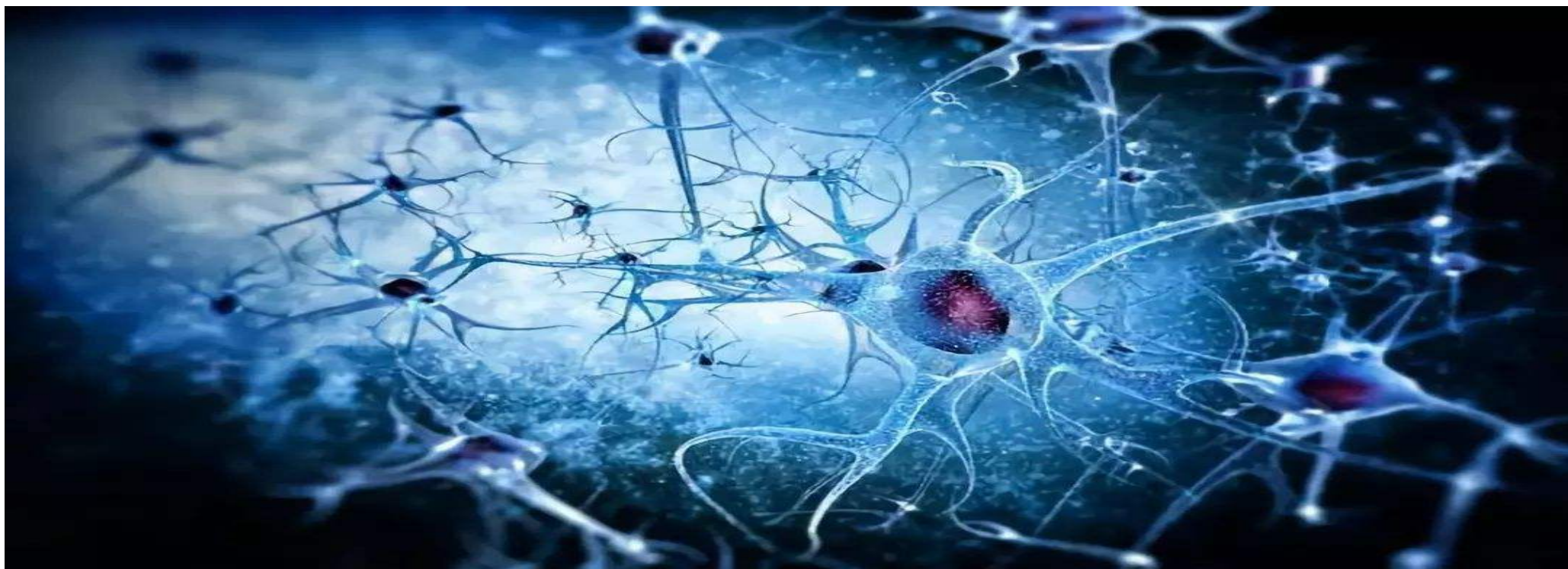


第七章 神经计算



神经计算

- 最早人们并不知人的“智慧”是人的大脑的功能，以为“智慧”是从“肚子”中来，如说“宰相肚里能撑船”；又如以为智慧是发自“心”，如说“某人很有心计”。直到近代科学才明确，智慧（思维）是人的大脑的功能的表现。
- 大脑是由无数的脑细胞组成。既然“思维”是大脑的功能的表现，即智慧是脑神经网络的功能。那么人们希望利用人工神经网络来模拟人脑的神经网络，研究其性能，希望从中悟出人的思维的一些“奥秘”。这就是所谓的人工神经网络技术，这种技术为人工智能提供新的解决问题的方法，并广泛应用于各个领域

生物神经系统

- 生物神经系统是一个有高度组织和相互作用的数量巨大的细胞组织群体。
- 神经细胞也称**神经元**，是**神经系统的基本单元**，它们按不同的结合方式构成了复杂的神经网络。**通过神经元及其联接的可塑性，使得大脑具有学习、记忆和认知等各种智能。**

生物神经系统

- 生物神经元主要由以下3个部分组成：
 - **细胞体**，是神经细胞的本体；
 - **树突**，用于接受来自其它细胞元的信号；
 - **轴突**，用于输出信号，与多个神经元连接；
-
- **突触**，是神经元之间相互连接的的接口部分，即一个神经元的神经末梢与另一个神经元的树突相接触的交界面，位于神经元的神经末梢尾端。

神经元结构

树突

- Dendrites (inputs)

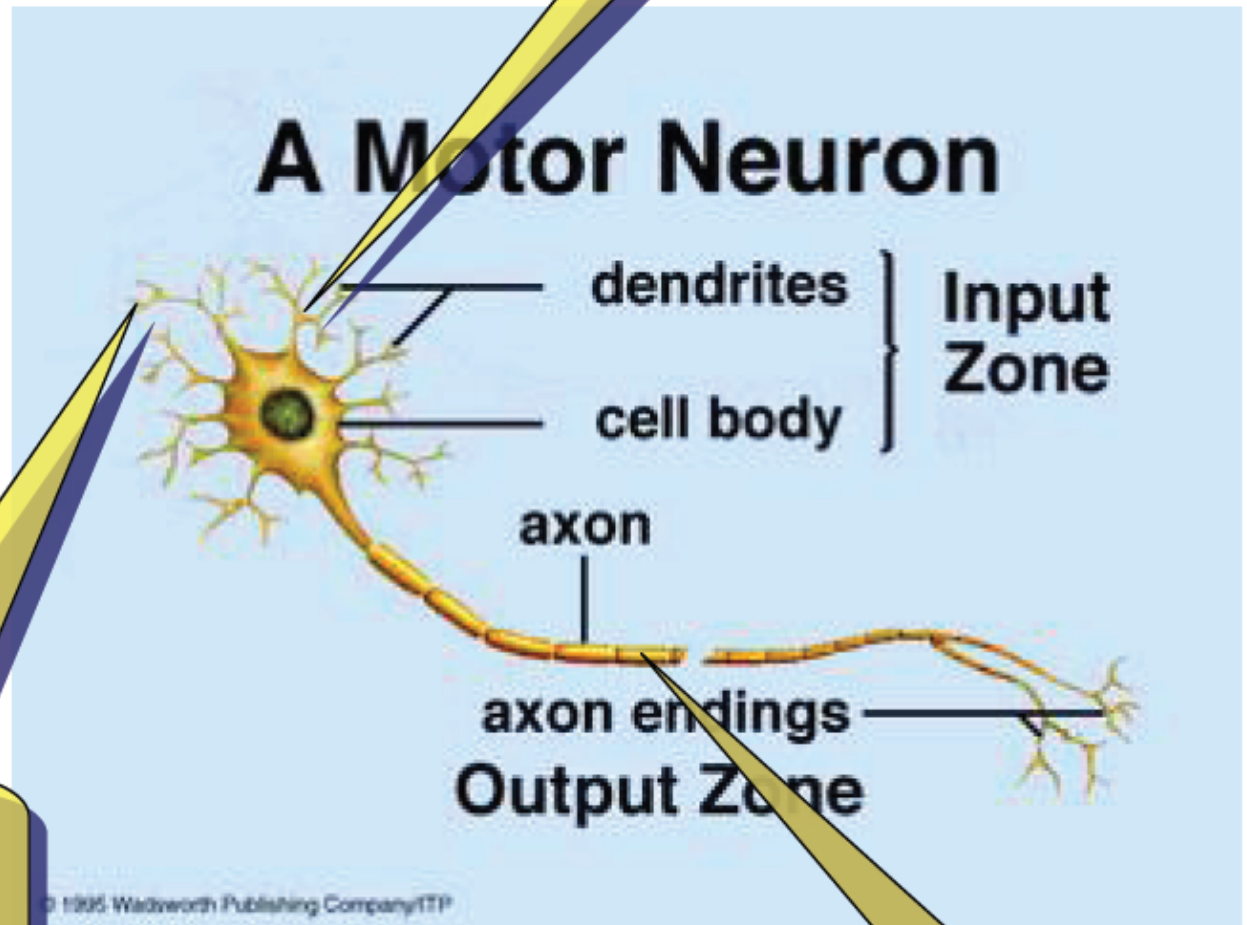
细胞体

- Cell body

轴突

- Axon (output)

二神经元之神经丝接合部



树状突

轴突

生物神经元的基本工作机制

一个神经元有两种状态-**兴奋和抑制**。

平时处于**抑制状态**的神经元，其**树突和细胞体**接受其它神经元经由**突触**传来的兴奋电位，多个输入在神经元中以代数和的方式叠加。

如输入兴奋总量超过**阈值**，神经元被激发进入**兴奋状态**，发出输出脉冲，由轴突的突触传递给其它神经元。

生物神经特性

(1) 并行分布处理的工作模式

实际上大脑中单个神经元的信息处理速度是很慢的，每次约1毫秒(ms)，比通常的电子门电路要慢几个数量级。每个神经元的处理功能也很有限，估计不会比计算机的一条指令更复杂。但是人脑对某一复杂过程的处理和反应却很快，一般只需几百毫秒。由此可见，**大脑信息处理的并行速度已达到了极高的程度。**

生物神经特性

(2) 神经系统的可塑性和自组织性。

神经系统的可塑性和自组织性与人脑的生长发育过程有关。

例如，人的幼年时期约在9岁左右，学习语言的能力十分强，说明在幼年时期，大脑的可塑性和柔软性特别良好。从生理学的角度看，它体现在**突触的可塑性和联接状态的变化**，同时还表现在神经系统的自组织特性上。例如在某一外界信息反复刺激下，接受该信息的神经细胞之间的**突触结合强度会增强**。这种可塑性反映出大脑功能既有先天的制约因素，也有可能通过后天的训练和学习而得到加强。

神经网络的学习机制就是基于这种可塑性现象，并通过修正突触的结合强度来实现的。

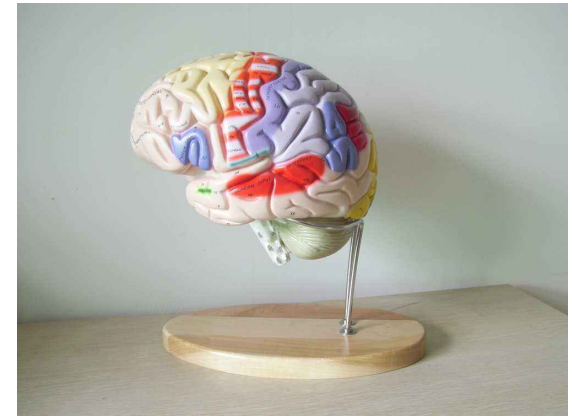
生物神经特性

(3) 信息处理与信息存贮合二为一。

大脑中的信息处理与信息存贮是有机结合在一起的，而不像现行计算机那样。存贮地址和存贮内容是彼此分开的。由于大脑神经元兼有信息处理和存贮功能，所以在进行回忆时，不但不存在先找存贮地址而后再调出所存内容的问题，而且还可以由一部分内容恢复全部内容。

生物神经特性

(4) 信息处理的系统性



大脑是一个复杂的大规模信息处理系统，单个的元“神经元”不能体现全体宏观系统的功能。实际上，可以将大脑的各个部位看成是一个大系统中的许多子系统。各个子系统之间具有很强的相互联系，一些子系统可以调节另一些子系统的行为。例如，视觉系统和运动系统就存在很强的系统联系，可以相互协调各种信息处理功能。

