# 机器学习背后的朴素思想

文档编号： ML-T-00101

JEROD YAN*

December 13, 2019

**摘要**: 本文档介绍机器学习过程中所涉及的基础概念与基本流程， 以使得准备进入机器学习领域的人员能够有清晰且正确的概念，少走些弯路，少被人忽悠。

## 目　录



## 1 学习技术的方法

任何一门学问或是技术，都是由一系列的概念构成的。 如果你准确地理解了其中的概念和概念产生的思维过程， 那么这门学问就不能难学了。 通常，一个概念在产生的时候，它来自于简单的、朴素的思考。 英文中称之「Common Sense」。然后，可能是由于逻辑严谨性的原因， 学者们会使用一些看起来高深的数理化符号来做逻辑推导或证明， 其目的是为了防止朴素思考带来的思维偏差。

但是，作为学习者而言，这些概念通常已经是被证明正确了。 我们的目的是学会它。而逻辑符号及数理符号的抽象性，会学习带来障碍和困难。 所以，我认为，既然

*jerod74 DOT yan AT gmail DOT com

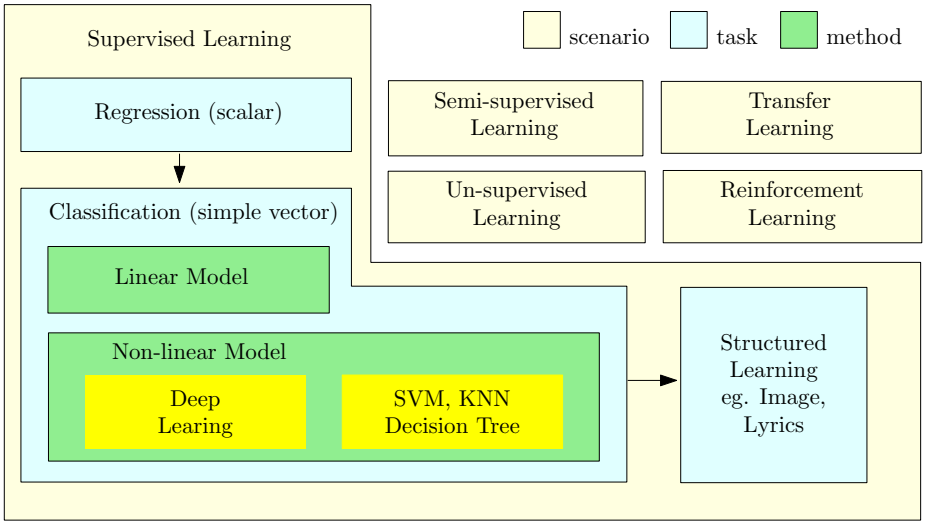


**图 1: 概念层次图**

概念是由朴素思想产生出来的。 那么，在学习的过程中，就要先去学习那些概念背后的朴素的思想。 试想一下，如果你是一个概念的发明人，你会直接上来就先想一个包括二阶导数的微积分公式吗?

通常，了解概念或定义其背后的思想会帮助你理解这个概念数理化定义。

然后，当你掌握了一门学科的概念后，你要做得是把这些概念放在一起， 比较一下，比较它们的区别与联系。 你可在「同中求异」和「异中求同」的两个思路下， 做一些分析工作，就可以建立起整个知识的体系。

# 2 机器学习框架概念

## 2.1 概念层次的划分

1.) 首先，如图1所示，从输入的数据(Input)来划分。机器学习方法是通过已经采样好的数据来区分学习的场景（Scenario）。先看输入数据的整体，根据全量的数据是否标注过，分为监督学习（Supervised Learning）和非监督学习（Unsupervised Learing)。如果是有部分数据被标注过，而还有一些未被标记过，称为半监督学习（Semi-supervised Learing）。如果输入数据的部分和本次任务有关，部分无关，被称为迁移学习（Transfer Learning)。如果是只有实时的采样且有一定的最后成败判断规则，完全由规则来确定学习的结果，可以称为增强学习（Reinforcement Learning）。

