



第五章: 神经网络

主讲:连德富特任教授|博士生导师

邮箱: <u>liandefu@ustc.edu.cn</u>

手机: 13739227137

主页: http://staff.ustc.edu.cn/~liandefu

2016年AI技术重大突破

AlphaGo 以4:1比分赢得Lee Sedol



Versions	Hardware	Elo	Date	Results		
AlphaGo Fan	176 GPUs, distributed	3,144	Oct-15	5:0 against Fan Hui		
AlphaGo Lee	48 TPUs, distributed	3,739	Mar-16	4:1 against Lee Sedol		
AlphaGo Master	4 TPUs, single machine	4,858	May-17	60:0 against professional players; Future of Go Summit		
AlphaGo Zero (40 block)	4 TPUs, single machine	5,185	Oct-17	100:0 against AlphaGo Lee 89:11 against AlphaGo Master		
AlphaZero (20 block)	4 TPUs, single machine	5,018	Dec-17	60:40 against AlphaGo Zero (20 block)		



Rank	Name	3°₽	Flag	Elo
1	<u>Shin Jinseo</u>	ð	:•:	3800
2	<u>Ke Jie</u>	8	*)	3726
3	<u>Park Junghwan</u>	8		3692
4	<u>Gu Zihao</u>	ð	*)	3667
5	<u>Lian Xiao</u>	ð	*)	3596
6	<u>Fan Tingyu</u>	3	*)	3589
7	<u>Fan Yunruo</u>	ð	*3	3576
8	<u>Jiang Weijie</u>	3	*)	3574
9	<u>Shin Minjun</u>	8		3572
10	Yang Dingxin	8	*)	3570
11	<u>Xie Erhao</u>	8	*)	3566
12	Mi Yuting	8	*)	3562
13	<u>Xie Ke</u>	3	*)	3557
14	<u>Ding Hao</u>	8	*)	3556
15	<u>Tuo Jiaxi</u>	3	*)	3555
16	<u>Ichiriki Ryo</u>	ð	•	3554
17	<u>Chen Yaoye</u>	8	*)	3550
18	<u>Xu Jiayang</u>	ð	*)	3538
19	<u>Iyama Yuta</u>	8	•	3538
20	<u>Tong Mengcheng</u>	8	*)	3530
21	<u>Byun Sangil</u>	8		3527
22	<u>Lee Donghoon</u>	8		3525
23	<u>Tao Xinran</u>	8	*)	3522
24	Zhao Chenyu	ð	*)	3519
25	<u>Li Weiqing</u>	ð	*)	3518
26	<u>Kang Dongyun</u>	ð	:• :	3504
27	<u>Liao Yuanhe</u>	ð	*)	3501
28	Shi Yue	ð	*)	3499

AlphaGo中的机器学习



• 策略网络

Policy network

Value network

监督学习

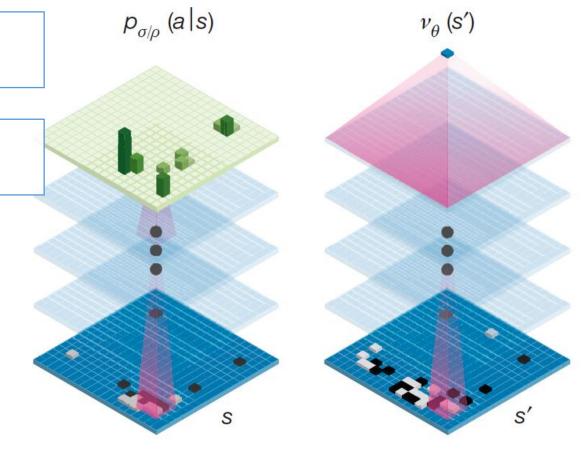
• 预测人类如何下下一步棋

强化学习

• 学习如何下下一步棋以最大化赢率

• 值网络 估计给定棋局的赢率

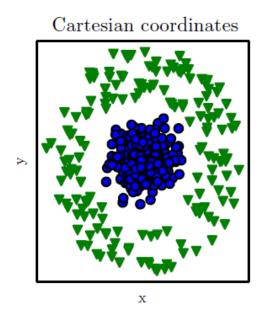
通过 (深度) 神经网络来实现

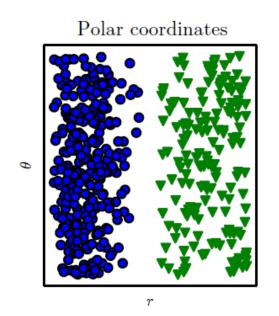


神经网络是什么?



- 线性模型 $y = w^T x$: 无法建模任何两个输入变量之间的相互作用
- 扩展线性模型来表示 x 的非线性函数, $y = \phi(x)^{\mathsf{T}} w$
- 简单机器学习方法常通过特征工程设计 $\phi(x)$





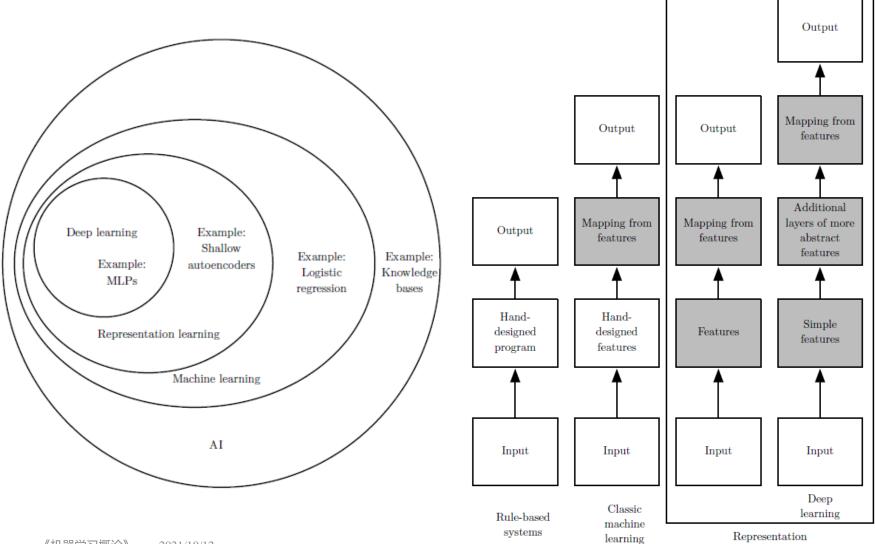
• (深度) 神经网络直接学习特征表示, 即 $y = f(x; \theta, w) = \phi(x; \theta)^T w$

《机器学习概论》 2021/10/12

神经网络是什么?



learning



《机器学习概论》 2021/10/12

神经网络发展史—第一阶段



- 1943年, McCulloch和Pitts 提出第一个神经元数学模型, 即M-P模型, 并从原理上证明了人工神经网络能够计算任何算数和逻辑函数
- 1949年, Hebb 发表《The Organization of Behavior》一书, 提出生物神经元学习的机理, 即Hebb学习规则
- 1958年, Rosenblatt 提出<mark>感知机网络</mark> (Perceptron) 模型和其学习规则
- 1960年, Widrow和Hoff提出自适应线性神经元 (Adaline) 模型和最小均方学习算法
- 1969年, Minsky和Papert 发表《Perceptrons》一书, 指出单层神经网路不能解决非线性问题, 多层网络的训练算法尚无希望. 这个论断导致神经网络进入低谷