生物神经特性

(5) 能接受和处理模糊的、模拟的、随机的信息。

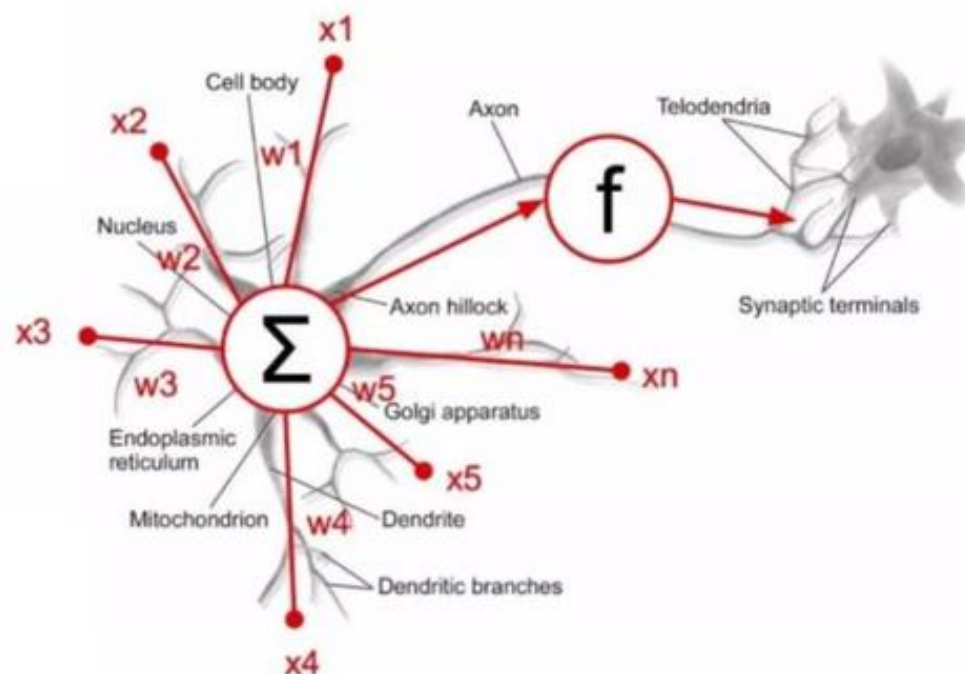
(6) 求满意解而不是精确解。

人类处理日常行为时，往往都不是一定要按最优或最精确的方式去求解，而是以能解决问题为原则，即求得满意解就行了。

(7) 系统的恰当退化和冗余备份（鲁棒性和容错性）

人工神经网络

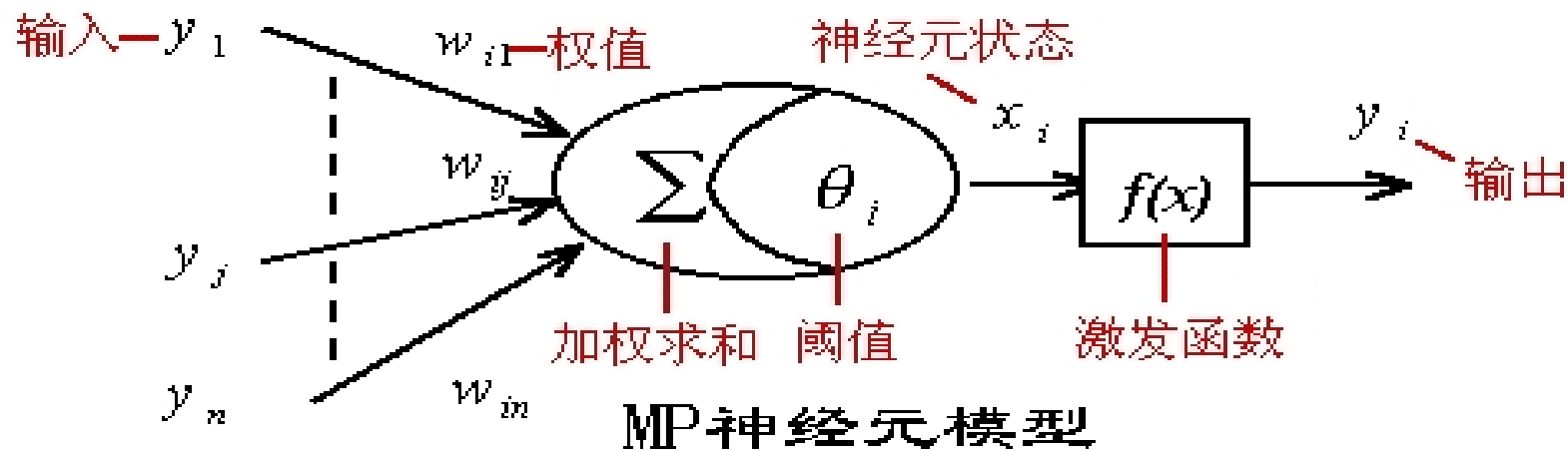
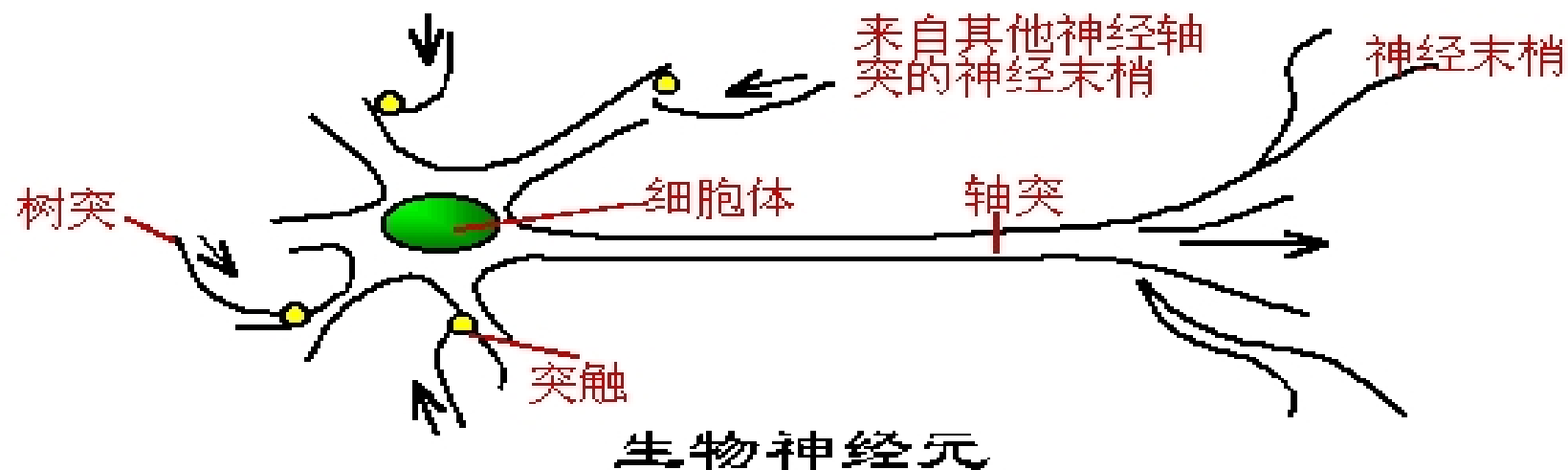
- **人工神经网络** (Artificial Neural Network, ANN) 是由大量处理单元经广泛互连而组成的人工网络，用来模拟脑神经系统的结构和功能。而这些处理单元称作**人工神经元**。



人工神经网络的结构

- 结构：**人工神经网络**（ANN）可以看成是以人工神经元为结点，用有向加权弧连接起来的**有向图**。
- 在此有向图中，**人工神经元**就是对**生物神经元**的模拟，而**有向弧**则是**树突—突触—轴突**对的模拟。**有向弧的权值**表示相互连接的两个**人工神经元**间相互作用的强弱。

人工神经网络的结构



人工神经网络的进展

- **初创阶段**（二十世纪四十年代至六十年代）
 - ◆ 1943年，美国心理学家W. S. McCulloch和数理逻辑学家W. Pitts 合作，以数学逻辑为研究手段，探讨了客观事件在神经网络的形式问题，在此基础上提出了神经元的数学模型，即MP（McCulloch-Pitts）模型。
 - ◆ 1960年，威德罗和霍夫率先把神经网络用于自动控制研究。
- **过渡阶段**（二十世纪六十年代初至七十年代）
 - ◆ M. Minsky和S. Papert经过多年的潜心研究，于1969年出版了影响深远的《Perceptron》一书，从理论上证明了以单层感知机为代表的网络系统在某些能力方面的局限性。
 - ◆ 60年代末期至80年代中期，神经网络控制与整个神经网络研究一样，处于低潮

人工神经网络的进展

- **高潮阶段（二十世纪八十年代）**
- ◇ 1982和1984年，美国加州理工学院的生物物理学家，J. Hopfield 在美国科学院院刊发表的两篇文章，有力地推动了人工神经网络的研究与应用，并引发了研究神经网络的一次热潮。
- ◇ 80年代后期以来，随着人工神经网络研究的复苏和发展，对神经网络控制的研究也十分活跃。这方面的研究进展主要在神经网络自适应控制和模糊神经网络控制及其在机器人控制中的应用上
- **平稳发展阶段（二十世纪九十年代以后）**

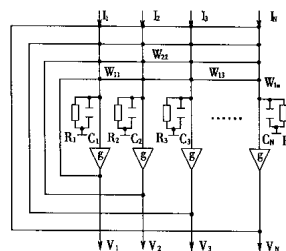
神经网络发展史



Donald Hebb
心理学/数学家
Hebb学习规则
1949年



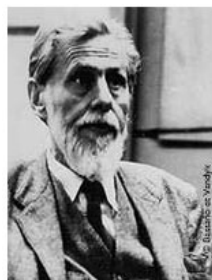
Minsky & Papert
《Perceptron》
，进入相对低潮
阶段1969年



Hopfield
Hopfield模型
1982年
(第二次研究高潮)



