生成式对抗网络的研究进展与展望

王飞跃
中国科学院自动化研究所

关键词：生成式对抗网络　平行智能　深度学习　平行学习

GAN：生成式对抗网络

生成式对抗网络 (Generative Adversarial Networks, GANs) 是古德费洛 (Goodfellow) 在 2014 年提出的一种采用对抗的思路来生成数据的思想。想象我们有两张图片，一张是真的，一张是假的。对人类而言，如何去判断这幅画究竟是伪造的还是真的？比如图 1 中，这幅赝作的问题在于“画中人”画得不对，不是人，而是一只兔子，所以可以认为它是假的。而对于伪造者，他会想：这里是该画人的地方，画得不对，以后在这个地方改进，就可以画出更真实的画。第二次，等他画好后，大家可能又会发现有另外的问题。这样循环迭代，不断改进，就可以提升生成器（即赝作画家）的水平。同时，侦探的水平也提高了。

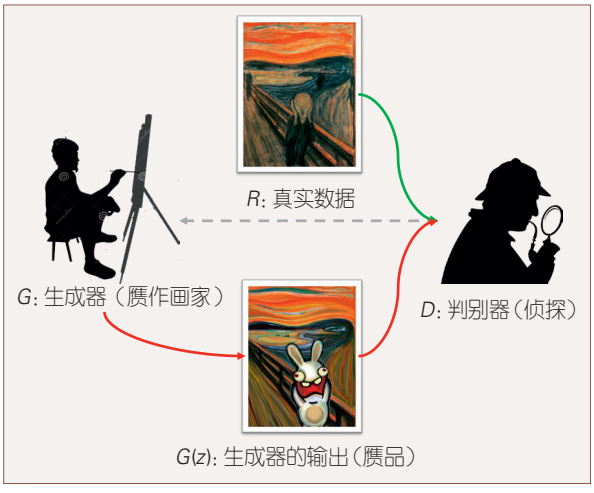

图1　生成式对抗网络示意图

GAN 已在计算机图像生成等任务中取得了极大的成功。除此之外，GAN 还涉及许多其他内容，例如关于加密与安全、机器人，甚至包括天体物理。GAN 的发展方向正在不断深入和扩大，从传统的计算机视觉向其他领域扩展。乐昆 (LeCun) 在访谈中提到，对于深度学习，10 年内最值得关注的一个想法就是 GAN，因为这种方法使得许多以前不可能完成的任务成为了可能。

GAN的提出背景

智能的研究

在人工智能六十余年的发展历程中，相关的研究者大体可分为两个学派，即所谓的“纯净派 (Neats)”和“邋遢派 (Scruffies)”。“纯净派”认为要建立一个人工的智能系统，必须首先彻底地了解其形式上的特性，倾向于以数学，特别是数理逻辑为解析工具来研究人工智能，追求透明，且能证明因果关系的构造智能系统之理论与方法。而“邋遢派”则注重功能和效率，采用较为“进化”的观念，不太关心“证明”或“解释”，认为最重要的是干下去，先建立这样的“智能”实体再说，从最初的计算神经方法、启发式的智能程序设计、多智能体，到今天火热的深度学习和各种各样的计算智能方法。两派争论的焦点之一就是单纯的程序设计能不能作为人工智能的理论基础[1]。当然，长期以来，从理论上揭示智能的本质，在工程上建立智能机器，是所

有人工智能研究人员的共同目标。

近年来，以深度学习为代表的“邋遢派”方法在语音分析、图像识别和自然语言处理等问题上取得了“纯净派”方法长期未能实现的突破，再加上大数据的热潮，引发大家对大数据和大计算驱动的人工智能方法的极大向往。问题是，大数据从何而来？成本如何？又如何从数据走向智能？