2.) 其次，从输出的结果(Output)或是学习的目的（Task）来划分。如果输出的结果是个标量（Scalar），可以称之为回归（Regression）。如果输出的结果是

个简单向量，可以称之为分类（Classification）。如果输出的结果是个复杂向量或矩阵（Matrix）或高阶矩阵（张量Tensor），称之为（Structure Learning）。Structure Learning 的任务的例子，比如中英文的机器翻译，人的语音到文字的识别，生成一首歌词，生成一张世界上不存在的人的头像[1]。

3.) 最后，对于模型的复杂类型可简单分为线性模型（Linear Model）和非线性模型（Non-Linear Model)。线性模型中最常见就是线性回归模型。而非线性模型就分为黑盒模型，如神经网络模型，深度神经网络模型（Deep Learning），以及灰白盒模型，如SVM，Decision Tree，K-NN等。

打个比方，就是你有什么数据，想做什么的任务（输出什么样的结果），然后设计一个线性或非线性的模型。对于非线性的模型，你可以使用黑盒的方式，让计算机的强大的算力和足够多的数据，自己去学习模型中的参数的具体取值；也可以采用白盒的方式，自己设计输入数据特征，数据变换的方法，来得到模型中事先定义好的有意义的模型参数的具体取值。

举个例子，你任务是要识别图片中动物是猫或是狗。你有 10,000 张图片，都是猫和狗的，也请人标记了每一张是猫或是狗，你这个场景就属于监督学习。如果你经费紧张，请人标记了其中 5,000 张，场景就变成了半监督学习。

再举个例子，你任务还是要识别图片中动物是猫或是狗。你有 10,000 张种类繁多的图片，你打开一些图片文件看了一下，乱七八糟的，有猫、狗、大象、老虎，甚至还有卡通人物，如一休哥的，蝙蝠侠、钢铁侠、蜘蛛侠的。你没经费，只能自己标记，标记了20 分钟时间，一共标记了410张图片，其中 200 张是狗，100 张是猫，50 张是大象、50 张是老虎，10 张是一休哥的。然后，你不想标记了，那么到此为止，你遇到的场景是迁移学习。注意，迁移学习场景中隐含了一个意思，就是你要使用所有 10,000 张图片，那些没有标记的图像，甚至是与任务目标无关的图片也可以对完成任务有帮助。这个可以理解为，我们小时候，并不是看到的所有的东西，都会有人给你指正，有时看到东西虽然不知道是什么，但是对于分辨其它已知的东西，仍旧是有帮助的。

无监督学习的场景，就是要让机器无师自通，在没有直接反馈及帮助的情况下学习。把这 10,000 张没标记过的图片，统统让它看一遍，可能它会把猫、狗、老虎认为一类事物，而一休，蝙蝠侠，钢铁侠是一类事物。这个例子当前不是太好，这要和具体的任务相结合。

最后我们提一下增强学习。

后面提到吴恩达在学术上的成就，主要是使用增强学习来控制无人直升机的。增强学习的特点与遗传算法有点像，都是要多步以后才能看到效果。增强学习的例子，

[1]建议你点开这个网址感觉一下 Nvidia 公司的算法实力。https://thispersondoesnotexist.com/

主要集中在打游戏，包括电子游戏或是围棋类的游戏。 这类场景的特点是，周围环境不是太复杂，而且规则比较明确。 机器做出了一系列的决策和环境的反馈之后，只有在最后才知道成败。 因为决策的次数太多以及环境的随机反馈，不太可能回溯整个决策的每一个步骤。 这样的场景通常可以归为增强学习。 如果拿打游戏来做比喻，增强学习是第一人称的游戏，你看的世界就是周围的世界， 你不太能注意到自身。而监督学习是拿了超级权限或开了外挂的第三人称的游戏， 而且是拥有后台数据库读权限的大 Boss 的第三者视角来看的游戏中的各种行动， 是个上帝视角。游戏的角色的行为一举一动，你都知道其结果的对错。