《机器学习概论》

神经网络发展史—第二阶段



- 1982年, 物理学家Hopfield提出了一种具有联想记忆、优化计算能力的递归网络模型, 即Hopfield 网络
- 1986年, Rumelhart 等编辑的著作《Parallel Distributed Proceesing: Explorations in the Microstructures of Cognition》报告了反向传播算法
- 1987年, IEEE 在美国加州圣地亚哥召开第一届神经网络国际会议 (ICNN)
- 90年代初, 伴随统计学习理论和SVM的兴起, 神经网络由于理论不够清楚, 试错性强, 难以训练, 再次进入低谷

《机器学习概论》

神经网络发展史—第三阶段



- 2006年, Hinton提出了深度信念网络(DBN), 通过"预训练+微调" 使得深度模型的最优化变得相对容易
- 2012年, Hinton 组参加ImageNet 竞赛, 使用 CNN 模型以超过第二 名10个百分点的成绩夺得当年竞赛的冠军
- 伴随云计算、大数据时代的到来,计算能力的大幅提升,使得深度学习模型在计算机视觉、自然语言处理、语音识别等众多领域都取得了较大的成功

Images & Video





Text & Language



REUTERS **

Associated Press



神经元模型



•神经网络的定义

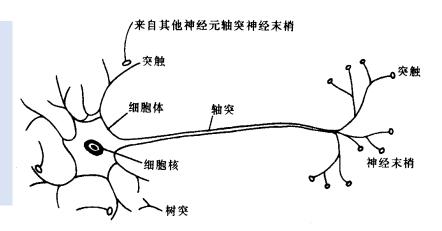
"<mark>神经网络</mark>是由具有适应性的<mark>简单单元</mark>组成的广泛<mark>并行互联</mark>的网络, 它的组织能够模拟生物神经系统对真实世界物体所作出的反应"

[Kohonen, 1988]

- 机器学习中的神经网络通常是指"神经网络学习"或者机器学习与神经网络两个学科的交叉部分
- •神经元模型即上述定义中的"简单单元"是神经网络的基本成分

生物神经网络

每个神经元与其他神经元相连,当它"兴奋"时,就会向相连的神经元发送化学物质,从而改变这些神经元内的电位;如果某神经元的电位超过一个"阈值",那么它就会被激活,即"兴奋"起来,向其它神经元发送化学物质

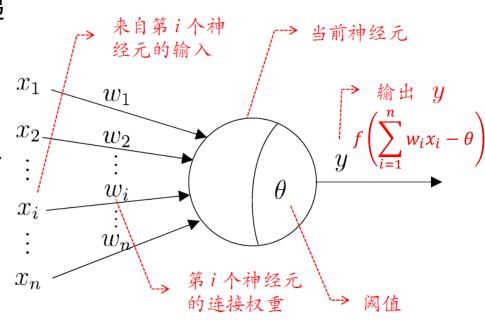


神经元模型



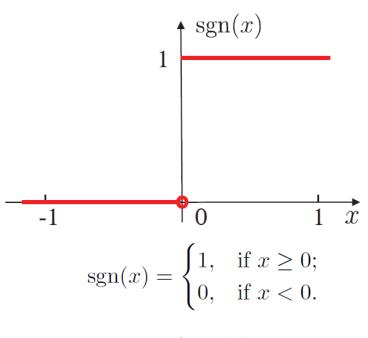
M-P 神经元模型 [McCulloch and Pitts, 1943]

- 输入:来自其他*n*个神经云传递 过来的输入信号
- 处理:输入信号通过带权重的 连接进行传递,神经元接受到总 输入值将与神经元的阈值进行 比较
- 输出:通过激活函数的处理以得到输出



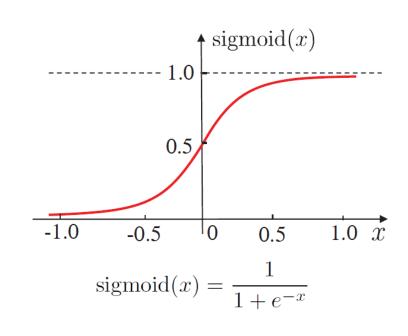
神经元模型—激活函数





(a) 阶跃函数

理想激活函数是阶跃函数 0表示抑制神经元;1表示激活神经元



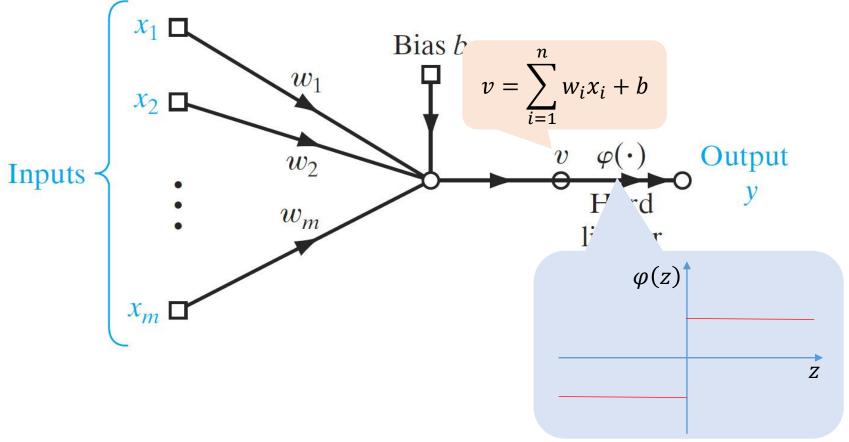
(b) Sigmoid 函数

阶跃函数具有不连续、不光滑等不好的 性质, 常用的是 Sigmoid 函数

感知机



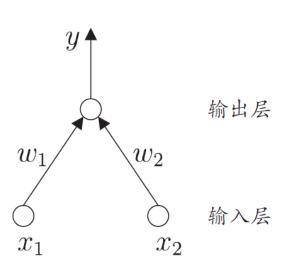
• 感知机由两层神经元组成, 输入层接受外界输入信号传递给输出层, 输出层是M-P神经元(阈值逻辑单元)

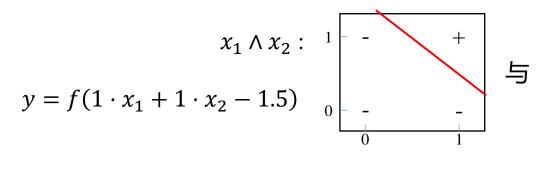


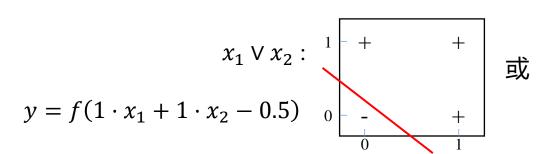
感知机



• 感知机能够容易地实现逻辑与、或、非运算







感知机学习



- 给定训练集, 权重 $w_i(i=1,2,\cdots,n)$ 与阈值 θ 可以通过学习得到
- 感知机学习规则

对训练样例(x,y),若当前感知机的输出为 \hat{y} ,则感知机权重调整规则为:

$$w_i \leftarrow w_i + \eta(y - \hat{y})x_i$$

学习率

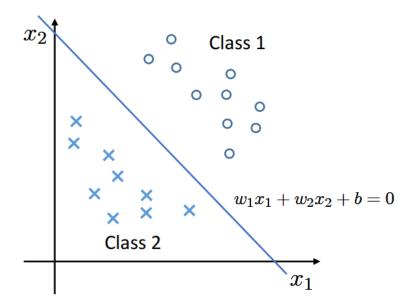
对应如下更新规则

若对训练样本(x,y)预测正确,则感知机不发生变化;若预测值更大,降低激活输入的权重;若预测值更小,增加激活输入的权重

感知机学习



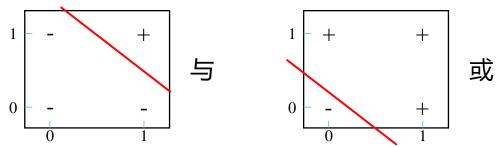
- 若两类模式<mark>线性可分</mark>,则感知机的学习过程一定会收敛;否感知机的学习过程将会发生震荡 [Minsky and Papert, 1969]
- 单层感知机的学习能力非常有限, 只能解决线性可分问题



