人工智能研究的新前线: 生成式对抗网络

林懿伦 [1, 2, 3] 戴星原 [1, 2, 3] 李 力 [4] 王 晓 [1, 3] 王飞跃 [1, 5, 6]

摘 要 生成式对抗网络 (Generative adversarial networks, GAN) 是当前人工智能学界最为重要的研究热点之一. 其突出的生成能力不仅可用于生成各类图像和自然语言数据, 还启发和推动了各类半监督学习和无监督学习任务的发展. 本文概括了 GAN 的基本思想, 并对近年来相关的理论与应用研究进行了梳理, 总结了 GAN 常见的网络结构与训练方法, 博弈形式, 集成方法, 并对一些应用场景进行了介绍. 在此基础上, 本文对 GAN 发展的内在逻辑进行了归纳总结.

关键词 深度学习, 生成式对抗网络, 生成模型, 对抗学习, 平行学习

引用格式 林懿伦, 戴星原, 李力, 王晓, 王飞跃. 人工智能研究的新前线: 生成式对抗网络. 自动化学报, 2018, **44**(5): 775−792

DOI 10.16383/j.aas.2018.y000002

The New Frontier of AI Research: Generative Adversarial Networks

LIN Yi-Lun[1, 2, 3] DAI Xing-Yuan[1, 2, 3] LI Li[4] WANG Xiao[1, 3] WANG Fei-Yue[1, 5, 6]

Abstract Recently, generative adversarial networks (GAN) have become one of the most popular topics in artificial intelligent field. Its outstanding capability of generating realistic samples not only revived the research of generative model, but also inspired the research of semi-supervised learning and unsupervised learning. In this paper, we introduce the basic idea of GAN, and comb its recent development in theory and practice. By concluding its improvements of network structures, optimization methods, the form of the game, the ensemble methods, and its applications, we found the inner logic of its development.

Key words Deep learning, generative adversarial networks, generative model, adversarial learning, parallel learning

Citation Lin Yi-Lun, Dai Xing-Yuan, Li Li, Wang Xiao, Wang Fei-Yue. The new frontier of AI research: generative adversarial networks. *Acta Automatica Sinica*, 2018, **44**(5): 775−792

近年来, 人工智能领域, 特别是机器学习方面的研究取得了长足的进步. 得益于计算能力的提高, 信息化工具的普及以及数据量的积累, 人工智能研究的迫切性和可行性都大为提高. 以 Google 等为代表的 IT 企业, 利用其掌握的海量数据资源, 结合新的硬件结构和人工智能算法, 实现了一系列新突破和新应用, 并获得了可观的收益. 这些企业获得的成功进一步带动了机器学习的研究热度, 使得人工智能的研究进入了一个新的高潮时期.

在此次的人工智能浪潮中, 以统计机器学习, 深度学习为代表的机器学习方法是主要的研究方向之一. 相比符号主义的研究方法, 基于机器学习的人工智能系统降低了对人类知识的依赖, 转而使用统计的方法从数据中直接习得知识. 机器学习理论是一次重要的范式革命, 使人工智能领域的研究重点从算法设计转向了特征工程与优化方法.

一般而言, 依据数据集是否有标记, 机器学习任务可被分为有监督学习 (又称预测性学习, 数据集有标记) 与无监督学习 (又称描述性学习, 数据集无标记)[1]. 随着数据收集手段, 算力与算法的不断发展, 在诸多监督学习任务中, 如图像识别[2−3], 语音识别[4−5], 机器翻译[6−7] 等, 机器学习方法, 特别是深度学习方法都取得了目前最好的成绩.

然而, 有监督学习需要人为给数据加入标签. 这带来了两个问题: 一是数据集采集后需要大量人力

收稿日期 2018-03-01 录用日期 2018-05-01
Manuscript received March 1, 2018; accepted May 1, 2018
国家自然科学基金 (61533019, 61702519), 北京市科技项目 (D17110600030000, ZC179074Z) 资助
Supported by National Natural Science Foundation of China (61533019, 61702519), Beijing Municipal Science and Technology Commission Program (D17110600030000, ZC179074Z)
本文责任编委 刘德荣
Recommended by Associate Editor LIU De-Rong

