

# 深度学习基础理论与方法综述

褚一凡

郑州工业应用技术学院

DOI:10.12238/acair.v3i3.15554

**[摘要]** 深度学习在计算机视觉、自然语言处理等领域取得重大进展,但理论基础仍待完善。本文回顾了深度学习核心理论,包括神经网络原理、反向传播算法和深度网络的表达特性。分析了四种主流架构:前馈神经网络构建了基础框架,卷积神经网络通过局部连接实现图像处理突破,循环神经网络解决序列建模问题,Transformer通过注意力机制提升性能。梳理了SGD到Adam等优化算法的发展,探讨了Dropout、批量归一化等正则化技术。分析了大规模预训练模型趋势和模型压缩等前沿技术,指出计算资源增长、可解释性不足等挑战。

**[关键词]** 深度学习; 神经网络; 优化算法

**中图分类号:** TP183 **文献标识码:** A

## A Review of the Basic Theories and Methods of Deep Learning

Yifan Chu

Zhengzhou University of Industrial Technology

**[Abstract]** Deep learning has made significant progress in fields such as computer vision and natural language processing, but its theoretical foundation still needs improvement. This paper reviews the core theories of deep learning, including the principles of neural networks, the backpropagation algorithm, and the expressive characteristics of deep networks. It analyzes four mainstream architectures: feedforward neural networks form the basic framework, convolutional neural networks achieve breakthroughs in image processing through local connections, recurrent neural networks solve sequence modeling problems, and Transformers enhance performance through attention mechanisms. It also sorts out the development from SGD to Adam and other optimization algorithms, and discusses regularization techniques such as Dropout and batch normalization. It analyzes the trend of large-scale pre-trained models and frontier technologies such as model compression, and points out challenges such as the growth of computing resources and insufficient interpretability.

**[Key words]** Deep learning; Neural networks; Optimization algorithms

### 引言

深度学习作为机器学习的重要分支,近年来在计算机视觉、自然语言处理、语音识别等领域取得了突破性进展。从2006年Hinton提出深度信念网络概念,到2012年AlexNet在ImageNet竞赛中的卓越表现,再到近期大型语言模型的涌现,深度学习技术不断刷新着人工智能应用的边界。然而,深度学习的快速发展也带来了理论基础相对滞后的问题。虽然实践应用成果丰硕,但对于深度网络为何有效、如何优化、泛化能力从何而来等核心问题,学术界仍在探索之中。同时,随着网络结构日益复杂、参数规模急剧增长,如何在保证性能的同时提高训练效率、降低计算成本,成为亟待解决的关键挑战。本文旨在系统梳理深度学习的基础理论框架与核心方法,分析当前研究的热点问题与发展趋势,为相关领域的研究者提供全面的参考视角。

### 1 深度学习基础理论

#### 1.1 神经网络基本原理

神经网络的基本单元是人工神经元,其数学模型为:

$$y = f\left(\sum_{i=1}^n w_i x_i + b\right)$$

其中  $w_i$  为权重参数,  $b$  为偏置项,  $f$  为激活函数。常用激活函数包括ReLU、Sigmoid和Tanh等,其中ReLU函数 ( $f(x) = \max(0, x)$ ) 因其计算简单且能有效缓解梯度消失问题而被广泛采用。

多层感知机通过堆叠多个神经元层构成,每层的输出作为下一层的输入。前馈神经网络的信息传递过程为单向的,从输入层经隐藏层最终到达输出层。网络的表达能力与其深度和宽度密切相关,根据万能逼近定理,具有足够多隐藏单元的单独隐藏层

网络理论上可以逼近任意连续函数,但实践中深层网络往往表现更优。

### 1.2 反向传播算法

反向传播算法是训练神经网络的核心方法,基于链式法则计算损失函数对各层参数的梯度。设损失函数为 $L$ ,第 $l$ 层的权重为 $W^{[l]}$ ,则梯度计算公式为:

$$\frac{\partial L}{\partial W^{[l]}} = \frac{\partial L}{\partial z^{[l]}} = \frac{\partial z^{[l]}}{\partial W^{[l]}}$$

