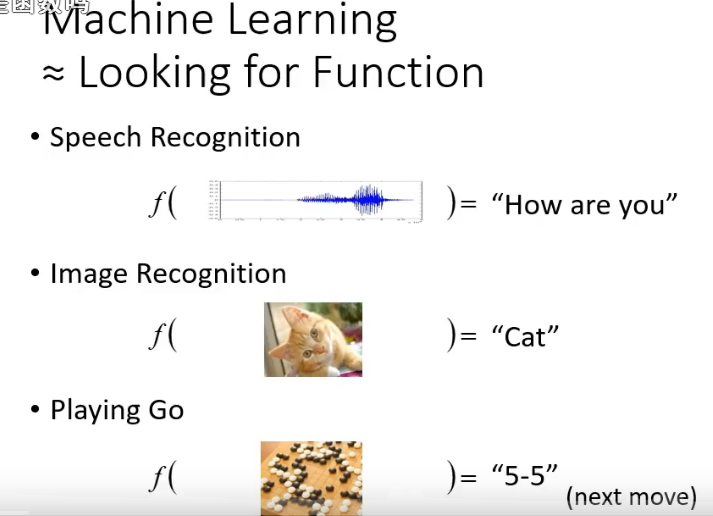
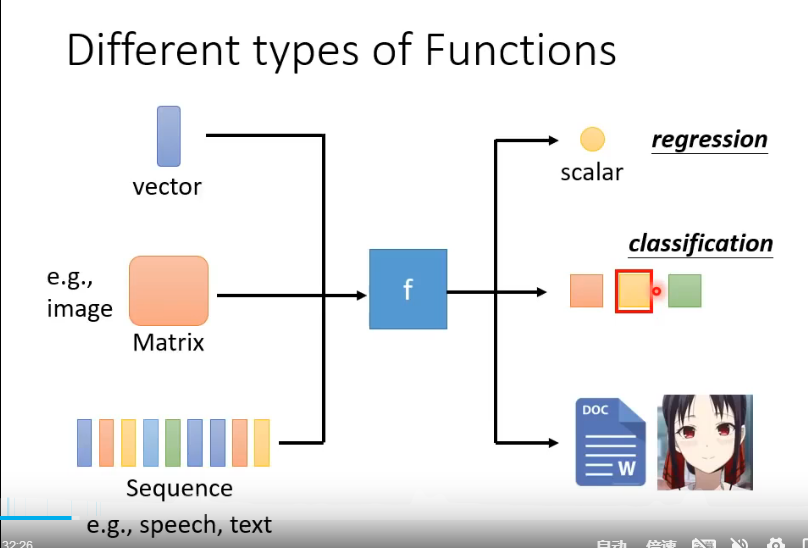
什么是机器学习？