再举一个不是太恰当的例子， 增强学习有点类似我们大学毕业后，走向真实的社会中的学习。 没有人告诉你，今天这点做的对，那一点不太好，要改进。 你忙碌了几个月的项目，甚至一整年，得到的是一个非零即一的结果。 幸运的话，努力没白费，成功了。 不幸的话，项目失败了。无论成功与否，你都回头复盘， 你有可以回想到的决策，而大量的细小的决策基于于当时决策前的环境， 可能包括各种因素，有形的，无形的，你可能都想不起来了。 这时，你如何总结学习到成功的经验或是失败的教训呢？ 我想如果增强学习能够发展起来的话，那么可能机器真是有了些智慧呢。

你读到这里，我想问一个问题：如果一个问题被归为监督学习场景， 那么是还可以使用所谓的增强学习方法吗？想一下？

……

对于监督学习和增强学习这两个概念，是针对场景而言的。 其划分标准是输入数据的情况。监督学习的输入数据都会请人提前做标注好， 而增强学习的数据是训练过程中，一边训练，一边收集到的，也没有人标注它。 所以， 如果一个输入数据已经被归为监督学习的场景，那么就不能再归为其它的场景。 每一个场景都是独立的，他们之间本质上是没有交集的。 换句话说，就是适用于监督学习领域的方法，是不太会在其它场景中有较好效果的。 反过来，也一样。所以，上面问题的答案是：不行。

## 2.2 机器学习的步骤

机器学习的任务是输入一些数据，再输出一些数据，其就是一种数据转换器。 从数学意义上讲，就是一个合适的函数映射。 我们的目的是要找到一个可以完成任务的映射函数。 如图2所示： [1]