W.S. McCulloch
h/W. Pitts
MP模型
1943年

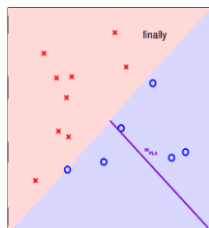


Warren McCulloch



Walter Pitts

F. Rosenblatt
1957年 **Perceptron**
(最早神经网络)
(第一次研究高潮)



Paul Werbos
反向传播训练
算法
1974年



DBN, CNN, AE
VAE, RNN,
GAN
2006年
第三次研究高潮

从海量数据/大数据中学习并理解数据，是现今深度学习技术研究和产品发展的驱动力。



Paul Werbos



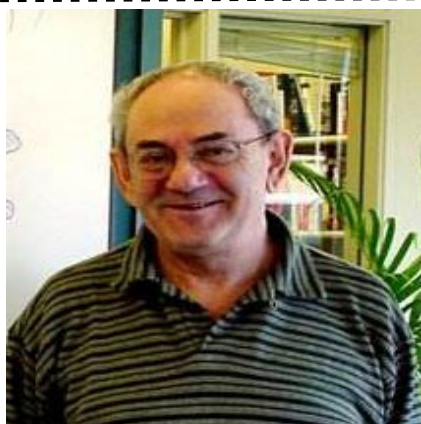
Hopfield



Michael I. Jordan



Geoffrey Hinton



Vladimir Vapnik



Yann LeCun



Yoshua Bengio

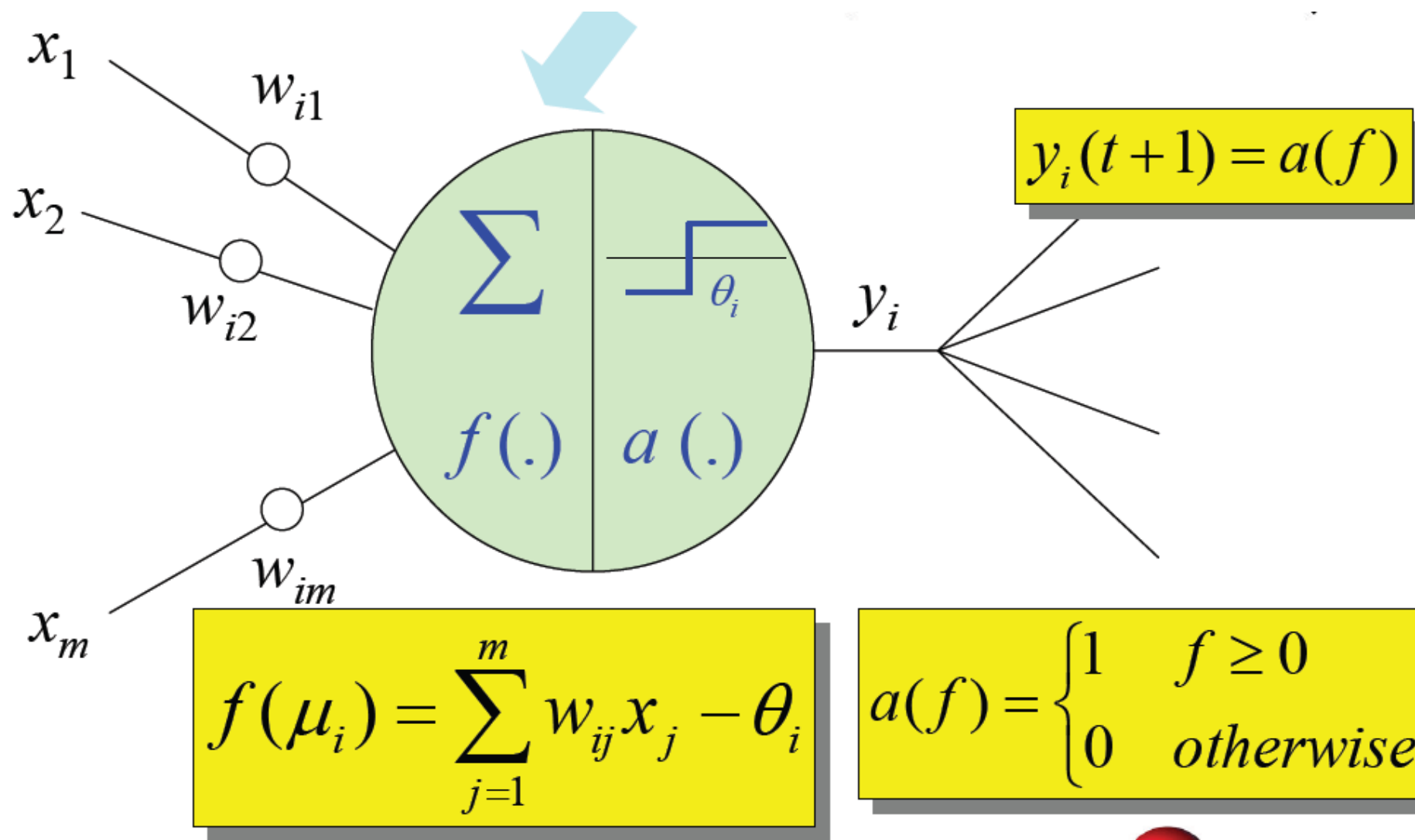


Andrew Ng

人工神经网络的特性

1. 可以充分逼近任意复杂的**非线性关系**
2. 所有定量或定性的信息都等势分布贮存于网络内的各神经元，故有很强的**鲁棒性和容错性**
3. 采用**并行分布处理**方法，使得快速进行大量运算成为可能
4. 可**学习和自适应**不知道或不确定的系统
5. 能够同时处理定量、定性知识。
6. 可以通过软件和硬件实现。

人工神经元模型



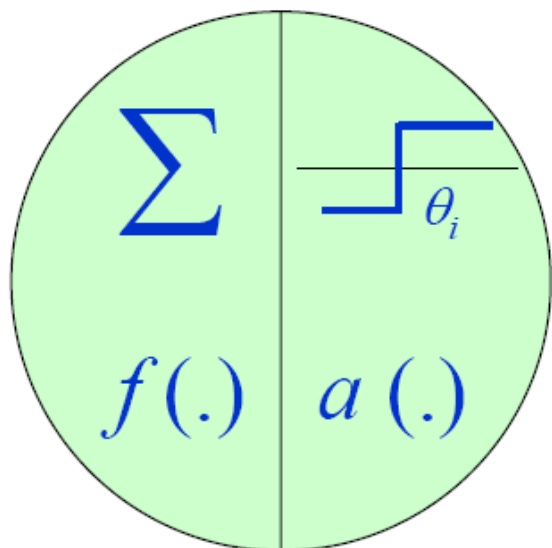
人工神经元模型

- 神经元单元由多个输入 x_i , $i=1, 2, \dots, n$ 和一个输出 y 组成。中间状态由输入信号的权和表示, 而输出为

$$y_j = a\left(\sum_{i=1}^n \omega_{ji} x_i - \theta_j\right)$$

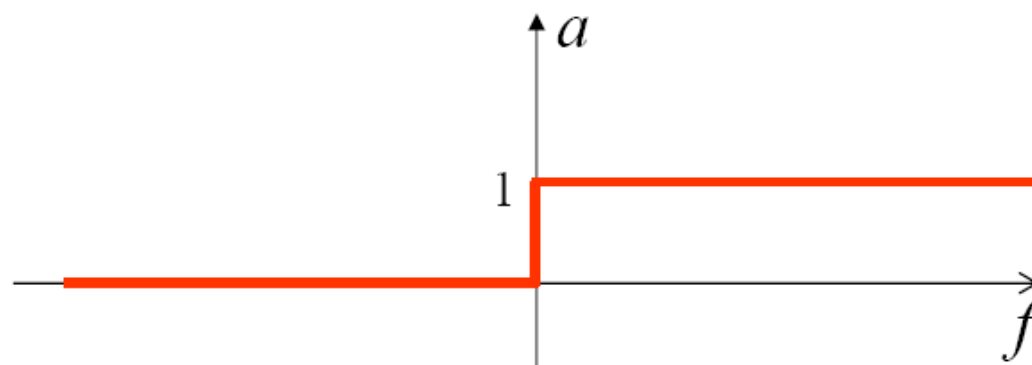
式中, θ_j 为神经元单元的偏置或阈值, w_{ji} 为连接权系数。 n 为输入信号数目, y_j 为神经元输出, $a(\square)$ 为输出变换函数, 也叫激励函数, 特性函数。

神经元的激励函数

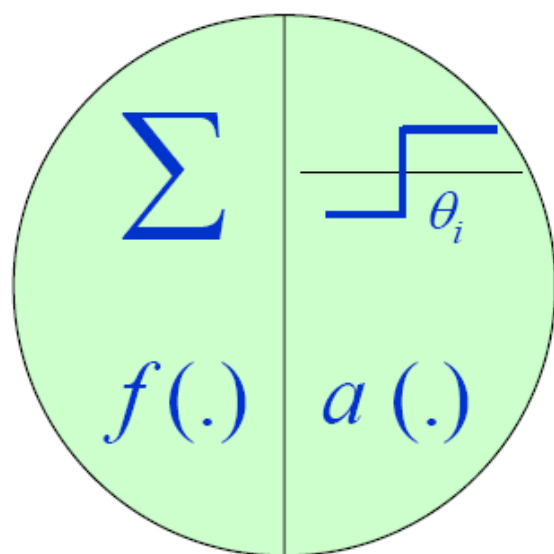


阶跃型函数

$$a(f) = \begin{cases} 1 & f \geq 0 \\ 0 & \text{otherwise} \end{cases}$$

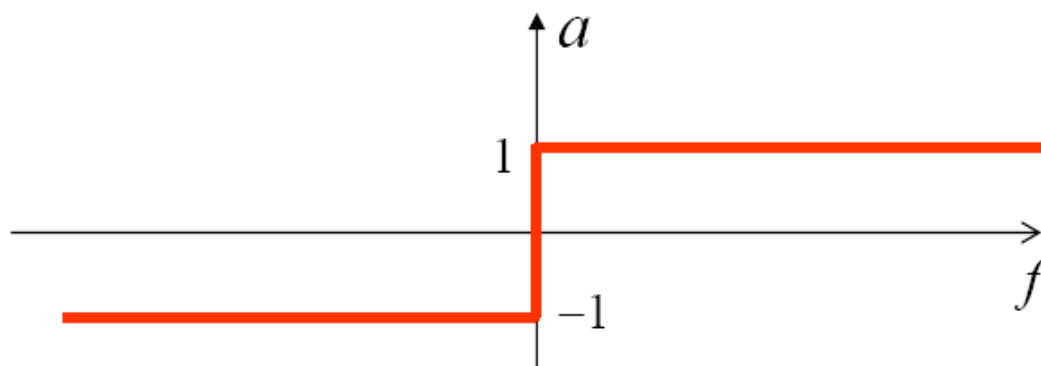


神经元的激励函数



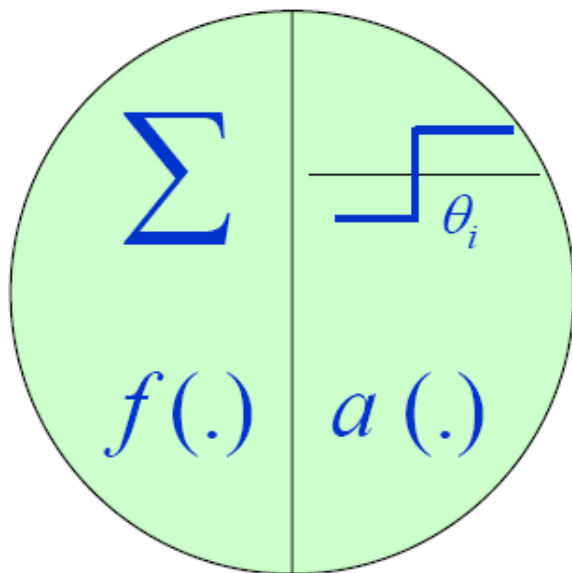
门限型函数

$$a(f) = \text{sgn}(f) = \begin{cases} 1 & f \geq 0 \\ -1 & f < 0 \end{cases}$$

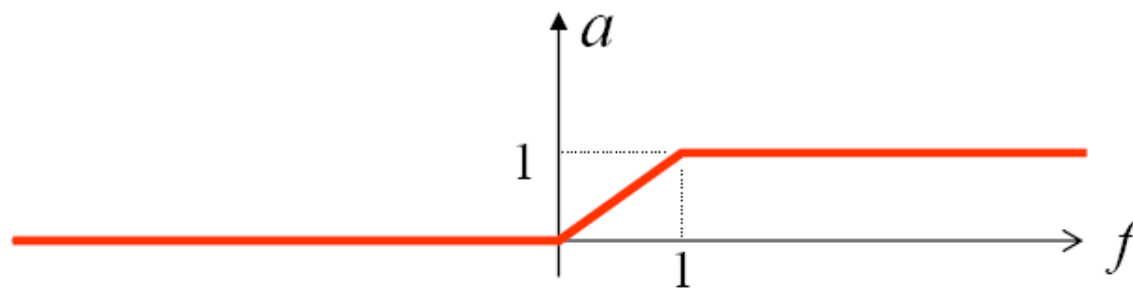


神经元的激励函数

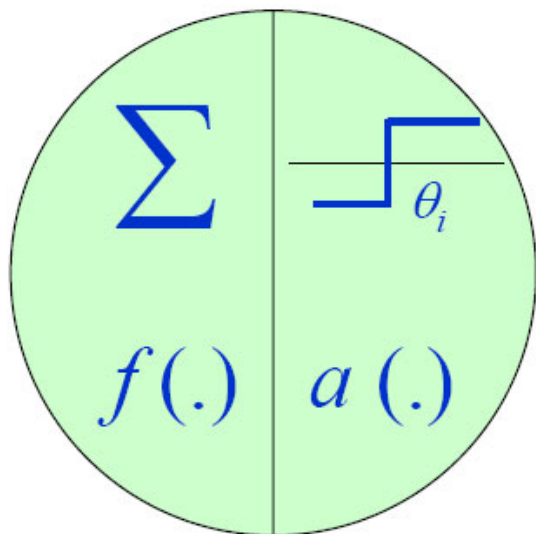
坡型函数



$$a(f) = \begin{cases} 1 & f > 1 \\ f & 0 \leq f \leq 1 \\ 0 & f < 0 \end{cases}$$

