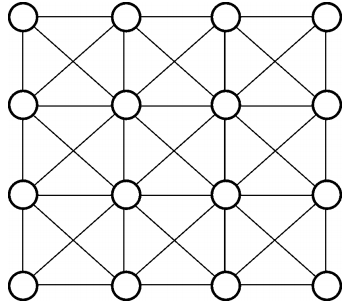
1. 全互连型

网络中的每个节点均与所有其他节点连接，如图：



(B) 局部互连型

网络中的每个节点只与其邻近的节点有连接，如图：



(C) 稀疏连接型

网络中的节点只与少数相距较远的节点相连。

2. 网络信息流向类型

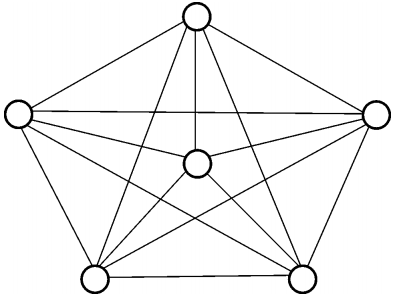
根据神经网络内部信息的传递方向，可分为两种类型。

（1） 前馈型网络

前馈是因网络信息处理的方向是从输入层到各隐层再到输出层逐层进行而得名 。网络中的节点从信息处理能力看可分为两种：一种是输入节点，只负责从外界引入信息后向前传递给第一隐层；另一种是具有处理能力的节点，包括各隐层和输出层节点。前馈网络中某一层的输出是下一层的输入，信息的处理具有逐层传递进行的方向性，一般不存在反馈环路。

（2）反馈型网络

在反馈网络中所有节点都具有信息处理功能，而且每个节点既可以从外界接收输入，同时又可以向外界输出。单纯全互连结构网络是一种典型的反馈型网络，可以用下图所示的完全的无向图表示：



神经网络学习

人工神经网络的功能特性由其连接的拓扑结构和突触连接强度，即连接权值决定。神经网络全体连接权值的可用一个矩阵W表示，它的整体反映了神经网络对于所解决问题的知识存储。神经网络能够通过对样本的学习训练，改变网络的连接权值以及拓扑结构，以达到输出更加接近期望的输出。这就是神经网络的学习或训练，本质为可改变权值的动态调整。神经网络的学习方式是决定神经网络信息处理的第三大要素，因此对于学习的研究在神经网络研究具有重要的作用。神经网络的学习算法很多，通常将神经网络的学习算法归纳为３类。一类是有导师学习，一类为无导师学习，还有一类是灌输式学习。有导师学习也称为有监督学习，这种学习模式采用的是纠错规则。在训练过程中需要不断输入正确标签的数据集和所对应期望的输出结果。将神经网络输出结果与期望结果进行对比，当输出与期望不符时，根据差错的方向和大小按一定的规则调整权值，以使下一步网络的输出更接近期望结果。无导师学习也称为无监督学习，学习过程中，

需要不断提供动态输入信息，网络能根据自身的内部结构和学习规则，在输入信息中发现任何可能存在的模式和规律，同时根据网络的功能和输入信息调整权值，这个过程称为自组织，其结果为对输入的信息进行自动分类。灌输式学习中网络的权值不是通过训练逐渐形成的，而是通过某种设计方法得到的，权值一旦设计好即一次性“灌输”给神经网络不再变动。

训练学习的目的是为了从训练数据中提取隐含的知识和规律，并存储于网络中供工作阶段使用。

<https://www.cnblogs.com/wangzhongqiu/p/9856628.html>

<https://www.cnblogs.com/zlslch/p/6965585.html>

<https://blog.csdn.net/weixin_41152041/article/details/107231890>

https://zhuanlan.zhihu.com/p/33794257#:~:text=Machine%20Learning%3A%20%E5%8D%81%E5%A4%A7%E6%9C%BA%E5%99%A8%E5%AD%A6%E4%B9%A0%E7%AE%97%E6%B3%95%201%20%E7%BA%BF%E6%80%A7%E5%9B%9E%E5%BD%92%E7%AE%97%E6%B3%95%20Linear%20Regression%202,%E9%99%8D%E7%BB%B4%E7%AE%97%E6%B3%95%20Dimensional%20Reduction%2010%20%E6%A2%AF%E5%BA%A6%E5%A2%9E%E5%BC%BA%E7%AE%97%E6%B3%95%20Gradient%20Boosting.%20

https://wiki.mbalib.com/wiki/%E6%B7%B1%E5%BA%A6%E5%AD%A6%E4%B9%A0

https://www.cnblogs.com/huty/p/8519249.html