

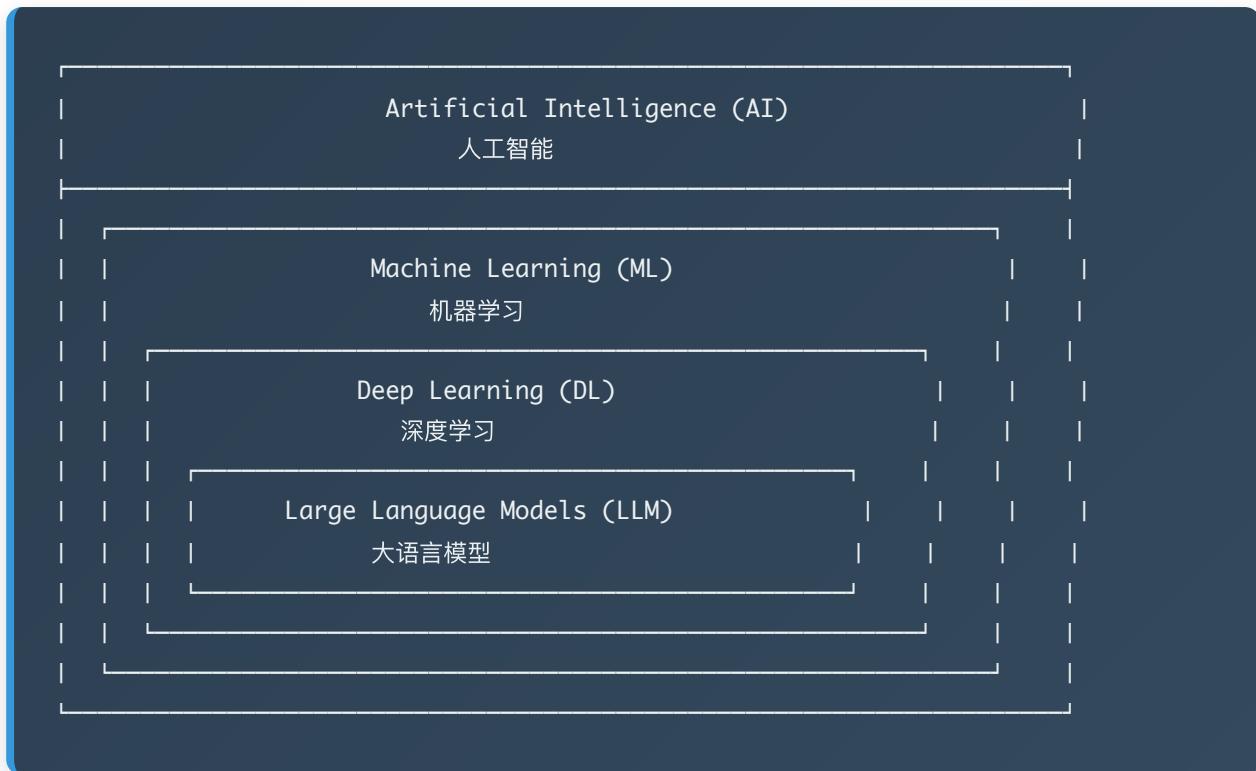
AI核心算法全景图：Machine Learning、Deep Learning与LLM

本文档系统梳理人工智能领域三大核心方向的主流算法、应用场景、典型案例，并精选优质动画教学资源，助力深度学习之旅。

目录

1. 概述：AI三大领域关系图谱
2. Machine Learning 机器学习
3. Deep Learning 深度学习
4. Large Language Models 大语言模型
5. 优质动画教学资源汇总
6. 学习路线建议

1. 概述：AI三大领域关系图谱



三者关系说明

领域	定义	核心特点
Machine Learning	让机器从数据中学习规律的算法总称	特征工程、统计模型、解释性强
Deep Learning	使用深层神经网络的机器学习子集	自动特征提取、端到端学习
LLM	基于Transformer的超大规模语言模型	海量参数、涌现能力、通用智能