1.) 第一步，定义一个函数集合（Model， A set of functions)。这个集合中的每一个元素都是一个有确定参数的函数。

2.) 第二步，因为要在此函数集合中选一个函数，所以要确定一个函数的挑选准

[1] https://datawhalechina.github.io/leeml-notes/

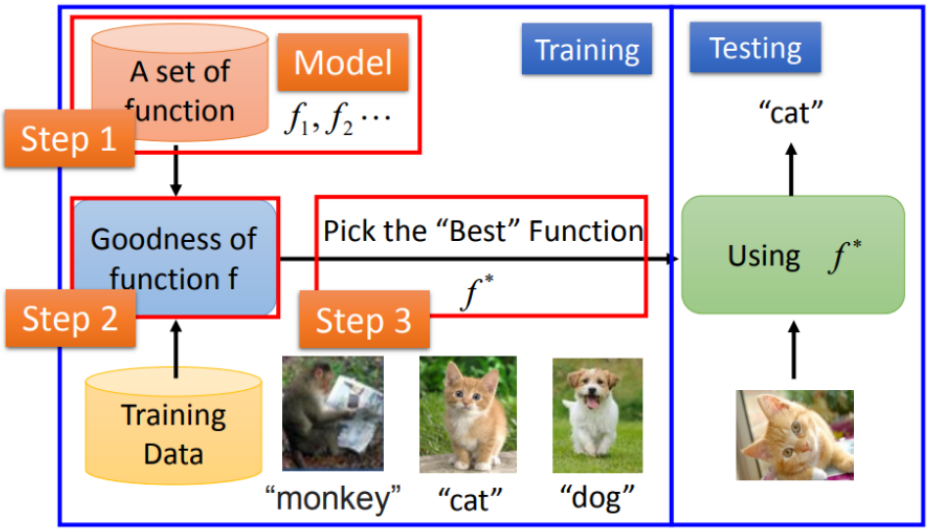


**图 2: 机器学习的步骤**

则（Goodness of function f)。

3.) 第三步，在上述函数集合中，根据挑选的准则以及训练数据（Training Data）具体地找到那个函数（Pick the best function）。

4.) 第四步，在测试数据（Testing Data）上测试，测试刚刚找到这个函数的效果。

前三步被称为训练（Trainning），最后一步称为测试（Testing）。

打个比方，把大象放到冰箱里，也分为三个步骤：打开冰箱门，把大象赶过去，关上冰箱门。这里，我们也是三个步骤来搞定它。当拿到一个任务，确定输入数据和输出数据后，那么基本可以确定大的方向。然后，要设计一个函数映射的集合。在这个集合里，各个元素函数看起来大模样都差不多，只有参数的系数不一样。注意，这个集合里包含的函数通常有无穷多个。我们只能通过一个方法来描述这个函数，譬如说一个方程或是一个拓扑结构。接下来，我们的目的是挑一个好用的，合适的函数，所以要确定一个准则来判断，哪个函数好用。比如说，让所有训练用的数据使得函数映射的误差最小。最后，我们所要做的是根据准则找到一组具体的参数系数。当所有参数系数都确定下来的时候，即一个合适的函数映射也找到了。至此，训练过程也结束了。

通常，用深度学习方法来确定函数的形式，其并不是一个传统意义上的数学表达式或代数式子。它是一个用网络拓扑结构描述的函数映射关系。其参数数量一般都是几百万个。与之相对的，传统方法的映射函数所涉及的参数或系数数量级就小得多。一般就是几个，十几个，上百个系数的都不多见。这个设计函数集合的思路，初学的时候要特别注意。而且，传统方法中的参数一般会有明确的意义，或者说设计者会去

分析这些参数及系数的意义。 但是深度学习中的参数第一太多，没法分析；第二，好像也分析不出来什么意义。

当前的学术界研究方向以及工业界的应用，也都是在这三个步骤中开展的。 有的聚焦于设计函数映射集合；有的着重在设计误差准则； 有的精力放在如何更快地、更方便地训练，找到那个合适的函数。 每一步骤中推进，都会对任务的解决有帮助。 其实，在工作中，如果最终实际应用效果不好（或称之为泛化能力不足）， 你努力的方向也是这三个方面。

# 3 周边的相关概念

## 3.1 概念之间的关系

编程与程序员： 在一般的IT公司中， 程序员只要基于常识性的知识就可以对业务理解， 再辅以充足的时间和编程技巧，已经足够完成任务。 而机器学习，其实是一种数据编程的思路，确定好一个函数的大模样， 让程序通过数据自己去确定函数参数的具体值。

科学家与工程师： 在一般人的想象中，科学家更喜欢纸上谈兵，就是发文章，写书籍。 但是当前，在机器学习领域，一流的科学家是写代码的。他们也是一流的工程师。 如果你仔细翻看大牛们简历，他们写的代码又多又好，都是动手能力超强的人。 如卷积神经网络的发明人 Yann Lecun，是 Djvu Viewer 的软件作者。 吴恩达开发过 Citeseer 搜索引擎的代码。

学术界与工业界： 学术界与工业界紧密分工合作关系 系统研究者负责构建更好的工具，统计学家建立更的模型， 分工也使得深度学习可以更快地发展。同时， 与传统行业的技术封锁相比，机器学习领域的研究人员， 受互联网开源思维的影响， 他们对自己的算法、数据和成果一向采取开放的态度。 各个国家，各个公司的研究团队一起参加比赛，并相互切磋， 追求的是共同的进步。

算法与数据：优秀的算法、快速而廉价的算力、 大量的数据以及方便好用的软件工具， 使得机器学习可从学术界的纸上谈兵开始走向商业中的产品。

## 3.2 相关的人物

在机器学习的领域，杰出人物极多。我个人认为，下面三个人可以简单介绍一下。

Jeoffrey Hinton，其贡献在于设计优秀的机器学习算法。 其提出了在深度学习的网络中， 使用降维和逐层训练的方法及应用的办法。他解决了优秀的算法应该如何做

的问题。[1]

