

周志华：关于机器学习的一点思考



【新智元导读】机器学习如今大获成功的原因有哪些？如何才能取得进一步的突破？南京大学周志华教授在 AI WORLD 2018 大会上分享他关于机器学习的一点思考：我们需要设计新的、神经网络以外的深度模型；让智能体在弱监督条件下也能够学习，以及考虑开放动态任务环境下的学习。

南京大学计算机系主任、人工智能学院院长周志华分享了他《关于机器学习的一点思考》。周志华教授表示，当前机器学习成功的背后，实际上离不开三点：1）有效的深度模型，现阶段基本上就是深度神经网络；2）存在强监督信息，也即数据都要有标注，而且越精准越好；3）学习的环境较为稳定。

因此，如果未来机器学习要取得进一步突破，就必须：1）设计新的、多样化的深度模型；2）让智能体能够在弱监督条件下学习；3）考虑开放动态任务环境下的学习。

周志华教授说，机器学习界早就很清楚，“没有免费的午餐”，也即任何一个模型可能只适用于一部分的任务，而另外一些任务是不适用的。

例如，Kaggle 竞赛中有各种各样的任务，但在图像、视频、语音之外的很多任务上，比如订机票、订旅馆之类，还是传统机器学习技术（如随机森林或 XGBoost）表现更好，尤其是涉及符号建模、离散建模、混合建模等问题。

周志华教授着重介绍了他带领团队提出的“深度森林”，这是一种以决策树为基础构建的深度模型。深度森林在超大型互联网金融企业的非法套现检测任务中，近 2 亿的真实交易数据实测上，性能超越了包括深度神经网络在内的其他模型。这也验证了周志华教授及其团队的猜想——在很多其他任务上，非神经网络的深度模型能找到用武之地。

不过，周志华教授也表示，任何一个理论的提出，都需要经过长时间的发展与完善。深度森林目前尚处于初级阶段，好比打开了“深度学习”这间小黑屋的一扇门，还有更多需要去探索。

周志华：关于机器学习的一点思考

以下是南京大学计算机系主任、人工智能学院院长周志华教授在 AI WORLD 2018 世界人工智能峰会上发表的演讲。

周志华：各位朋友，大家上午好！谢谢新智元杨总的邀请，前面一直没有机会参加，今天很高兴有这个机会。我本人从事的是机器学习方面的研究，今天就和大家汇报一些关于机器学习方面粗浅的看法，谈一谈机器学习发展取得了哪些成功，后面会有哪些问题值得进一步关注。

关于机器学习的一点思考

周志华

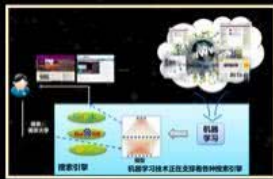
南京大学

<http://cs.nju.edu.cn/zhoush/>

Email: zhoush@nju.edu.cn

大家都知道，这一轮的人工智能热潮很大程度上是由于机器学习，特别是其中深度学习技术取得了巨大的成功。可以说今天每个人、每天都在谈机器学习，机器学习已经无所不在，各种各样的智能应用当中如果离开了机器学习，基本上是不可想像的。

机器学习已经“无处不在”