2. Machine Learning 机器学习

2.1 算法分类体系

```
Machine Learning
├─ 监督学习 (Supervised Learning)
|  ├─ 回归 (Regression)
|  |  ├─ 线性回归 (Linear Regression)
|  |  ├─ 多项式回归 (Polynomial Regression)
|  |  └─ 岭回归/Lasso (Ridge/Lasso Regression)
|  └─ 分类 (Classification)
|    ├─ 逻辑回归 (Logistic Regression)
|    ├─ 决策树 (Decision Tree)
|    ├─ 随机森林 (Random Forest)
|    ├─ 支持向量机 (SVM)
|    ├─ K近邻 (KNN)
|    ├─ 朴素贝叶斯 (Naive Bayes)
|    └─ 梯度提升 (XGBoost/LightGBM)

|
├─ 无监督学习 (Unsupervised Learning)
|  ├─ 聚类 (Clustering)
|  |  ├─ K-Means
|  |  ├─ DBSCAN
|  |  └─ 层次聚类 (Hierarchical)
|  ├─ 降维 (Dimensionality Reduction)
|  |  ├─ PCA
|  |  ├─ t-SNE
|  |  └─ UMAP
|  └─ 关联规则 (Association Rules)
    └─ Apriori

|
└─ 强化学习 (Reinforcement Learning)
    ├─ Q-Learning
    ├─ SARSA
    ├─ DQN
    ├─ Policy Gradient
    ├─ Actor-Critic
    └─ PPO/SAC
```

2.2 核心算法详解

2.2.1 线性回归 (Linear Regression)

项目	内容
原理	通过最小化均方误差，找到最佳拟合直线 $y = wx + b$
适用场景	连续值预测、趋势分析
典型案例	房价预测、销量预测、股票趋势
优点	简单直观、可解释性强、计算快速
缺点	只能处理线性关系

2.2.2 逻辑回归 (Logistic Regression)

项目	内容
原理	使用Sigmoid函数将线性输出映射到[0,1]概率区间
适用场景	二分类问题、概率预测
典型案例	垃圾邮件检测、疾病诊断、信用评分
优点	输出概率值、训练快速、易于正则化
缺点	线性决策边界、特征工程依赖

2.2.3 决策树 (Decision Tree)

项目	内容
原理	通过信息增益/基尼系数递归分裂节点
适用场景	分类和回归、规则挖掘
典型案例	客户流失预测、贷款审批、医疗诊断
优点	可视化强、无需特征缩放、处理非线性
缺点	容易过拟合、对噪声敏感

2.2.4 随机森林 (Random Forest)

项目	内容
原理	多棵决策树的集成，通过投票/平均得到结果
适用场景	复杂分类回归、特征重要性分析
典型案例	金融风控、推荐系统、图像分类
优点	抗过拟合、处理高维数据、并行训练
缺点	模型较大、预测速度慢

2.2.5 支持向量机 (SVM)

项目	内容
原理	寻找最大间隔超平面，通过核函数处理非线性
适用场景	高维小样本分类
典型案例	文本分类、人脸识别、生物信息学
优点	泛化能力强、核技巧灵活
缺点	大数据集训练慢、参数敏感