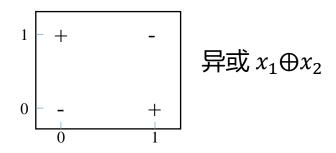
感知机学习



• 与、或、非问题是线性可分的,因此感知机学习过程能够求得适当的权值向量



• 异或问题不是线性可分的, 感知机学习不能求得合适解



对于非线性可分问题, 如何求解?

多层感知机

多层感知机



输出层与输入层之间的一层神经元,被称之为隐层或隐含层,隐含层和输出层神经元都是具有激活函数的功能神经元

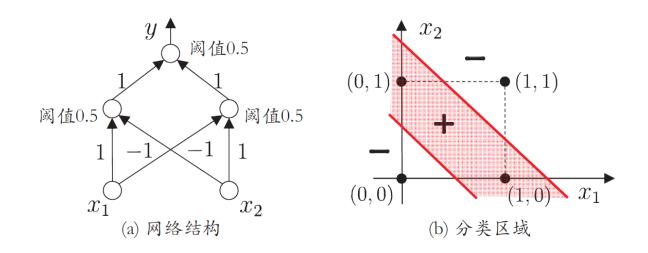


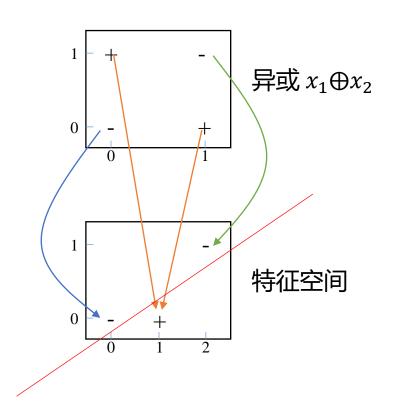
图 5.5 能解决异或问题的两层感知机

多层感知机



•
$$\boldsymbol{h} = max \left(0, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \boldsymbol{x} + \begin{bmatrix} 0 \\ -1 \end{bmatrix}\right)$$

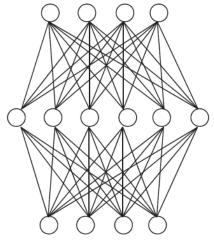
•
$$y = [1, -2] h - 0.5$$



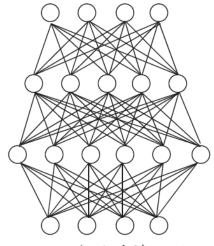
多层前馈神经网络



- 定义: 每层神经元与下一层神经元全互联,神经元之间不存在同层连接也不存在跨层连接
- 前馈: 输入层接受外界输入, 隐含层与输出层神经元对信号进行加工, 最终结果由输出层神经元输出
- 学习:根据训练数据来调整神经元之间的"连接权"以及每个功能神经元的"阈值"
- 多层网络: 包含隐层的网络



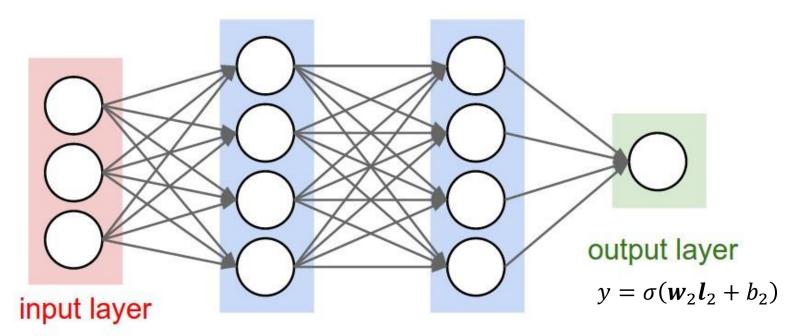
(a) 单隐层前馈网络



(b) 双隐层前馈网络

多层前馈神经网络—表示能力





hidden layer 1 hidden layer 2

$$\boldsymbol{l}_1 = \tanh(\boldsymbol{W}_1 \boldsymbol{x} + \boldsymbol{b}_1)$$
 $\boldsymbol{l}_2 = \tanh(\boldsymbol{W}_2 \boldsymbol{l}_1 + \boldsymbol{b}_2)$

多层前馈神经网络



• 如何学习多层前馈神经网络的参数呢?

