DeepMind 综述无监督学习：通用智能路上的踏脚石，让 AI 更聪明

人工智能2019-04-12

在过去十年中，机器学习在图像识别、自动驾驶汽车和围棋等领域取得了前所未有的进步。这些成功在很大程度上是靠监督学习和强化学习来实现的。

这两种方法都要求由人设计训练信号并传递给计算机。在监督学习的情况下，这些是“目标”（例如图像的正确标签）;在强化学习的情况下，它们是成功行为的“奖励”（例如在 Atari 游戏中获得高分）。因此，机器学习的极限是由人类训练师决定的。

但是学习知识还应该有其他的策略，就像让幼儿学习，不仅有指导（监督学习）和鼓励（强化学习），还应该有自由探索世界（无监督学习）。如果要让 AI 脱离人类发展成出通用智能，必须要让它掌握无监督学习的技能。

DeepMind 今天在官方博客中对无监督学习的原理、近年来取得的成果、发展前景进行了综述。

无监督学习关键的特点是，传递给算法的数据在内部结构中非常丰富，而用于训练的目标和奖励非常稀少。无监督学习算法学到的大部分内容必须包括理解数据本身，而不是将这种理解应用于特定任务。

解码视觉元素

2012 年是深度学习的里程碑，AlexNet 席卷了 ImageNet 图像分类竞赛，但是更引人注目的是藏在 AlexNet 之下的事情。

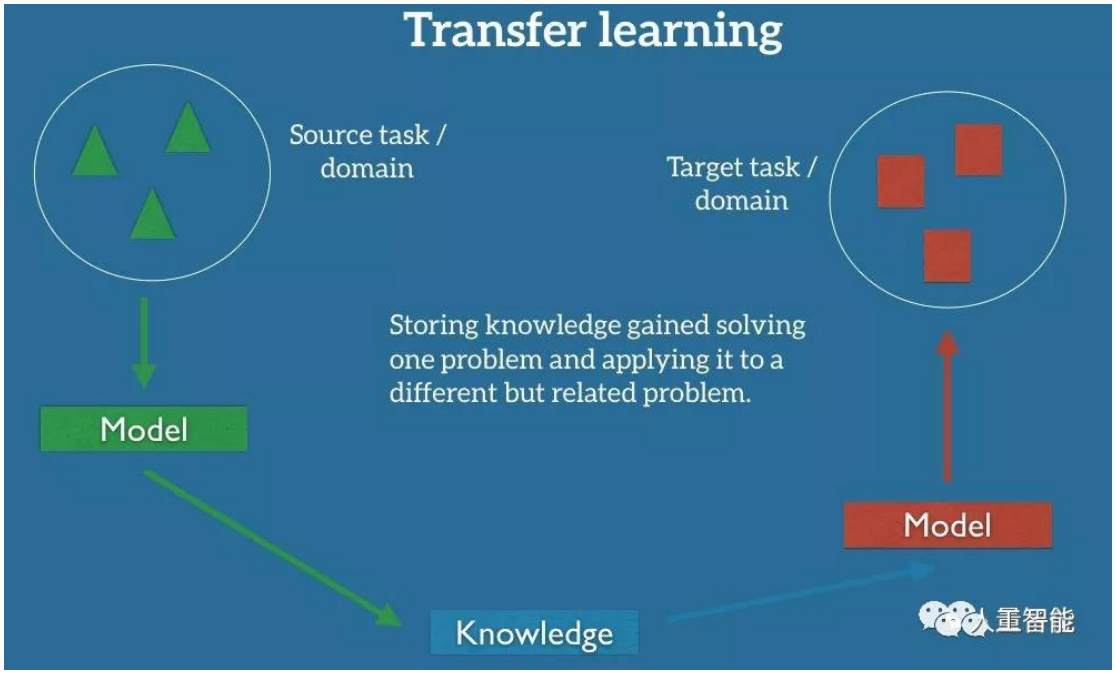
研究人员在分析 AlexNet 时发现，它通过为输入构建复杂的内部表示来解释图像，低层次的特征，如纹理和边缘在底层中表示，然后将它们组合在一起形成高级概念，例如更高层次中的轮子和狗。

这与我们的大脑中处理信息的方式非常相似，其中初级感官处理区域中的简单边缘和纹理，然后组装成复杂对象。因此复杂场景的表示可以由“视觉基元”所构建，这种方式与单词构成句子大致相同。

在没有人类明确的指导的情况下，研究人员发现 AlexNet 的层可以通过基本的“视觉词汇”来解决任务。

迁移学习

AlexNet 还可以被迁移到训练之外的视觉任务中，例如识别整个场景而不是单个图像。



人类就非常擅长这种学习方法，我们能迅速调整自己的经验，以适应新的技能和理解收集到的信息。例如，经过专业训练的钢琴家可以相对轻松地掌握弹奏爵士钢琴的方法。

理论上，构成世界正确内部表征的智能体应该能够做同样的事情。

但是 AlexNet 等分类器所学到的表示仍具有局限性，特别是网络只用单一类别标记图像训练时，那些推断标签时用不上的信息，无论它在其他任务中用处多大，都可能被网络所忽略。如果标签总是指向前景，则表示可能无法获取图像的背景。

一种可能的解决方案是提供更全面的训练信号，比如描述图像的详细内容，不单单把图像描述成“狗”，而是“柯基犬在阳光明媚的公园里叼飞盘”。

但是，这些信息很难大规模提供，而且这样做仍然有可能不足以捕获完成任务所需的全部信息。

无监督学习的基本前提是学习丰富、可广泛转移表示的最佳方式，这种方式可以学习关于数据的全部内容。

如果你觉得转移的概念看起来过于抽象，那么请想象一个学习简笔画的孩子。她发现了人体形态的特征。通过增加具体细节，她可以为她的所有同学绘制肖像，加上眼镜、红色 T 恤的同桌等等。

