内部资料

注意保密

经信研究院 译文

江苏省经济和信息化研究院　第 2 期　总第 24 期　2018 年 2 月 6 日

2018 年人工智能技术十大发展趋势

【导读】在过去的 2017 年，以深度学习等关键技术为核心，以云计算、生物识别等数据及计算能力为基础支撑的人工智能产业已经成为全球最受关注的科技前沿。随着计算机技术的提升，更多数据得以采集，人工智能正从实验室中的构想渐渐变为可应用的现实，政府和企业都在思考该如何推动产业发展。然而，与任何新兴技术一样，人工智能的广泛应用仍面临诸多挑战，企业尚没有发现人工智能应用的正确途径。为此，普华永道的研究团队以科学家和企业家需紧密关注的前沿发展和关键业务为重点，总结了 2018 年十大人工智能技术发展趋势。本文对这些技术的内涵及选定理由做了简要介绍，供各方参考。

一、深度学习技术：揭示神经网络的工作原理

是什么：深度神经网络通过模仿人类的大脑，拥有“学习”图像、音频和文本数据的能力。然而，即使在使用了十多年之后，我们仍然对深度学习有很多不了解的地方，比如神经网络是如何学习的，以及为什么它们表现得如此出色。但是未来这可能会因为一个新理论而发生改变，如信息瓶颈在深度学习上的应用。从本质上说，这表明在初始拟合阶段之后，一个深度神经网络将“忘记”并压缩噪声数据，而这些噪声数据可能就是包含了大量额外无意义信息的数据集。

为什么入选：准确理解深度学习的工作原理将推进其更好的发展和应用。例如，它可以洞察优化的网络设计和体系结构，同时为关键性安全或管理应用程序提供更好的透明性。从对这个理论的探索中也可以产生更多的成果，并应用于其他类型的深度神经网络和深度神经网络设计。

二、胶囊网络：模拟大脑的视觉处理能力

是什么：胶囊网络是一种新型的深层神经网络，其处理视觉信息的方式与大脑相似，这意味着它们可以维持空间层次关系。这与卷积神经网络形成了鲜明的对比，卷积神经网络作为最广泛使用的神经网络之一，没有考虑到简单和复杂对象之间重要的空间层次结构，从而导致错误分类和高错误率。

为什么入选：对于典型的识别任务，胶囊网络能通过减少错误（最多可减少 50%）来提高准确性，且不需要很多数

据来强化模型。未来，预计在许多问题领域和深层神经网络体系中会使用胶囊网络。

三、深度强化学习：与环境互动，解决商业问题

是什么：深度强化学习（DRL）是一种神经网络，通过观察、行动和回报与环境相互作用来学习，目前已被用来学习游戏策略，例如 Atari 和 Go 程序——包括著名的击败了人类围棋冠军的 AlphaGo。

为什么入选：深度强化学习是所有学习技术中最通用的，它可以在很多业务应用程序中被使用。相较其他技术，它需要强化其模型的数据更少。更值得注意的是，它可以通过模拟进行训练，进而不再需要标签数据。鉴于这些优势，预计在未来一年将会有更多的结合深度强化学习和智能代理仿真的业务应用程序面世。

四、生成式对抗网络：对神经网络进行配对以促进学习和减轻处理负载

是什么：生成式对抗网络（GAN）是一种无监督的深度学习系统，它通过两个相互竞争的神经网络实现。第一个网络（即生成器），用来创建看起来和真实数据集完全一样的假数据。第二个网络（即鉴别器），用来输入真实数据和合成数据。随着时间的推移，这两个神经网络都得到了改进，以习得给定数据集的分布。

为什么入选：生成式对抗网络向更大范围的非监督任务开放，在这些任务中标记那些不存在的，或者代价太大无法获得的数据。并且，因为这里有两个网络分担负荷，减少了

深度神经网络所需要的负荷。未来将看到更多的生成式对抗业务应用程序面世，比如在网络检测中使用生成式对抗网络。

五、精益和增强数据学习：处理标签数据挑战

是什么：机器学习中最大的挑战（特别是深度学习）是利用大量标记数据的可用性来训练系统。这一挑战有两种广泛的技术解决途径：（1）合成新数据;（2）将训练过的模型转移到另一个任务或域。一些特定的技术，例如转移学习（从一个任务/领域学到的见解转移到另一个任务/领域）或一次性学习（将学习转移到只学习一个或没有相关例子的情况），使他们成为“精益数据”的学习技术。同样，通过模拟或插值合成新数据有助于获得更多数据，从而增加现有数据，以此提高学习能力。