机器学习是帮我们找一个复杂的函数来解决问题

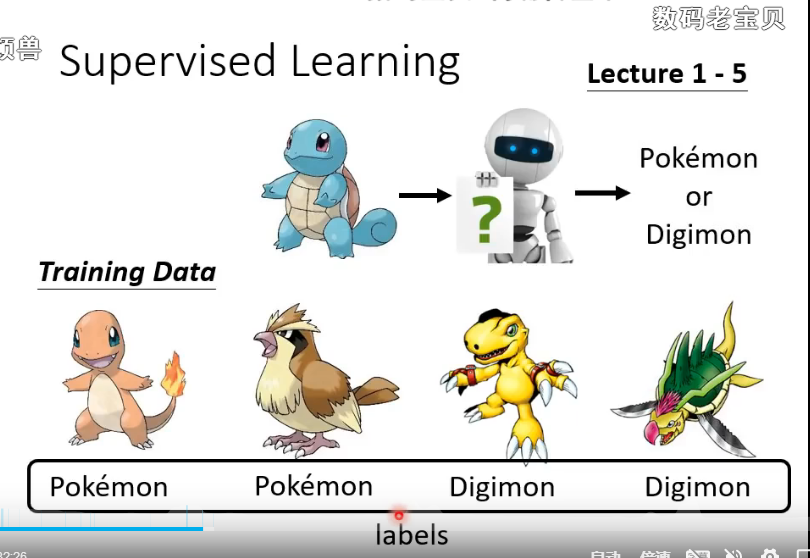


函数的输入可以是一个向量、矩阵(一个图片)、序列(声音或者一句话或者是一段文字)。

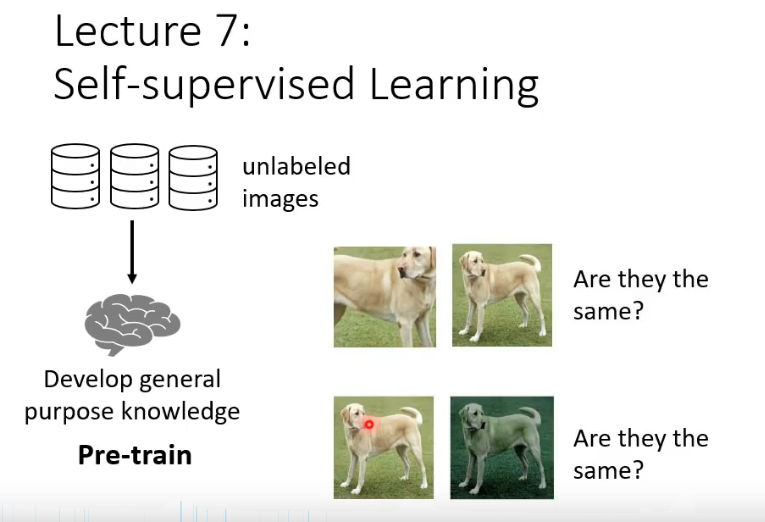
输出可以是一个数值(regression)、类别(classification)、文章或者图片。



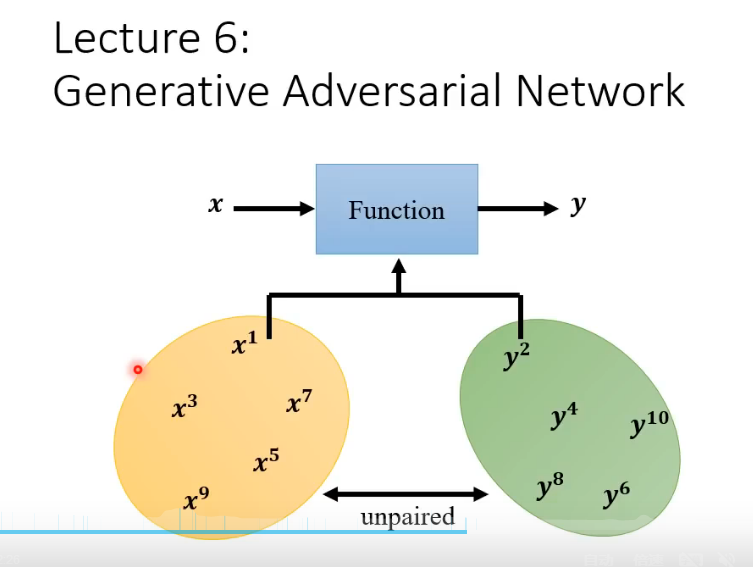
监督学习的做法就是要收集大量的训练资料，在收集过程中要给出对应的标签。在训练的过程中将图片放入网络中然后输出结果与其对应的标签做对比计算损失进而更新网络参数。



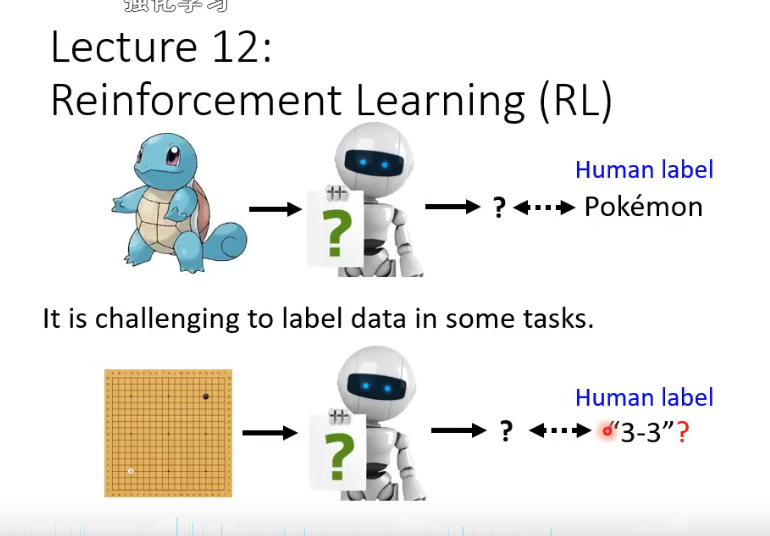
半监督学习就是在训练模型之前做预训练，让机器学会做各种不同的影像辨识相关任务的基本功，练好后就可以在新的任务上做好。



