人工智能基础大纲

上海交通大学 移动与物联网安全实验室

一阶段

> 参考书籍《解析深度学习 卷积神经网络原理与视觉实践》，该书仅作基础入门，请自行查阅更多书籍（如花书等）和视频（B站视频很多，注意筛选）

- 神经网络基础知识
  - 神经网络基本原理（一次交流）
    - 神经网络是什么?
    - 人工神经元的结构是什么？与生物神经元有什么区别?
    - 神经元如何构成神经网络?
    - 激活函数有哪些?
    - 输入、隐藏、输出层又是什么?
  - 反向传播算法（一次交流）
    - 反向传播算法的过程是什么?
    - 反向传播算法为什么要使用梯度?
    - 反向传播算法中的梯度如何求得?
    - 反向传播算法有哪些缺陷?
  - 神经网络性能的判别标准（一次交流）
    - 混淆矩阵
    - F1值
    - ROC曲线
    - Top-5错误率
- 常见的神经网络
  - 自动编码器（一次交流）
    - 自动编码器的应用主要有什么?
    - 什么是自动编码器的结构？为什么这样的结构可以使自动编码器拥有这样的功能?
    - 如何训练自动编码器?
    - 具体在对于图像降噪的应用中，自动编码器是怎样使用的?
  - 循环神经网络（一次交流）
    - 为什么需要循环神经网络？它在哪些领域发挥作用?
    - 循环神经网络的结构是什么？为什么要用这样的结构?
    - 循环神经网络是如何训练，如何进行反向传播的?
    - 什么是梯度消失和梯度爆炸？为什么循环神经网络需要解决这些问题?
  - 卷积神经网络（一次交流）
    - 为什么需要卷积神经网络?
    - 卷积神经网络的结构是什么？为什么要用这样的结构?
    - 卷积和池化的目的是什么?
    - 卷积神经网络是如何训练的?
  - 残差神经网络（一次交流）
    - 为什么需要残差神经网络?
    - 残差神经网络残差块的原理是什么?
    - 它是怎么解决梯度消失与梯度爆炸问题的?
    - 残差神经网络中1×1的卷积块有什么用?
  - 生成对抗网络（一次交流）

        - 生成对抗网络的应用有哪些?
        - 生成对抗网络的结构是什么，又是怎么训练的?
- 神经网络的一般应用

    > 至少按照目标检测给出的结构模板

    - 目标检测（一次交流）
        - 什么是目标检测?
        - 目标检测分为哪些流程?
        - 有哪些常用算法，都有什么改进?
        - 目标检测有哪些应用场景?
    - 人脸检测（一次交流）
    - 步态识别（一次交流）
    - 图像识别（一次交流）
    - 自然语言处理（一次交流）
    - 自动驾驶（一次交流）
    - 强化学习（一次交流）
    - 对抗样本（一次交流）

二阶段

- 神经网络编程基础
    - numpy的使用方法（一次交流）
        - 为什么要使用numpy？它的运行速度比起Python如何?
        - 如何构建numpy数组（ndarray）？
        - size、dtype、shape、ndim各是什么?
        - 创建数组的函数：
            - range、linspace
            - zeros、ones、diag、eye、np.random.rand
            - zeros_line、ones_like
        - 改变数组形状的函数：
            - reshape、 T、squeeze、flatten
            - np.append、concatenate、stack
        - 索引
            - 元素
            - 高级索引
        - 运算
            - 四则运算
        - 函数
            - np.sqrt、np.power、np.sin、np.log
            - cumsum、diff
        - 统计函数
            - a.sum()、a.mean()、a.std()
            - 矩阵运算
            - 向量积、矩阵乘法
    - pytorch使用方法（一次交流）
        - 与numpy区别、数组互相转换

        - 函数名最后带下划线的函数与不带下划线的函数有什么区别?
        - 自动求导与backward函数
- 使用pytorch搭建、训练简单的神经网络
    - 数据集Dataset、Dataloader、损失函数、优化函数（一次交流）
    - 训练、测试整体过程（MNIST手写体识别）（一次交流）

三阶段

- 论文阅读
    - 每人选择1-2篇与对抗样本（对抗攻击、对抗防御、对抗检测等）有关的英文论文进行深入阅读，并制作PPT交流。论文应选择近3年的、发表在CCF-A类（CCF推荐国际学术刊物目录-中国计算机学会）会议或期刊上的论文。论文中不是论文提出的方法，则不需要深入探究。深入阅读某篇论文应该得到以下结果：
        - 论文的领域和问题背景?
        - 该问题之前的解决方法是什么?
        - 论文在之前的方法基础上面提出了什么创新?
        - 提出的创新的效果如何?