1. 中国科学院自动化研究所复杂系统管理与控制国家重点实验室 北京 100190 2. 中国科学院大学 北京 100049 3. 青岛智能产业技术研究院 青岛 266109 4. 北京信息科学与技术国家研究中心, 清华大学自动化系 北京 100084 5. 国防科学技术大学军事计算实验与平行系统技术中心 长沙 410073 6. 中国科学院大学中国经济与社会安全研究中心 北京 101408
1. The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190 2. University of Chinese Academy of Sciences, Beijing 100049 3. Qingdao Academy of Intelligent Industries, Qingdao 266109 4. Department of Automation, Beijing National Research Center for Information Science and Technology (BNRist), Tsinghua University, Beijing 100084 5. Research Center of Military Computational Experiments and Parallel System, National University of Defense Technology, Changsha 410073 6. Center of China Economic and Social Security, The University of Chinese Academy of Sciences, Beijing 101408

物力进行标注, 大规模数据集的构建十分困难; 二是对于许多学习任务, 如数据生成, 策略学习等, 人为标注的方法较为困难甚至不可行. 研究者普遍认为, 如何让机器从未经处理的, 无标签类别的数据中直接进行无监督学习, 将是 AI 领域下一步要着重解决的问题.

在无监督学习的任务中, 生成模型是最为关键的技术之一. 生成模型是指一个可以通过观察已有的样本, 学习其分布并生成类似样本的模型. 深度学习的研究者在领域发展的早期就极为关注无监督学习的问题, 基于神经网络的生成模型在神经网络的再次复兴中起到了极大的作用. 在计算资源还未足够丰富前, 研究者提出了深度信念网络 (Deep belief network, DBN)[8], 深度玻尔兹曼机 (Deep Boltzmann machines, DBM)[9] 等网络结构, 这些网络将受限玻尔兹曼机 (Restricted Boltzmann machine, RBM)[10], 自编码机 (Autoencoder, AE)[11] 等生成模型作为一种特征学习器, 通过逐层预训练的方式加速经网络的训练[12].

然而, 早期的生成模型往往不能很好地泛化生成结果. 随着深度学习的进一步发展, 研究者提出了一系列新的模型. 生成式对抗网络 (Generative adversarial networks, GAN) 是生成式模型最新, 也是目前最为成功的一项技术, 由 Goodfellow 等在 2014 年第一次提出[13].

GAN 的主要思想是设置一个零和博弈, 通过两个玩家的对抗实现学习. 博弈中的一名玩家称为生成器, 它的主要工作是生成样本, 并尽量使得其看上去与训练样本一致. 另外一名玩家称为判别器, 它的目的是准确判断输入样本是否属于真实的训练样本. 一个常见的比喻是将这两个网络想象成伪钞制造者与警察. GAN 的训练过程类似于伪钞制造者尽可能提高伪钞制作水平以骗过警察, 而警察则不断提高鉴别能力以识别伪钞. 随着 GAN 的不断训练, 伪钞制造者与警察的能力都会不断提高[14].

GAN 在生成逼真图像上的性能超过了其他的方法, 一经提出便引起了极大的关注. 尤为重要的是, GAN 不仅可作为一种性能极佳的生成模型, 其所启发的对抗学习思想更渗透进深度学习领域的方方面面, 催生了一系列新的研究方向与应用[15].

本文梳理了生成式对抗网络的最新研究进展, 并对其发展趋势进行展望. 第 1 节介绍了 GAN 的提出背景、基本思想与原始 GAN 存在的缺陷; 第 2 节介绍了 GAN 在生成机制方面的改进; 第 3 节介绍了 GAN 在判别机制方面的改进; 第 4 节对 GAN 的应用发展进行了介绍; 最后总结了 GAN 领域研究的内在逻辑与存在的问题, 并对其下一步发展做出展望.

1 GAN 的背景与提出

GAN 是在深度生成模型的基础上发展而来, 但又与以往的模型有显著区别. 本节首先简要介绍深度学习与深度生成模型的基本思想与发展历史, 然后介绍原始 GAN 的模型结构与训练方法, 最后讨论原始 GAN 中存在的不足.

1.1 深度学习

深度学习是机器学习的一种实现方法. 相比一般的机器学习方法, 深度学习最主要的区别是不依赖人工进行特征工程. 研究者认为, 手工设计的特征描述子往往过早地丢失掉有用信息, 直接从数据中学习到与任务相关的特征表示, 比手工设计特征更加有效[16].

