* **machine learning的本质就是寻找一个function**

**当然它可以相当复杂，以至于根本没有人能够把这个function的数学式给手写出来**

* 首先要做的是明确你要找什么样的function，大致上分为以下三类：
  + Regression——让机器输出一个数值，如预测PM2.5
  + Classification——让机器做选择题
    - 二元选择题——binary classification，如用RNN做文本语义的分析，是正面还是负面
    - 多元选择题——muti-class classification，如用CNN做图片的多元分类
  + Generation——让机器去创造、创生
    - 如用seq2seq做机器翻译
    - 如用GAN做二次元任务的生成
* 其次是要告诉机器你想要找什么样的function，分为以下三种方式：
  + Supervised Learning：用labeled data明确地告诉机器你想要的理想的正确的输出是什么
  + Reinforcement Learning：不需要明确告诉机器正确的输出是什么，而只是告诉机器它做的好还是不好，引导它自动往正确的方向学习
  + Unsupervised Learning：给机器一堆没有标注的data，看看机器到底能做到哪一步
* 接下来就是机器如何去找出你想要的function

当机器知道要找什么样的function之后，就要决定怎么去找这个function，也就是使用loss去衡量一个function的好坏

* + 第一步，给定function寻找的范围
    - 比如Linear Function、Network Architecture都属于指定function的范围

两个经典的Network Architecture就是RNN(会用到Seq2Seq的架构里)和CNN(会用到大部分其他的架构里)

* + 第二步，确定function寻找的方法
    - 主要的方法就是gradient descent以及它的扩展

可以手写实现，也可以用现成的Deep Learning Framework——PyTorch来实现

* 前沿研究
  + Explainable AI

举例来说，对猫的图像识别，Explained AI要做的就是让机器告诉我们为什么它觉得这张图片里的东西是猫 (用CNN)

* + Adversarial Attack

举例来说，现在的图像识别系统已经相当的完善，甚至可以在有诸多噪声的情况下也能成功识别，而Adversarial Attack要做的事情是专门针对机器设计噪声，刻意制造出那些对人眼影响不大，却能够对机器进行全面干扰使之崩溃的噪声图像 (用CNN)

* + Network Compression

举例来说，你可能有一个识别准确率非常高的model，但是它庞大到无法放到手机、平板里面，而Network Compression要做的事情是压缩这个硕大无比的network，使之能够成功部署在手机甚至更小的平台上 (用CNN)

* + Anomaly Detection

举例来说，如果你训练了一个识别动物的系统，但是用户放了一张动漫人物的图片进来，该系统还是会把这张图片识别成某种动物，因此Anomaly Detection要做的事情是，让机器知道自己无法识别这张图片，也就是能不能让机器知道“我不知道”

* + Transfer Learning (即Domain Adversarial Learning)

在用于学习的过程中，训练资料和测试资料的分布往往是相同的，因此能够得到比较高的准确率，比如黑白的手写数字识别，但是在实际场景的应用中，用户给你的测试资料往往和你用来训练的资料很不一样，比如一张彩色背景分布的数字图，此时原先的系统的准确率就会大幅下降，而Transfer Learning要做的事情是，在训练资料和测试资料很不一样的情况下，让机器也能学到东西

* + Meta Learning

Meta Learning的思想就是让机器学习该如何学习，也就是Learn to learn，传统的机器学习方法是人所设计的，是我们赋予了机器学习的能力；而Meta Learning并不是让机器直接从我们指定好的function范围中去学习，而是让它自己有能力自己去设计一个function的架构，然后再从这个范围内学习到最好的function，我们期待用这种方式让机器自己寻找到那个最合适的model，从而得到比人类指定model的方法更为有效的结果

传统：我们指定model->机器从这个model中学习出best function

Meta：我们教会机器设计model的能力->机器自己设计model->机器从这个model中学习出best function

原因：人为指定的model实际上效率并不高，我们常常见到machine在某些任务上的表现比较好，但是这是它花费大量甚至远超于人类所需的时间和资料才能达到和人类一样的能力；相当于我们指定的model直接定义了这是一个天资不佳的机器，只能通过让它勤奋不懈的学习才能得到好的结果；由于人类的智慧有限无法设计高效的model才导致机器学习效率低下，因此Meta learning就期望让机器自己去定义自己的天赋，从而具备更高效的学习能力

* + Life-long Learning

一般的机器学习都是针对某一个任务设计的model，而life-long learning想要让机器能够具备终身学习的能力，让它不仅能够学会处理任务1，还能接着学会处理任务2、3...也就是让机器成为一个全能型人才