误差逆传播算法

<mark>误差逆传播算法</mark> (Error BackPropagation, 简称BP) 是最成功的训练多层前馈神经网络的学习算法



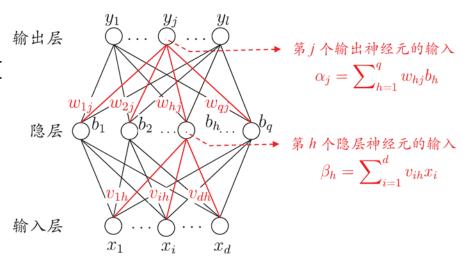
输出l维实值向量y

 θ_i : 输出层第j个神经元阈值

whi: 隐层与输出层神经元之间的连接权重

 γ_h : 隐含层第h个神经元阈值

v_{ih}:输入层与隐层神经元之间的连接权重



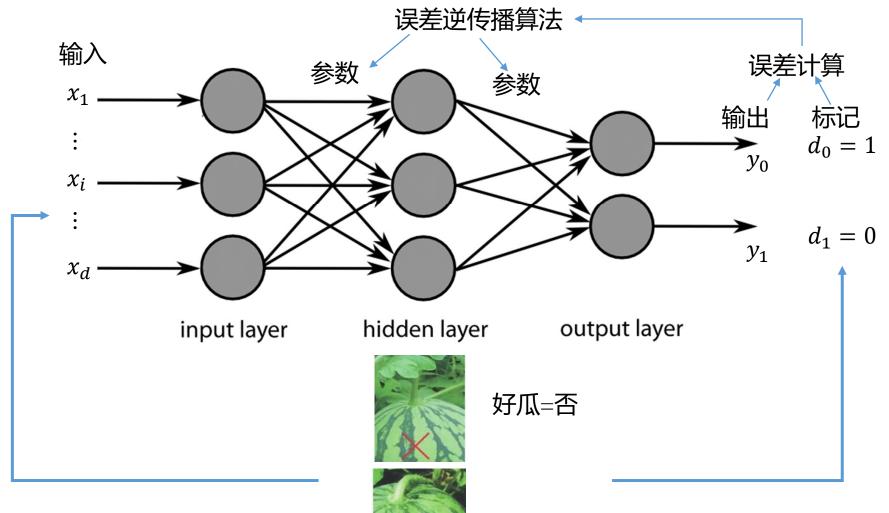
网络中需要 (d + l + 1)q + l 个参数 需要优化

输入示例x由d个属性描述

BP是一个迭代学习算法, 在迭代的每一轮中采用广义的感知机学习规则对参数进行更新估计, 任意的参数v的更新估计式为

$$v \leftarrow v + \Delta v$$





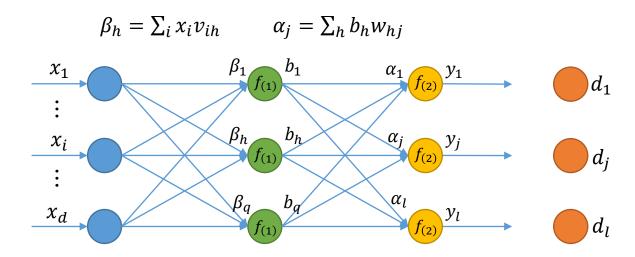
好瓜=是

训练样本

《机器学习概论》 2021/10/12

误差逆传播算法—前向



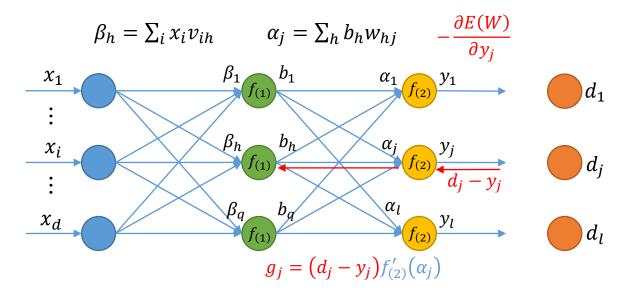


前向预测

$$x \xrightarrow{\beta_h = \sum_i x_i v_{ih}} b_h \xrightarrow{\alpha_j = \sum_h b_h w_{hj}} y_j$$

误差逆传播算法—后向





后向传播

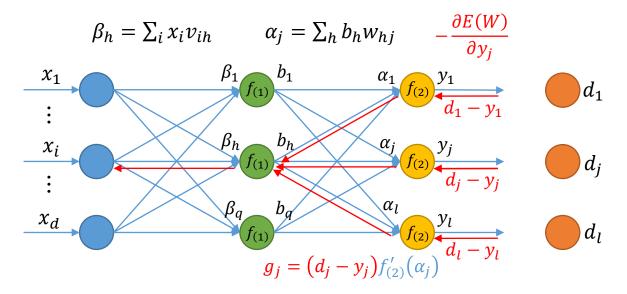
$$w_{hj} = w_{hj} + \Delta w_{hj} + \Delta w_{hj} = \eta \operatorname{Error}_{j} \operatorname{Output}_{\mathbf{h}} = \eta g_{j} b_{h} \\ E(\mathbf{W}) = \frac{1}{2} \sum_{j=1}^{l} (y_{j} - d_{j})^{2}$$

$$\Delta w_{hj} = -\eta \frac{\partial E(W)}{\partial w_{hj}} = -\eta \frac{\partial E(W)}{\partial y_j} \frac{\partial y_j}{\partial \alpha_j} \frac{\partial \alpha_j}{\partial w_{hj}} = \eta (d_j - y_j) f'_{(2)}(\alpha_j) b_h = \eta g_j b_h$$

《机器学习概论》 2021/10/12

误差逆传播算法—后向





后向传播

$$v_{ih} = v_{ih} + \Delta v_{ih} \qquad \Delta v_{ih} = \eta \operatorname{Error}_{h} \operatorname{Output}_{i} = \eta \operatorname{e}_{h} x_{i} \\ E(\mathbf{W}) = \frac{1}{2} \sum_{j=1}^{l} (y_{j} - d_{j})^{2}$$

$$\Delta v_{ih} = -\eta \frac{\partial E(W)}{\partial v_{ih}} = -\eta \frac{\partial E(W)}{\partial b_h} \frac{\partial b_h}{\partial \beta_h} \frac{\partial \beta_h}{\partial v_{ih}} = \eta \sum_j g_j w_{hj} f'_{(1)}(\beta_h) x_i = \eta e_h x_i$$

《机器学习概论》 2021/10/12

BP算法: 简单例子



• 考虑如下简单网络 假设激活函数为Sigmoid函数

Input: $0.35 \times 0.1 + 0.9 \times 0.8 = 0.755$ 0.7525

Output: 0.68 0.6797

Error: $e1=g*w1*o*(1-o)=-0.0406*0.3*0.68*(1-0.68)=-2.650*10^{-3}$

 $w3^{+}=w3+e1*A=0.1+(-2.650*10^{-3})*0.35=0.0991$ 0.1Input 0.3 w^{1+} =w1+g*o1=0.3+ (-0.0406)* 0.68=0.2724 A=0.350.8 0.7976 Output=0.5 0.4-0.3971 Input: $0.3 \times 0.68 + 0.9 \times 0.6637 = 0.80133$ 0.6 Output: 0.69 0.6820 误差从0.19降到0.1820 Input 0.9 Error: g=(t-o)(1-o)o=(0.5-0.69)(1-0.69)0.69=-0.0406B = 0.9 $w2^{+}=w2+g*o2=0.9+(-0.0406)*0.6637=0.8731$ $w6^{+}=w6+e2^{*}B=0.6+(-8.156*10^{-3})*0.9=0.5927$

Input: $0.35 \times 0.4 + 0.9 \times 0.6 = 0.68 \quad 0.6724$

Output: 0.6637 0.6620

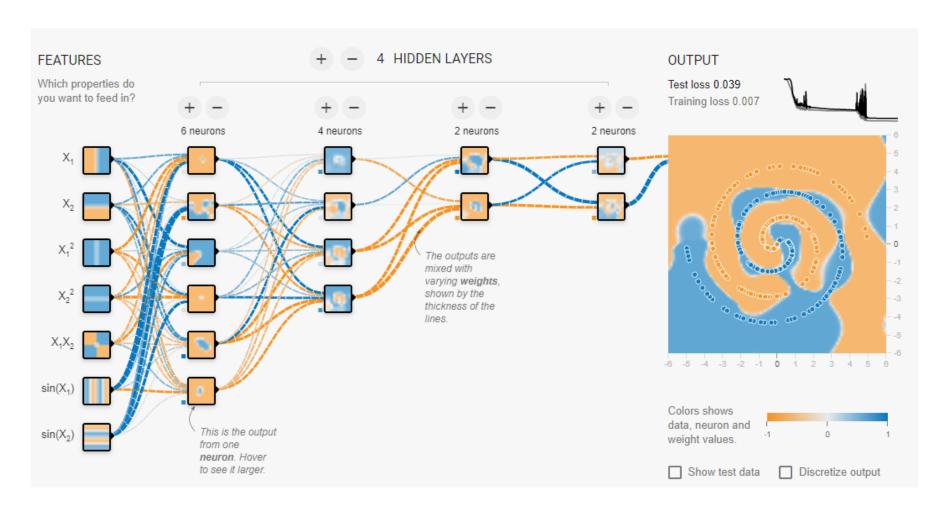
Error: $e2=g*w2*o*(1-o)=-0.0406*0.9*0.6637*(1-0.6637)=-8.156*10^{-3}$

《机器学习概论》

2021/10/1

BP演示





http://playground.tensorflow.org/



```
输入: 训练集 D = \{(\boldsymbol{x}_k, \boldsymbol{y}_k)\}_{k=1}^m; 学习率 \eta.
```

过程:

1: 在(0,1)范围内随机初始化网络中所有连接权和阈值

2: repeat

3: for all $(\boldsymbol{x}_k, \boldsymbol{y}_k) \in D$ do

4: 根据当前参数和式(5.3) 计算当前样本的输出 $\hat{m{y}}_k;$

5: 根据式(5.10) 计算输出层神经元的梯度项 g_j ;

6: 根据式(5.15) 计算隐层神经元的梯度项 e_h ;

7: 根据式(5.11)-(5.14) 更新连接权 w_{hj}, v_{ih} 与阈值 θ_j, γ_h

8: end for

9: until 达到停止条件

输出:连接权与阈值确定的多层前馈神经网络

图 5.8 误差逆传播算法



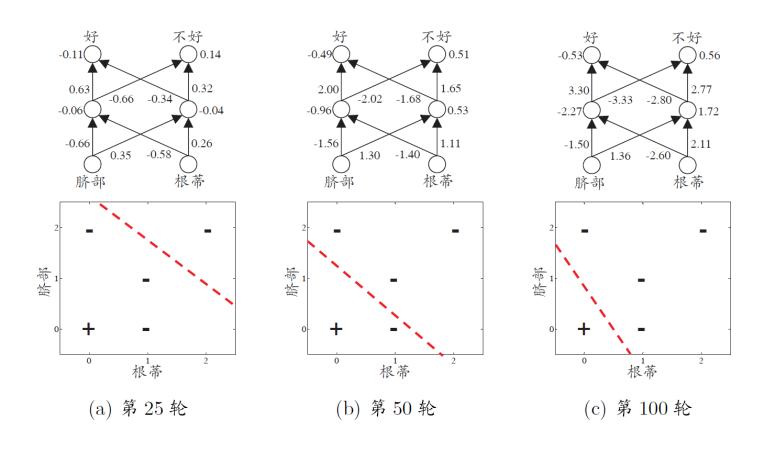


图 5.9 在 2 个属性、5 个样本的西瓜数据上, BP网络参数更新和分类边界的变化情况



- 标准 BP 算法
 - 每次针对单个训练样例更新权值与阈值

也称为随机梯度下降

• 参数更新频繁, 不同样例可能抵消, 需要多次迭代.

- 累计 BP 算法
 - 优化的目标是最小化整个训练集上的累计误差

$$E = \frac{1}{m} \sum_{k=1}^{m} E_k$$

• 读取整个训练集一遍才对参数进行更新, 参数更新频率较低.

但在很多任务中,累计误差下降到一定程度后,进一步下降会非常缓慢,这时标准BP算法往往会获得较好的解,尤其当训练集非常大时效果更明显.



- 标准 BP 算法 Stochastic Gradient Descent
 - 每次针对单个训练样例更新权值与阈值
- •累计 BP 算法
 - 优化的目标是最小化整个训练集上的累计误差

$$E = \frac{1}{m} \sum_{k=1}^{m} E_k$$

• 小批量随机梯度下降法 Mini-Batch Stochastic Gradient Descent

$$\frac{\partial E}{\partial \boldsymbol{\theta}} = \frac{1}{m} \sum_{k=1}^{m} \frac{\partial E_k}{\partial \boldsymbol{\theta}} \approx \frac{1}{n} \sum_{i=1}^{n} \frac{\partial E_i}{\partial \boldsymbol{\theta}} \qquad n \ll m, \text{ 称为batch size}$$

机器学习概论》 2021/10/12



- 多层前馈网络局限
 - 神经网络由于强大的表示能力, 经常遭遇过拟合

表现为: 训练误差持续降低, 但测试误差却可能上升

早停

• 在训练过程中, 若训练误差降低, 但验证误差升高, 则停止训练

正则化

- 在误差目标函数中增加一项描述网络复杂程度的部分, 例如连接权值与阈值的平方和
- 如何设置隐层神经元的个数仍然是个未决问题

实际应用中通常使用"试错法"调整

《机器学习概论》

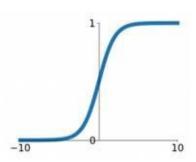
2021/10/12

激活函数



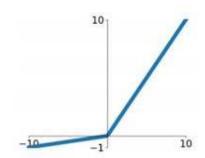
Sigmoid

$$\sigma(x) = \frac{1}{1 + e^{-x}}$$



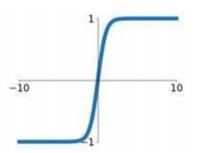
Leaky ReLU

 $\max(0.1x,x)$



tanh

tanh(x)

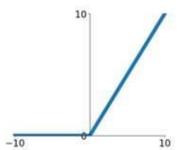


Maxout

 $\max(w_1^T x + b_1, w_2^T x + b_2)$

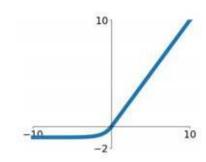
ReLU

 $\max(0,x)$



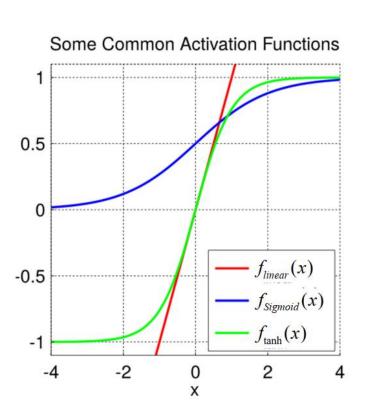
ELU

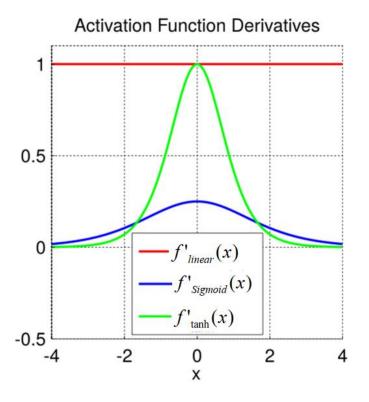
$$\begin{cases} x & x \ge 0 \\ \alpha(e^x - 1) & x < 0 \end{cases}$$