深度学习使用多层神经网络 (Multilayer neural network)[17] 对数据进行表征学习. 相比传统的神经网络方法, 深度学习主要在四方面进行了突破: 1) 使用了卷积神经网络 (Convolutional neural network, CNN)[18−19], 递归神经网络 (Recurrent/recursive neural network, RNN)[20−22] 等特殊设计的网络结构, 这些新的网络结构大大加强了神经网络的建模能力; 2) 使用了整流线性单元 (Rectified linear unit, ReLU)[23]、Dropout[24]、Adam[25] 等新的激活函数、正则方法与优化算法, 这些新的训练技术有效提高了神经网络的收敛速度, 使得大规模的神经网络训练成为可能; 3) 使用了图形处理器 (Graphics processing unit, GPU)[2, 26]、现场可编程逻辑门阵列 (Field-programmable gate array, FPGA)[27]、应用定制电路 (Application-specific integrated circuit, ASIC)[28] 以及分布式系统[29] 等新的计算设备与计算系统, 这些设备使得神经网络的训练时间大大缩短, 从而具有被实际部署的可能性; 4) 形成了较为完善的开源社区, 出现了 Theano[30], Torch[31−32], Tensorflow[33] 等被广泛使用的算法库, 开源社区的发展降低了深度学习的应用门槛, 提高了该领域新发现的可重复性, 吸引了越来越多的研究者加入研究行列.

深度学习在模型、算法、硬件设施与开发社区四方面的突破改变了过往神经网络优化困难, 应用受限, 计算缓慢, 认可度不高的问题, 使得该技术的影响力不断扩大. 目前, 深度学习已成为人工智能研究中的一种主流方法. 深度学习在监督学习任务, 尤其是在图像识别[34] 任务上的突破尤为令人瞩目.

1.2 深度生成模型

无监督学习具有重要的研究与应用价值. 其一是有标记的数据较为稀缺, 或是数据的标注与所希望研究的问题不直接相关, 此时必须使用无监督或

半监督学习的方法[35]; 其二是高层次的表征学习有助于其他任务的学习, 可以帮助模型避免陷入局部最优点, 或是添加一定的限制使得模型泛化能力提高[36]; 其三是在一些强化学习的场景下, 我们无法得知未来任务的具体形式, 而仅知道这些任务与环境有较为确定性的关系. 无监督学习可提高代理 (Agent) 对环境的预测能力, 从而有效提高代理的表现水平[37]; 最后, 对于一些问题我们希望有多样化的回答而不仅仅是返回一个确定性的答案, 有监督学习到的模型无法实现这一要求[14, 36].

生成模型是无监督学习的核心任务之一. 虽然深度学习在早期研究中使用了自编码机, 受限玻尔兹曼机等一系列生成模型, 但这些模型往往会出现过拟合现象, 不能很好地泛化以生成多样性样本.

为了解决这一问题, 研究者提出了一种名为随机反向传播 (Stochastic back-propagation)[38] 的方法. 通过加入额外的独立于模型的随机输入 z, 我们可以将确定性的神经网络 $f(x)$ 转化为具有随机性的 $f(x,z)$, 并使用反向传播的方法进行训练. 这一方法可以提高生成模型输出样本的多样性.

以变分自编码机 (Variational auto-encoder, VAE)[39] 为例. 如图 1 所示, VAE 的一种简单实现是假设生成样本 x 为高斯分布, 即

$$\hat{x} = f(x),\ x \sim \mathcal{N}\left(\mu,\ \sigma^2\right) \tag{1}$$

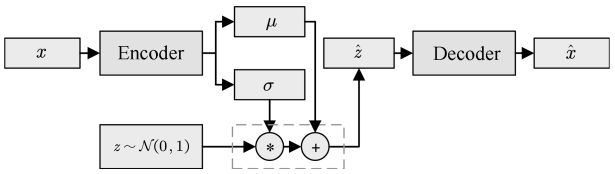


图 1　变分自编码机

Fig. 1　Variational auto-encoder

若将某一随机变量直接输入网络中, 由于此时 $\hat{x}$ 与输入 x 的关系不唯一, 网络可能出现优化困难的问题. 我们可以通过设置随机变量 $z \sim \mathcal{N}(0,1)$, 并构建编码器网络 $\mu = g_1(x)$, $\sigma = g_2(x)$, 原网络转化为

$$\hat{x} = f(\hat{z}), \hat{z} = \mu + \sigma z \tag{2}$$

通过反向传播算法, 网络可以获得更好的均值与标准差估计, 不断提高生成模型的生成效果. 在 VAE 的工作中, 这一方法被称为重参数化技巧 (Reparameterization trick).