互联网搜索



生物特征识别



汽车自动驾驶



火星机器人



美国总统选举



军事决策助手

我们可能要问这样一个问题：

机器学习取得了这么多的成功，这些成功的背后到底是什么呢？

大家常说，现在成功的智能应用后面有三个重要的条件：一是现在有大数据了，二是现在有很强大的计算能力了，三是我们在算法方面取得了很多突破。

这三个因素都特别重要，但今天我们将主要聚焦于机器学习技术本身，谈一谈机器学习技术本身取得这些进展，背后到底有哪些原因。

机器学习 “成功的背后”？

- 有效的深度模型
- 存在强监督信息
- 任务环境较稳定
-

其实，无外乎就是三个因素：

- 1、能找到有效的深度模型
- 2、存在很多很强的监督信息
- 3、任务都是比较稳定的环境

现在所有成功的机器学习应用背后都离不开这三者，下面我们分别来看。

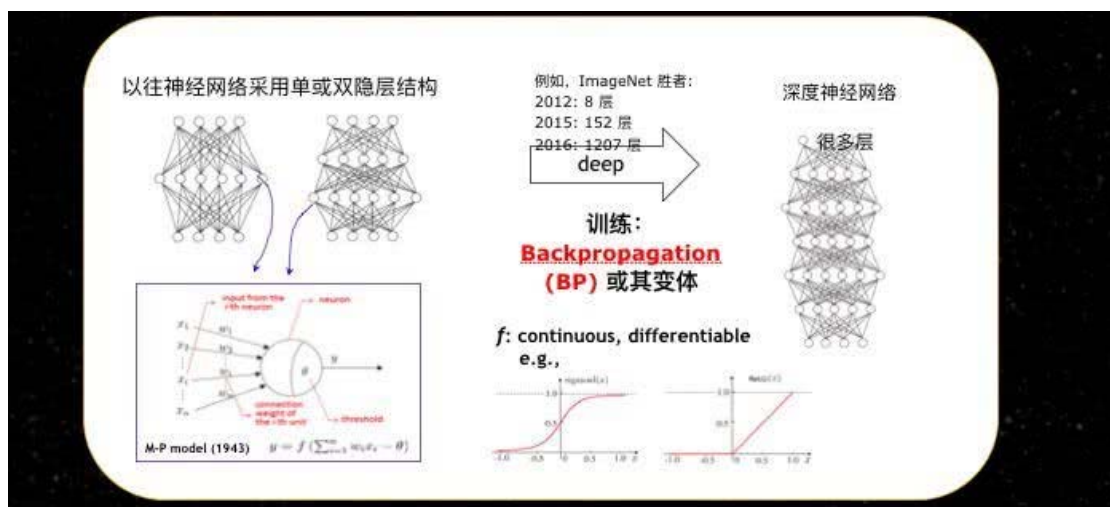


天下没有免费的午餐，深度神经网络必然有不适用的任务

首先是深度模型。

现在深度学习在图像、视频、语音这些数字信号建模任务当中取得了巨大的成功。如果我们问一问大家，“深度学习”是什么？我想从绝大多数人那里得到的答案都会是：

深度学习就是深度神经网络，甚至认为“深度学习”就是“深度神经网络”的同义词，谈到深度学习就要从深度神经网络或者从神经网络谈起。



事实上，神经网络并不是新事物，我们已经研究了半个多世纪，只不过以前我们通常研究的是有一个隐层或两个隐层这种比较浅的神经网络，其中每个计算单元都是非常简单的模型。早在 1943 年，我们就已经把它抽象成了这样一个非常简单的数学公式，就是从外界收到输入 X ，经过 W 放大，总的输入如果要比 θ 高，我们会用激活函数处理进行输出。这样的模型到今天依然在沿用。

深度神经网络带来的最大区别是什么呢？虽然有各种各样的模型，各种各样的算法，但是**最根本的差别就是现在我们用了很多很多层。**

深度神经网络最著名、最早的成功来自 2012 年，在计算机视觉领域最著名的 ImageNet 比赛上获胜。当时这个获胜的模型用了 8 层，2015 年获胜的模型用了 152 层，2016 年就用到了 1207 层，今天几千层的模型比比皆是。

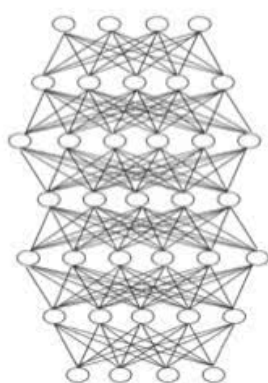
实际上，这样的模型当中有大量参数需要计算，所以需要非常复杂、非常庞大的计算系统。虽然现在我们有了很强的计算设备和很巧妙的算法，但是**我们能够做到这一切，根本的原因之一是神经网络中基本计算单元激活函数是连续可微的。**原来浅层神经网络用的是左边的函数，也是连续可微的，深度学习的年代我们通常会用右边这样的函数或变体。

不管怎么样，可微性给我们带来了非常重要的结果，就是可以很容易地计算出梯度，基于梯度的调整就可以用著名的 BP 算法来训练整个模型。

这一点非常重要，因为如果不是从事机器学习研究的朋友会觉得，神经网络半个世纪之前就有了，到了今天我们之所以能够做更深的神经网络，只不过是因为计算能力强，现在能够训练了。实际上不是这样的。

2006 年之前，可以说我们都不知道怎么训练出 5 层以上的神经网络，根本原因是一旦层数高了以后，用 BP 算法梯度就会消失，然后就不知道该怎么学习下去。所以，2006 年的时候 Geoffrey Hinton 做了很重要的工作，通过逐层训练来缓解梯度消失，使得深层模型能够被训练出来。后来有了一系列深度学习的工作，包括到今天为止的很多前沿研究，都是在防止深层网络中梯度消失，使得梯度更新搜索能持续下去使训练能够完成。

深度神经网络模型的缺陷



- 太多超参数
 - 调参难，“跨任务”经验难分享
 - 重复结果难，即便使用相同数据、相同模型，不知道超参数设置就无法重现结果
- 模型一旦选定，模型复杂度即确定；通常远大于“所需”复杂度
- 大训练数据
- 理论分析难
- 黑箱模型
- ...

神经网络取得了非常大的成功，但任何一个模型都必然存在缺陷，神经网络也是这样。

常用神经网络的朋友知道，现在深度神经网络有很多问题。大家经常说的一件事情就是要花大量的精力调整参数，参数实在太多了。不仅如此，这还会带来另外一个严重的问题：**哪怕我告诉你同样的算法、用同样的数据，如果不告诉你参数是怎么调的，可能就没有办法得到同样的结果。**

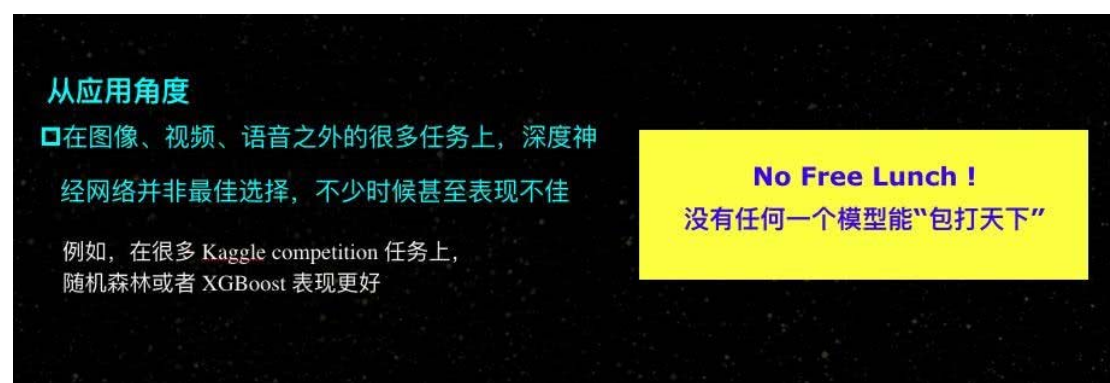
此外，还有很多别的问题，比如我们现在用的神经网络模型的复杂度是固定的，一旦先确定了一个模型，就把这个模型用下去。问题是，在解决一个现实问题之前，我们怎样才能知道什么样的模型是最恰当的呢？我们不知道，所以通常会用一个过度复杂的模型来做问题，做的过程当中不断把它简化。