算法分为前向传播和反向传播两个阶段。前向传播计算各层的激活值和最终输出,反向传播从输出层开始,逐层计算误差信号并更新参数。具体而言,对于第 $l$ 层,误差信号 $\delta^{[l]} = \frac{\partial L}{\partial z^{[l]}}$ 的计算依赖于下一层的误差:

$$\delta^{[l]} = (W^{[l+1]})^T \delta^{[l+1]} \odot f'(z^{[l]})$$

其中 $\odot$ 表示逐元素乘积。该算法的时间复杂度为 $O(w)$ ,其中 $w$ 为网络中权重参数的总数,使得大规模网络的训练成为可能。

### 1.3 深度网络的理论基础

深度网络的表达能力源于其分层特征学习机制。从信息论角度看,深层网络通过逐层抽象,将原始输入映射到高维特征空间,实现了从低级特征到高级语义的递进式表示。Bengio等人的研究表明,某些函数类需要指数级的浅层网络才能表示,而深层网络则可以用多项式级的参数高效表达。深度网络的优化landscape呈现复杂的非凸特性,存在大量局部最优解和鞍点。然而,研究发现高维空间中的局部最优解往往接近全局最优,且随机梯度下降能够有效逃离鞍点。损失函数的Hessian矩阵特征值分析显示,深度网络训练过程中负特征值(对应鞍点)比正特征值更常见。泛化理论方面,传统的VC维和Rademacher复杂度理论难以解释深度网络的泛化能力。新兴的研究从隐式正则化、梯度下降的归纳偏置等角度,揭示了深度网络良好泛化性能的内在机制。

## 2 主要网络架构与方法

### 2.1 前馈神经网络

前馈神经网络(Feedforward Neural Network)是最基础的神经网络架构,信息从输入层单向流向输出层,不存在反馈连接。典型的多层感知机(MLP)包含输入层、一个或多个隐藏层和输出层。每个神经元通过加权求和后经过非线性激活函数进行变换,常用的激活函数包括ReLU、Sigmoid和Tanh。网络的核心学习机制是反向传播算法,通过计算损失函数对权重的梯度来更新参数。前馈网络的表达能力由万能逼近定理保证,即具有足够宽度的单隐藏层网络可以逼近任意连续函数。然而,深度网络在实际应用中表现更优,因为其分层特征提取能力更强。前馈网络广泛应用于分类、回归等基础任务,是构建更复杂架构的基础

组件,网络性能很大程度上依赖于架构设计、激活函数选择和正则化策略。

### 2.2 卷积神经网络

卷积神经网络(CNN)专门设计用于处理具有网格结构的数据,如图像。其核心操作是卷积运算,通过可学习的卷积核在输入上滑动进行特征提取。卷积层具有局部连接、权重共享和平移不变性三个重要特性,大幅减少了参数数量并提高了模型的泛化能力。典型的CNN架构包含卷积层、池化层和全连接层。池化层通过下采样操作降低特征图尺寸,增强模型对位置变化的鲁棒性,常用的有最大池化和平均池化。从LeNet-5到AlexNet、VGGNet、ResNet的发展历程展现了CNN架构的演进:网络越来越深,引入了批量归一化、残差连接等技术解决梯度消失问题。CNN在计算机视觉任务中取得了突破性进展,包括图像分类、目标检测、语义分割等。现代CNN变体如DenseNet、EfficientNet等进一步优化了参数效率和计算复杂度。

### 2.3 循环神经网络

循环神经网络(RNN)设计用于处理序列数据,其核心特征是隐藏状态的循环连接,使网络能够保持对历史信息的记忆。标准RNN通过隐藏状态 $h_t = \tanh(Wx_t + Wh_{t-1} + bh)$ 递归更新状态,理论上可以处理任意长度的序列。然而,标准RNN存在梯度消失和梯度爆炸问题,难以学习长期依赖关系。为解决这一问题,长短期记忆网络(LSTM)引入了门控机制,包括遗忘门、输入门和输出门,通过细胞状态维护长期记忆。门控循环单元(GRU)是LSTM的简化版本,仅使用重置门和更新门,计算效率更高。RNN及其变体在自然语言处理、语音识别、时间序列预测等序列建模任务中表现优异。双向RNN通过同时处理正向和反向序列信息进一步提升了性能。尽管Transformer架构在某些任务上超越了RNN,但RNN在流式处理和内存受限场景中仍具有独特优势。

### 2.4 注意力机制与Transformer

注意力机制的核心思想是让模型在处理序列时能够动态关注不同位置的信息,而非仅依赖固定的隐藏状态。自注意力(Self-Attention)机制通过计算序列中每个位置与其他所有位置的相关性来构建表示,具体通过查询(Query)、键(Key)和值(Value)三个矩阵计算注意力权重:  $\text{Attention}(Q, K, V) = \text{softmax}(QK^T / \sqrt{dk})V$ 。Transformer架构完全基于注意力机制构建,摒弃了循环和卷积操作。编码器-解码器结构中,多头注意力允许模型同时关注不同的表示子空间,位置编码则为序列提供位置信息。残差连接和层归一化保证了深层网络的训练稳定性。相比RNN,Transformer最大的优势是并行化计算能力,训练效率显著提升。

## 3 优化技术与发展趋势

### 3.1 优化算法发展

深度学习优化算法经历了从基础梯度下降到自适应优化器的重要演进。随机梯度下降(SGD)作为基础优化方法,通过小批量样本估计梯度进行参数更新,其动量变体Momentum通过累积历史梯度信息加速收敛并减少震荡。自适应学习率优化器的出

