# 第29章 深度学习

# 29.1 深度神经网络

### 命题 29.1.1 (浅层与深层神经网络对比)

设隐藏层数为 L, 记 浅层网络 Shallow NNet: L 较小, 深层网络 Deep NNet: L 较大.

	浅层网络	深层网络
训练效率	高 (🗸)	训练困难(※)
结构设计	简单 (✔)	复杂 (*)
理论表达能力	已足够(✔)	任意强大(✔)
特征抽象	有限	更具"语义"层次

结论 深层神经网络(深度学习)虽训练更复杂,却因更强的表达能力与层次特征而近年备受关注。

### 定义 29.1.1 (深度学习)

深度学习(Deep learning), 又称深度结构化学习(deep structured learning) 或层次式学习(hierarchical learning), 是机器学习算法的一个子类, 其核心特征如下:

- 1. 采用多层非线性处理单元级联(cascade)对原始输入进行特征提取与变换,每一层都以紧邻前一层输出作为输入;
- 2. 支持有监督、半监督或无监督的学习范式;
- 3. 学习多层次数据表征,对应不同抽象层级,形成概念的层次结构。

### 命题 29.1.2 (深度学习的主要挑战与关键技术)

深度网络在实践中面临四大难题,同时发展出相应的解决技术。

- 1. 结构决策困难 网络拓扑依赖主观领域知识,如图像任务常用卷积神经网络(CNN)。
- 2. 模型复杂度高

数据量足够时复杂度并非主要瓶颈:通过噪声鲁棒的正则化手段抑制过拟合

- Dropout: 对网络内部随机失活保持鲁棒;
- Denoising: 对输入扰动保持鲁棒。
- 3. 优化困难

非凸目标易陷坏局部极小:采用 预训练 (pre-training) 进行谨慎初始化, 避开劣质局部解。

4. 计算开销巨大

大数据放大计算需求:借助新型硬件/架构

- GPU 并行计算:
- Mini-batch 策略降低每次迭代成本。

结论 精心的正则化设计与权重初始化是当前深度学习成功的两大核心技术。



### 命题 29.1.3 (两步式深度学习框架)

将深度网络的训练解耦为两个阶段、既能缓解优化困难、又能提升最终性能。

### Step 1: 预训练(Pre-training)

逐层贪婪预训练:固定已训练层权重  $W^{(\ell-1)}$ , 仅更新当前层  $W^{(\ell)}$ ,  $\ell=1,\ldots,L$ 。该过程 为网络提供良好的初始权重,避免陷入劣质局部极小。

#### Step 2: 微调 (Fine-tuning)

在预训练所得权重基础上,使用反向传播(Backprop)对整个网络进行端到端微调,联合更新所有 $W^{(\ell)}$ 。

结论 "预训练+微调"构成当前最简洁有效的深度学习方法,后续可进一步结合正则化(如 Dropout)以控制过拟合。

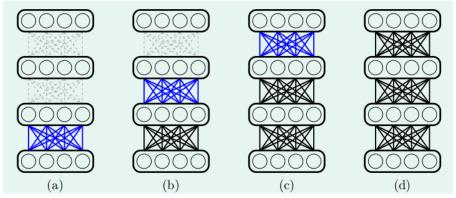


图 29.1.1: 深度学习预训练过程

### 例题 29.1 选择题:深度神经网络第一层隐藏层提取的特征

对于从原始像素进行手写字符识别的深度神经网络(deep NNet),在第一个隐藏层之后,更可能提取出以下哪种类型的特征?

- 1) pixels (像素)
- 2) strokes (笔画)
- 3) parts (部件)
- 4) digits (数字)

解答 正确选项为 2 。深度神经网络 (deep NNet) 处理手写字符识别时,特征提取是"逐步抽象"的:

- 输入是原始像素 (pixels),第一层隐藏层会学习基础的局部组合特征。对于手写字符,这些基础 特征对应笔画 (strokes) (如横竖撇捺等简单结构)。
- 后续层会基于笔画进一步组合,提取更复杂的"部件(parts)",最终识别出完整"数字(digits)"。 因此,第一个隐藏层后更可能提取出笔画(strokes)特征。