最近如果大家关心深度学习方面的一些前沿研究，可能就会发现现在有大量的论文是关于模型压缩、模型简化等等，事实上都是由这个原因导致的。我们能不能在使用模型的最初不要使用那么复杂的东西？先使用一个比较简单的，然后随着数据和训练的过程让它自适应地、自动地提升复杂度呢？很遗憾，我们对神经网络很难做到这一点，因为我们一旦用 **BP** 算法基于梯度搜索来做这件事情，如果事先结构都完全不知道，那么求梯度的对象也就知道了。

这里有很多的问题，更不用说还有其它的缺陷，比如大的训练数据、理论分析很困难、黑箱模型等等。

有些工业界的朋友可能会说，前面你们谈到的这些缺陷都是从学术角度来说的，我关心实践，只要性能好就行，至于学术上有什么缺点我不关心。实际上就算从这个角度来看，可能也还有很多的需求希望我们去研究其它的模型。

如果我们真正看一看今天的深度神经网络到底在哪些任务上取得了成功，其实我们可以看到无外乎主要就是图像、视频、语音，涉及到这些对象的任务。它们非常典型，都是一些数值信号建模的任务。而在很多其他的任务上，深度神经网络表现并没有那么好，比如可能有的朋友接触过 Kaggle 这个数据分析竞赛的网站，上面每天都有很多数据分析的任务，有订机票的，有订旅馆的，到今天为止，虽然深度学习网络这么成功，很多这样的任务上我们可以看到获胜的通常还是一些相对传统的机器学习技术，而不是深度神经网络。



从应用角度

□在图像、视频、语音之外的很多任务上，深度神经网络并非最佳选择，不少时候甚至表现不佳

例如，在很多 Kaggle competition 任务上，随机森林或者 XGBoost 表现更好

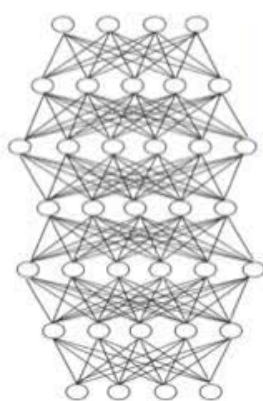
No Free Lunch !
没有任何一个模型能“包打天下”

事实上，机器学习界早就很清楚这件事情了，我们有一个经过严格证明的定理，叫做“没有免费的午餐定理”，也就是任何一个模型可能只有一部分任务是适用的，另外一些任务是不适用的。

所以，虽然深度神经网络在有些任务上很成功，但对别的应用来说，我们有没有可能设计出新的模型，在这些任务取得以往没有取得的效果？这可能也是非常值得关注的一件事情。

基于非可微构件、非神经网络的深度模型，是下一步很值得探索的方向

重新审视深度模型



目前，深度模型就是深度神经网络，更确切地说：
multiple layers of parameterized differentiable nonlinear modules that can be trained by backpropagation

- 现实世界中并非所有规律性质都是“可微”(differentiable)，或者通过可微构件建模最优
- 机器学习中有许多“不可微”构件（它们无法通过backpropagation训练）

如果我们重新审视深度模型自身的话，会发现今天我们所谈的深度模型其实都是指深度神经网络，而用更学术的话来说，这是由多层参数化可微的非线性模块搭建起来的模型，而它本身能够用 **BP** 算法去训练。

最近有些深度学习网络的研究在考虑怎样用一些不可微的激活函数，但是实际上是怎么做的呢？先用了一个不可微的激活函数对现实建模，然后在优化的过程当中逐渐近似放松，最后还要把它变成一个可微的东西求解，所以最终还是离不开可微性。

但是，现实世界当中并不是所有规律都是可微的，或者能够利用可微构件最优建模的，而且另一方面我们机器学习界早就经过了很多年的

研究，也有很多不可微的构件，这些构件以后有没有用呢？现在我们就在考虑这样一个很基础的问题，就是能不能基于不可微构件进行深度学习？

A Grand Challenge

能否基于不可微构件进行深度学习？

Can we realize deep learning with non-differentiable modules?

这个问题相当本质，对它的研究将可能使我们理解：

- Deep models ?= DNNs
- 如何能基于不可微构件“做深”？（不使用BP）
- 能否使得图像、语音、视频之外的更多任务受益于深度模型？
-

这个问题如果得到答案，我们可以得到一系列其它问题的答案，比如深度模型是不是只能用深度神经网络来做？我们有没有可能不通过BP算法来做出这种深度模型？我们能不能在图像、视频、语音之外的任务也能够获得一些深度模型，帮助我们获得更好的性能？

新探索：深度森林 (Deep Forest)

- 使用不可微的树模型；不通过BP训练
- 超参数数目远少于DNN → 易于训练
- 模型复杂度可以根据数据自适应确定
→ 小数据也适用
- 在很多任务上性能接近或超过DNN



The image shows three screenshots of the Deep Forest software interface. The top screenshot displays the 'Model Configuration' window with various parameters like 'Number of trees', 'Maximum depth', and 'Learning rate'. The middle screenshot shows the 'Training Results' window with a table of performance metrics. The bottom screenshot shows the 'Model Evaluation' window with a table of performance metrics.