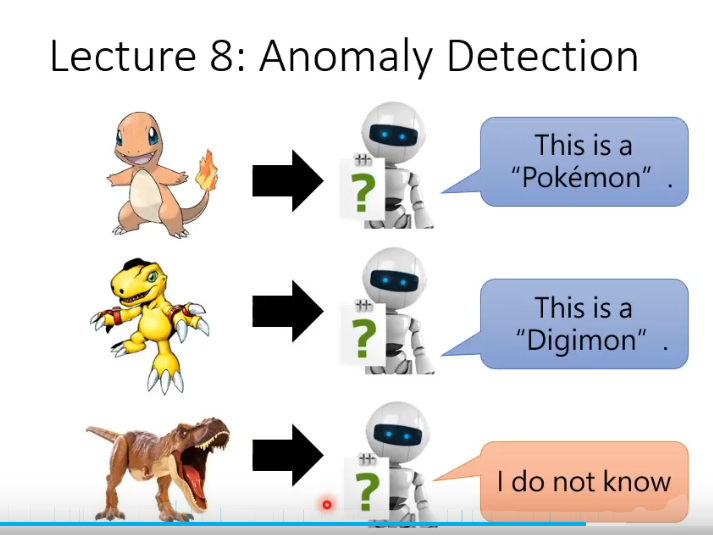
生成对抗网络只需要收集到大量的x和大量的y不需要它们之间成对的关系机器就可以自动把它们之间的关联找出来



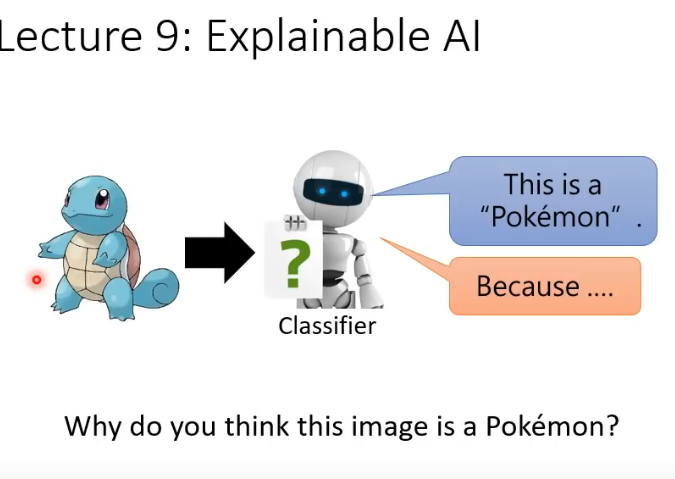
强化学习当不知道怎么标注资料但是可以判断好坏并且可以定义什么叫做成功的时候就可以使用强化学习来解决。



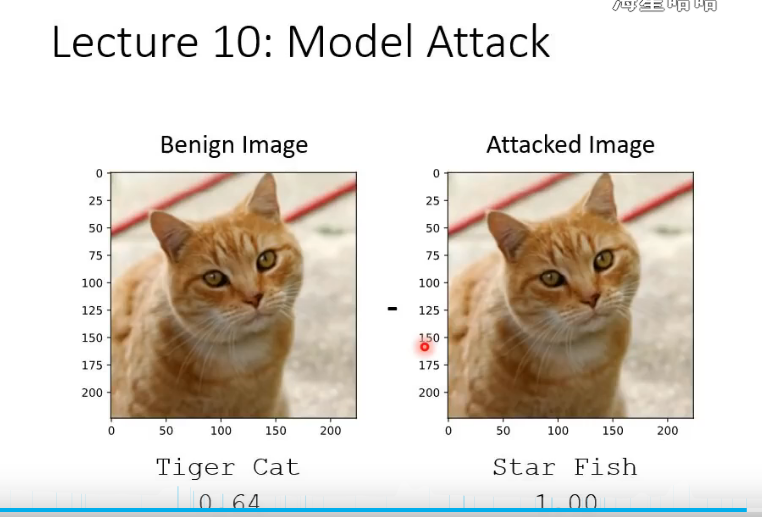
异常检测就是当出现一个类别是当前模型没有学习过的类别时需要模型输出我不知道。所以异常检测就是要让模型能够输出我不知道。