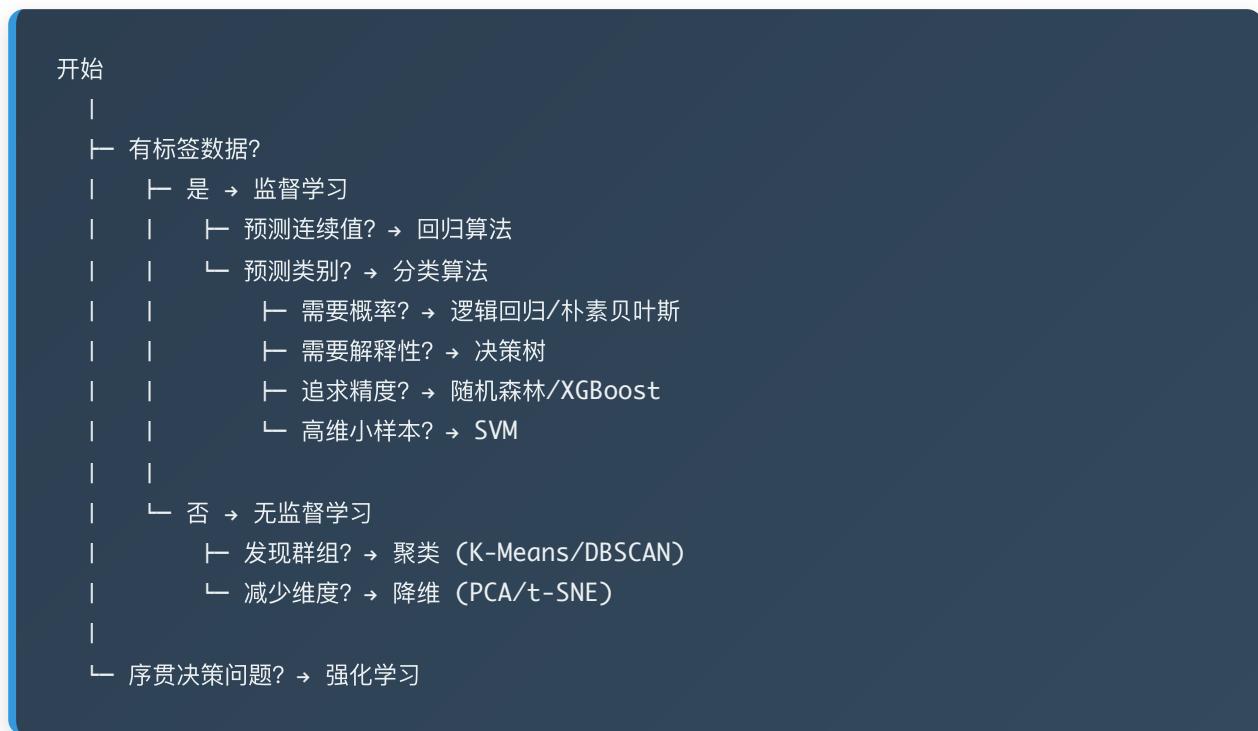
2.2.6 K-Means 聚类

项目	内容
原理	迭代更新K个聚类中心，最小化簇内距离
适用场景	客户分群、图像压缩、异常检测
典型案例	市场细分、社交网络分析、文档聚类
优点	简单高效、易于实现
缺点	需预设K值、对初始化敏感

2.2.7 强化学习 (Reinforcement Learning)

项目	内容
原理	智能体与环境交互，通过奖励信号学习最优策略
适用场景	序贯决策、游戏AI、机器人控制
典型案例	AlphaGo、自动驾驶、推荐系统
核心概念	状态(State)、动作(Action)、奖励(Reward)、策略(Policy)

2.3 算法选择指南



3. Deep Learning 深度学习

3.1 神经网络架构体系

Deep Learning

- ├─ 基础架构
 - | ├─ 多层感知机 (MLP/DNN)
 - | ├─ 激活函数 (ReLU, Sigmoid, GELU, Swish)
 - | └─ 优化器 (SGD, Adam, AdamW)
 - |
 - | ├─ 卷积神经网络 (CNN)
 - | ├─ LeNet-5 (1998)
 - | ├─ AlexNet (2012)
 - | ├─ VGGNet (2014)
 - | ├─ GoogLeNet/Inception (2014)
 - | ├─ ResNet (2015)
 - | ├─ DenseNet (2017)
 - | ├─ EfficientNet (2019)
 - | └─ ConvNeXt (2022)
 - |
 - | ├─ 循环神经网络 (RNN)
 - | ├─ Vanilla RNN
 - | ├─ LSTM (1997)
 - | ├─ GRU (2014)
 - | └─ Bidirectional RNN
 - |
 - | ├─ Transformer架构
 - | ├─ 原始Transformer (2017)
 - | ├─ BERT (2018)
 - | ├─ GPT系列 (2018-)
 - | ├─ Vision Transformer/ViT (2020)
 - | └─ Swin Transformer (2021)
 - |
 - |
 - | ├─ 生成模型
 - | ├─ 自编码器 (Autoencoder/VAE)
 - | ├─ 生成对抗网络 (GAN)
 - | | ├─ DCGAN
 - | | ├─ StyleGAN
 - | | └─ CycleGAN
 - | └─ 扩散模型 (Diffusion Model)
 - | └─ DDPM
 - | └─ Stable Diffusion
 - | └─ DALL-E