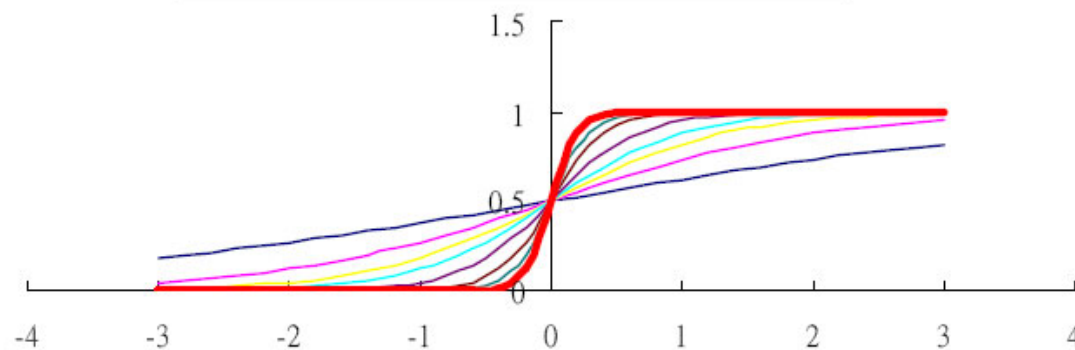


神经元的激励函数

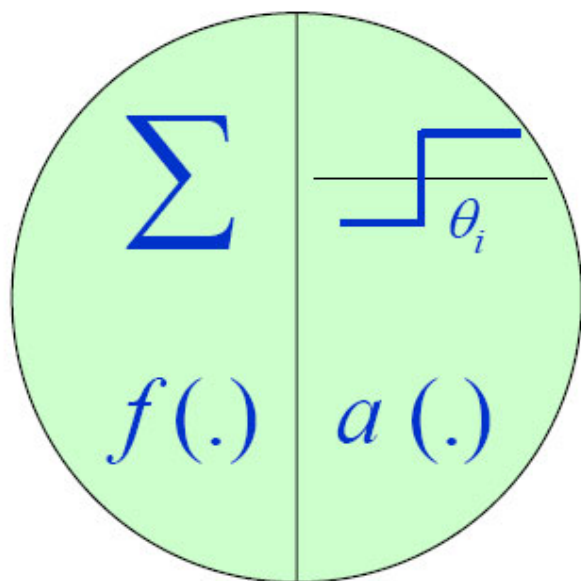


单极**sigmoid**函数

$$a(f) = \frac{1}{1 + e^{-\lambda f}}$$

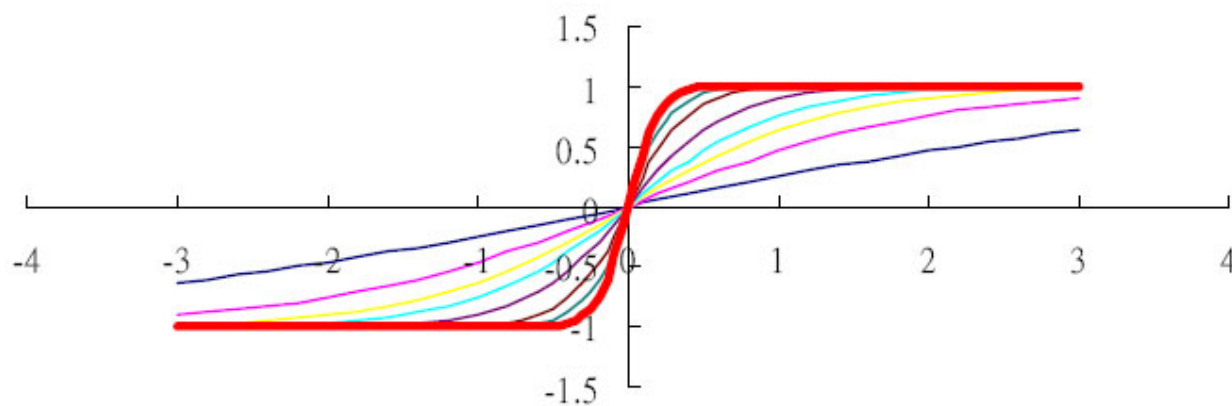


神经元的激励函数

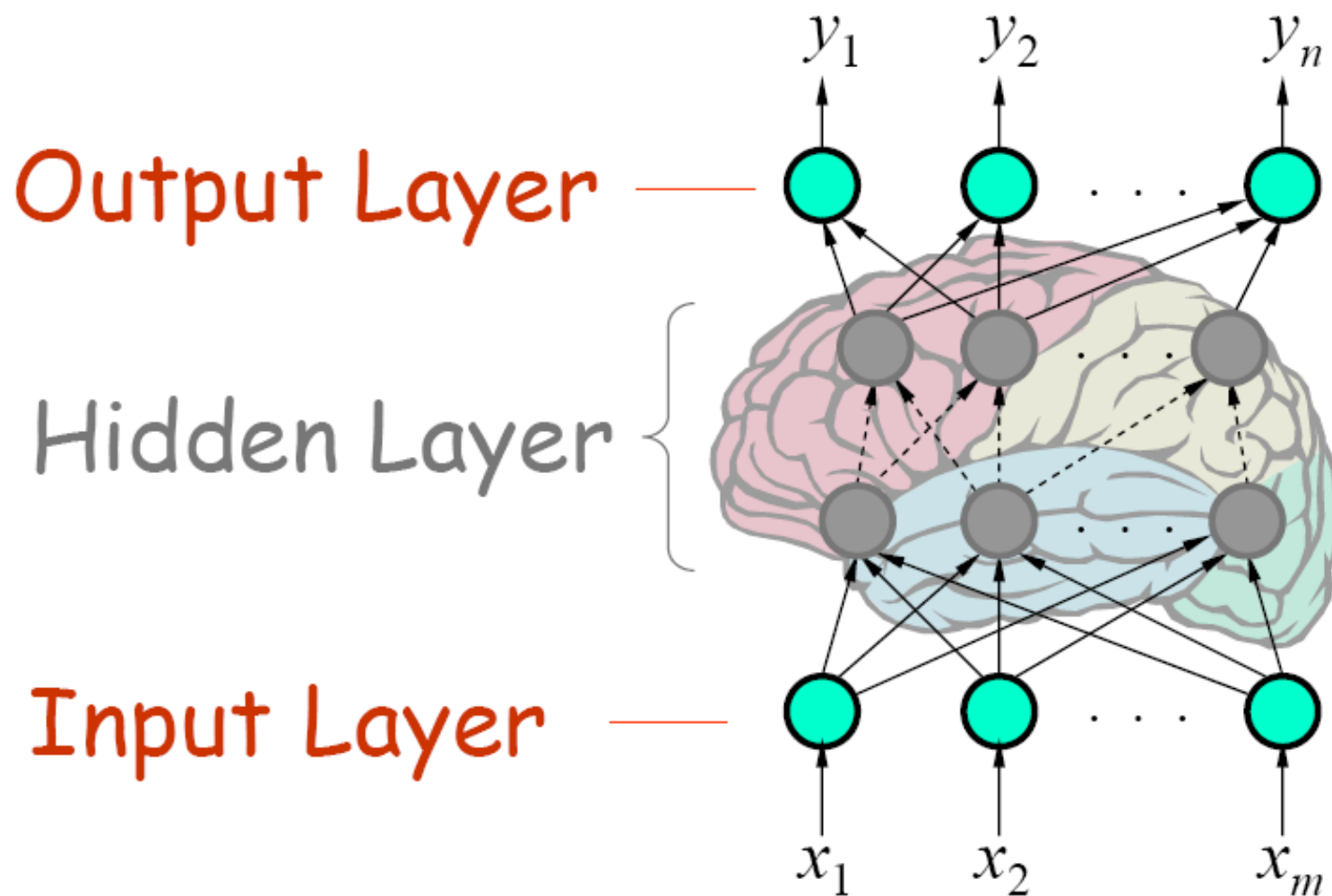


双极sigmoid函数

$$a(f) = \frac{2}{1 + e^{-\lambda f}} - 1$$



人工神经网络结构



神经网络的基本特性和结构

- 人工神经网络是具有下列特性的有向图

- ◇ 对于每个节点 i , 存在一个状态变量 x_i ; ☐
- ◇ 从节点 i 至节点 j , 存在一个连接权系数 w_{ij} ;
- ◇ 对于每个节点 i , 存在一个阈值 θ_i ;
- ◇ 对于每个节点 i , 定义一个激活函数。

神经网络中的常见模型

- 神经网络中的常见模型：**前馈神经网络（也叫前向神经网络）**；**反馈神经网络（也叫递归神经网络）**。
- **前馈神经网络**：具有递阶分层结构，神经元从一层连接至下一层，不存在同层神经元间的连接。
- **反馈神经网络**：有些神经元的输出被反馈至同层或前层神经元。其输入数据决定反馈系统的初始状态，然后系统经过一系列的状态转移后逐渐收敛于平衡状态，即为反馈神经网络经过计算后的输出结果。