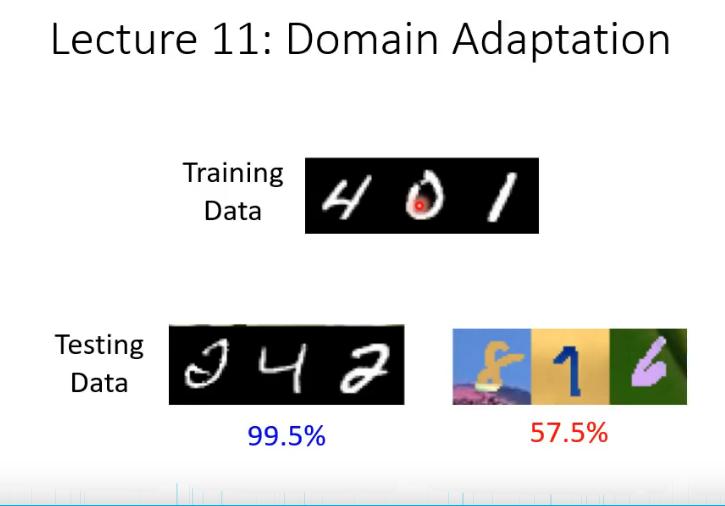
可解释性AI就是要让模型让我们知道为什么它能够知道答案是这个。



模型攻击就是通过在图片上添加一些人肉眼看不出来的噪音，使得模型识别错误



Domain Adaptation就是假设训练资料和测试资料的分布是类似的但是在实际应用的时候可能会与训练和测试的资料有差异，这种差异就有可能使得模型识别正确率暴跌，Domain Adaptation就是来解决这个问题。



机器学习的类别

Regression:模型的输出是一个数值。

例子：通过输入今天的PM2.5的值、平均温度和平均的臭氧气浓度等输出每天中午的MP2.5的值，找这个函数的任务就叫做Regression。

Classification：通过给出一些选项也就是类别来作为模型的输出。

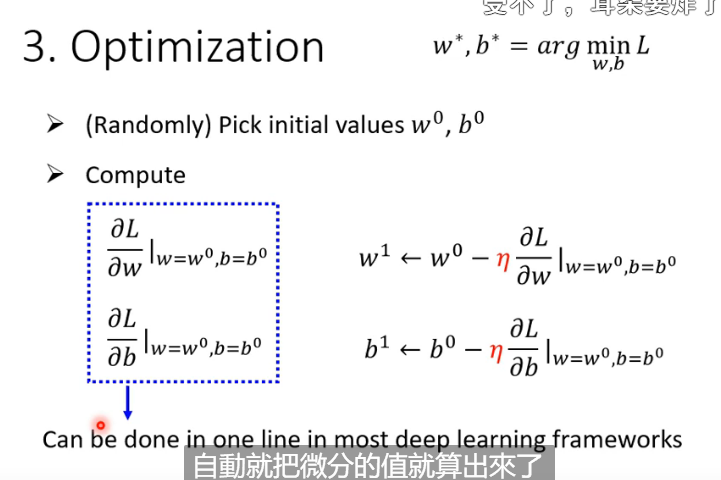
例子：通过输入一封邮件模型来判断并输出这封邮件是否是垃圾邮件。

Structured Learning：输出是一个有结果的东西

例子：机器画一张图、写一篇文章。

机器学习找出一个函数分为三个步骤

1. 写出一个带有未知参数的函数，为y=wx+b,y是要预测的值，w和b分别是权重和偏置，x则是一些已知的数值，w和b是要通过学习不断更新得到的参数。
2. 损失函数是通过输入模型的输出值和真实值来计算它们之间的差异，从而得知当前函数的参数学习的好坏。损失函数通常有MAE、MSE、Cross-entropy等。
3. Optimization就是去找出最佳的w和b使得损失值降到最低，通过梯度下降来调整w和b的值找到最小值点获得最佳的w和b。通过计算w和b的微分乘以学习率来获得新的w和b的值，通过设置epoch来确定学习的次数。



线性模型