- |
 - 图神经网络 (GNN)
 - |— GCN
 - |— GraphSAGE
 - |— GAT

3.2 核心架构详解

3.2.1 卷积神经网络 (CNN)

项目	内容
核心组件	卷积层、池化层、全连接层
核心思想	局部感受野、权重共享、层次特征提取
适用场景	图像分类、目标检测、语义分割
典型案例	ImageNet分类、自动驾驶视觉、医学影像诊断
里程碑模型	AlexNet(2012突破)、ResNet(残差连接)、EfficientNet(高效率)

CNN核心操作：

输入图像 → [卷积→激活→池化] × N → 展平 → 全连接 → 输出

↓

特征图提取：边缘→纹理→部件→整体

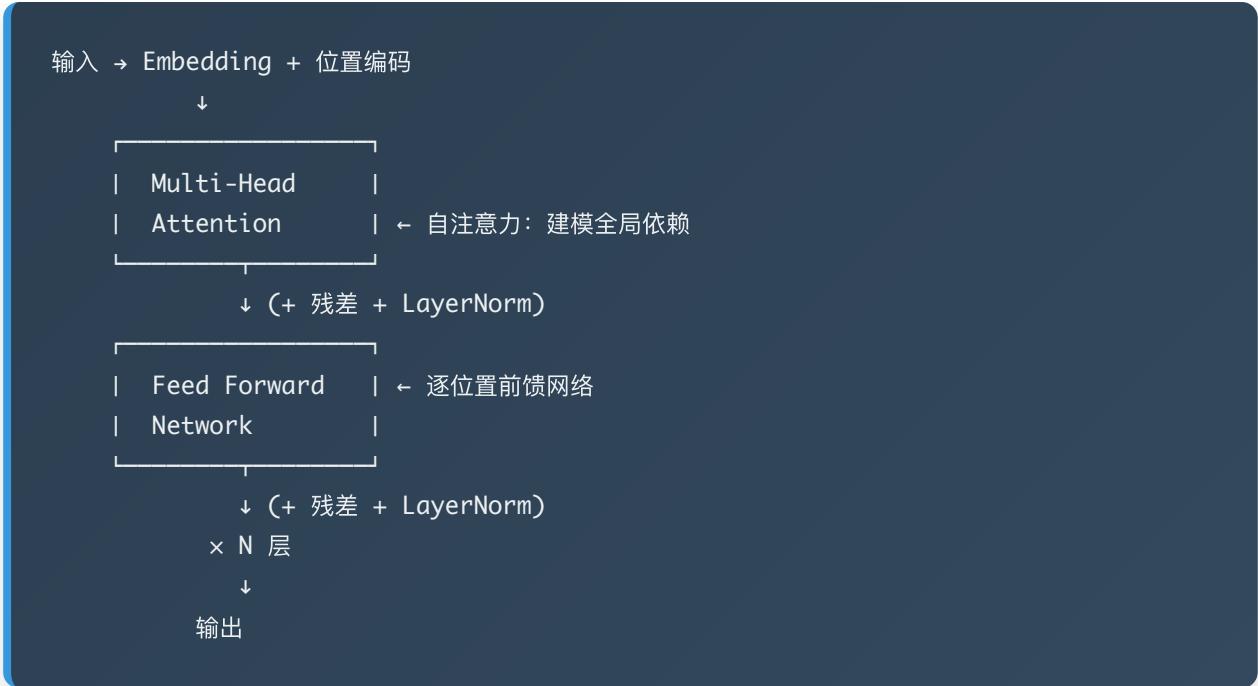
3.2.2 循环神经网络 (RNN/LSTM/GRU)

项目	内容
核心思想	处理序列数据，维护隐藏状态记忆历史信息
LSTM改进	引入门控机制(遗忘门、输入门、输出门)解决梯度消失
GRU改进	简化门控(重置门、更新门)，参数更少
适用场景	时序预测、机器翻译、语音识别
典型案例	股价预测、情感分析、语音转文字