前馈神经网络

●前馈网络具有递阶分层结构，由同层神经元间不存在互连的层级组成。

从输入层至输出层的信号通过单向连接流通；神经元从一层连接至下一层，不存在同层神经元间的连接，前馈网络的例子有：

反向传播神经网络（BP）

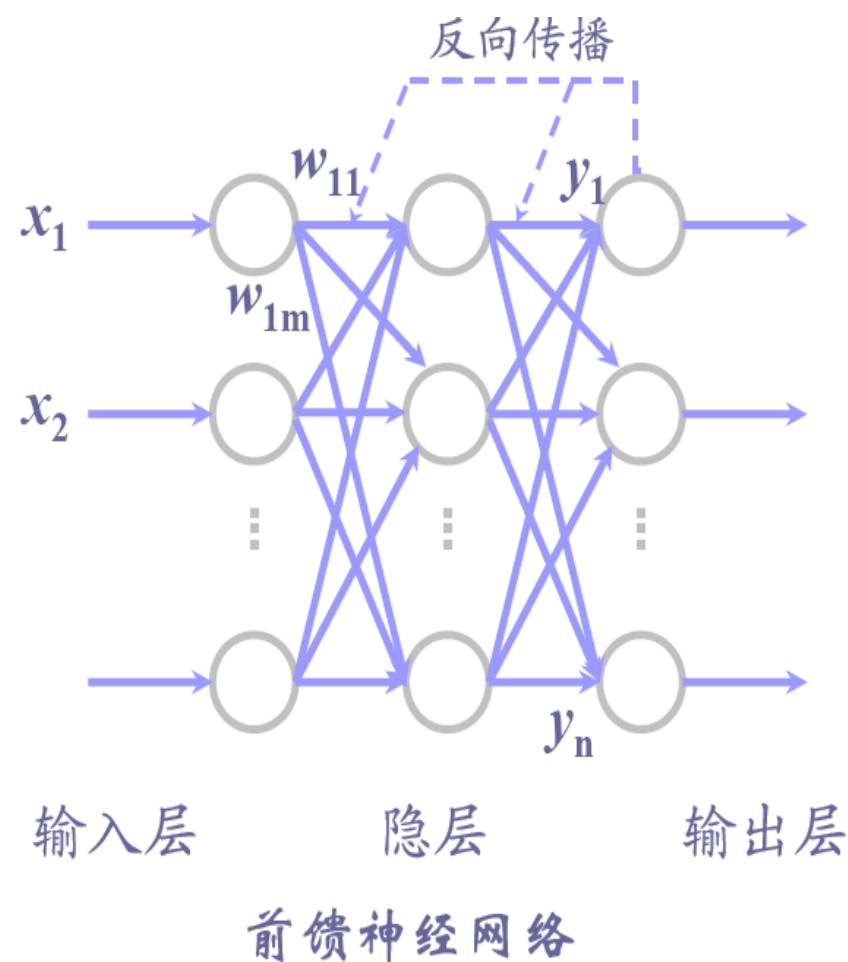
径向基神经网络（RBF）

多层感知器（MLP）

学习矢量量化（LVQ）网络

小脑模型联接控制（CMAC）

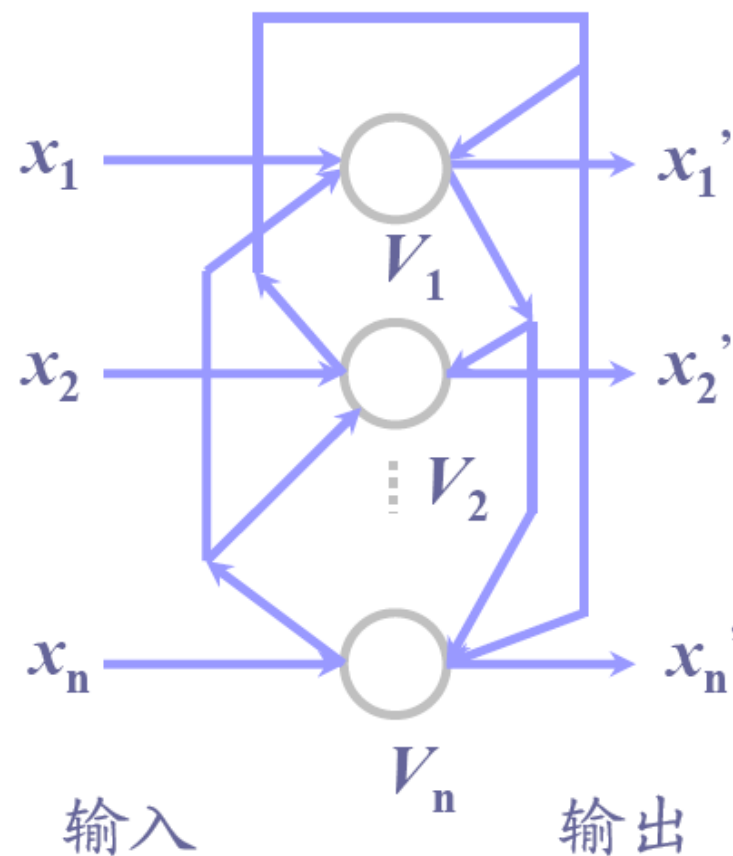
网络



反馈神经网络

反馈网络又叫做**递归网络**。在反馈（递归）神经网络中，多个神经元互连以组织一个互连神经网络。如图所示。**有些神经元的输出被反馈至同层或前层神经元**。因此，信号能够从正向和反向流通。

Hopfield网络，**Elmman网络**和**Jordan网络**是递归网络有代表性的例子。



反馈网络模型

神经网络的主要学习算法

人工神经网络最具有吸引力的特点是它的学习能力。人工神经网络的学习过程就是对它进行训练的过程。

学习是神经网络研究的一个重要内容，它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。

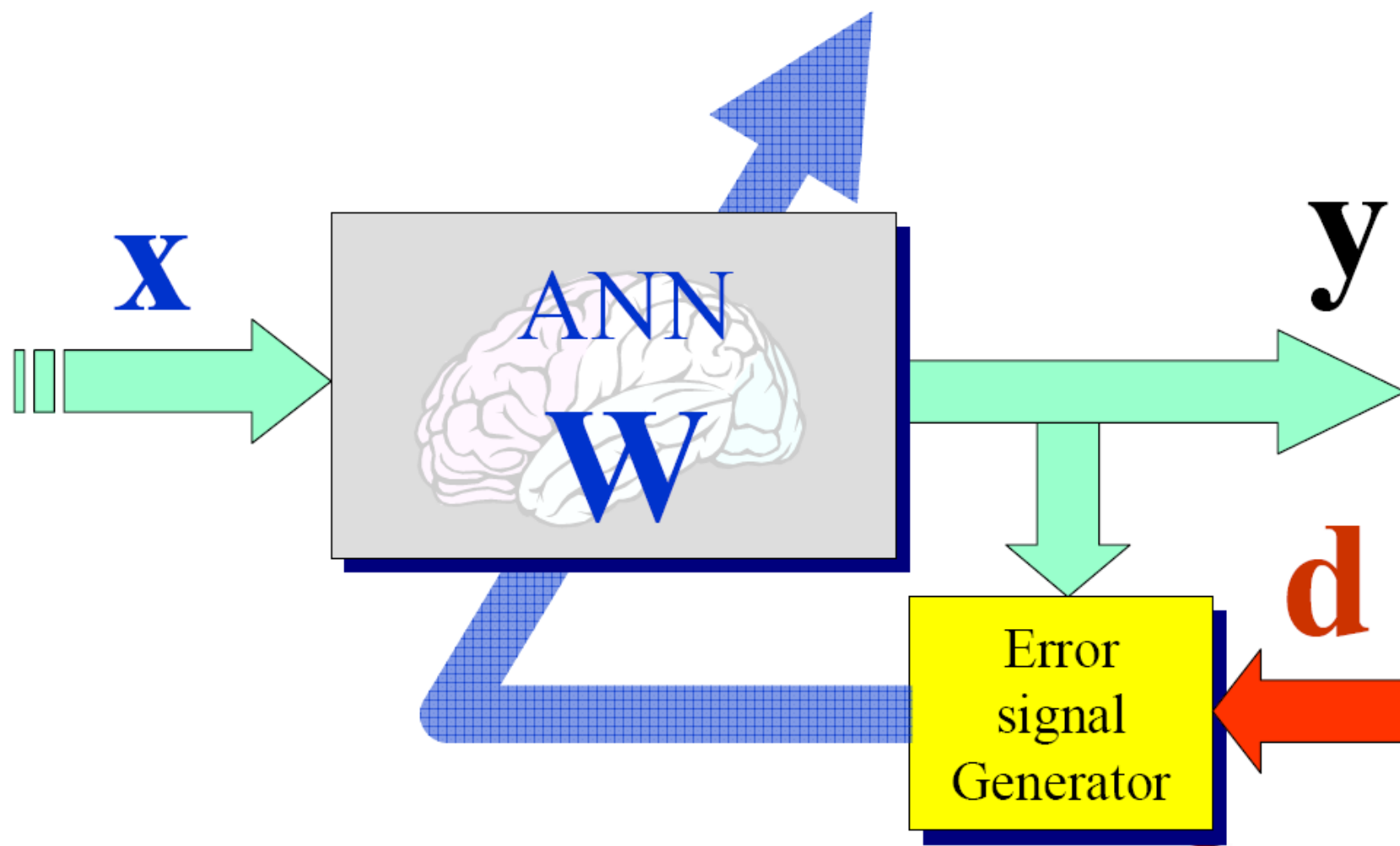
- 神经网络主要通过**指导式（有师）学习算法**和**非指导式（无师）学习算法**。此外，还存在第三种学习算法，即**强化学习算法**；可把它看做有师学习的一种特例。

有师学习

- 有师学习算法能够根据**期望的**和**实际的**网络输出（对应于给定输入）间的**差**来调整**神经元间连接的强度或权**。因此，有师学习需要有个老师或导师来**提供期望或目标输出信号**。