深度学习与随机反向传播方法的出现使得使用神经网络生成复杂随机样本成为可能, 如何使得生成样本在具备多样性的同时保持原样本的模式特征成为了主要的研究问题.

1.3　生成式对抗网络

Goodfellow 等提出了生成式对抗网络模型. GAN 由一组对抗性的神经网络构成 (分别称为生成器和判别器), 生成器试图生成可被判别器误认为真实样本的生成样本. 与其他生成模型相比, GAN 的显著不同在于, 该方法不直接以数据分布和模型分布的差异为目标函数, 转而采用了对抗的方式, 先通过判别器学习差异, 再引导生成器去缩小这种差异. 生成器 G 接受隐变量 z 作为输入, 参数为 θ. 判别器 D 的输入为样本数据 x 或是生成样本 $\tilde{x} = G(z)$, 参数为 ϕ. GAN 的网络结构如图 2 所示:

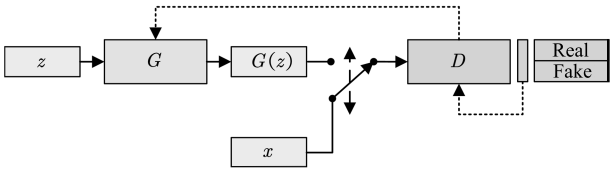


图 2　生成式对抗网络

Fig. 2　Generative adversarial networks

GAN 中的生成器与判别器可被视作博弈中的两个玩家. 两个玩家有各自的损失函数 $J^{(G)}(\theta,\phi)$ 与 $J^{(D)}(\theta,\phi)$, 训练过程中生成器和判别器会更新各自的参数以极小化损失. GAN 的训练实质是寻找零和博弈的一个纳什均衡解, 即一对参数 (θ,ϕ) 使得 θ 是 $J^{(G)}$ 的一个极小值点, 同时 ϕ 是 $J^{(D)}$ 的一个极小值点. 两个玩家的损失函数都依赖于对方的参数, 但是却不能更新对方的参数, 这与一般的优化问题有很大的不同.

在 GAN 的原始论文中, Goodfellow 将判别器的损失函数定义为一个标准二分类问题的交叉熵. 真实样本对应的标签为 1, 生成样本对应的标签则为 0. $J^{(D)}$ 的形式为

$$J^{(D)}(\theta,\phi) = -\frac{1}{2}\underbrace{\mathrm{E}_{x\sim p_{data}}\left[\log D(x)\right]}_{\mathrm{Loss_{real}}} - \frac{1}{2}\underbrace{\mathrm{E}_{z\sim p_z}\left[\log\left(1-D\left(G(z)\right)\right)\right]}_{\mathrm{Loss_{fake}}} \tag{3}$$

对于生成器的损失函数, 根据博弈形式的不同有所区别. 对于最简单的零和博弈, 生成器的损失即为判别器所得:

$$J^{(G)} = -J^{(D)} \tag{4}$$

在这一设定下, 我们可以认为, GAN 的关键在于优化一个关于判别器的值函数:

$$V(\theta,\phi) = -J^{(D)}(\theta,\phi) \tag{5}$$

此时, GAN 的训练可以看作一个 min-max 优化过程:

$$\theta^{(G)*} = \arg\min_{\theta}\max_{\phi} V(\theta,\phi) \tag{6}$$

相比以往的生成模型, GAN 模型具有以下几点明显的优势: 一是数据生成的复杂度与维度线性相关, 对于较大维度的样本生成, 仅需增加神经网络的输出维度, 不会像传统模型一样面临指数上升的计算量; 二是对数据的分布不做显性的限制, 从而避免了人工设计模型分布的需要; 三是 GAN 生成的手写数字、人脸、CIFAR-10 等样本较 VAE、PixelCNN 等生成模型更为清晰[14]. 然而, 原始 GAN 模型也存在许多问题.