3.2.3 Transformer

项目	内容
核心创新	自注意力机制(Self–Attention)，并行处理序列
关键公式	$\text{Attention}(Q,K,V) = \text{softmax}(QK^T / \sqrt{d})V$
架构组成	多头注意力、前馈网络、位置编码、残差连接
适用场景	NLP、CV、多模态任务
典型案例	BERT(理解)、GPT(生成)、ViT(视觉)

Transformer架构：



3.2.4 生成对抗网络 (GAN)

项目	内容
核心思想	生成器(G)与判别器(D)对抗训练
训练目标	G尽量生成逼真样本骗过D, D尽量区分真假
适用场景	图像生成、风格迁移、数据增强
典型案例	人脸生成、图像超分辨率、艺术创作
代表模型	DCGAN、StyleGAN(高质量人脸)、CycleGAN(风格转换)

3.2.5 扩散模型 (Diffusion Model)

项目	内容
核心思想	正向逐步加噪→纯噪声，逆向逐步去噪→生成图像
训练目标	学习预测每一步添加的噪声
适用场景	高质量图像生成、图像编辑
典型案例	Stable Diffusion、DALL-E 2/3、Midjourney
优势	生成质量高、训练稳定、可控性强

3.3 深度学习发展里程碑

年份	里程碑	意义
2012	AlexNet	CNN在ImageNet突破，开启深度学习时代
2014	GAN	生成模型革命性突破
2015	ResNet	残差连接突破深度限制
2017	Transformer	"Attention is All You Need"， NLP革命
2018	BERT	预训练+微调范式确立
2018	GPT	大规模语言模型开端
2020	GPT-3	涌现能力，少样本学习
2021	DALL-E	文本到图像生成
2022	ChatGPT	对话AI突破，RLHF技术
2023	GPT-4	多模态大模型

4. Large Language Models 大语言模型

4.1 LLM技术栈

LLM 技术栈

- ├ 基础架构
 - | └ Transformer Decoder
 - | └ 位置编码 (RoPE, ALiBi)
 - | └ 注意力优化 (Flash Attention, MQA, GQA)
 - | └ 激活函数 (GELU, SwiGLU)
- |
- ├ 预训练
 - | └ 自回归语言建模 (Causal LM)
 - | └ 掩码语言建模 (Masked LM)
 - | └ 大规模语料训练
- |
- ├ 对齐技术
 - | └ 监督微调 (SFT)
 - | └ RLHF (人类反馈强化学习)
 - | └ DPO (直接偏好优化)
 - | └ Constitutional AI
- |
- ├ 推理优化
 - | └ 量化 (INT8, INT4, GPTQ, AWQ)
 - | └ 蒸馏 (Knowledge Distillation)
 - | └ 剪枝 (Pruning)
 - | └ 推测解码 (Speculative Decoding)
- |
- └ 应用技术
 - └ Prompt Engineering
 - └ In-Context Learning
 - └ Chain-of-Thought
 - └ RAG (检索增强生成)
 - └ Agent/Tool Use
 - └ 多模态融合

4.2 主流LLM模型对比

模型	发布方	参数量	开源	特点
GPT-4	OpenAI	~1.8T(传)	否	多模态、最强综合能力
Claude 3	Anthropic	-	否	长上下文、安全对齐
Gemini	Google	-	部分	原生多模态
LLaMA 3	Meta	8B–405B	是	开源最强、社区活跃
Qwen 2.5	阿里	0.5B–72B	是	中文优秀、全尺寸覆盖
DeepSeek	DeepSeek	7B–236B	是	MoE架构、性价比高
Mistral	Mistral AI	7B–8x22B	是	欧洲开源、效率出色

4.3 LLM核心技术详解

4.3.1 自注意力机制 (Self-Attention)

Query(Q)、Key(K)、Value(V) 来自同一输入序列

计算步骤：

1. 计算注意力分数: $score = Q \cdot K^T / \sqrt{d_k}$
2. 归一化: $weights = softmax(score)$
3. 加权求和: $output = weights \cdot V$

作用：让每个token能够“关注”序列中其他所有token

4.3.2 位置编码

方法	原理	特点
正弦位置编码	使用sin/cos函数编码位置	原始Transformer, 固定长度
可学习位置编码	位置embedding可训练	BERT使用
RoPE	旋转位置编码	LLaMA使用, 支持长度外推
ALiBi	注意力线性偏置	无需位置编码, 外推能力强