一般来说，研究人工智能的出发点主要可分为两类。一类是从人类理解数据的角度去研究生成的东西。由于人类的经验是非常有限的，我们必须从某种数学或者现实中能够感受到的直观例子去学习。做生成模型时，我们会预先设定一个分布（比如高斯分布），假设图像符合这个分布，只是参数的分布未知，我们可以通过数据去拟合这个分布。另一类是让机器或模型直接去理解这个数据，我们对数据不进行假设，而是让一个模型生成数据，然后再判断这个数据究竟是对的还是错的，是像真实数据一样，还是和真实数据相差太远，我们根据这个判断反复修正这个模型。以往的生成模型研究主要从人类理解数据的角度出发，希望使用一个显式的分布假设去设计模型。GAN 可以说是第一个广为人知的，从机器或者数据的角度出发拟合数据的模型：我们不再给它任何的数据模型分布，而是直接去学习。

GAN理论与实现

基于上述技术，古德费洛提出了 GAN 的思想。即，设计这样一个游戏，包括两个玩家，其中一个就是生成器 (Generator, G)，它的工作是生成图片，并且使得这个图片看上去就是来自训练样本，另外一个玩家是判决器 (Discriminator, D)，判决输入图片是否真的是训练样本，而不是生成的。GAN 的整体框架如图 2 所示。该框架包含一个隐空间的随机变量 z——它可能采样自一个高斯分布，也可能是具有某种信息意义上的一个隐变量，其维度可能比真实样本、真实空间小。将这个隐变量输入生成器，这是一个可微的函数 $G(z)$。$G(z)$ 与真实样本 x 都被放入判决器中，它尽量判决生成图像是一个假的图像。而 G 会尽量让判断器误以为这个图像是来自真实的图像。判决器会将它的梯度回传给 G 和 D，这也就是为什么要强调 G 和 D 都是可微函数，因为如果不可微，误差就无法回传。这就是原始的 GAN 结构。

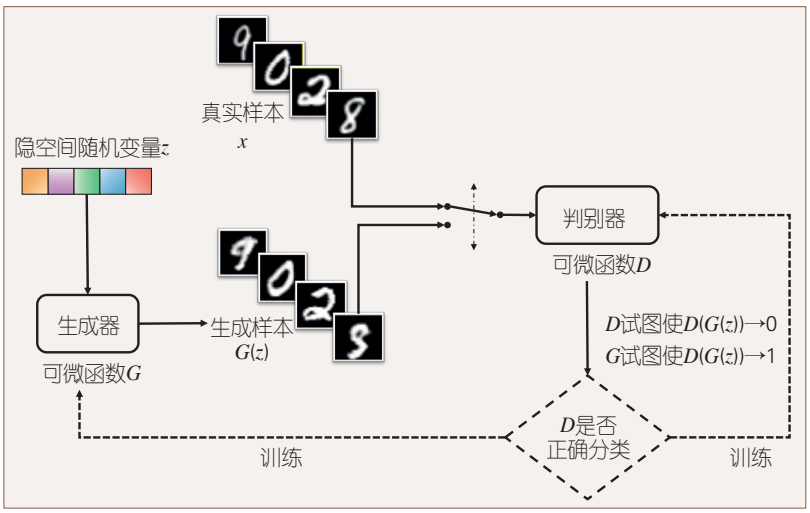

图2　GAN的整体框架

原始的 GAN 的判别器和生成器都是全连接网络，用于生成图像。目前，各种应用主要使用卷积神经网络 (CNN) 去设计输入输出图像。

相比传统模型，GAN 的优点如下。首先，生成的数据的复杂度和维度是线性相关的。如果要生成一个更大的图像，不会像传统模型一样面临指数上升的计算量，它只是一个神经网络线性增大的过程。其次，先验假设非常少，这是相比传统模型最大的一个优点。与以往模型相比最突出的一点不同是，GAN 不对数据进行任何的显式参数分布假设。第三，

[1] D. Partridge, “Workshop on the foundations of AI: Final report,” *AI. Magazine*., vol. 8, no. I, pp. 55-59, Spring 1987.