吴恩达，其贡献在于基于 GPU 的算力的推广。他极力推广GPU在机器学习中的应用。 最终使得 GPU 被广泛地应用在机器学习领域，并使得 Nvidia 一个原本生产 游戏显卡的硬件公司，在机器学习领域占了一席之地。[2]

李飞飞，其贡献在于对大量数据的理解和实践。其创建的 ImageNet， 人工标记了 1400 万张图片，使得算法研究者终于相信， 大量数据的输入会使得算法的效果得到惊人的提升， 证明了数据与算法是同等重要的。[3]

### 3.3 人工智能的派别

人工智能的目标是让机器通过某种方式具备了类似于人类的智慧。 而这种方式，自打这门学科创立以后，有两个派别：

1.) 唯物主义派，其核心思维是重建人类的大脑。我们要造一个 可以模拟大脑神经网络的机器或是程序。先别管为啥大脑长这个样， 然后，用大量的数据去让这个机器自己去学就好了。比如，想让它识别猫狗问题， 就搞大量的标注后的猫狗图片输入机器，然后机器就学会了识别猫狗。 尼克在他的书中称之为 「吃啥补啥」[2]。

2.) 唯心主义派，其核心思维是，我们要根据已经证明「正确的逻辑系统或基于规则式的方法（rule-based）和符号系统（symbolic systems）」，将相关领域的人类专家智慧写进软件，进而搭建一套智能系统。其强调要顶层设计，至顶向下，仔细规划和理解系统中每一个部分。 然后，上线运行，一定能OK。此派又戏称为「想啥来啥」。

两派长时间论战，各自都有道理。唯心派批评唯物派，只模仿不理解。 就像学开车，会开却不理解。啥都不懂，有啥用？ 要对其中发动机原理，机械传动要门清，否则出了问题都不知道是哪里的问题。 没有才是专家教授应有的样子。 唯物派批评唯心派，你们的模型太简单，处理不了实际的复杂问题，有啥用？ 形势情况比人强，能用再说，以后再慢慢琢磨其中的原理。 当然，如果两条腿走路那就是最好不过了。

## 4 回归分析

[1]这里小八卦一下，Hinton 是布尔代数的创始人布尔的后代。 Hinton 的姥姥的妈妈，是布尔的亲闺女。

[2]吴恩达曾在斯坦福大学建立了一个超级大的神经网络，有112 亿个参数。 如此规模的网络，也必须使用 GPU 才能行。

[3]李飞飞 1999 年大学毕业后，在中国西藏做过一年的医学药物研究。

## 5 增强学习

增强学习有两个理论基础：

1.）马尔可夫决策过程

2.）动态规划

（未完待续）

## 致谢

本文档承蒙好友 Hyde 对初稿给出的建设性意见， 使文档的质量与可读性有了质的提高，在此表示十分感谢！ [1]

## 参考文献

[1] This Person Does Not Exist. https://thispersondoesnotexist.com/

[2] 尼克. 人工智能简史. 人民邮电出版社，2017

[3] Khalid Sayood. 数据压缩导论. 人民邮电出版社，2014.

[4] Ian Goodfellow and Yoshua Bengio et.al. . Deep Learning. MIT Press，2016.

[5] 阿斯顿·张，李沐等. 动手学深度学习. 人民邮电出版社，2019.

[6] Hung-yi Lee. Machine Learning. https://www.youtube.com/playlist?list=PLJV_el3uVTsPy9oCRY30oBPNLCo89yu49.

[7] 李飞飞. https://zh.wikipedia.org/wiki/%E6%9D%8E%E9%A3%9B%E9%A3%9B

(THE END) ■

[1] 本文档中出现的图片除ML相关的图片为作者手工绘制以外， 其余的只是学习时，从互联网上搜索得到，当时未存留原始的一些标记信息。 所以，当前还不能准确地标注每幅图片的出处与原始作者信息。 在此，首先衷心地感谢这些图片的原始作者， 正是他们精致且恰当的图片使得本文档得以顺利完成； 其次，在后面的写作更新中，我 会逐步找到它们的原始出处，并在此文档中标注出来。