1.4 GAN 存在的问题

阻碍原始 GAN 发展的首要问题是不收敛问题. 对于有明确目标函数的深度学习问题, 一般可以使用基于梯度下降的优化算法加以训练. GAN 的训练与这类问题不同, 其目的是要找到一个纳什均衡点. 由于一个玩家沿梯度下降的更新过程可能导致另一个玩家的误差上升, 在二者行为可能彼此抵消的情况下, 目前没有理论分析证明 GAN 总可以达到一个纳什均衡点. 在实践中, 生成式对抗网络通常会产生振荡, 这意味着网络在生成各种模式的样本之间徘徊, 从而无法达到某种均衡. 一种常见的问题是 GAN 将若干不同的输入映射到相同的输出点, 如生成器输出了包含相同颜色与纹理的多幅图片, 这种非收敛情形被称为模式坍塌 (Model collapse, 又称 the Helvetica scenario).

其次, 原始 GAN 只能用于生成连续数据, 无法生成离散数据 (如自然语言). 从直观上理解, 由于生成器每次更新后的输出是之前的输出加判别器回传的梯度, 其输出必须是连续可微的. 更进一步地, 有研究者指出, 是由于原始 GAN 论文中使用了 Jensen-Shannon(JS) 散度 $JSD\left(P_r||P_g\right)$ 作为衡量生成样本的度量标准[40], 即使使用词的分布或 embedding 等连续的表示方法也无法实现很好的离散数据生成.

最后, 相比其他的生成模型, GAN 的评价问题更加困难. 与 VAE 不同, GAN 的输入仅有随机数据, 无法使用 MAE 等重构指标进行衡量. 一般而言, 除了通过人类测试员对生成样本进行评价外, 研究者还使用 Inception score (IS)[41], Frechet inception distance (FID)[42−43] 等方法评价生成图像, 使用 BLEU 分数评判机器翻译质量[44]. 由于这种方式可以自动进行大规模的评估与展示, 研究者往往将在这些自动化评价指标上的提升作为主要的贡献.

然而, 有研究指出, 在评价分数上的提升更可能来自计算资源与调参技巧上的改进, 而非算法上的突破[45]. 此外, 对于图像生成任务而言, 基于概率估计的评价方法与视觉评价方法相互独立, 一个具有更高评价分数的模型并不能必然地产出更高质量的样本[46]. 在实际中, 研究者需要根据具体目的去选择合适的评价指标.

2 GAN 生成机制的发展

面对原始 GAN 的种种不足, 研究者从多个方面尝试加以解决. 在生成机制方面, 研究者主要利用了深度学习在有监督学习任务上取得的成果对 GAN 加以改进. 主要包括了使用新的网络结构、添加正则约束、集成多种模型、改变优化算法等改进. 需要说明的是, 这四类方法往往会同时出现在一个工作中, 本文根据它们的主要贡献作为分类依据.

2.1 网络结构

DCGAN[47] 是 GAN 发展早期比较典型的一类改进. 卷积神经网络 (Convolutional neural network, CNN) 是图像处理任务中常用的一种网络结构, 被认为可以自动提取图像的特征[36]. DCGAN 将生成器中的全连接层用反卷积 (Deconvolution) 层[48] 代替, 在图像生成的任务中取得了很好的效果, 其参数设置如图 3 所示. 此后, 使用 GAN 进行图像生成任务时, 默认的网络结构一般都与 DCGAN 类似的设置. 目前, GAN 在网络结构方面的改进主要通过添加额外信息或是对隐变量进行特殊处理来实现. 研究人员发现使用半监督的方式, 如添加图像分类标签的方法会极大地提高 GAN 生成样本的质量[41]. 这可能是由于添加了图像标签等信息后, GAN 会更关注对于阐释样本相关的统计特征, 并忽略不太相关的局部特征.

基于这种猜想, 条件生成式对抗网络 (Conditional GAN, CGAN)[49] 提出了一种带条件约束的 GAN, 在生成模型 G 和判别模型 D 的建模中均引入条件变量 c, 使用额外信息对模型增加条件, 以指导数据的生成过程. CGAN 结构如图 4 所示.