可以生成更高质量的样本。相比传统模型，GAN也有缺点。一般来说，传统判别模型也是一个优化函数，对于凸优化而言，肯定有最优解。但是GAN是在一个双人游戏中去寻找一个纳什均衡点[2]，对于一个确定的策略，比如神经网络，输入一个量肯定能得到一个确定的输出，这时候不一定能找到一个纳什均衡点。对于GAN寻找和优化纳什均衡点是一项很困难的工作，目前还缺乏对这方面的研究。

GAN的发展与应用

GAN的收敛问题

目前，不收敛问题是GAN最主要的一个问题。在实际训练中，往往需要设置很多的参数，去平衡G和D的能力，才能使得它最终达到收敛。不收敛问题主要有两种表现。第一，梯度消失问题，原始GAN使用分类误差作为真实分布与生成分布相近度的度量，这种方法在最优判别器的条件下，生成器的损失函数等价于最小化真实分布与生成分布之间的JS散度。然而，已被证明，当真实分布与生成分布的重叠区域可忽略时，JS散度为一个常数，此时生成器获得的梯度为0。第二，模式崩塌问题，也就是说生成器可能生成同样的数据而不是多样的数据。这个问题主要原因是，在优化时使用梯度下降的方法，实际上不区分min-max和max-min，这导致生成器希望多生成一些重复但是很安全的样本。而我们希望生成样本尽量与真实样本的多样性一致。这些问题可以通过设计更好的网络结构、差异的度量方式或者一些训练的trick来解决，一般都会结合使用。例如WGAN就是通过使用Wasserstein距离来代替JS散度，同时使用了权值裁剪的trick，实现了很好的效果。**如何将众多的trick技巧系统化、形式化和工具化，是决定GAN能否更加深入普及的关键一步。**

增强学习与模仿学习

先说增强学习，有一篇2016年的文章讲到了GAN和Actor-Critic[3]的相似之处。GAN的网络结构类似于图3(a)，而Actor-Critic作为增强学习的一种方法，它的结构如图3(b)所示。

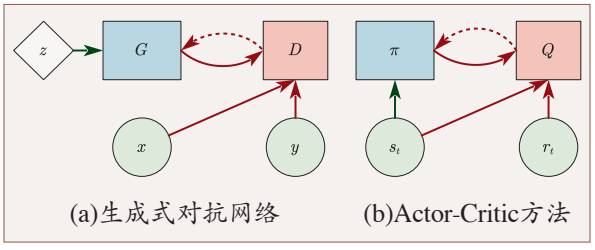

图3　GAN和Actor-Critic对比

对于GAN来说，z输入给G，然后由D判断G的输出究竟对不对。而对于Actor-Critic，会将环境中的状态输入给π，然后由π来输出给Q，也就是由评判者(Critic)去评判策略。增强学习和GAN的区别就在于这个z和s_t，因为环境的状态具有一定的随机性，只需要输入一个状态就够了，而在GAN中，状态与随机信号被分离开来。我们看到这两个方法的结构上具有一致性，但是它们是不是训练方法具有一致性呢？从实践的情况来看确实是这样，在Actor-Critic训练中的许多技巧都可以移植到GAN的训练中去，而且一般都有效。

另一方面，GAN可以给增强学习提供一些数据。对于增强学习，数据很稀缺，可能很久也得不到这样一个数据，或者说需要很高的代价去采集数据，那我们可以将GAN生成的数据交给增强学习去处理。

生成式模仿学习(Generative Adversarial Imitation Learning, GAIL)是GAN的另一个有趣的应用，其结构如图4所示。在之前进行模仿学习时，需

[2] 纳什均衡是一种策略组合，使得同一时间内每个参与人的策略是对其他参与人策略的最优反应。

[3] D. Pfau and O. Vinyals, "Connecting Generative Adversarial Networks and Actor-Critic Methods," arXiv:1610.01945 [cs, stat], Oct. 2016.