4.3.3 RLHF (人类反馈强化学习)

RLHF训练流程：

1. SFT阶段：
预训练模型 + 人工标注数据 → 监督微调模型
2. 奖励模型训练：
人类对比排序 → 训练Reward Model
3. PPO强化学习：
SFT模型 + Reward Model → PPO优化 → 对齐模型

4.4 LLM应用场景

应用领域	具体场景	典型产品
对话交互	智能客服、AI助手	ChatGPT、Claude
内容创作	文案、代码、翻译	GitHub Copilot、文心一言
知识问答	搜索增强、文档问答	Perplexity、秘塔搜索
代码开发	代码生成、Debug	Cursor、CodeBuddy
多模态	图像理解、视频分析	GPT-4V、Gemini
Agent	自主任务执行	AutoGPT、MetaGPT

5. 优质动画教学资源汇总

5.1 顶级交互式可视化平台

5.1.1 Georgia Tech Polo Club (强烈推荐 ★★★★★)

工具名称	链接	描述
CNN Explainer	https://poloclub.github.io/cnn-explainer/	卷积神经网络交互式可视化，理解卷积、池化、激活过程
GAN Lab	https://poloclub.github.io/ganlab/	在浏览器中玩转GAN，可视化生成器与判别器对抗过程
Transformer Explainer	https://poloclub.github.io/transformer-explainer/	理解Transformer/GPT工作原理的交互式工具
Diffusion Explainer	https://poloclub.github.io/diffusion-explainer/	可视化Stable Diffusion文本到图像生成过程

5.1.2 TensorFlow 官方工具

工具名称	链接	描述
TensorFlow Playground	https://playground.tensorflow.org/	神经网络入门必备，可视化神经元、层、激活函数
Embedding Projector	https://projector.tensorflow.org/	高维嵌入可视化，支持PCA/t-SNE降维

5.1.3 Amazon MLU-Explain (强烈推荐 ★★★★★)

主题	链接	描述
Neural Networks	https://mlu-explain.github.io/neural-networks/	神经网络基础动画讲解
Linear Regression	https://mlu-explain.github.io/linear-regression/	线性回归交互式学习
Logistic Regression	https://mlu-explain.github.io/logistic-regression/	逻辑回归可视化
Decision Trees	https://mlu-explain.github.io/decision-tree/	决策树分裂过程动画
Random Forest	https://mlu-explain.github.io/random-forest/	随机森林集成原理
ROC & AUC	https://mlu-explain.github.io/roc-auc/	评估指标可视化理解
Bias–Variance	https://mlu-explain.github.io/bias-variance/	偏差方差权衡动画
Reinforcement Learning	https://mlu-explain.github.io/reinforcement-learning/	强化学习入门
Cross–Validation	https://mlu-explain.github.io/cross-validation/	交叉验证原理

5.1.4 Distill.pub (高质量学术可视化)

文章主题	链接	描述
Attention机制	https://distill.pub/2016/augmented-rnns/	注意力机制可视化概述
t-SNE使用指南	https://distill.pub/2016/misread-tsne/	如何正确使用t-SNE降维
特征可视化	https://distill.pub/2017/feature-visualization/	CNN特征理解
GNN入门	https://distill.pub/2021/gnn-intro/	图神经网络可视化介绍
动量优化	https://distill.pub/2017/momentum/	优化器动量原理

5.2 经典博客与教程

5.2.1 Colah's Blog (神经网络圣经 ★★★★★★)

文章	链接	描述
Understanding LSTM	http://colah.github.io/posts/2015-08-Understanding-LSTMs/	LSTM最佳入门，配图清晰
Neural Networks, Manifolds	http://colah.github.io/posts/2014-03-NN-Manifolds-Topology/	神经网络的拓扑学视角
Conv Nets Modular	http://colah.github.io/posts/2014-07-Conv-Nets-Modular/	卷积网络模块化理解

5.2.2 3Blue1Brown (数学动画大师 ★★★★★)

视频系列	平台	描述
Neural Networks	YouTube/Bilibili	神经网络本质、反向传播动画讲解
Linear Algebra	YouTube/Bilibili	线性代数可视化，理解矩阵、特征值
Calculus	YouTube/Bilibili	微积分直觉，理解梯度下降