她发展出这项技能不是为了完成一项特定任务或获得奖励，而是为了反映她描绘周围世界的基本要求。

生成模型和 GAN

无监督学习的最简单目标是训练算法生成自己的数据实例，但是模型不应该简单地重现之前训练的数据，否则就是简单的记忆行为。

它必须是建立一个从数据中的基础类模型。不是生成特定的马或彩虹照片，而是生成马和彩虹的图片集；不是来自特定发言者的特定话语，而是说出话语的一般分布。

生成模型的指导原则是，能够构建一个令人信服的数据示例是理解它的最有力证据。正如物理学家理查德·费曼所说：“我不能创造的东西，我就不能了解”（WhatIcannotcreate,Idonotunderstand.）。

对于图像来说，迄今为止最成功的生成模型是生成对抗网络（GAN）。它由两个网络组成：一个生成器和一个鉴别器，分别负责伪造图片和识别真假。

生成器产生图像的目的是诱使鉴别者相信它们是真实的，同时，鉴别者会因为发现假图片而获得奖励。

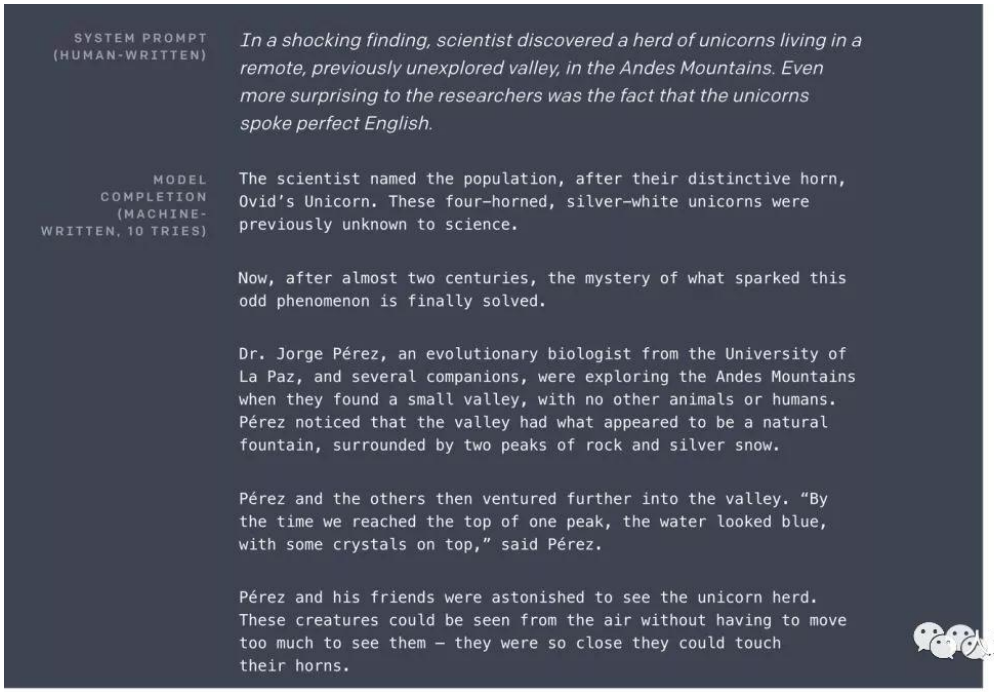
GAN 开始生成的图像是杂乱的和随机的，在许多次迭代中被细化，形成更加逼真的图像，甚至无法与真实照片区别开来。最近英伟达的 GauGAN 还能根据用户草图生成图片。

通过预测创建内容

无监督学习中另一个值得注意的成员是自回归模型，它把数据分成一系列小片段，每个片段依次被预测。这些模型可以通过连续猜测接下来会发生什么来作为输入，并能够再次生成猜测数据。

在语言模型中，每个单词都是从它之前的单词预测出来的。它能够支持在电子邮件和消息应用程序中弹出的文本预测内容。

最近 OpenAI 公布的 GPT-2 模型还能能够生成以假乱真的文字段落。



通过控制用于调节输出预测的输入序列，自回归模型也能用于将一个序列转换为另一个序列。例如将文本转换为逼真的手写体、自然的语音，还能将一种语言翻译成另一种语言。

自回归模型以预测特定顺序数据的方式来理解数据。通过预测任何其他数据的任何部分，可以构建更一般的无监督学习算法。

例如从句子中删除一个单词，并试图从剩余的内容中预测它。通过学习进行大量局部预测，系统被迫从整体上理解数据。

生成模型的出现让人们产生了一种担忧，就是它们可能被滥用。虽然通过照片、视频和音频编辑操纵证据历史已久，但生成模型让恶意编辑媒体内容变得更加容易。一个知名的“deepfakes”范例是奥巴马演讲视频片段。

令人鼓舞的是，人们已经做出了面对这些挑战的努力，包括利用统计技术帮助检测伪造内容和验证真实内容、提高公众意识、以及围绕限制生成模型使用范围展开讨论。

生成模型本身也能用在检测伪造内容和异常数据。例如，检测虚假语音或识别支付异常，保护客户免受欺诈。研究人员需要研究生成模型，以便更好地理解它们并降低风险。

实现通用智能

生成模型本身很吸引人，DeepMind 的主要兴趣是用它作为通用智能的踏脚石。赋予智能体生成数据的能力是一种赋予其想象力的方式，从而能够规划和推理未来。

DeepMind 的研究表明，即使没有明确的生成数据，学习预测环境的不同方面可以丰富智能体的世界模型，从而提高其解决问题的能力。