要从专家样本中学习到一个价值函数 (reward function)，再用这个价值函数去训练增强学习智能体 (reinforcement learning agent)。生成式模仿学习借鉴了GAN的思想，不直接学习价值函数，而是直接学习状态到行为的映射 (s_t, a_t)。GAIL中的策略网络相当于GAN中的 G，而 a_t 相当于GAN中的 $G(z)$，通过这样的结构可以直接模仿专家的行为而不需要经过中间的步骤。

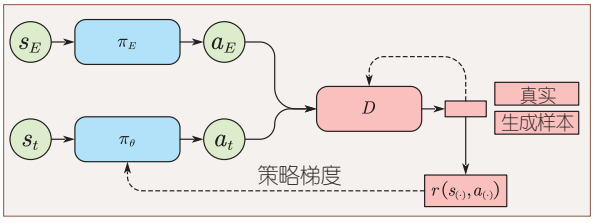

图4　生成式模仿学习

GAN与平行智能

新IT与第三轴心时代

我之所以对GAN感兴趣，要自己亲手做，是觉得GAN通过把真与假平行而立，将这一对矛盾对立统一，成为生产数据的一种有效手段。这与我提倡的虚与实平行的智能与学习方法不谋而合：GAN为平行智能[4]与平行学习[5]提供了具体深入细化的途径，而平行智能与平行学习又为GAN进一步的发展提出了方向。传统的思路里模型是分析的工具，建模就是为了分析，但GAN与基于ACP[6]的平行突破了这一认识，模型成为产生数据的“工厂”，从“大定律、小数据”的牛顿之路，转入“大数据、小定律”的默顿[7]之路。

实际上，AlphaGo也为我们指明了这条从牛顿到默顿之路，沿着此路，就是接下来的智能产业之路。AlphaGo之后，IT不再是信息技术，那已是旧IT了，现在是智能技术 (Intelligent Technology)，这是新IT。大家也别忘了，200年前IT是工业技术的意思，今天可称之为老IT。未来是三个IT的平行共用，这跟波普尔的三个世界理论密切相关。我们只知道物理世界、心理世界，但是波普尔告诉我们还有一个第三世界——人工世界，而工业、信息、智能“老、旧、新”IT技术分别是开发这三个世界的主打技术，所以今天是人工智能时代，所以数据成了“石油矿藏”（见图5）。

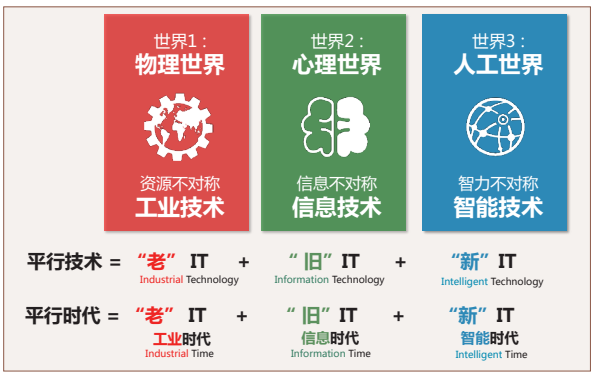

图5　三个IT与三个世界：平行技术和平行时代

我把这一信念称之为“AlphaGo Thesis”。因为80年前有个“Church-Turing Thesis”[8]，是纪念邱奇和图灵师徒二人的Lambda运算和有限状态机（图灵机）的，二者繁简不一，但数学上等价，就是冯·诺伊曼所认为的“所有可以计算的数都可以用图灵机算出”。其实这是一个假设，据此他总结出冯·诺伊曼结构，造了世界上第一台数字计算机，到今天

[4] Wang F Y, Wang X, Li L X, Li L. Steps toward Parallel Intelligence. *IEEE/CAA Journal of Automatica Sinica*, 2016, 3(4): 345-348.

[5] Li L, Lin Y, Zheng N, Wang F Y. Parallel Learning: a Perspective and a Framework. *IEEE/CAA Journal of Automatica Sinica*, 2017, 4(3): 389-395.

[6] 人工系统(Artificial system)、计算实验(Computational experiments)、平行执行(Parallel execution)

[7] 美国著名的社会学家，曾提出了默顿定律：由于信念和行为之间的反馈，预言直接或间接地促成了自己的实现。

[8] 邱奇-图灵论题(The Church-Turing Thesis)是计算机科学中以数学家阿隆佐·邱奇(Alonzo Church)和阿兰·图灵命名的论题。该论题最基本的观点表明，所有计算或算法都可以由一台图灵机来执行。该论题和以下说法等价：常规的编程语言可以足够有效地来表达任何算法。该论题被普遍假定为真，也被称为邱奇论题或邱奇猜想和图灵论题。