CGAN 中的条件变量 c 一般为含有特定语义信息的已知条件, 如样本的标签. 生成器接受噪声 z 与条件变量 c, 生成样本 $G\left(z|c\right)$ 与相同条件变量 c 控制下的真实样本一起用于训练判别器. 相应的, CGAN 的目标函数为:

$$\min_{G}\max_{D} V(D,G) = \mathrm{E}_x\left[\log D\left(x|c\right)\right] + \mathrm{E}_z\left[\log\left(1 - D\left(G\left(z|c\right)\right)\right)\right] \tag{7}$$

ACGAN[50] 是 CGAN 作者的后续工作. 它在判别器 D 的真实数据 x 也加入了类别 c 的信息, 进一步告诉 G 网络该类的样本结构如何, 从而生成更好的类别模拟.

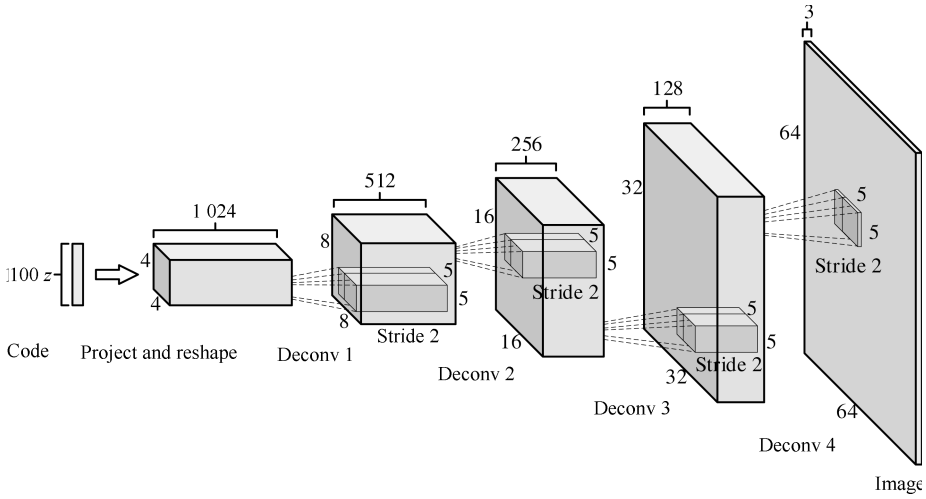


图 3　DCGAN 的拓扑结构[47]

Fig. 3　Schematic of DCGAN architecture[47]

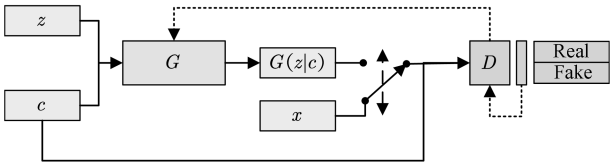


图 4　CGAN 的拓扑结构

Fig. 4　Schematic of CGAN architecture

InfoGAN[51] 发展了这种思想. 通过引入互信息量, InfoGAN 不仅免去了使用标注数据的必要性, 还使得 GAN 的行为具有了一定的可解释性. InfoGAN 的结构如图 5 所示

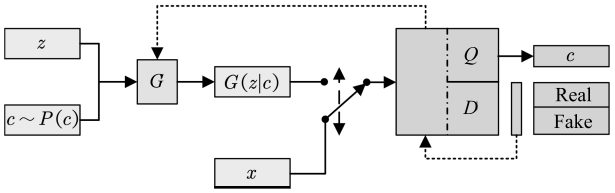


图 5　InfoGAN 的拓扑结构

Fig. 5　Schematic of InfoGAN architecture

InfoGAN 的生成器与 CGAN 类似, 同时接受噪声 z 与服从特定分布的隐变量 c 作为输入. 与 CGAN 不同的是, InfoGAN 接受的隐变量并非已知信息, 其含义需要在训练过程中去发现. 判别器会输出与原始 GAN 类似的判断, 同时 InfoGAN 还有一个额外的解码器 Q, 用于输出解码后的条件变量 $Q(c|x)$. InfoGAN 的目标函数为原始 GAN 的目标函数加上条件变量与生成样本间的互信息, 即:

$$G(z,c)=\min_G\max_D V(D,G)-\lambda I(c,G(z,c)) \quad (8)$$

其中第二项为互信息量约束:

$$I(c,G(z,c))=\mathrm{E}_{c\sim P(c),x\sim G(z,c)}[\log Q(c|x)+H(c)] \quad (9)$$

λ 是该约束项的超参数. 互信息量约束使得输入的隐变量 c 对生成数据的解释性越来越强.