# 29.2 自编码器

### 命题 29.2.1 (自编码器:信息保持的表示学习)

设网络权重集合 W 定义编码-解码映射  $\Phi$ ,其工作流程为:先通过编码权重  $W^{(1)}$  将输入 x(如图片、文本等数据)转换为隐藏表示(可理解为数据的压缩版特征),再经解码权重  $W^{(2)}$  还原输入本身,形成闭环映射。

1. 信息保持准则

理想权重需满足重建误差极小化约束:

$$\Phi(x) \approx x$$

该约束确保编码后信息可通过不同表示形式复用,且解码过程能近似还原原始输入。

2. 自编码器 (autoencoder) 结构与目标

自编码器是典型的  $d \to \tilde{d} \to d$  结构神经网络,包含:

- 编码阶段: 通过权重  $W_{ij}^{(1)}$  将含偏置项的输入  $\mathbf{x} = [x_0, x_1, \dots, x_d]^{\mathsf{T}}$  映射到隐藏层 (常用 tanh 激活函数);
- 解码阶段: 通过权重  $W_{ii}^{(2)}$  映射回输出 g(x),目标是逼近恒等函数  $g_i(x) \approx x_i$ 。

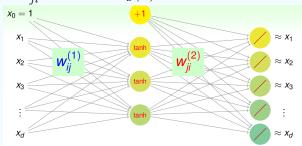


图 29.2.1: 自编码器 (autoencoder) 结构

核心用途

- 监督学习: 隐藏表示  $\Phi(x)$  作为信息浓缩特征, 可提升下游任务性能;
- 无监督学习
  - 密度估计:  $\|\Phi(x) x\|$  越小, 样本符合典型分布的概率越高;
  - 异常检测:  $\|\Phi(x) x\|$  显著偏大时判定为异常样本。

结论 自编码器通过近似恒等映射挖掘数据的紧凑可解释表示,由于其无需依赖大量标签,却能有效提取数据核心信息,是深度学习中预训练与特征提取的核心工具。

### 定义 29.2.1 (基本自编码器(Basic Autoencoder))

设输入维度为d, 隐藏层维度为 $\tilde{d}$ , 则基本自编码器为以下前馈网络:

$$d \xrightarrow{\text{in}} \tilde{d} \xrightarrow{\text{in}} d.$$

训练目标 给定数据集

$$\mathcal{D} = \{(x_1, y_1 = x_1), (x_2, y_2 = x_2), \dots, (x_N, y_N = x_N)\},\$$

最小化重建误差

$$E(W) = \sum_{n=1}^{N} \sum_{i=1}^{d} (g_i(x_n) - x_{n,i})^2.$$

特点

- 网络浅层, 易于训练, 可直接使用反向传播;
- 若 $\tilde{d} < d$ , 则隐藏层提供压缩(降维)表示;
- 常被视为无监督学习方法;
- 可附加权重共享或正则化约束(如  $W^{(2)}=W^{(1)\top}$ )以进一步控制模型复杂度。

用途 作为深度学习中的 浅层预训练手段,为基本网络提供良好的初始权重。

### 命题 29.2.2 (利用自编码器的预训练流程)

将深度网络逐层解耦为若干浅层自编码器,实现稳定且高效的预训练:

#### 1.逐层预训练

对  $\ell = 1, 2, ..., L$ :

- 1. 固定已训练层权重  $W^{(\ell-1)}$ :
- 2. 以第  $\ell-1$  层输出作为输入,构造维度为  $d^{(\ell)}$  的 基本自编码器

$$d^{(\ell-1)} \longrightarrow d^{(\ell)} \longrightarrow d^{(\ell-1)}$$
:

3. 通过最小化重建误差训练该自编码器,得到 $W^{(\ell)}$ 。

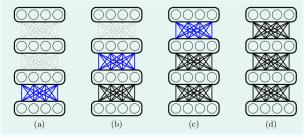


图 29.2.2: 逐层预训练示意图

#### 2. 微调

完成逐层预训练后,以所得权重为初始值,对整个网络执行端到端的反向传播微调。 进阶方案 成功案例常采用结构或正则化更复杂的自编码器,如

- 稀疏自编码器 (Sparse Autoencoder),
- 去噪自编码器 (Denoising Autoencoder),
- 收缩自编码器(Contractive Autoencoder)。

#### 例题 29.2 选择题:深度神经网络预训练时间计算

假设训练一个  $d - \tilde{d} - d$  的自动编码器(autoencoder),使用反向传播(backprop)大约需要  $c \cdot d \cdot \tilde{d}$  秒。那么,预训练一个  $d - d^{(1)} - d^{(2)} - d^{(3)} - 1$  的深度神经网络(deep NNet),总共需要多少秒?