我们还借鉴他的结构，使计算机和信息产业发展到当下的程度。我认为，AlphaGo 论题对智能产业产生的效应，就是邱奇 - 图灵论题对于信息产业所产生的效应。

回顾人类发展历史，我们围绕着物理世界从农业技术发展到工业技术，围绕着心理世界发展了信息技术。我们走到今天，将要开发的是第三世界，即人工世界，在这个世界里，大数据、人口、智力都变成了资源，导致智能技术变成新 IT。从工业时代到信息时代，再到智能时代，我们进入了一个平行的世界。

这是一个崭新的时代，我称之为第三轴心时代。轴心时代是卡尔·雅斯贝思 70 年前在其《历史的起源与目标》一书中提出的概念，曾在人类思想界产生过巨大的影响。但我认为他的轴心时代只是物理第一世界的轴心时代，三个世界都应有自己的轴心时代。心理世界的第二轴心时代就是从文艺复兴到现代科学体系建立的 500 多年，而人工世界的第三轴心时代，其实是从哥德尔不完备定理的发现就已正式登场，随之而来的就是人工智能研究的发起。三个轴心时代，分别代表着人类在人性、理性和智性上的大觉醒，以及接踵而来的哲学、科学和技术上的大突破。人类的思维和认识之范式，也从永恒的上帝认可，到因果规律的科学认可，再到关联 (association) 关系的数据认可。我们需要数据，我们必须要产生数据，我们必须能够从数据提炼出知识，提炼出智能。

所以我认为，像 GAN 这类算法只是开了个头。希望大家能好好掌握这类方法，而且还要开创出自己的方法。将小数据导成大数据，将大数据导成小知识。实现从牛顿系统到默顿系统的跨越，从真假平行到虚实平行，走向平行学习，走向平行智能。

平行智能与平行学习

我们这里做的，就是人工组织，就是广义模型、软件定义的模型。不仅有物理的模型，还要把行为模型加进去。怎么导成大数据？就是靠计算实验。好多实验，因为受到成本、法律、道德、科学上的约束，做不了物理实验。通过把模型的行为和实际的行为在社会物理信息空间 CPSS 上进行大的反馈，就可以进行平行学习，实现平行智能，这就是基于 ACP 的平行思想。

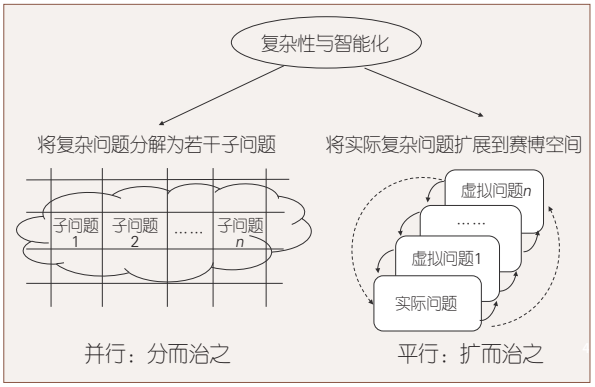

图6　并行与平行：从GAN到平行智能

因此，以后所有的系统都应当是实际加人工。虚实之间可以一对一、多对一、一对多、多对多。它与传统的并行的区别在于，并行是分而治之，平行是扩而治之。

其实 GAN 就是一个最简单的平行系统，但它两端都不全。它用一个判别器实现物理的系统，利用生成器产生人工系统，实现真假的平行。对我而言，这就是未来平行机的一个简单原型。它的进一步发展，就可以打通 3 个世界：物理世界、心理世界、人工世界，实现从牛顿到默顿的跨越，使人类进入智能产业和智慧社会。 ■

（本文由中科院自动化所复杂系统管理与控制国家重点实验室博士生白天翔和林懿伦整理而成。源自作者在中国自动化学会智能自动化学科前沿讲习班的录音，有删节。）

王飞跃
CCF杰出会员。中科院自动化所研究员。主要研究方向为社会计算、平行智能、知识自动化、智能系统和复杂系统的建模、分析和控制。
feiyue.wang@ia.ac.cn