有师学习算法的例子包括 δ 规则、广义 δ 规则或反向传播算法以及 L V Q 算法等。

有师学习

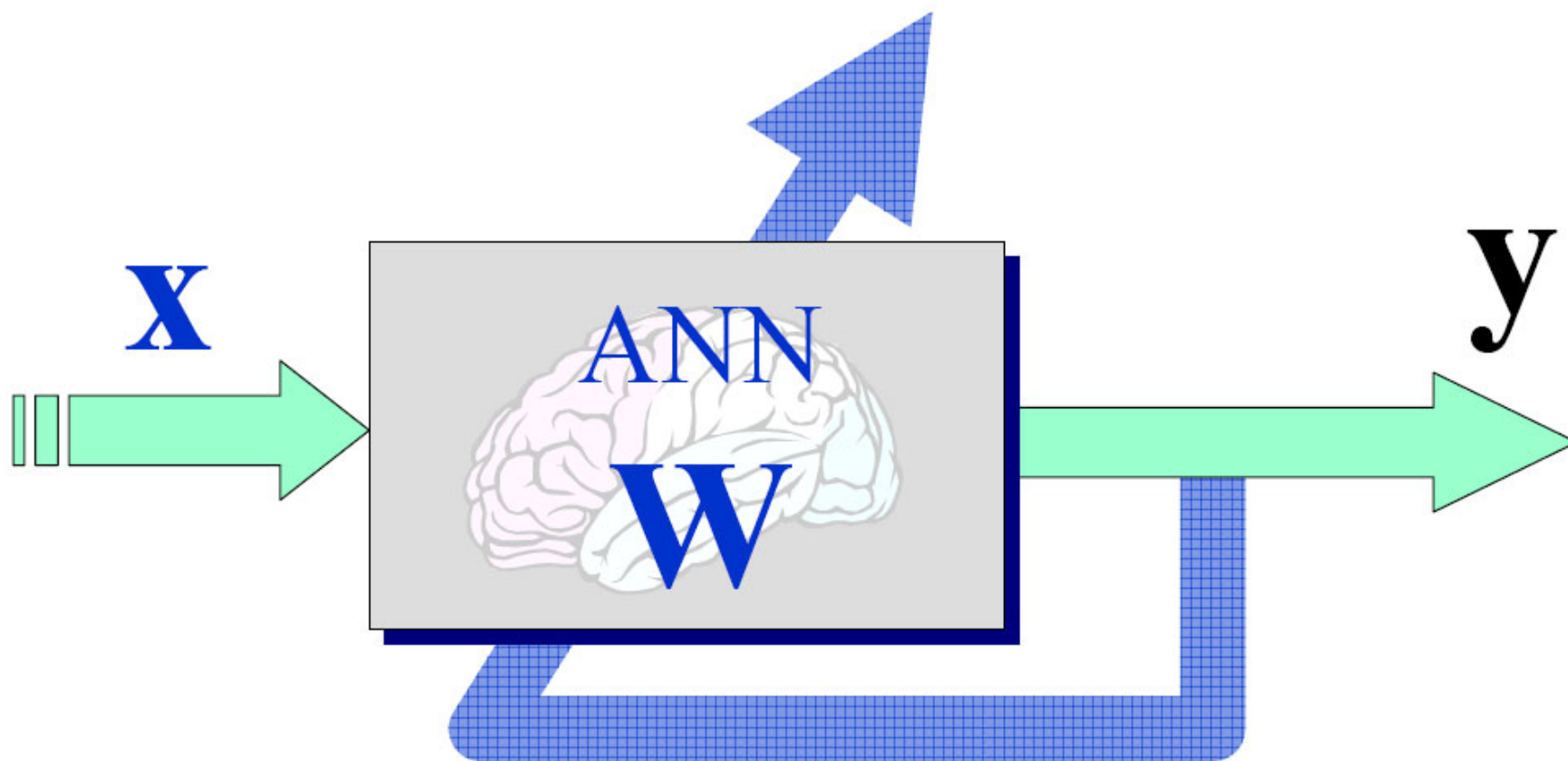


无师学习

- 无师学习算法**不需要知道期望输出**。在训练过程中，只要向神经网络提供输入模式，神经网络就能够自动地适应连接权，以便按相似特征把输入模式分组聚集。

无师学习算法的例子包括Kohonen算法和Carpenter-Grossberg自适应谐振理论（A R T）等。

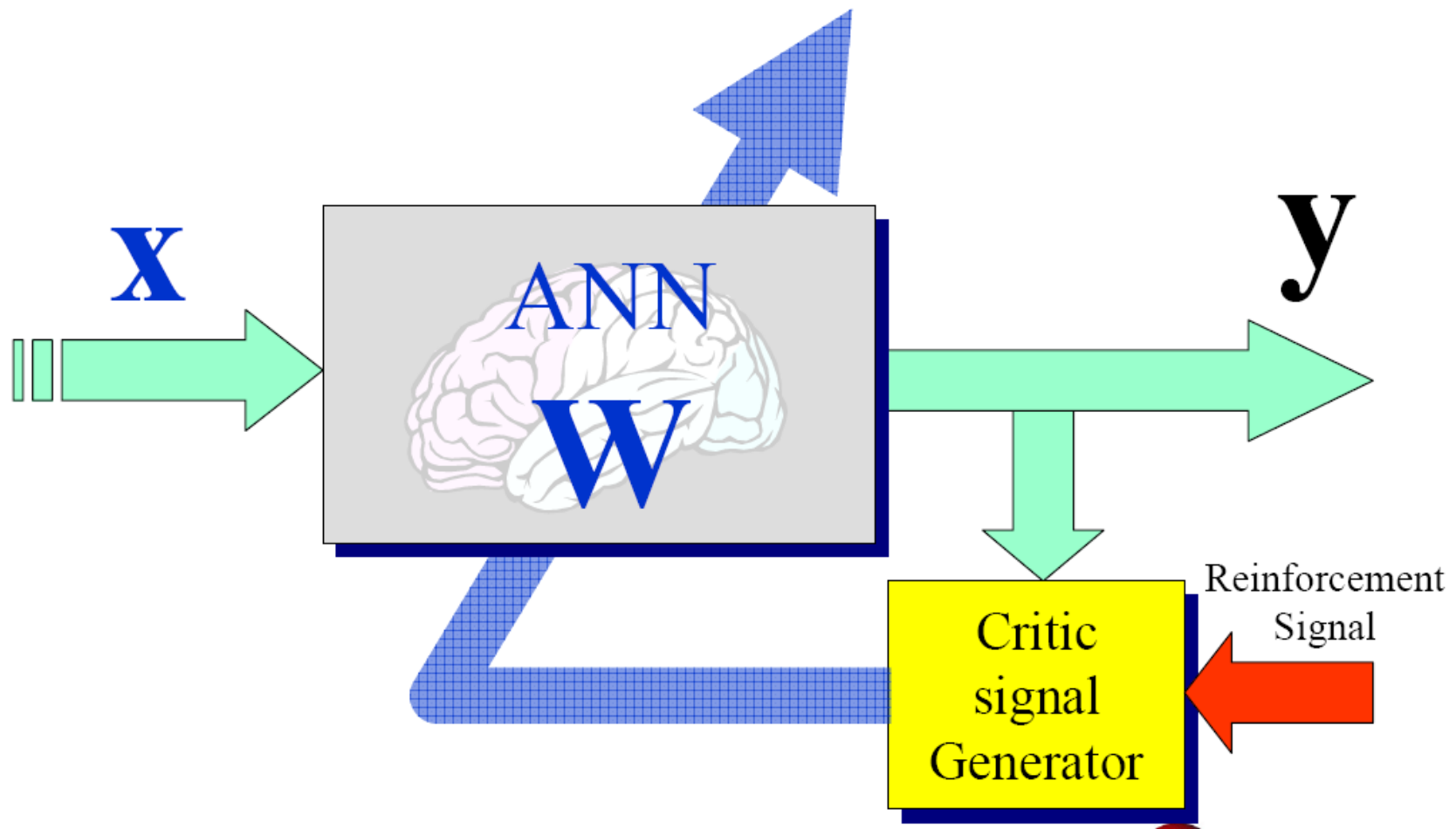
无师学习



强化学习

- **强化（增强）学习是有师学习的特例。它不需要老师给出目标输出。强化学习算法采用一个“评论员”来评价与给定输入相对应的神经网络输出的优度（质量因数）。**

强化学习



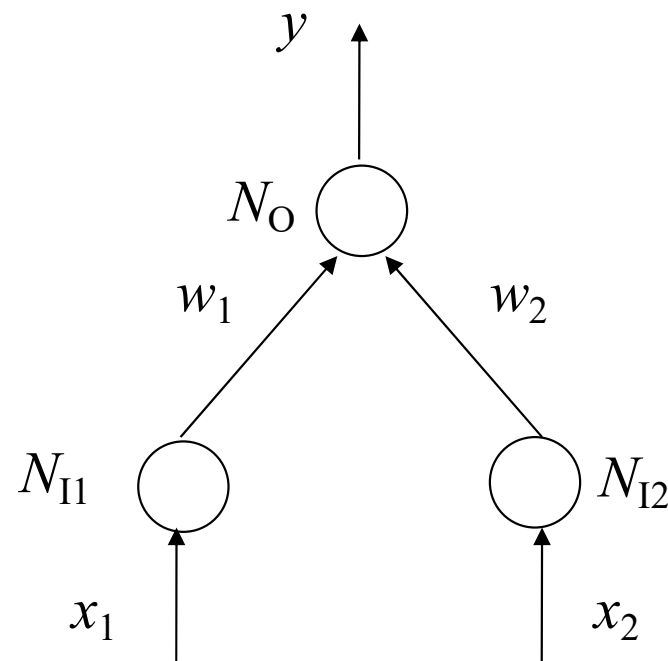
基于神经网络的知识表示与推理

- 基于神经网络的知识表示

在基于神经网络的系统中，知识的表示方法与传统人工智能系统中所用的方法（如产生式系统、框架、语义网络等）完全不同。人工智能系统中所用的方法是知识的显式表示，而神经网络中的知识是一种隐式的表示方法。在这里，知识并不像在产生式系统中那样独立地表示为每一条规则，而是将某一问题的若干知识在同一网络中表示。