- 1)  $c \left(d + d^{(1)} + d^{(2)} + d^{(3)} + 1\right)$
- 2)  $c \left( d \cdot d^{(1)} \cdot d^{(2)} \cdot d^{(3)} \cdot 1 \right)$
- 3)  $c \left( dd^{(1)} + d^{(1)}d^{(2)} + d^{(2)}d^{(3)} + d^{(3)} \right)$
- 4)  $c \left( dd^{(1)} \cdot d^{(1)}d^{(2)} \cdot d^{(2)}d^{(3)} \cdot d^{(3)} \right)$

解答 正确选项为 3。自动编码器训练时间与层间连接权重数量相关(如  $d-\tilde{d}-d$  模型中,时间为  $c\cdot d\cdot \tilde{d}$  ,对应  $d\times \tilde{d}$  个连接权重)。

对于  $d - d^{(1)} - d^{(2)} - d^{(3)} - 1$  深度神经网络预训练,需分解为多个自动编码器步骤:

- $d \to d^{(1)}$ : 连接权重数  $d \times d^{(1)}$ , 时间约  $c \cdot dd^{(1)}$ ;
- $d^{(1)} \rightarrow d^{(2)}$ : 连接权重数  $d^{(1)} \times d^{(2)}$ , 时间约  $c \cdot d^{(1)} d^{(2)}$ ;
- $d^{(2)} \to d^{(3)}$ : 连接权重数  $d^{(2)} \times d^{(3)}$ , 时间约  $c \cdot d^{(2)} d^{(3)}$ ;
- $d^{(3)} \to 1$ : 连接权重数  $d^{(3)} \times 1$ , 时间约  $c \cdot d^{(3)}$ 。

总时间为各步骤时间之和,即  $c\left(dd^{(1)}+d^{(1)}d^{(2)}+d^{(2)}d^{(3)}+d^{(3)}\right)$ 。

# 29.3 去噪自编码器

### 命题 29.3.1 (深度学习的正则化与过拟合再审视)

深度网络因高模型复杂度极易过拟合,需在结构与优化环节双重正则化。

- 1. 正则化手段
  - 结构约束: 人为设计网络拓扑(如 CNN)以限制参数量;
  - 权重正则化:
    - 权重衰减 Weight Decay:  $\Omega(w) = \lambda ||w||_2^2$ ,
    - 权重消除 Weight Elimination:  $\Omega(w) = \lambda \sum_i \frac{w_i^2}{1+w_i^2}$ ;
  - 早停 (Early Stopping): 在验证误差最低时终止训练。
- 2. 过拟合成因回顾

设数据量 N、噪声水平  $\sigma$ 、模型能力 P (如参数量),则

过拟合风险 
$$\propto \frac{\sigma}{N} \cdot P$$
.

因此:

- 噪声↑→过拟合↑;
- 数据量 ↓ → 过拟合 ↑;
- 模型能力↑→ 过拟合↑。

结论深度网络必须结合结构约束、权重正则化与早停,才能在高复杂度场景下抑制过拟合。

### 命题 29.3.2 (噪声处理:去噪自编码器)

面对数据中的噪声, 可将"人工添加噪声"本身作为一种正则化手段。

去噪自编码器(Denoising Autoencoder)

1. 构造含噪输入

$$\tilde{x}_n = x_n + \varepsilon_n, \quad \varepsilon_n \sim \text{人工噪声}.$$

2. 训练目标

$$\min_{W} \sum_{n=1}^{N} ||g(\tilde{x}_n) - x_n||^2,$$

即网络不仅要还原原始 $x_n$ ,还需在 $\tilde{x}_n$ 扰动下保持稳健。

3. 效果

- 在数据/图像处理中, q(x) 成为去噪后的版本;
- 强制网络学习噪声不变特征, 等价于在损失中引入正则项;
- 人工噪声作为"提示 (hint)", 可推广到其他神经网络或模型。

结论 去噪自编码器用"加噪→去噪"代替传统人工清洗,既提升鲁棒性又充当正则化,是深度学习中的常用预处理与正则策略。

### 例题 29.3 选择题:正则化技术判断

以下哪一项不能被视为正则化技术?