激活函数





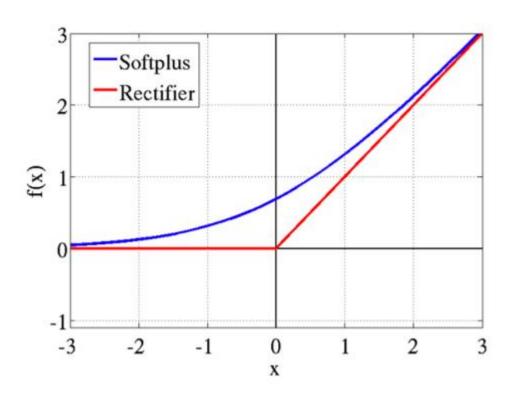


激活函数

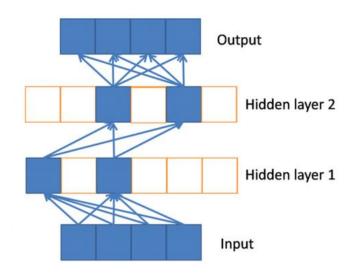


- ReLU(整流线性单元)
- $f_{\text{ReLU}}(x) = \max(0, x)$
- •与Softplus函数近似

$$f_{\text{Softplus}}(x) = \log(1 + e^x)$$



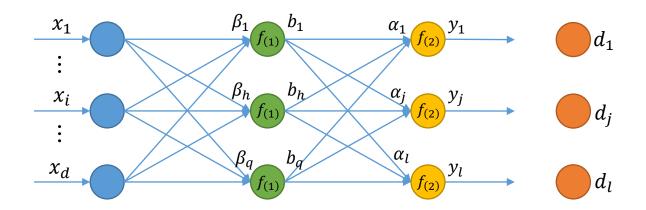
ReLU支持稀疏表示 只有一部分神经元被激活



损失函数



均方误差
$$\frac{1}{2}\sum_{j}(y_{j}-d_{j})^{2}$$



多分类损失 Cross Entropy $-\sum_j d_j \log y_j$

one-hot向量

$$H(P,Q) = \sum_{x} P(x) \log Q(x)$$

$$y_{j} = \frac{\exp(\alpha_{j})}{\sum_{i'} \exp(\alpha_{i'})}$$

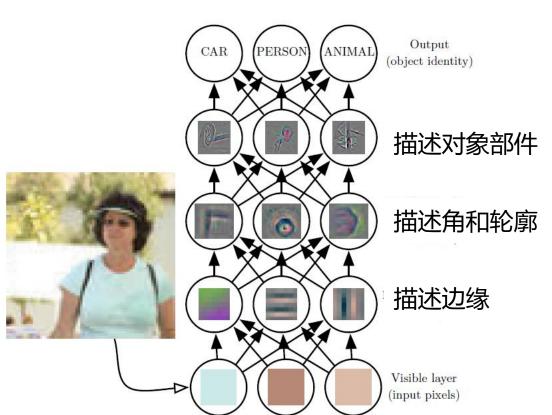
二分类损失 Cross Entropy l = 1 $-d \log y - (1 - d) \log(1 - y)$

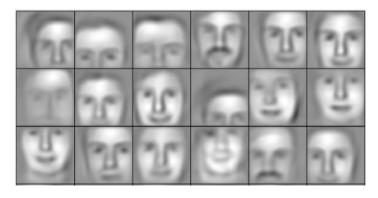
$$y = \frac{1}{1 + \exp(-\alpha)}$$

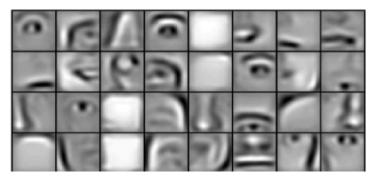
深度学习初探

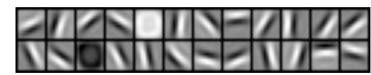


- 深度学习将大千世界表示为嵌套的层次概念体系
 - 由较简单概念间的联系定义复杂概念
 - 从一般抽象概括到高级抽象表示



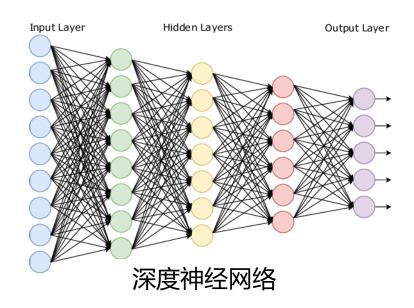


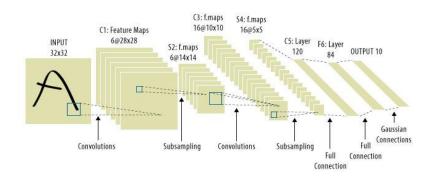




深度神经网络



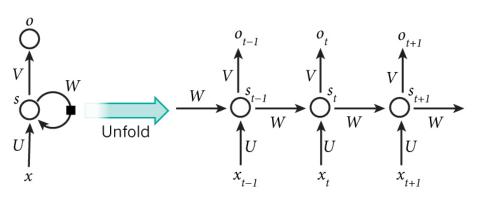


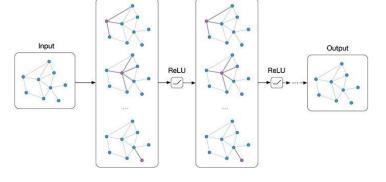


深度卷积网络

Hidden layer

Hidden layer





循环神经网络

图卷积网络

深度卷积网络



•一维卷积

$$s(t) = \int x(a)w(t-a)da$$

$$s(t) = \sum_{a} x(a)w(t - a)$$

输入

s(t) = (x * w)(t)

核函数

• 二维卷积

$$S(i,j) = (I * K)(i,j) = \sum_{m} \sum_{n} I(m,n)K(i-m,i-n)$$

$$S(i,j) = (I * K)(i,j) = \sum_{m} \sum_{n} I(i-m,j-n)K(m,n)$$

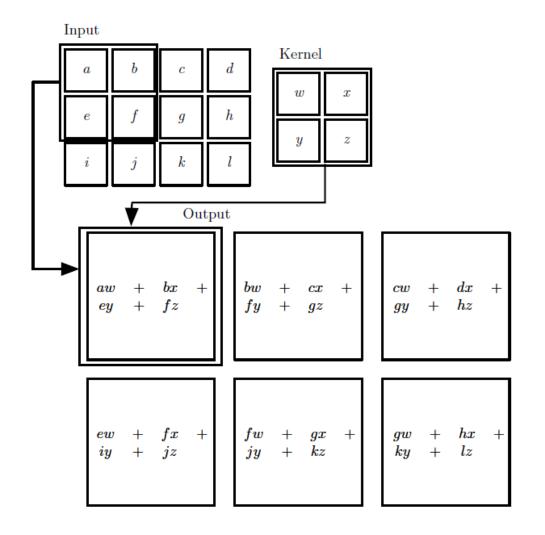
• 互相关函数

$$S(i,j) = (I * K)(i,j) = \sum_{m} \sum_{n} I(i+m,j+n)K(m,n)$$

卷积网络中的卷积

卷积的例子





卷积的例子



7x7的输入 3x3的核

5x5的输出

卷积的例子



I			

7x7的输入 3x3的核 步幅为2

3x3的输出

卷积

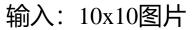


N

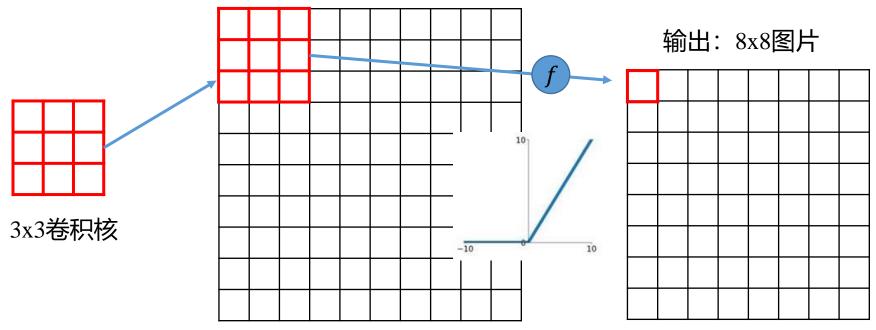
	ш		
F			

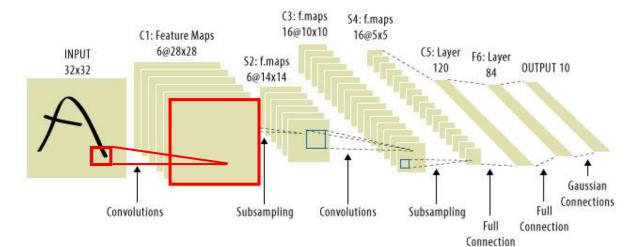
- 输出大小: (N-F)/S+1
 - S为步幅大小
- 比如N=7, F=3
 - 步幅为1, (7-3)/1+1=5
 - 步幅为2, (7-3)/2+1=3
 - 步幅为3, (7-3)/3+1=2.3..

