AI 技术的天花板

即使将来 AI 会超越人类智能，也至少不会基于这一代的计算机技术和理论，或许会是基于量子计算

人工智能（AI）的基本假设是“认知即计算”。但目前对认知本质的理解不同发展出了多个学派，典型的如基于数理逻辑的符号学派、模仿生物行为特征的行为主义学派，以及模仿生物神经网络的连接学派。

60 多年来，AI 已多次起伏。本轮兴起的主因是硬件能力的飞跃、数据的海量增长和算法的明显改进，尤其是神经网络（更准确地说是深度学习）在计算机视觉和自然语言识别方面取得了突破。当然，云计算、开源运动和摩尔定律，也起到了至关重要的推动作用。

但目前基于深度学习的 AI 技术还存在诸多限制。例如，算法还是个黑盒子，无法做因果解释，调参数主要还是靠运气。另外，机器学习的训练是个吞噬算力的“算老虎”。第三，数据透明性不够，诱导性或对抗性数据容易改变学习的结果等。这些都导致目前的 AI 技术还无法与其他学派有机结合起来。

最关键的，所有 AI 的实现都要依靠各类计算机，从 PC、服务器到 GPU（图形处理器），它们都是 “图灵机”

的具体实现。但理论上已证明，图灵机是无法建立起“自我”意识的概念。换言之，即使将来 AI 会超越人类智能，也至少不会基于这一代的计算机技术和理论，或许会基于量子计算。 AI 三大学派进阶

起源于 60 年前的 AI 理论，建立在“智能的本质是计算”的基本假设上。但因为对智能本质的认知不同，基于计算机如何构造 AI 已形成了三大学派。

第一个叫符号主义学派。主张智能源于数理逻辑，认为人类的认知和思维的基本单元是符号，认知过程就是对符号的逻辑运算。其代表作是在电视问答竞赛中战胜人类选手的 IBM Watson。

第二个叫行为主义学派。主张的基础是诺伯特?维纳的控制论，把关注的焦点从人类转向了整个生物界的智能（比如昆虫的个体和群体智能），终极形式是二进制的人工生命。其代表作是麻省理工学院的“六足机器人”。

第三个叫连接主义学派。主张将智能建立在大量简单的计算单元上，经过复杂连接后，并行运算的结果。这一学派基于神经生物学和认知科学，因为人类大脑就是由 1 万亿个简单的神经元细胞，错综复杂地连接起来产生的。

神经网络诞生于上世纪 60 年代，最初只包括输入层、隐藏层和输出层。输入层和输出层通常由应用决定，隐含层包含神经元可供训练。2006 年，多伦多大学教授 Geoffrey

Hinton 的团队在《科学》上发表了一篇文章，提出了深度学习的概念，指出可以用更多隐藏层（比如 5 层-10 层）做算法训练，因为实验效果显著，开启了学界和产业界 AI 的新浪潮。

相比传统的机器学习，深度学习可以让机器自动习来特征，无需人工事先设定。针对不同的应用场景，传统机器学习算法需要把软件代码重写一遍，而深度学习只需要调整参数就能改变模型。

深度学习是用数据来做训练。一般而言，学习的深度越深和广度越大，需要的数据量就越大，需要的数据种类就越多。当然不能一概而论，也不是数据越多越好，可能会出现“过度训练”。

深度学习的训练分两种。一种是有监督的，就是人工为数据加了标签，这种方法的缺点是，现实世界中被打了标签的数据太少了。另外一种是无监督的，只有数据没有人工的标签，计算机不知道正确答案就可以训练。 这一轮的动力

AI 的新算法和新数据，都以大幅增加对计算资源的消耗为前提。业界找到的新动力，或者说新的计算资源，就是 GPU（图形处理单元）。

60 多年来 AI 市场规模一直很小，内部帮派林立，支撑不起 AI 专用芯片的市场。因此早期的机器学习，只能基于廉价而广泛存在的 CPU 提供计算资源，或者极少数情况下用

代，设计专用于高并发计算、GPU?Q 生于上世纪 90 年代
大量浮点计算和矩阵计算能力的视频游戏和图形渲染等应用，即计算密集型应用。深度学习正好就是计算密集型的。大约在 2008 年-2012 年，业界逐步摸索到了，如何将深度学习与 GPU 有机结合起来的工程方法，直接将深度学习的速度加速了数百倍，让产业界看到了把 AI 实用化的希望。