这是第一个“非神经网络”、
不使用BP算法训练的深度学习模型

最近我们的课题组做了一些研究，提出了一个新的模型叫做“深度森林”，这是不基于神经网络来做的模型，它的基本构件是决策树，本身是不可微的，所以不能用 BP 训练，模型复杂度可以自己根据数据调整，超参数比深度神经网络要小。除了大规模的图像类任务之外，很多的任务上它的性能已经达到或者接近了深度神经网络的性能。从学术上来说，特别值得关注的就是它是第一个非神经网络，不使用 BP 算法训练的深度学习模型。



后来国际上关于这件事情也有一些反响和探讨。Keras 的创始人说，这种可微层是当前深度学习模型的根本弱点，现在我们的模型本身是不使用可微层的；深度学习的奠基人 Geoffrey Hinton 说放弃 BP 从头开始，现在我们的模型就完全没有使用 BP 算法。这类模型不一定仅限于“深度森林”这样的模型，基于非可微构件、非神经网络的深度模型可能是下一步很值得探讨的方向。大家知道深度神经网络已经研究了二十多年，再往下研究的空间可能不见得那么大，但是其它的模型有没有可能做深呢？一旦我们往前走了一步，可能会给我们带来巨大的空间。

这只是学术上的意义，来自工业界做应用的朋友可能会问，应用上到底有什么东西用它做比较好？在图像、视频、语音这些纯的数值建模之外，涉及到符号数据、离散数据、混合建模的问题，可能是这种不可微模型能够发挥作用的地方。

A real application:

Detection of Illegal cash-out (非法套现)



Very serious, particularly when considering the big amount of online transactions per day

For example, in 11.11 2016, more than 100 millions of transactions are paid by Ant Credit Pay

Big loss even if only a very small portions were fraud

比如最近我们和国内一个非常大的互联网金融公司合作，做在线支付的非法套现检测。这个公司非常大，大家每天都在接触它，每天有大量的网上交易，比如在 2016 年“双 11”这一天，一天就有 1 亿多交易是通过网上支付来做的。非法套现是一个很大的问题。

Results

Table 1: The number of the training and test samples.

	# Pos. Ins.	# Neg. Ins.	# All Ins.
Train	171,784	131,235,963	131,407,704
Test	66,221	52,423,308	52,489,529

More than 5,000 features per transaction, categorical/numeric (details are business confidential)

Evaluation with common metrics

	AUC	F1	KS
LR	0.9887	0.4334	0.8956
DNN	0.9722	0.3861	0.8551
MART	0.9957	0.5201	0.9424
gcForest	0.9970	0.5440	0.9480

Evaluation with specified metrics

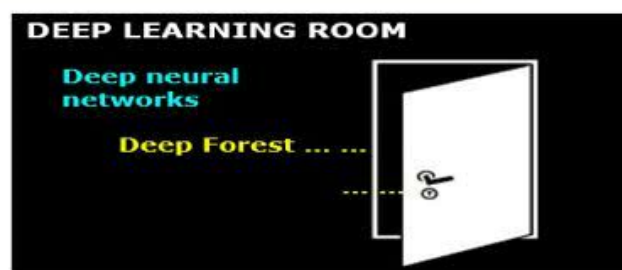
	1/10000	1/1000	1/100
LR	0.3708	0.5603	0.8762
DNN	0.3165	0.4991	0.8471
MART	0.4661	0.6716	0.9358
gcForest	0.4880	0.6950	0.9470

1/100 means that 1/100 of all transactions are interrupted

Deep forest performs much better than others

我们给大家看个结果，训练数据用了 1 亿 3 千多万的真实交易，测试数据用了 5 千多万真实交易，这可能是世界上最大的关于互联网交易非法套现的数据。这家公司内部有一个大型分布式机器学习系统，他们的工程师很厉害，做了深度森林的大规模分布式实现，实测结果来看比系统中以往的模型包括深度神经网络在内的性能都还要更好一些。这也验证了我们所猜想的，在很多其它任务上，图像、视频、语音之外的任务上，非神经网络模型能找到用武之地。

深度森林 (Deep Forest)

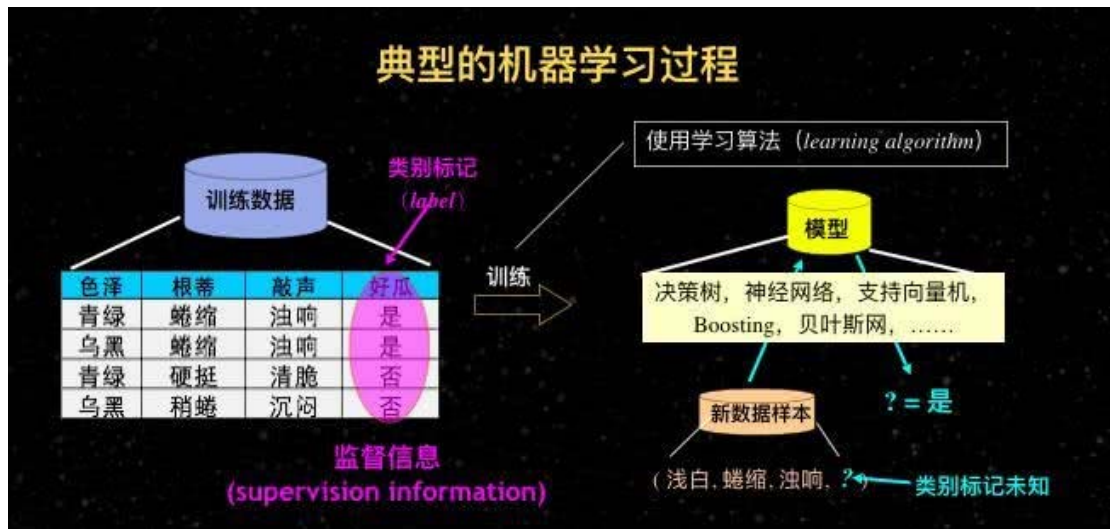


Z.-H. Zhou and J. Feng, Deep forest: Towards an alternative to deep neural networks. arXiv1702.08835.