- 1) 使用人工生成的含噪声数据训练模型
- 2) 提前停止梯度下降
- 3) 添加权重消除正则项
- 4) 以上都是正则化技术

解答 正确选项为 4。正则化技术用于限制模型复杂度、避免过拟合:

- 选项 1: 添加噪声数据,增加数据多样性,迫使模型学习通用特征,属于正则化。
- 选项 2: 提前停止梯度下降, 防止模型在训练集过度拟合, 属于正则化。
- 选项 3: 权重消除正则项(如 L1/L2 正则),直接约束权重大小,限制模型复杂度,属于正则化。 因此,以上方法均为正则化技术。

# 29.4 主成分分析

### 定义 29.4.1 (线性自编码器假设)

设输入 $x \in \mathbb{R}^d$ (不含偏置项 $x_0$ ),为保证解的非平凡性,令隐藏层维度 $\tilde{d} < d$ 。对第k个隐藏分量,采用线性假设:

$$h_k(\boldsymbol{x}) = \sum_{j=0}^{\tilde{d}} w_{kj} \left( \sum_{i=1}^{d} w_{ij} x_i \right), \quad 1 \le k \le \tilde{d}$$

通过以下约束简化模型 (正则化与非平凡解保证):

- 排除冗余偏置: 若忽略  $x_0$ , 可令 i 的取值范围与 k 一致 (即  $i \in [1, \tilde{d}]$  或按需调整);
- 权重对称约束: 令  $w_{ij}^{(1)}=w_{ji}^{(2)}=w_{ij}$ ,记权重矩阵  $\mathbf{W}=[w_{ij}]\in\mathbb{R}^{d\times\tilde{d}}$ ,则线性自编码器的整体映射可推导为:

$$\boldsymbol{h}(\boldsymbol{x}) = \boldsymbol{W} \boldsymbol{W}^{\top} \boldsymbol{x}$$

• 非平凡解保证:  $\tilde{d} < d$  确保模型不是"恒等映射",强制学习低维特征表示。 核心特性

- 1. 高效与稳健性:线性结构简单,训练计算高效;d < d限制复杂度,降低过拟合风险,契合"先线性、再拓展非线性"的建模思路;
- 2. 与 PCA 的关联: 当权重对称且  $\tilde{d} < d$  时, $WW^{\top}$  可对应低秩重构矩阵,与主成分分析 (PCA) 的子空间投影逻辑等价,实现输入数据的低维主子空间提取。

### 命题 29.4.1 (线性自编码器的最优解)

给定中心化数据矩阵

$$oldsymbol{X} = egin{bmatrix} oldsymbol{x}_1 & oldsymbol{x}_2 & \dots & oldsymbol{x}_N \end{bmatrix} \in \mathbb{R}^{d imes N},$$

线性自编码器通过优化权重矩阵  $oldsymbol{W} \in \mathbb{R}^{ ilde{d} imes d}$  ( $ilde{d} < d$ ) 最小化重构误差:

$$E_{\text{in}}(\boldsymbol{W}) = \frac{1}{N} \sum_{n=1}^{N} \|\boldsymbol{x}_n - \boldsymbol{W}^{\top} \boldsymbol{W} \boldsymbol{x}_n\|^2.$$

求解过程如下:

1. 谱分解: 矩阵 → 正交变换 + 缩放 由于  $W^{\top}W \in \mathbb{R}^{d \times d}$  是对称半正定矩阵. 可做特征分解:

$$W^{\top}W = V\Gamma V^{\top},$$

其中:

- $V \in \mathbb{R}^{d \times d}$  是正交矩阵 (满足  $V^{\top}V = VV^{\top} = I_d$ ), 其列构成  $\mathbb{R}^d$  的标准正交基;
- $\Gamma$  是对角矩阵, 秩为  $\tilde{d}$  (即恰好  $\tilde{d}$  个非零对角元)。