基于神经网络的知识表示

- 例：使用二层神经网络实现与（and）逻辑。
- 如右图所示， x_1 ， x_2 为网络的输入， w_1 ， w_2 为连接边的权值， y 为网络的输出。



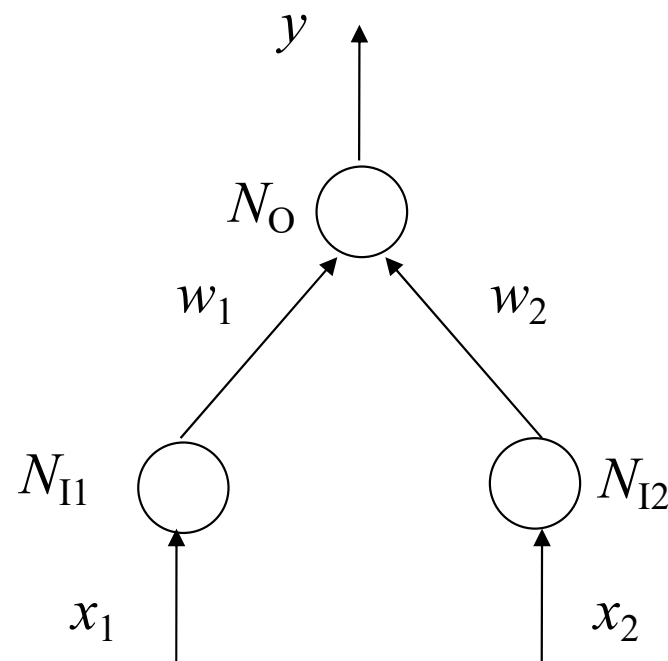
基于神经网络的知识表示

- 定义一个输入输出关系函数：

$$f(a) = \begin{cases} 0, & a < \theta \\ 1, & a \geq \theta \end{cases}$$

- 其中， $\theta = 0.5$ 。
- 根据网络的定义，网络的输出为

$$y = f(x_1 w_1 + x_2 w_2)$$



基于神经网络的知识表示

- 只要有一组合适的权值 w_1 , w_2 , 就可以使输入数据 x_1 , x_2 和输出 y 之间符合与 (and) 逻辑。

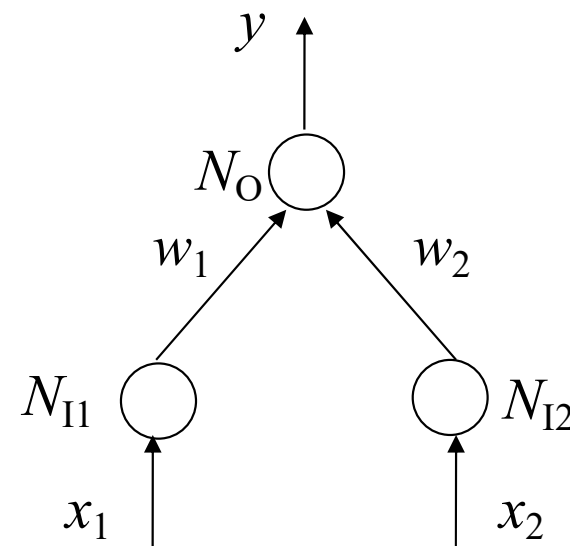
- 网络输入输出的与 (and) 关系

x_1	x_2	y
0	0	0
0	1	0
1	0	0
1	1	1

基于神经网络的知识表示

- 根据实验得到了如下几组 w_1 , w_2 权值数据。

w_1	w_2
0.20	0.35
0.25	0.30
0.20	0.40
0.40	0.20

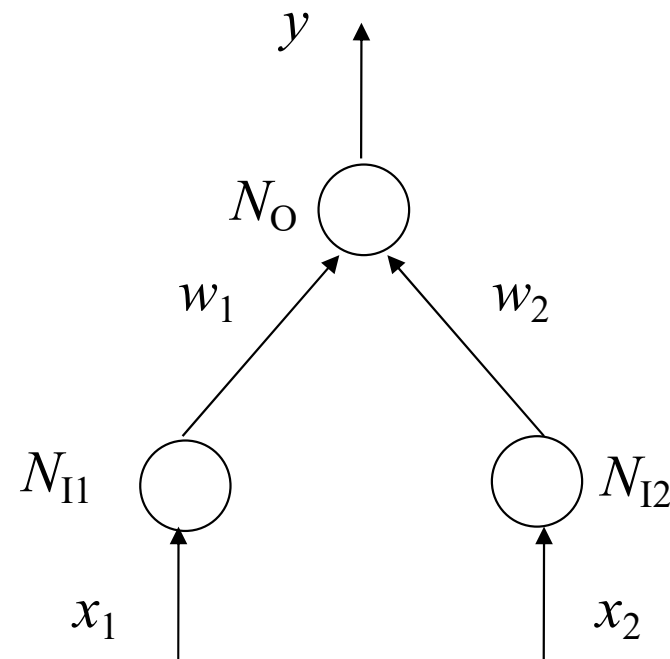


$$y = f(x_1 w_1 + x_2 w_2)$$

$$f(a) = \begin{cases} 0, & a < \theta \\ 1, & a \geq \theta \end{cases}$$

基于神经网络的知识表示

- 由此可见权值数据对整个网络非常重要。
- 假设其他条件不变，能否使用右图的网络来实现异或逻辑（XOR）？
- 由推导可知，二层网络结构不能实现异或逻辑。



基于神经网络的知识表示

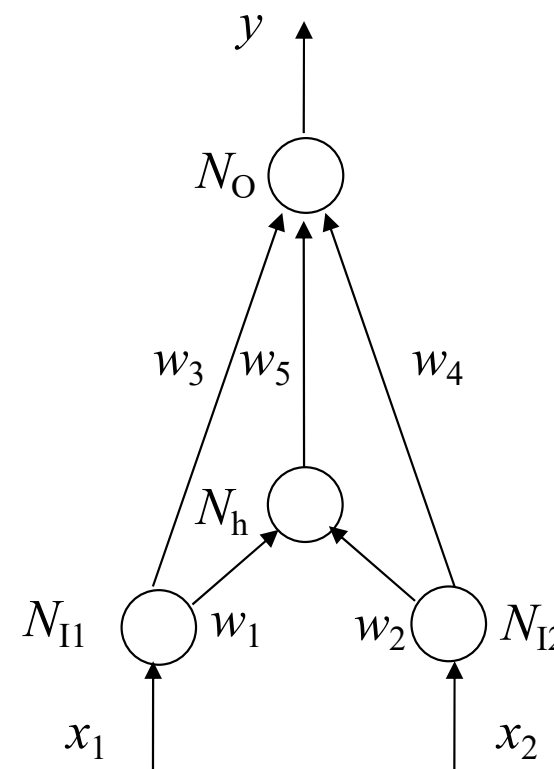
- 如果在网络的输入和输出层之间加入一个隐层，情况就不一样了。如右图所示，取权值向量(w_1, w_2, w_3, w_4, w_5)为(0.3, 0.3, 1, 1, -2)，按照网络的输入输出关系：

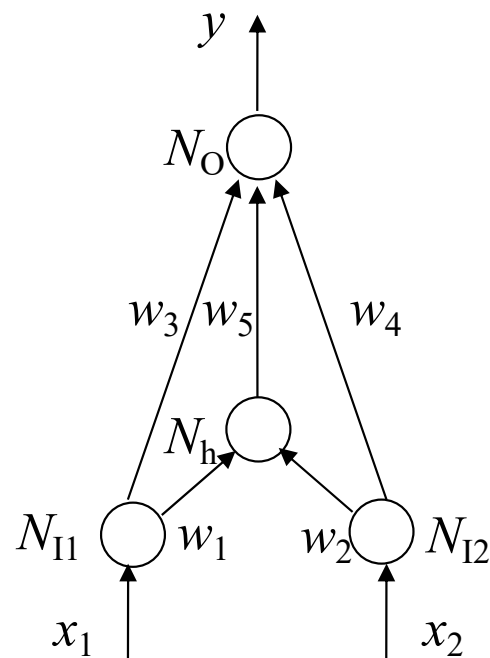
$$y = f(x_1 \cdot w_3 + x_2 \cdot w_4 + z \cdot w_5)$$

- 这里 z 为隐层节点的输出，

$$z = f(x_1 \cdot w_1 + x_2 \cdot w_2)$$

- $f(\cdot)$ 为输入输出关系函数， θ 均为 0.5





- 如果用产生式规则描述，则该网络代表下述四条规则：
- IF $x_1=0$ AND $x_2=0$ THEN $y=0$
- IF $x_1=0$ AND $x_2=1$ THEN $y=1$
- IF $x_1=1$ AND $x_2=0$ THEN $y=1$
- IF $x_1=1$ AND $x_2=1$ THEN $y=0$

基于神经网络的知识推理

- 基于神经网络的知识推理**实质上是在一个已经训练成熟的网络基础上对未知样本进行反应或者判断。**
- 神经网络的训练是一个网络对训练样本内在规律的学习过程，而对网络进行训练的**目的主要是为了让网络模型对训练样本以外的数据具有正确的映射能力。**

基于神经网络的知识推理

- 通常将神经网络在训练完成后输入其训练样本以外的新数据时获得正确输出的能力定义为**神经网络的泛化能力**（推广能力）。
- 它是人工神经网络的一个属性，称为泛化性能。

基于神经网络的知识推理

- 泛化性能的好坏取决于人工神经网络是否从训练样本中找到内在的真正规律。
- 影响泛化能力的因素主要有：
 - 1) 训练样本的质量和数量
 - 2) 网络结构
 - 3) 问题本身的复杂程度
- 神经网络的训练次数也称为神经网络的学习时间。在一定范围内，训练次数的增加可以提高神经网络的泛化能力。

基于神经网络的知识推理

- 然而，在神经网络的训练过程中经常出现一种**过拟合现象**，即在训练样本的误差逐渐减小并达到某个定值以后，往往会出现网络对训练样本以外的测试样本的误差反而开始增加的情况。因而，**对网络的训练，并不是使训练误差越小越好，而是要从实际出发，提高泛化能力。**
- **最佳的泛化能力往往出现在训练误差的全局最小点出现之前，最佳泛化点出现存在一定的时间范围。只要训练时间合适，较大的神经网络也会有好的泛化能力。**

基于神经网络的知识推理

- 训练完成后，**基于神经网络的推理是通过网络计算实现的**。把用户提供的初始证据用作网络的输入，通过网络计算最终得到输出结果。

基于神经网络的知识推理

- 网络推理的大致过程。一般来说，正向网络推理的步聚如下：
 - (1) 把**已知数据输入**网络输入层的各个节点。
 - (2) 利用**特性函数**分别计算网络中各层的输出。计算中，**前一层的输出作为后一层有关节点的输入**，逐层进行计算，直至计算出输出层的输出值为止。
 - (3) 用**阈值函数**对输出层的输出进行判定，从而得到输出结果。

基于神经网络的知识推理

- 上述推理具有如下特征：
- (1) 同一层的处理单元（神经元）是完全并行的，但层间的信息传递是串行的。由于层中处理单元的数目要比网络的层数多得多，因此它是一种并行推理。
- (2) 在网络推理中不会出现传统人工智能系统中推理的冲突问题。
- (3) 网络推理只与输入及网络自身的参数有关，而这些参数又是通过使用学习算法对网络进行训练得到的，因此它是一种自适应推理。

本讲内容小结

主要内容：

人工神经网络的结构

人工神经元模型

神经元的激励函数

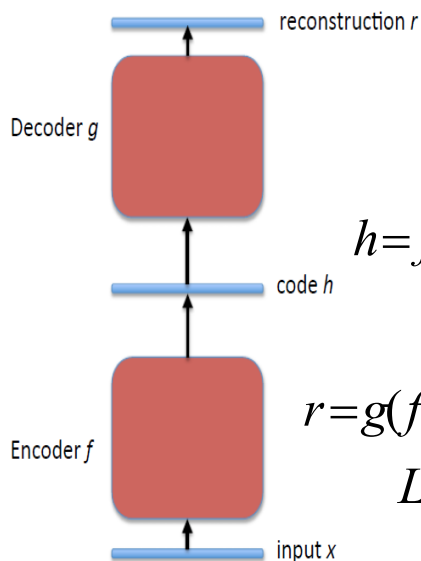
神经网络中的常见模型

神经网络的主要学习算法

基于神经网络的知识表示与推理

实例讲解

自编码 (Autoencoder)



x : 输入值

f : 编码函数

$h=f(x)$: 编码或内部表示

g : 解码函数

$r=g(f(x))$: 输出, 也称“重建值”

$L(r,x)$: 损失函数, 用于测量重建的好坏, 目标是 minimize L 的期望值

- 稀疏自编码 (Sparse Autoencoder)
- 栈式自编码 (Stacked Autoencoder)
- 去噪自编码 (Denoising Autoencoder)

几种自编码的共同点

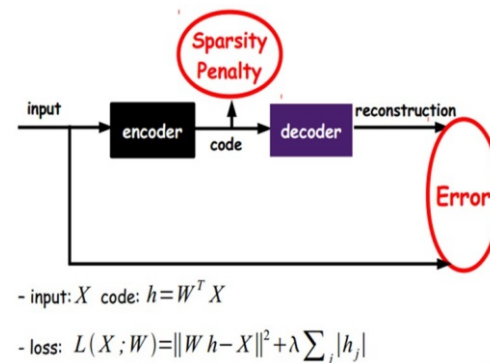
除了预防针对 x 简单地学习一个恒等函数外, 还包含对以下两个要素取折中:

1、学习到一个针对 x 的表示 h , x 也能通过一个解码器从 h 中还原; (**重建误差**)

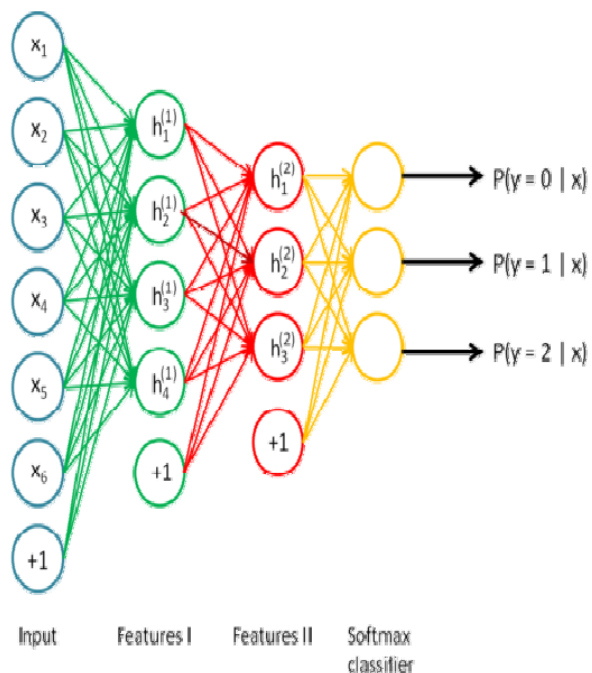
2、减小模型代表性的能力, 使在尽可能多的输入方向上不敏感。 (**模型的表达能力**)