当然 GPU 可能也还是太通用了，于是更加专用的 FPGA（Field Programmable Gate Array，现场可编辑阵列）和 ASIC（Application Specific Integrated Circuit，专用集成电络）纷纷登场。谷歌新近发布的 TPU（Tensor Processing Unit）芯片，号称处理速度比 CPU 和 GPU 快 15 倍-30 倍，性能功耗比高出约 30 倍-80 倍，当然是神经网络专用场景。

摩尔定律说，同样成本每隔 18 个月晶体管数量会翻倍，反过来同样数量晶体管成本会减半。近年来摩尔定律虽然有所减速，但仍然是 CPU、GPU 和 TPU 等快速发展的基础。

云计算也是 AI 发展的坚实基础。产业界云计算“大佬”纷纷推出“GPU/FPGA/算法/数据 as a Service”业务，可以通过云端直接租用资源，方便用户做深度学习。

近十年来，不仅是软件定义世界，而且是开源软件定义世界。如果说 2017 年 AI 技术最大的变化是专用硬件的设计潮，那么 2016 年 AI 技术的最大变化则是巨头们纷纷开源了

深度学习框架，比如 Facebook 的 Torch 和 Caffe，谷歌的 Tensorflow，亚马逊的 MXnet，微软的 CNTK，IBM 的 SystemML 等。十年前，谷歌开源了 Android 操作系统，成功打造了智能手机的 Android 生态。现在，谷歌等纷纷开源 AI 框架，希望打造“AI 优先”时代的新生态，重现往日辉煌。

技术仍有局限性

深度学习的效果取决于网络结构的设计、训练数据的质量和训练方法的合理性等。无论是从统计学还是对智能的基本认知的角度看，这次深度学习牵引的 AI 产业化浪潮还存在不少局限性。　　首先是在算法方面。深度学习目前仍然是黑盒子，缺乏理论指导，对神经网络内部涌现出的所谓“智能”还不能做出合理解释;二是事先无法预知学习的效果。为了提高训练的效果，除了不断增加网络深度和节点数量、喂更多数据和增加算力，然后反复调整参数，基本就没别的招数了;三是调参还像玄学。还没有总结出一套系统经验做指导，完全依赖个人经验，甚至靠碰运气;四是通用性仍有待提高。目前几乎所有的机器学习系统都是被训练执行单一任务，没有之前任务的记忆。

其次是在计算方面。目前的机器学习基本还是蛮力计算，是吞噬“算力”的巨兽。一是在线实时训练几乎不可能，还只能离线进行;二是虽然 GPU 等并行式计算硬件取得了巨大进步，但算力仍然是性能的巨大瓶颈;三是能够大幅提高算力

的硅芯片，已逼近物理和经济成本上的极限。摩尔定律已经衰老，计算性能的增长曲线变得不可预测。

第三是在数据方面。一是数据透明度。虽然学习方法是公开透明的，但训练用的数据集往往是不透明的;二是数据攻击。输入数据的细微抖动就可能导致算法的失效，如果在利益方的诱导下发起对抗性样本攻击，系统就直接被“洗脑”了;三是监督学习。深度学习需要的海量大数据，需要打上标签做监督学习，而对实时海量的大数据人工打上标签几乎不可能。

第四是与其他学派结合。目前 AI 取得的进步属于连接学派，因此在对智能的认知方面，缺乏分析因果关系的逻辑推理能力，还无法理解实体的概念，无法识别关键影响因素，不会直接学习知识，不善于解决复杂数学运算，缺乏伦理道德等方面的常识。

到 2017 年，机器学习的神经网络已具有数千到数百万个神经元和数百万个连接。这样的复杂度还只相当于一个蠕虫的大脑，与有 1000 亿神经元和 1 万亿连接的人类大脑，差了 N 个数量级。但尽管如此，神经网络下围棋的能力已远高于一只蠕虫，而一只蠕虫所具有的自繁衍、捕食和躲避天敌等智能，人工智能都还望尘莫及。

?F 在，业界只知道深度学习在图像处理和语音识别等方面表现出色，未来在其他领域也可能有潜在的应用价值，但