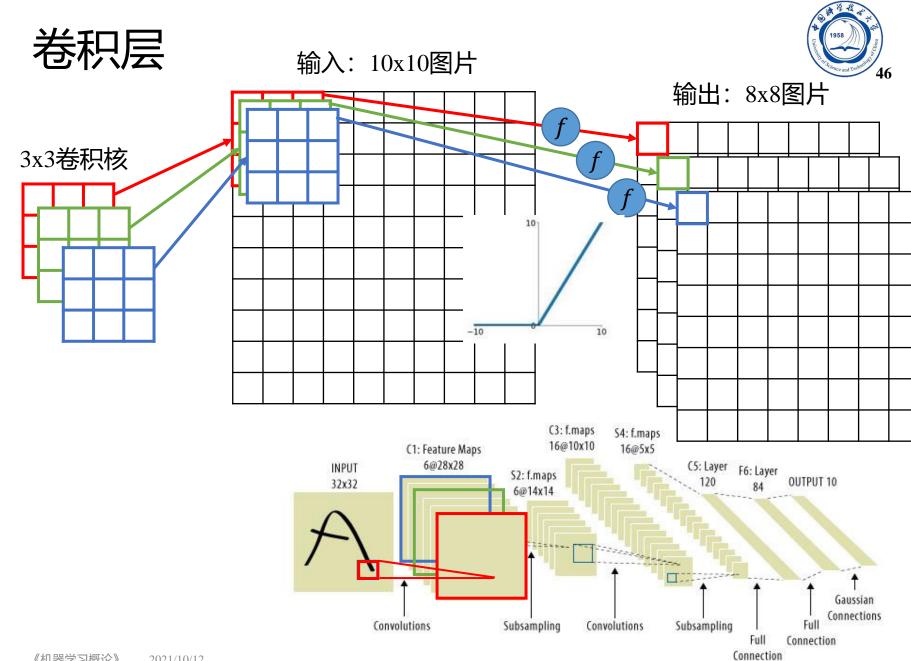












池化层



 1
 1
 2
 4

 5
 6
 7
 8

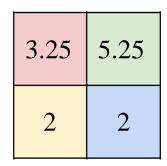
 3
 2
 1
 0

 1
 2
 3
 4

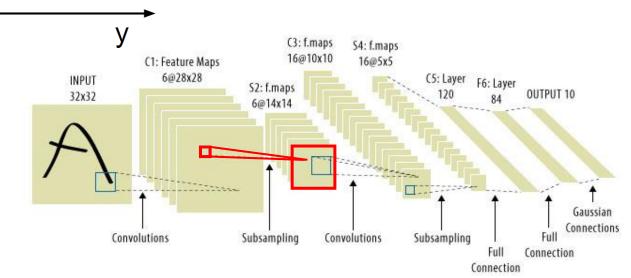
2x2的核, 步幅为2



6	8		
3	4		
最大池化			



平均池化



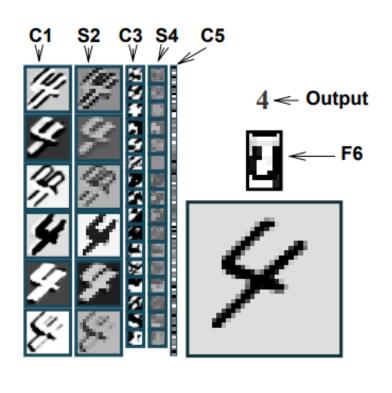
手写字符识别



• MNIST (handwritten digits) 数据集

http://yann.lecun.com/exdb/mnist/

6万训练样本和1万测试样本





错误案例

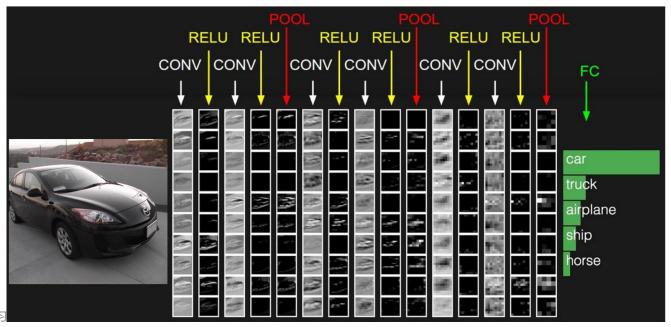
图片分类





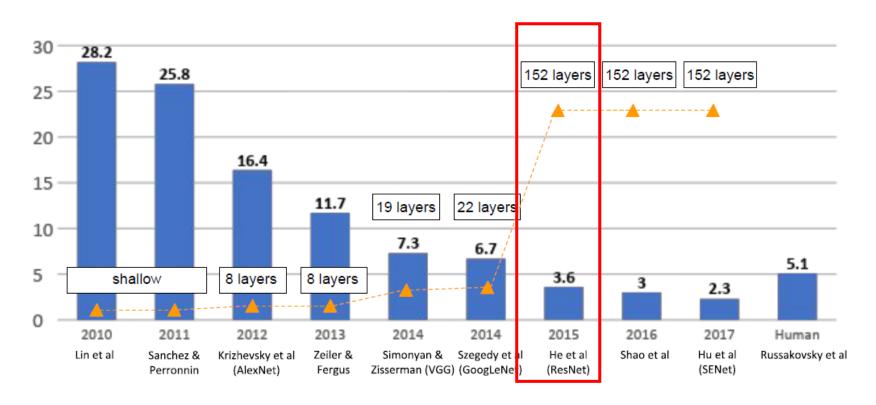
ImageNet数据集

大约2万2千个类别,1 千5百万张经过Amazon 众包平台标注过的图片



图片分类



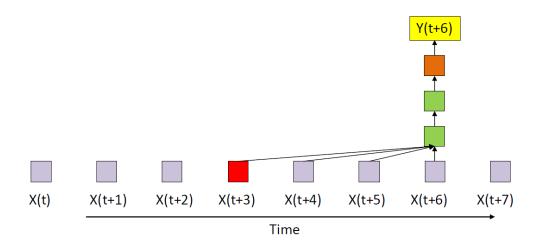


微软ResNet

在ImageNet图像数据库上,达到4.94%的错误率,低于人类5.1%的错误率



• 建模序列数据, 比如文本、时间序列等



有限响应模型

今天的信息只会对未来N天内的 预测有用

$$Y_t = f(X_t, X_{t-1}, \cdots, X_{t-N})$$

Time

无限响应模型

今天的信息对未来任何时刻的 预测都有用

$$Y_t = f(X_t, X_{t-1}, \cdots, X_{t-\infty})$$



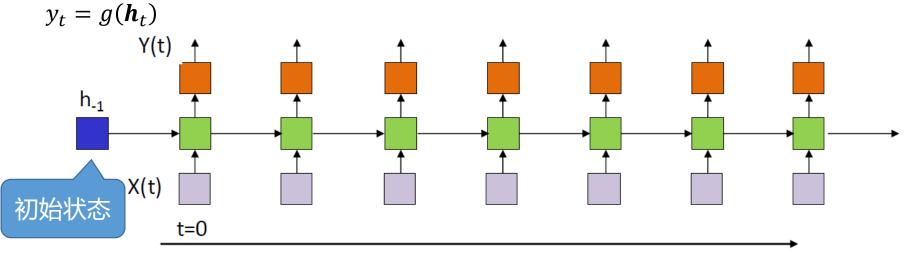
•用隐状态变量(状态) h_t "存储" 直到t时刻的历史数据 $\{x_1, \dots, x_t\}$,并用状态转移方程进行描述