为什么入选：使用这些技术，我们可以解决更广泛的问题，特别是那些历史数据较少的情况。希望未来能有更多变化的增强数据，以及不同类型的学习用于解决广泛的业务问题。

六、概率编程：简化模型开发的语言

是什么：一种高级编程语言，能够让开发人员更加快捷的设计概率模型，然后自动“处理”这些模型。概率编程语言使可重用模型库成为可能，支持交互建模和形式验证，并提供必要的抽象层，以及通用模型类中的有效推理。

为什么入选：概率编程语言具有适应业务领域中常见的不确定和不完全信息的能力。未来，我们将看到这些语言的广泛应用，并期望它们也适用于深度学习。

七、混合学习模式：结合模型不确定性的方法

是什么：不同类型的深度神经网络，如生成式对抗网络或深度强化学习，对不同类型数据的表现及广泛应用方面有很大的价值。然而，深度学习模型则不能像贝叶斯定理或概率方法一样对不确定性进行建模。混合学习模式结合了两种方法的长处，一些混合模型的例子包括贝叶斯深度学习、贝叶斯生成对抗网络以及贝叶斯假定生成对抗网络。

为什么入选：混合学习模式使扩展业务的多样性成为可能，包括深度学习和不确定性。这可以帮助我们获得更好的性能和模型的可解释性，从而可以得到更广泛的应用。未来将看到，更多的概率编程语言开始吸收深度学习的的成果。

八、自动化机器学习（AutoML）：没有编程的模型创建

是什么：开发机器学习模型非常耗时，并且需要专业知识对工作流进行辅助，包括数据准备、特性选择、模型或技术选择、培训和调优。自动化机器学习旨在使用各种不同的统计和深度学习技术来使这个工作流自动化。

为什么入选：自动化机器学习是人工智能工具大众化的一部分，它使用户能够在没有深度编程背景的情况下开发机器学习模型，并且它还能减少数据科学家创建模型所需的时间。未来，将在更大的机器学习平台上看到众多业务自动化包和自动化集成。

九、数字孪生：工业应用之外的虚拟副本

是什么：数字孪生是一种虚拟模型，用于促进对物理或心理系统的详细分析和监测。数字孪生的概念起源于工业领域，它被广泛用于分析和监控诸如风车农场或工业系统之类的东西。现在，通过基于代理的建模（模拟自主代理的动作和交互的计算模型）和系统动力学（一种计算机辅助的策略分析和设计方法），数字孪生正在应用于非物质对象和进程，包括客户行为预测。

为什么入选：数字孪生可以促进物联网的发展并带来更广泛的应用，提供预测性诊断和物联网系统维护的方法。展望未来，在物理系统和对消费者选择的建模中，将看到更多的数字孪生应用。

十、可以解释的人工智能：理解黑匣子

是什么：今天，有许多机器学习算法在不同的应用程序中使用。然而很多这样的算法对于外界来说是黑匣子，人们并不知道它是如何起作用的。正在兴起的可解释的人工智能活动，是一种开发机器学习技术的活动，它能产生更多可解释的模型。

为什么入选：人工智能是可解释的、可证明的、透明的，它将是建立信任的关键，并有助于人们更广泛地采用机器学习技术。在开始广泛部署人工智能之前，可解释的人工智能会是企业应用的一种需求或最佳实践，而政府可能会在未来对人工智能提出相应的监管要求。

（原文摘自普华永道官方网站，由经信研究院整理翻译）

主编：石晓鹏　副主编：陈英武　责任编辑：殷俊

报：省经信委　送：各市（县）经信主管部门

电话：025-83348908　邮箱：jssjjyjs@163.com

翻译：朱文　审校：张睿、王兴伟