只是一个开头，大量进一步探索、改进的工作

另外一方面，这毕竟只是一个起点，因为深度神经网络研究了 20 多年，深度神经网络经过几十万上百万研究实践者这么多年的探索改进，而非神经网络深度学习的研究才刚刚开始，只有几个人做了一点点事情，未来有非常多可以探索的东西。任何一个新技术往前走的话都有很多工作要做。关于深度模型真正重要的意义是，以前我们以为深度学习只有深度神经网络，现在知道这里面可以有其它的东西。

当前机器学习高度依赖于强监督信息，弱监督学习还有很大空白



关于监督信息。对于一个机器来说，我们拿到很多数据之后，经过训练得到模型，这个模型能够发挥作用，能够做精确预测。这里面很重要的是我们需要有很多数据，而且这些数据需要有监督信息。

机器学习

目前高度依赖：**强监督信息！**

例如：深度学习需要大量样本

- > 2012年在ImageNet竞赛夺冠的CNN共8层，使用了超过22000类别的1500多万样本
- > 2016年夺冠使用的网络共1207层，.....

大数据时代，数据样本不成问题？

No！样本需要标记 (label)！

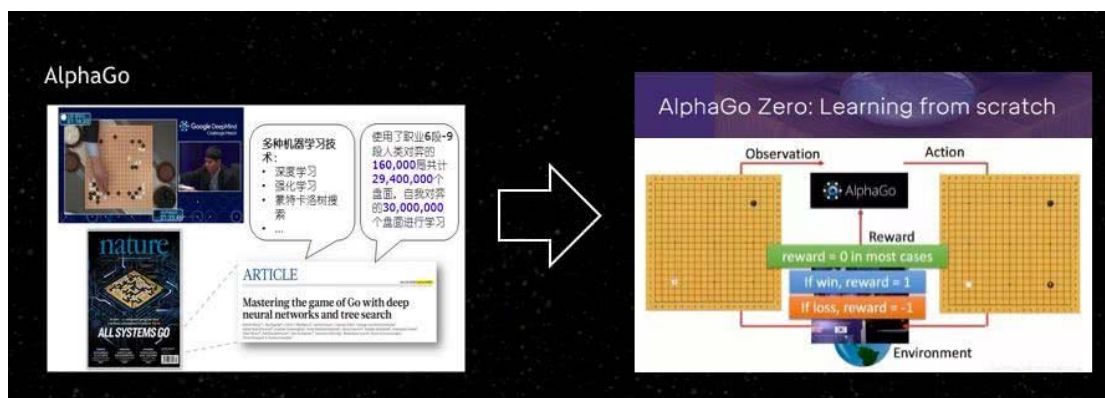
大量人力物力花在标注数据上

深度学习需要大量的样本，2012年ImageNet获胜的网络已经用到超过1500多万样本，而现在的网络越来越大，所需要的样本越来越多。大家可能会有一个误解，大数据时代数据样本是不是不成问题？



其实不是的。

样本需要标记，我们现在大量的人力物力都花在这件事上，比如前段时间有讨论人工智能会不会使得一些职业消亡。是不是消亡我们没看到，但是我们已经看到一个新的职业，就是数据标注已经变成一个产业。这件事情不管它好还是不好，反正它就在那儿，至少告诉我们机器学习技术现在对强监督信息是高度依赖的。



谈到这件事可能有的朋友会想到前段时间很热门的 AlphaGo，最早的 AlphaGo 使用人类职业六段以上的所有棋局，超过 16 万棋局进行学习。后来发明了 AlphaZero，不使用人类棋局，通过两个程序直接对弈提升性能，这样是不是不需要监督信息了呢？



所谓的 AlphaZero，DeepMind 说它是“从零开始学习”，第一天没有任何数据，第三天超过战胜李世石的版本，第 21 天超过 Alpha Master，第 40 天达到人类见到的最强能力。中间没有用任何人类的棋局，这是不是意味着它背后的强化学习技术真的不需要监督信息？