稀疏自动编码器 (Sparse Autoencoder)

类似人脑, 某个输入只是刺激某些神经元, 其他的大部分神经元是受到抑制的

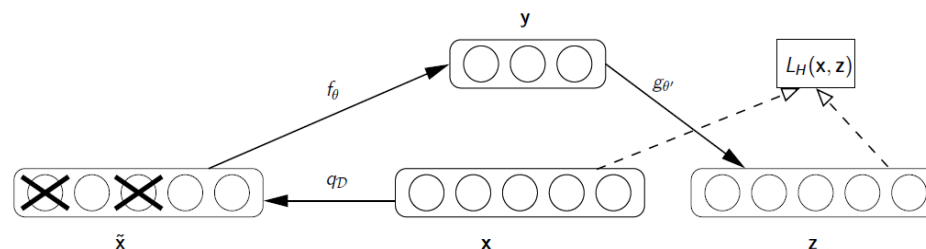


栈式自编码（Stacked Autoencoder）



栈式自编码神经网络是一个由多层稀疏自编码器组成的神经网络，其前一层自编码器的输出作为其下一层自编码器的输入。采用逐层贪婪训练法进行训练，获取栈式自编码神经网络参数。

去噪自编码（Denoising Autoencoder）

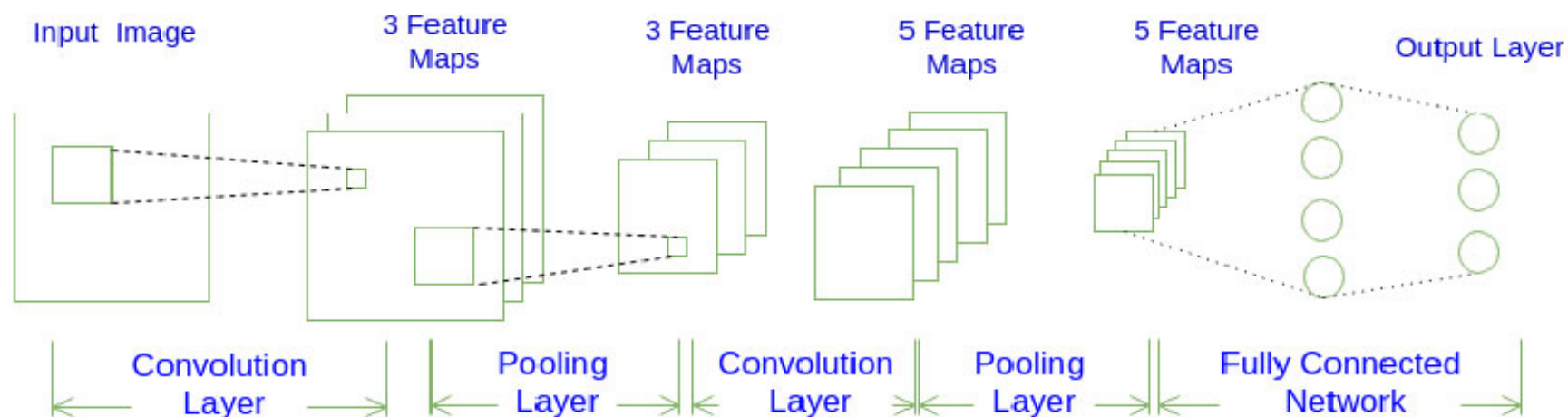


$$L_H(x, z) = - \sum_{k=1}^d [x_k \log z_k + (1 - x_k) \log(1 - z_k)]$$

去噪自动编码器DA是在自动编码器的基础上，训练数据加入噪声，所以自动编码器必须学习去去除这种噪声而获得真正的没有被噪声污染过的输入。

编码器学习输入信号的更加鲁棒的表达，它的泛化能力比一般编码器强。

卷积神经网络（Convolutional Neural Network, CNN）



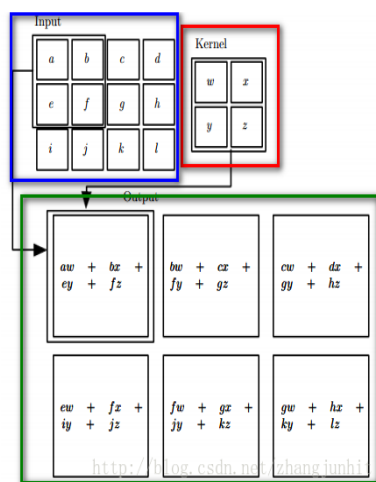
CNN的核心就是构造滤波器——模型训练

卷积神经网络是一种前馈神经网络，它的人工神经元可以响应一部分覆盖范围内的周围单元一个卷积神经网络由若干卷积层、**Pooling**层、全连接层组成。**CNN**主要用来识别位移、缩放及其他形式扭曲不变性的二维图形。**CNN**在图像图像处理及语音分析方面取得突出成绩。

卷积神经网络 (Convolutional Neural Network, CNN)

CNN中卷积操作

- (1)红色框内为 2×2 卷积核。
- (2)蓝色框内为 3×4 的输入图像。
- (3)绿色框为 2×3 的特征图。

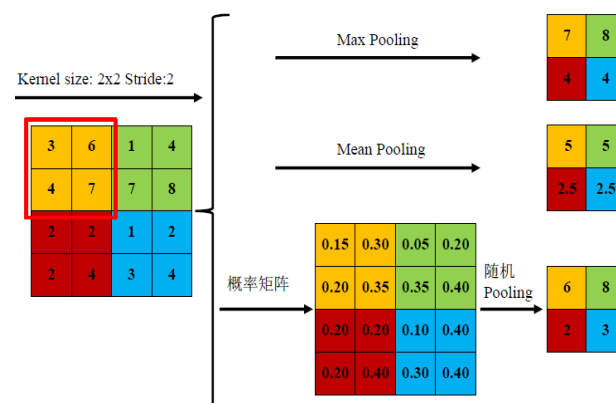


权值共享是每个卷积运算使用同一个卷积核，在上图中使用的是同一个卷积核，即共享权值。

CNN中池化操作

对输入的特征图进行压缩，一方面使特征图变小，简化网络计算复杂度；一方面进行特征压缩，提取主要特征。

- ◆ **Mean-pooling**: 对邻域内特征点只求平均，对背景保留比较好
- ◆ **Max-pooling**: 对邻域内特征点取最大值，对纹理保持比较好
- ◆ **Stochastic-pooling**: 介于两者之间，通过对像素点按照数值大小赋予概率，按概率进行采样

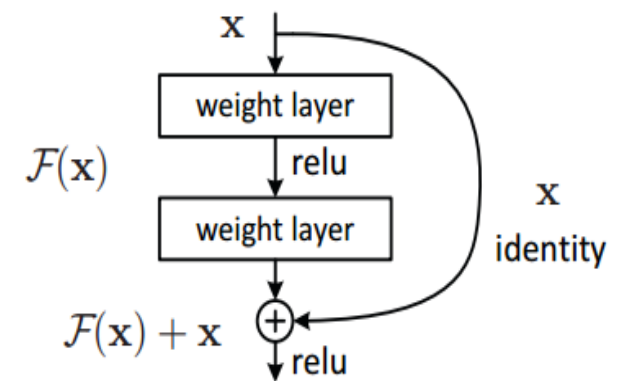


深度残差网络（Deep Residual Net）

ResNet（Residual Neural Network）由前微软研究院的 Kaiming He 等4名华人提出，通过使用Residual Blocks 成功训练152层深的神经网络，在ILSVRC 2015 比赛中获得了冠军。ResNet 的结构可以极快地加速超深神经网络的训练，模型的准确率也有非常大的提升。

随着网络层数的不断增加，网络训练过程中会出现**梯度消失**的现象，影响**back propagation**的权值更新过程。

残差结构的引入可以构造更深层次的神经网络，同时避免梯度消失的问题。**ResNet** 相当于将学习目标改变了，不再是学习一个完整的输出，而是最优解 **$H(X)$** 和全等映射 **x** 的差值，即残差 **$F(x)$** 。



He, Kaiming, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. "Deep residual learning for image recognition." In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 770-778. 2016.

生成对抗网络 (Generative Adversarial Net)

生成对抗网络 (Generative Adversarial Networks, GANs) 的概念最早是2014年由蒙特利尔大学的Ian Goodfellow提出的。其创造的算法模型在想法上绝对别具一格，尤其在应用性上的优势令人心动。GAN 启发自博弈论中的**二人零和博弈** (two-player zero-sum game)，两个博弈方分别称为**生成式模型** G (generative model) 和**判别式模型** D (discriminative model)。

生成模型 G 捕捉样本数据的分布，用服从某一分布（均匀分布，高斯分布等）的噪声 z 生成一个类似真实训练数据的样本，追求效果是越像真实样本越好。——**使判别器无法判别真假**

判别模型 D 是一个二分类器，估计一个样本来自于训练数据（而非生成数据）的概率，如果样本来自于真实的训练数据， D 输出大概率，否则， D 输出小概率。——**可以准确分辨真假样本**

Goodfellow, Ian, et al. “Generative adversarial nets.” Advances in Neural Information Processing Systems. 2014.

深度强化学习（Deep Reinforcement Learning）

将深度学习与强化学习结合起来从而实现从Perception感知到Action动作的端对端学习的一种全新的算法。目前在Deep Reinforcement Learning取得开拓性进展的主要集中在DeepMind和UC Berkeley团队。



强化学习教父

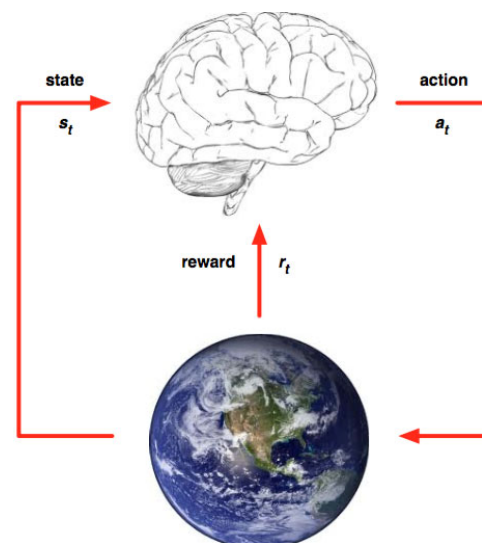
Richard Sutton

2030年之前实现强人工智能算法

一般用智能体（**Agent**）来表示一个具备行为能力的物体，比如机器人，无人车，人等等。那么增强学习考虑的问题就是智能体和**环境**之间交互的任务。

机械臂抓取

赛车游戏



- ▶ At each step t the agent:
 - ▶ Receives state s_t
 - ▶ Receives scalar reward r_t
 - ▶ Executes action a_t
- ▶ The environment:
 - ▶ Receives action a_t
 - ▶ Emits state s_t
 - ▶ Emits scalar reward r_t