对任意样本 $x_n$ ,  $W^{\top}Wx_n$  可拆解为三步几何操作:

$$oldsymbol{W}^ op oldsymbol{W} oldsymbol{x}_n \ = \ oldsymbol{V} oldsymbol{\Gamma} oldsymbol{V}^ op oldsymbol{x}_n$$

- (1)  $V^{\top}x_n$ : 将  $x_n$  投影到正交基  $\{v_1,\ldots,v_d\}$  上 (正交基变换,等价于旋转/反射,不改变向量长度);
- (2)  $\Gamma(V^{\top}x_n)$ : 对投影后的坐标做维度缩放,需将  $\geq d-\tilde{d}$  个分量置 0 (压缩冗余维度),剩余  $\tilde{d}$  个分量保留并缩放;
- (3)  $V(\Gamma V^{\top} x_n)$ : 将缩放后的坐标映射回原空间(逆正交基变换,等价于逆旋转/逆反射,重构数据)。
- 2. 最优 Γ: 二值化缩放因子

代入误差函数后,利用正交变换的保范性( $\|Vz\|=\|z\|$ ),重构误差等价于:

$$\min_{oldsymbol{V}} \min_{oldsymbol{\Gamma}} rac{1}{N} \sum_{n=1}^{N} \| oldsymbol{V}^{ op} oldsymbol{x}_n - oldsymbol{\Gamma} oldsymbol{V}^{ op} oldsymbol{x}_n \|^2$$

最小化该误差要求 Г的对角元满足二值化选择:

$$\gamma_i = \begin{cases} 1, & 1 \le i \le \tilde{d}, \\ 0, & \tilde{d} < i \le d, \end{cases}$$

即  $\Gamma = \begin{bmatrix} I_{\tilde{d}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$ , 表示保留前  $\tilde{d}$  维主成分信息、压缩其余  $d - \tilde{d}$  维冗余信息。

3. 最优 V: 主特征向量选择

将最优  $\Gamma$  代入后,误差最小化等价于最大化目标函数:

$$\min_{\mathbf{V}} \sum_{n=1}^{N} \left\| \begin{bmatrix} 0 & 0 \\ 0 & \mathbf{I}_{d-\tilde{d}} \end{bmatrix} \mathbf{V}^{T} \mathbf{x}_{n} \right\|^{2} \equiv \max_{\mathbf{V}} \sum_{n=1}^{N} \left\| \begin{bmatrix} \mathbf{I}_{\tilde{d}} & 0 \\ 0 & 0 \end{bmatrix} \mathbf{V}^{T} \mathbf{x}_{n} \right\|^{2}$$

根据瑞利商 (Rayleigh Quotient) 的极值性质, 其解由  $X^{T}X$  的前  $\tilde{d}$  个最大特征值对应的主

特征向量构成:

$$oldsymbol{V} = egin{bmatrix} oldsymbol{v}_1 & oldsymbol{v}_2 & \dots & oldsymbol{v}_{ ilde{d}} \end{bmatrix},$$

其中  $X^{\top}Xv_j = \lambda_j v_j$  且  $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{\tilde{d}}$ 。

4. 特殊验证: 恒等变换的抵消

当  $\Gamma = I_d$  (即不压缩维度,  $\tilde{d} = d$ ) 时,  $W^{\top}W = VI_dV^{\top} = I_d$ , 此时:

$$oldsymbol{W}^ op oldsymbol{W} oldsymbol{x}_n \ = \ oldsymbol{V} oldsymbol{I}_d oldsymbol{V}^ op oldsymbol{x}_n \ = \ oldsymbol{x}_n$$

结论 最优权重矩阵为  $\mathbf{W}_{\text{opt}} = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \dots & \mathbf{v}_{\tilde{d}} \end{bmatrix}^{\top}$ ,线性自编码器的编码过程等价于主成分分析(PCA)——通过正交基变换+维度缩放,提取数据方差最大的 $\tilde{d}$ 个主成分。