No！ 关于游戏本身的“胜负规则”（上帝判断）是极强的监督信息

在一般机器学习任务中，如何得到“上帝判断”？

更多的现实机器学习任务中：

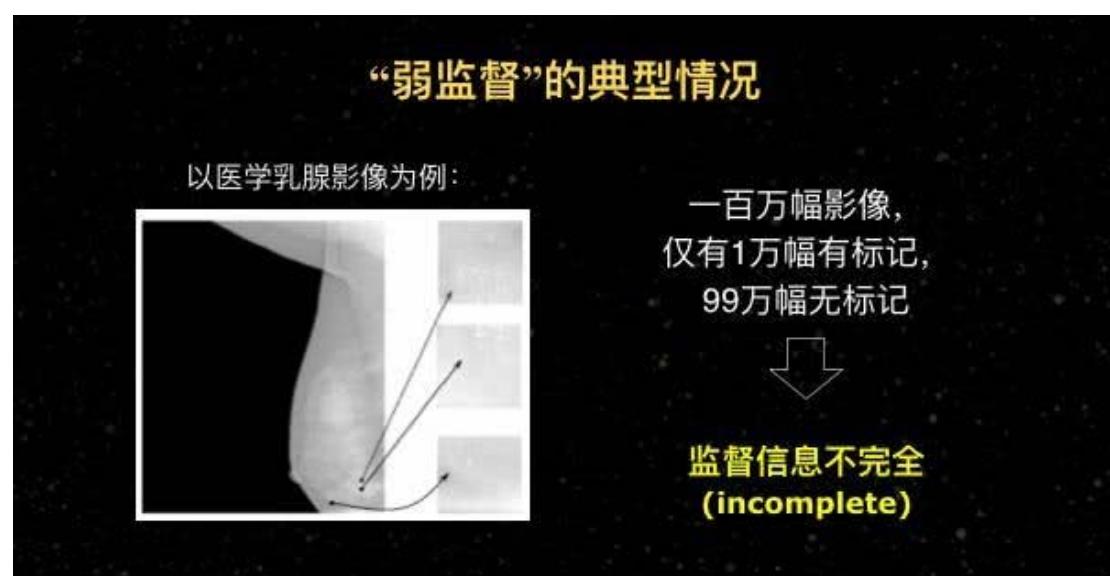
- 既缺乏大量“有标记数据”
- 也难以通过“无成本探索”获得大量训练样本

其实不是这样的。因为非常重要的一点，是当两个程序在对弈的时候，我们一定能够判断出胜负，而胜负规则是非常强的监督信息，是上帝判断。

打个比方来说，我要建一个能抵抗 18 级台风的桥，事先不知道怎么办，没有人教我怎么办，不管怎么样，如果我能建出一个东西来，就

有一个“上帝”告诉我，你这个东西能扛过去、那个东西扛不过去，有了这个指导信息，经过不断摸索最后就可能把这个桥建出来。

真正的现实应用中哪里能得到这样的上帝规则？根本得不到。我们也不可能通过无成本探索像围棋这样获得大量的样本。我们没有办法去做真正的不需要任何数据，不需要任何标记的学习。



我们现在能做的还是要往弱监督学习上做。

所谓的弱监督学习，就是希望监督信息不用那么多了，稍微少一点，它还是能够工作得很好。举几个典型的弱监督学习的例子：在医院里诊断乳腺图像的影像，希望看到影像中有没有钙化点。一个医院有很多数据，比如 100 万幅图像，但是医生只标注了一万幅，有 99 万幅没有标记，这种叫做监督信息不完全。

第二种情况，可能医生只告诉我们这个图像里面有病灶，但是病灶在哪儿没标出来，这时候我们把它叫监督信息不具体。

还有更多的情况，比如医生由于疲劳、疏忽等标注中间有错误，我们就把它叫做监督信息不精确，这是三种典型的情况。



事实上很多应用里这些问题都普遍存在，大量的应用都能看到这三种情况。对这些情况事实上机器学习界有一些探索，比如第一种情况我们做半监督学习、主动学习；第二种情况有多示例学习，有 MIML；第三种有众包学习、带噪学习。这是好的一方面。

另一方面，强监督学习我们已经研究很多，非常典型的弱监督学习也已经有研究，但是还有更多的弱监督状态，例如这个图中几朵云之间的过渡状态，这些状态有的连学术探讨的文献都还很少见。

关于弱监督学习，应该说还有大量的事情需要我們去做。

相关探索

监督信息不完全 (incomplete) \Rightarrow 半监督学习, 主动学习,

监督信息不具体 (inexact) \Rightarrow 多示例学习, MIML,

监督信息不精确 (inaccurate) \Rightarrow 带噪学习, 众包学习,

大量内容有待探索

参见: Z.-H. Zhou. A brief introduction to weakly supervised learning. *National Science Review*, 2018, 5(1): 44-53.

开放环境下的机器学习研究是通往鲁棒人工智能的重要环节

接下来谈一谈任务环境。

机器学习现在取得胜利，基本上都是在封闭静态环境里面。我们要假定很多东西都是固定的，比如我们要假定所有的数据都来自于独立同分布，数据分布恒定。

传统机器学习任务

主要针对 **封闭静态环境** (重要因素大多是“定”的)

色泽	根蒂	敲声
青绿	蜷缩	浊响
乌黑	蜷缩	浊响
青绿	硬挺	清脆
乌黑	稍蜷	沉闷

数据分布恒定

样本类别恒定

样本属性恒定

评价目标恒定

我们通常要假定样本类别恒定，训练数据只能让我识别苹果和梨，以后给我的东西我就只会识别成苹果和梨，给我一个菠萝也会只从苹果和梨当中选择一个，判断到底是两个中间的哪个。

样本属性也是恒定的。样本里面用一百个属性来描述我的数据，预测的时候也要把这一百个属性给我，中间不能发生变化。

甚至我们的目标也要恒定。一个模型好，我们就认为它就是好的，不管对谁来说都应该是一个好的模型。

传统机器学习任务

主要针对 **封闭静态环境**（重要因素大多是“定”的）

色泽	根蒂	敲声
青绿	蜷缩	浊响
乌黑	蜷缩	浊响
青绿	硬挺	清脆
乌黑	稍硬	沉闷

现实机器学习任务常面临

“开放动态环境”