5.3 LLM专题可视化

资源	链接	描述
LLM Visualization	https://bbycroft.net/llm	GPT模型3D可视化，逐层理解
BertViz	https://github.com/jessevig/bertviz	BERT注意力头可视化工具
Transformer论文图解	https://jalammar.github.io/illustrated-transformer/	经典图解Transformer
GPT-2图解	https://jalammar.github.io/illustrated-gpt2/	GPT-2架构详解
BERT图解	https://jalammar.github.io/illustrated-bert/	BERT预训练理解

5.4 资源分类速查表

学习阶段	推荐资源	特点
ML入门	MLU-Explain、TensorFlow Playground	交互式、零代码
DL基础	CNN Explainer、Colah's Blog	可视化架构
CNN深入	Distill特征可视化	学术深度
RNN/LSTM	Colah's LSTM文章	经典必读
Transformer	Transformer Explainer、Jay Alammar博客	从零理解
GAN	GAN Lab	实时交互训练
Diffusion	Diffusion Explainer	去噪过程可视化
LLM	LLM Visualization、BertViz	注意力理解

6. 学习路线建议

6.1 入门阶段 (1-2个月)

Week 1-2: 数学基础

- 线性代数 → 3Blue1Brown系列
- 微积分 → 梯度、导数
- 概率统计 → 贝叶斯、分布

Week 3-4: ML基础算法

- 线性/逻辑回归 → MLU-Explain
- 决策树/随机森林 → MLU-Explain
- 动手实践 → scikit-learn

Week 5-6: 神经网络入门

- 感知机、MLP → TensorFlow Playground
- 激活函数、损失函数
- 反向传播 → 3Blue1Brown

6.2 进阶阶段 (2-3个月)

Month 2: CNN

- 卷积、池化原理 → CNN Explainer
- 经典架构 → ResNet、VGG
- 实践 → 图像分类项目

Month 3: RNN/Transformer

- LSTM/GRU → Colah's Blog
- Attention机制 → Distill
- Transformer → Transformer Explainer
- 实践 → 文本分类、机器翻译

6.3 高级阶段 (3–6个月)

Month 4-5: 生成模型

- GAN原理与训练 → GAN Lab
- VAE变分自编码器
- Diffusion Model → Diffusion Explainer
- 实践 → 图像生成

Month 5-6: LLM

- GPT架构 → LLM Visualization
- 预训练与微调
- RLHF对齐
- Prompt Engineering
- 实践 → 微调开源LLM

6.4 实践项目建议

阶段	项目	技术栈
ML入门	泰坦尼克生存预测	pandas, sklearn
ML进阶	房价预测、信用评分	XGBoost, LightGBM
DL入门	MNIST手写数字识别	PyTorch/TensorFlow
CNN	猫狗分类、图像分类	ResNet, 迁移学习
RNN	股价预测、情感分析	LSTM, GRU
NLP	文本分类、命名实体识别	Transformer, BERT
生成	风格迁移、图像生成	GAN, Diffusion
LLM	微调Qwen/LLaMA	LoRA, QLoRA

附录：核心术语表

英文术语	中文	简要说明
Supervised Learning	监督学习	使用标签数据训练
Unsupervised Learning	无监督学习	无标签数据，发现模式
Reinforcement Learning	强化学习	通过奖励学习策略
Overfitting	过拟合	模型在训练集过度拟合
Regularization	正则化	防止过拟合的技术
Gradient Descent	梯度下降	优化算法，最小化损失
Backpropagation	反向传播	计算梯度的算法
Convolution	卷积	局部特征提取操作
Pooling	池化	降采样，减少参数
Attention	注意力	动态加权机制
Embedding	嵌入	将离散数据映射到连续向量
Fine-tuning	微调	在预训练模型上继续训练
Transfer Learning	迁移学习	将知识迁移到新任务
Tokenization	分词	将文本分割为token
Prompt	提示词	给模型的输入指令
Hallucination	幻觉	LLM生成虚假信息

 最后更新: 2024年12月

 建议: 学习时结合交互式可视化工具, 边看边操作, 效果更佳!