### 定义 29.4.2 (主成分分析(PCA) 与线性自编码器)

给定中心化数据矩阵  $X=[x_1 \cdots x_N] \in \mathbb{R}^{d\times N}$ ,计算协方差矩阵  $XX^{\top}$  的前  $\tilde{d}$  个最大特征值对应的特征向量

$$W = [w_1 \ w_2 \ \cdots \ w_{\tilde{d}}] \in \mathbb{R}^{d \times \tilde{d}}.$$

两种等价视角

• 线性自编码器:最大化投影后幅值平方和

$$\max_{W} \sum_{n=1}^{N} \|W^{\top} x_n\|^2, \quad W^{\top} W = I_{\tilde{d}}.$$

• 统计 PCA: 最大化投影后样本方差

$$\max_{W} \operatorname{Var}(W^{\top} x), \quad W^{\top} W = I_{\tilde{d}}.$$

统一结果 特征变换

$$\Phi(x) = W^{\top}(x - \bar{x}), \quad \bar{x} = \frac{1}{N} \sum_{n=1}^{N} x_n$$

完成线性降维, 其中 PCA 在统计与工程实践中更为常用。

### 例题 29.4 选择题: 优化问题的最优目标值

在求解优化问题  $\max_{\mathbf{v}} \sum_{n=1}^{N} \mathbf{v}^T \mathbf{x}_n \mathbf{x}_n^T \mathbf{v}$ (约束为  $\mathbf{v}^T \mathbf{v} = 1$ )时,已知最优  $\mathbf{v}$  是矩阵  $X^T X$  对应最大特征值  $\lambda$  的特征向量。那么该优化问题的最优目标值是多少?

- 1)  $\lambda^1$
- $\lambda^2$
- 3)  $\lambda^3$
- 4)  $\lambda^4$

解答 正确选项为 1 。

1. 目标函数变形:

利用矩阵求和性质, $\sum_{n=1}^{N} \mathbf{x}_n \mathbf{x}_n^T = X^T X$  (X 是以  $\mathbf{x}_n$  为列的矩阵),因此目标函数可写为:

$$\mathbf{v}^T \left( \sum_{n=1}^N \mathbf{x}_n \mathbf{x}_n^T \right) \mathbf{v} = \mathbf{v}^T (X^T X) \mathbf{v}$$

2. 特征值与特征向量的性质:

若  $\mathbf{v}$  是  $X^T X$  对应特征值  $\lambda$  的特征向量,则  $(X^T X)\mathbf{v} = \lambda \mathbf{v}$  。

3. 代入约束计算目标值:

结合约束  $\mathbf{v}^T\mathbf{v} = 1$ ,有:

$$\mathbf{v}^T(X^TX)\mathbf{v} = \mathbf{v}^T(\lambda \mathbf{v}) = \lambda \cdot (\mathbf{v}^T \mathbf{v}) = \lambda$$

由于  $\lambda^1 = \lambda$ ,因此最优目标值为  $\lambda^1$ ,对应选项 1。

## 29.5 总结

# Ŷ 笔记[深度学习]

- 深度神经网络: 解决困难的层级特征提取问题。
- 自编码器: 无监督神经网络, 用于学习数据表示。
- 去噪自编码器:将噪声作为"提示",实现正则化。
- 主成分分析: 线性自编码器的变体, 用于数据处理。
- 全记 [总体结论] 深度学习作为机器学习的重要分支,通过多层非线性处理单元构建层次化特征表示,实现对复杂数据的高效建模。其核心在于利用深度神经网络的层级结构,从原始输入中逐层提取抽象特征,并通过"预训练+微调"等策略缓解优化难题。自编码器作为无监督学习工具,通过编码-解码的闭环映射挖掘数据的紧凑表示,为深度网络提供有效的预训练初始化;去噪自编码器则将噪声引入训练过程,兼具特征学习与正则化功能,增强模型鲁棒性。主成分分析作为线性自编码器的特例,通过特征分解实现数据降维,为理解深度网络的线性基础提供了桥梁。尽管深度学习面临结构设计复杂、计算成本高、易过拟合等挑战,但凭借强大的表达能力与层次化特征提取优势,已成为处理图像、文本等复杂数据的核心技术,其发展依赖于正则化设计、优化算法与硬件算力的协同进步。