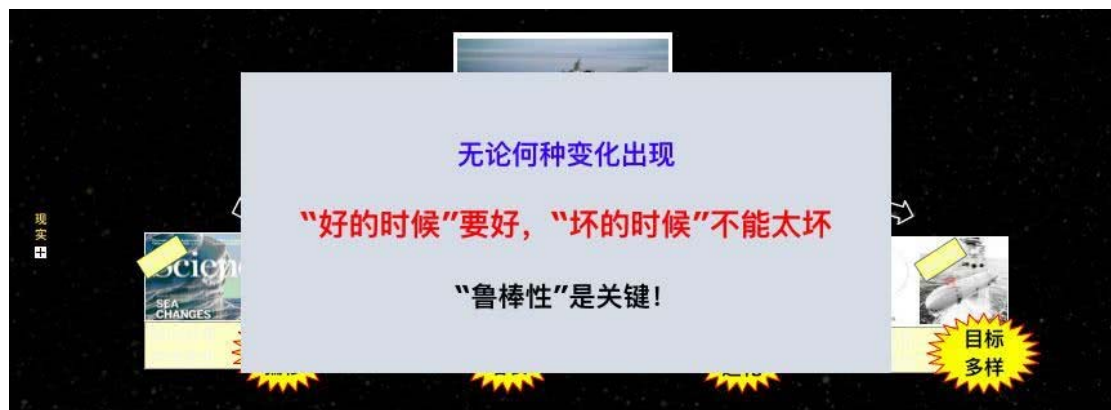
一切都可能“变”！

数据分布恒定
样本类别恒定
样本属性恒定
评价目标恒定

事实上，我们现在越来越多地碰到所谓的开放动态环境。在这样的环境中可能一切都会发生变化。

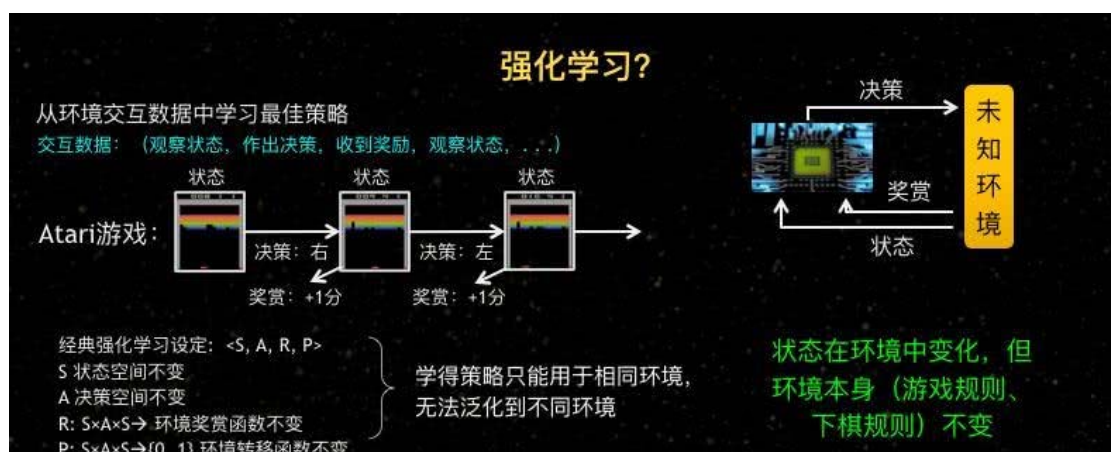
现在有一条船开到海上去，我们不断搜集海面的数据来做导航，可以知道今年在海上碰到的海冰分布和去年就是不一样的，这个数据其实每年都在变。这就是数据分布发生变化。

我们碰到以前没有见过的困难情况，这是新的类别。如果把船开到两极地区，由于环境恶劣，接入困难等等，有的属性丢失了拿不到，这时候我们怎么办？是不是属性不够就不能做预测，不能用了呢？



最后，我们同时要兼顾很多目标，只考虑一种目标得出来的模型往往可能是不能用的模型，必须要多个目标都不错才能用。

可能会出现很多的变化，但是不管什么样的变化出现，我们都希望好的时候要好，坏的时候不能太坏。这时候模型的鲁棒性是一个很根本的要求。



关于这个问题，可能有的朋友如果对机器学习比较熟悉的话，马上就会想到，不是有一种强化学习技术吗？这种强化学习技术是通过跟环境交互来进行学习的，它不就自动能适应环境吗？

事实上这可能是一个误解，现在虽然已经有很多强化学习的研究，包括用强化学习来打游戏，在很多游戏上获得胜利等等，看起来是和环境交互，但事实上，在整个强化学习的经典假定里面，它所考虑的是状态在环境中的变化，但是环境本身的基本规则比如下围棋的游戏规则，在游戏过程中是不变的。

绝对不是说在学习的过程中是一种环境，在用的时候环境变化了，我这个模型还能用，那是不行的。比方说训练下棋模型的时候原来是什么规则，以后模型使用的时候仍然是这样一种规则环境。

这个问题使用传统强化学习技术还远远解决不了。



国际上对AI发展的探讨

国际人工智能大会 (AAAI)
“主席报告”
("Presidential Address")

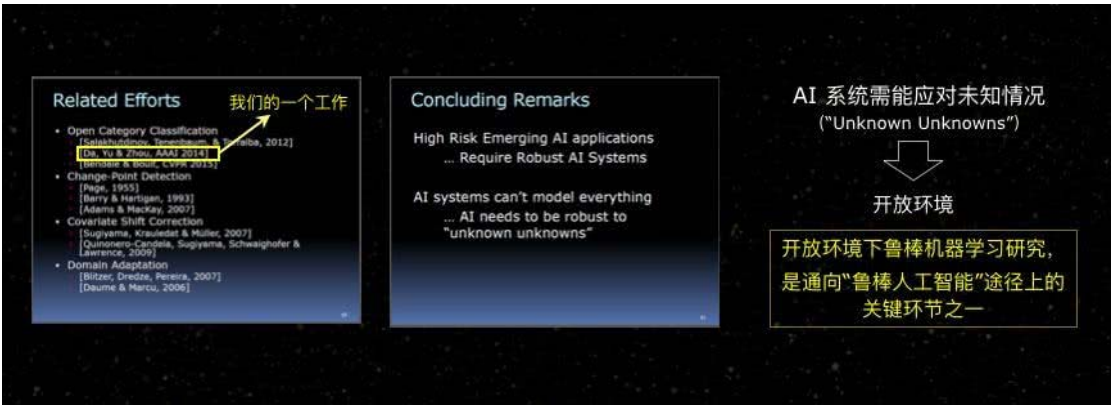
Tom Dietterich
ACM/AAAI/AAAS Fellow
国际机器学习学会创始主席; AAAI 主席
美国白宫《国家人工智能研究与发展战略规划》起草人之一