$$\mathbf{h}_t = f_W(\mathbf{h}_{t-1}, \mathbf{x}_t)$$

每个时间步上的函数相同

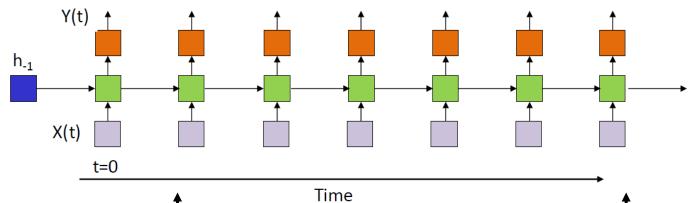
新状态 参数W 旧状态 t时刻的输入

$$\mathbf{h}_t = f_W(f_W(f_W(\mathbf{h}_{t-3}, \mathbf{x}_{t-2}), \mathbf{x}_{t-1}), \mathbf{x}_t)$$



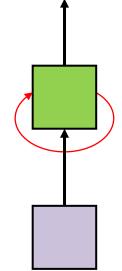
Time





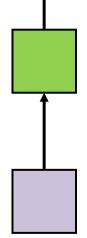
$$y_t = g(\boldsymbol{h}_t)$$

$$\boldsymbol{h}_t = f_{\boldsymbol{W}}(\boldsymbol{h}_{t-1}, \boldsymbol{x}_t)$$

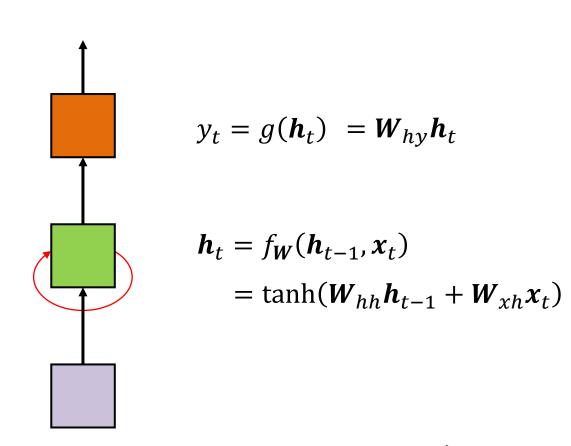


$$y_t = g(\boldsymbol{h}_t)$$

$$\boldsymbol{h}_t = f_{\boldsymbol{W}}(\boldsymbol{x}_t)$$

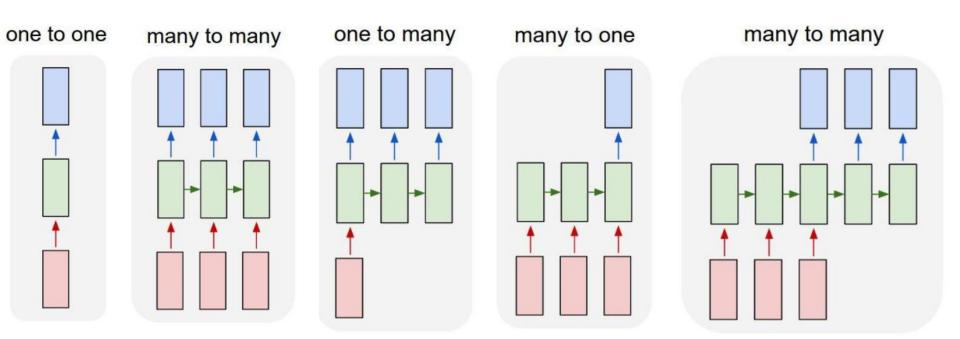






称Vanilla RNN 或Elman RNN





前向网络

例: 视频帧分类 例: 图像描述 视频帧 -> 类别

图像 -> 句子

例: 文本分类 文档 -> 类别

例: 机器翻译 句子 -> 句子



Image Captioning (图像描述)

循环神经网络

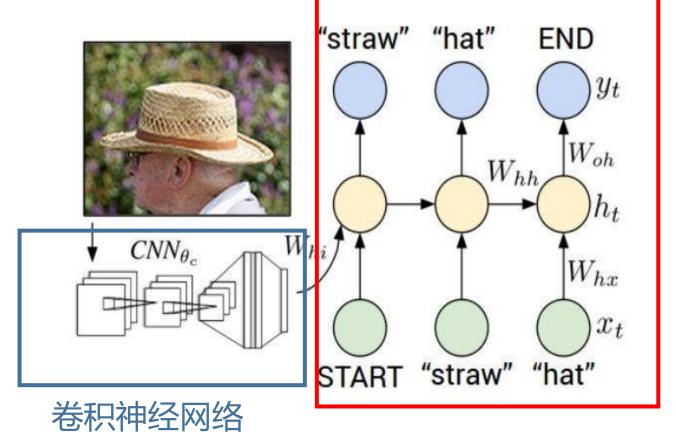




Image Captioning (图像描述)



A cat sitting on a suitcase on the floor



A cat is sitting on a tree branch



A dog is running in the grass with a frisbee



A white teddy bear sitting in the grass



Two people walking on the beach with surfboards



A tennis player in action on the court



Two giraffes standing in a grassy field

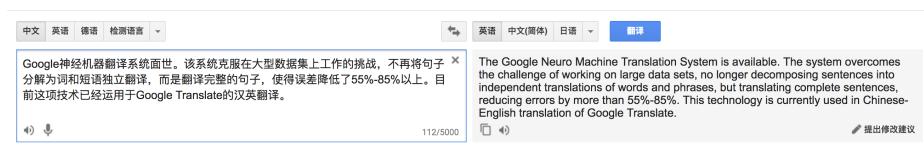


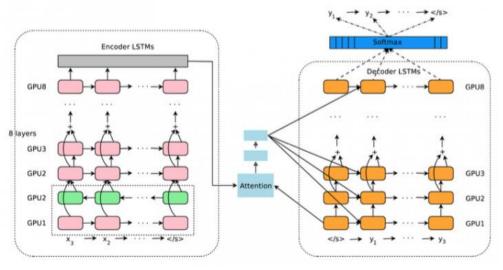
A man riding a dirt bike on a dirt track





机器翻译





2016 年,Google官方将全产品线的翻译算法换成了基于神经网络的机器翻译系统

作业



- 5.1
- 讨论 $\frac{\exp(x_i)}{\sum_{j=1}^{C} \exp(x_j)}$ 和 $\log \sum_{j=1}^{C} \exp(x_j)$ 的数值溢出问题
- 计算 $\frac{\exp(x_i)}{\sum_{j=1}^{C} \exp(x_j)}$ 和 $\log \frac{\exp(x_i)}{\sum_{j=1}^{C} \exp(x_j)}$ 关于向量 $\mathbf{x} = [x_1, \cdots, x_C]$ 的梯度
- 考虑如下简单网络,假设激活函数为ReLU,用平方损失 $\frac{1}{2}(y-\hat{y})^2$ 计算误差,请用BP算法更新一次所有参数(学习率为1),给出更新后的参数值(给出详细计算过程),并计算给定输入值x=(0.2,0.3) 时初始时和更新后的输出值,检查参数更新是否降低了平方损失值.