现标志着重要突破。AdaGrad通过累积平方梯度自适应调整学习率,解决了不同参数更新频率差异问题,但存在学习率单调递减的局限。RMSprop通过指数移动平均改进了AdaGrad的缺陷。Adam优化器结合了Momentum和RMSprop的优势,同时维护梯度的一阶和二阶矩估计,成为深度学习中应用最广泛的优化器。学习率调度策略对训练效果具有重要影响。常用策略包括步长衰减、余弦退火、循环学习率等。预热(Warmup)技术在大批量训练中尤为重要,通过逐步增加学习率避免训练初期的不稳定。近年来,AdamW通过解耦权重衰减进一步改进了Adam,在Transformer等大模型训练中表现优异。

### 3.2 正则化与泛化技术

正则化技术是防止深度网络过拟合、提高泛化能力的关键手段。Dropout通过训练时随机丢弃部分神经元连接,强制网络学习更鲁棒的特征表示,测试时通过集成效应提升性能。DropConnect进一步扩展了这一思想,随机丢弃权重连接而非神经元。批量归一化(Batch Normalization)通过标准化层输入分布,不仅加速了训练收敛,还具有正则化效果。其成功催生了Layer Normalization、Group Normalization等变体,适应不同的网络架构和应用场景。权重衰减(Weight Decay)通过在损失函数中加入L2正则项,约束模型复杂度。数据增强技术通过对训练数据施加变换生成新样本,有效扩充训练集并提高模型对数据变化的鲁棒性。早停(Early Stopping)通过监控验证集性能防止过训练。近年来涌现的新技术包括标签平滑、Mixup数据混合、Cutout随机遮挡等,这些方法从不同角度改善模型的泛化性能,在实际应用中取得了显著效果。

### 3.3 当前发展趋势与挑战

深度学习正朝着大规模预训练模型方向发展。GPT、BERT等语言模型展现了大规模无监督预训练的强大能力,通过在海量文本上预训练再进行下游任务微调,实现了跨任务的知识迁移。视觉领域的ViT、多模态领域的CLIP等模型进一步验证了这一范式的有效性。模型规模急剧增长带来了计算效率挑战。模型压缩技术包括知识蒸馏、网络剪枝、量化等方法,旨在在保持性能的同时减少计算和存储开销。神经架构搜索(NAS)通过自动化设计网络结构,提高了架构设计效率。当前面临的主要挑战包括:计算资源需求呈指数级增长,对硬件和能耗提出更高要求;

模型可解释性不足,限制了在安全关键领域的应用;数据隐私和公平性问题日益突出;少样本学习和领域泛化能力仍需提升。未来发展方向可能集中在高效模型架构、可解释AI、联邦学习、神经符号融合等领域,以实现更智能、更可靠、更高效的人工智能系统。

## 4 结语

深度学习的发展体现了从简单到复杂的架构演进过程。前馈网络奠定基础,卷积网络利用空间局部性,循环网络处理时序信息,Transformer实现全局建模。每种架构都针对特定数据特性设计,推动了相应领域的突破。优化技术从基础梯度下降发展到自适应优化器,正则化方法不断丰富,解决了训练中的实际问题。当前大模型展现了规模效应的价值,但计算成本、模型解释性、应用部署等问题日益突出。未来发展需要平衡模型能力与实用性,在追求性能的同时考虑效率和可解释性,推动深度学习向更成熟的技术方向发展。

### [参考文献]

- [1]柯美东.深度学习的理论基础探索[J].成才,2024,(4):4-7.
- [2]李超毅,宗京秀.基于深度学习的图像识别技术研究[J].中国战略新兴产业,2025,(11):57-60.
- [3]李伶俐.基于深度学习理论的人脸识别技术应用综述[J].计算机与数字工程,2021,49(09):1912-1914+1929.
- [4]韩小虎,徐鹏,韩森森.深度学习理论综述[J].计算机时代,2016,(06):107-110.
- [5]陈嘉毅,韩磊,叶敏,等.基于卷积神经网络的碎石撒布状态检测算法优化研究[J].工程机械,2025,56(05):62-66+10.
- [6]张宗宇,徐军,陈士超.基于Dropout策略的卷积神经网络的数字识别效果研究[J].兰州文理学院学报(自然科学版),2025,39(03):43-47+52.
- [7]汤学民,吴晓云.基于前馈神经网络电子病历辅助诊断系统的研究[J].中国数字医学,2023,18(03):42-48.
- [8]张浩,吴秀娟.深度学习的内涵及认知理论基础探析[J].中国电化教育,2012,(10):7-11+21.

### 作者简介:

褚一凡(2004--),男,回族,河南省周口市人,本科,主要研究方向:计算机深度学习。