国际上怎么看这件事？

在国际人工智能大会（AAAI）Tom Dietterich 教授做了一个主席报告，叫“通往鲁棒的人工智能”，特别提到现在人工智能技术取得巨大发展，越来越多地面临高风险应用。



所谓高风险应用是指自动驾驶汽车、自主武器、远程辅助外科手术等等，这一类应用无一例外都是一旦出现了问题，会造成巨大的损失。所以，我们才希望不要出问题，希望学习过程必须有鲁棒性。



他提出未来的人工智能系统需要能够应对未知情况，他给了一个说法，叫做“Unknown Unknowns”，指的就是开放环境。开放环境下机器学习研究是通往鲁棒人工智能的非常重要的环节。

最近有另外一个消息，美国国防部宣布开发下一代人工智能技术，用一句话来说，“旨在开发能够进行学习并适应不断变化环境的机器”。这句话其实就是把所谓的开放动态环境下的学习换了一个表述，并且用到军事应用里去。


相关探索	样本类别变化	⇒	[Da, Yu, & Zhou, AAAI'14] [Zhu, Ting, & Zhou, ICDM'16] [Mu, Ting, & Zhou, TKDE 17] [Mu, Zhu, Du, Lim, & Zhou, AAAI'17] [Zhu, Ting, & Zhou, ICDM'17] [Mu, Zhu, Liu, Lim, & Zhou, PAKDD'18] [Zhu, Ting, & Zhou, TKDE in press] [Xu, Niu, Han, Tsang, Zhou, & Sugiyama, arXiv.1805.09156]
	数据分布变化	⇒	[Zhang & Zhou, AAAI'14] [Zhang & Zhou, IJCAI'17] [Zhao & Zhou, arXiv 1706.02471]
	样本属性变化	⇒	[Hou & Zhou, PAMI in press] [Hou, Zhang, & Zhou, NIPS'17] [Xu, Niu, Han, Tsang, Zhou, & Sugiyama, arXiv.1805.09156]

从学术上来说，我们组里对这件事关注得比较早，有一些探索，前面Dietterich 教授的报告也提到了我们的一点工作。这张片子里面是我们最近关于应付各种变化的一些探索性工作。

OpenAI 强化学习竞赛 (2018.4.5-6.5)


操作一款经典电脑游戏
(刺猬索尼克)

- 输入：屏幕图像
- 评分：游戏得分



58个训练关卡
11个测试关卡

关卡图像、地形有很大差异



适应环境变化能力！

最近 OpenAI 组织了一个强化学习的比赛，比赛内容是打游戏。最近这段时间可能大家听到关于人工智能技术来打游戏的消息有不少了，比如 DeepMind 的消息等等。现在我们说的这件事和其他那些有什么不同呢？

以前打游戏的时候是把告诉你打什么游戏，学习程序可以把整个游戏都玩一遍，玩够之后再和人玩，也就是说训练的时候可以看到所有的场景。

而这个比赛和以前不太一样的是，它给我们的训练场景和测试场景是完全不一样的，训练场景 58 个关卡，测试 11 个关卡，环境变化非常明显，最重要的是考验我们怎么去适应环境变化的能力。

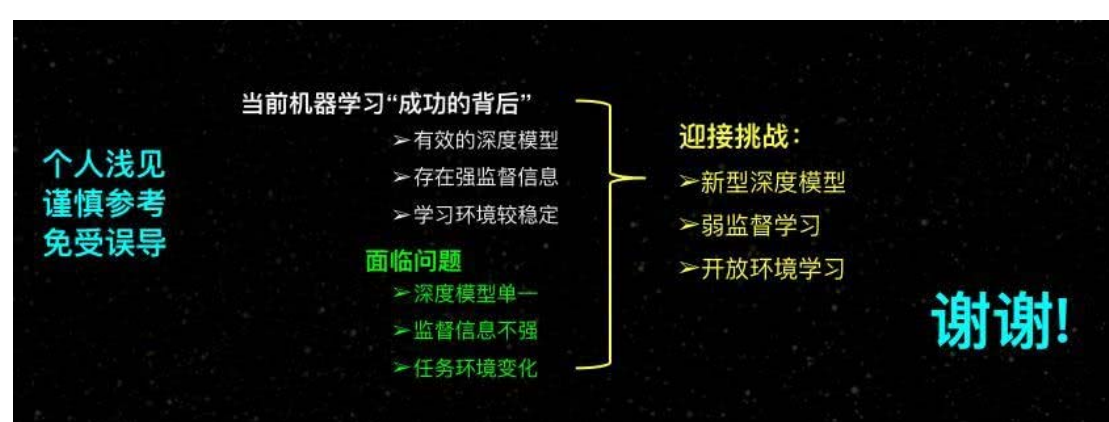


第一个是 2004 年我们提出的叫“二次学习技术”，先学一个模型，再做第二次学习得到进一步的加强。这个技术后来被 Geoffrey Hinton 重新命名为 Knowledge Distillation。

另外一个技术是我们通过集成学习研究得到启发，引入多样性激励。

如果只使用传统强化学习环境的激励，进去好的状态之后就很难再探索了；而现在引入多样性激励之后，一个地方做得好，会自动去探索别的地方。

我们这两个原创的小技术结合起来得到一个好的结果，比拿别人发明的技术获胜做起来更好玩。



总结一下，现在机器学习成功的背后主要有三个原因，有效的深度模型，存在强监督信息以及学习环境比较稳定。但是，现实应用里面这三件事情都不成立，有的场合可能还没有很适合的深度学习模型，监督信息也不够强，任务环境不断变化等等。

所以下一步，机器学习的研究或者应用特别要关注研究新型深度模型、弱监督学习以及开放环境的学习。

这只是我自己一些非常粗浅的看法，不一定准确，仅供大家批评，谢谢！