除了有助于提高 GAN 的生成质量, 该类网络还可实现生成指定类随机样本的功能. CGAN 通过直接在网络输入中加入条件信息 c 以达到输出特定类别样本的目的. InfoGAN 可以通过调整隐变量实现改变生成数字的倾斜角度, 对人脸的三维模型进行旋转等操作.

除了在目标函数中对隐变量添加约束外, 部分工作利用自编码机可学习隐变量表示的性质对 GAN 进行了改进. 以 VAE-GAN[52] 为例, 该模型将变分自编码机与 GAN 结合, 其结构如图 6 所示.

该类模型同时训练 GAN 与 VAE 模型, 其目标函数由三部分组成:

$$L=\mathcal{L}_{\text{prior}}+\mathcal{L}_{\text{like}}+\mathcal{L}_{\text{GAN}} \quad (10)$$

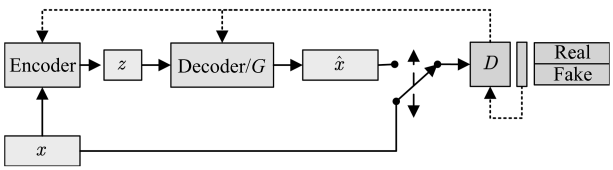


图 6　VAE/GAN 的拓扑结构

Fig. 6　Schematic of VAE/GAN architecture

其中, $\mathcal{L}_{GAN}$ 为 GAN 模型的目标函数, $\mathcal{L}_{\text{prior}}$ 为 VAE 的先验约束

$$\mathcal{L}_{\text{prior}}=D_{KL}(q(z|x)||p(z)) \quad (11)$$

$p(z)$ 为隐变量 z 的先验分布, $q(z|x)$ 为编码器 Encoder (x) 的输出分布.

$\mathcal{L}_{\text{like}}$ 为 VAE 的重构损失函数, 根据具体的目的往往有不同形式. 通过 AE + GAN 的设计模式, 该类方法可以提供具有更丰富信息的隐变量以提高生成质量. 通过设计不同的自编码机目标函数, 研究者还提出了 Denoise-GAN[53]、Plug & Play GAN[54]、α-GAN[55] 等模型变体. 该类模型可以获得较高清晰度的生成图像, 并在 3D 模型的生成工作中得到较好应用[56].

2.2 正则方法

对原始 GAN 的另一项重要改进是使用新提出的一系列正则方法. 批量规范化 (Batch normalization, BN)[57] 是深度学习中常用的一种正则方法. 其基本思想是每次更新权值时对相应的输入做规范化操作, 使得 mini-batch 输出结果的均值为 0, 方差为 1. 具体而言, 给定一批某中间层网络的输入 $U = \{u_1, \cdots, u_m\}$, 在使用激活函数对其进行非线性转换前, 首先做如下转换:

$$\begin{aligned} \mu_{\mathcal{B}} &\leftarrow \frac{1}{m}\sum_{i=1}^{m} u_i, \\ \sigma_{\mathcal{B}}^2 &\leftarrow \frac{1}{m}\sum_{i=1}^{m}(u_i - \mu_{\mathcal{B}})^2 \\ \hat{u}_i &\leftarrow \frac{u_i - \mu_{\mathcal{B}}}{\sqrt{\sigma_{\mathcal{B}}^2 + \epsilon}} \\ h_i &\leftarrow \gamma \hat{u}_i + \beta \end{aligned} \tag{12}$$

其中, γ、β 为待学习的参数, ϵ 为一极小常数. 正则化后, 网络使用转换过的 h_i 进行下一步操作. BN 可以极大地提高神经网络有监督学习的速度. DCGAN 首先将这一技术引入 GAN 的训练中, 并取得了很好的效果.

权值规范化 (Weight normalization, WN)[58] 是在有监督学习中常用的另一种正则化技术. 与 BN 不同的是, WN 主要针对神经网络的权值进行归一化, 常用的方法是将网络权值除以其范数. 在 GAN 中, 常见的形式是

$$y = \frac{W^{\mathrm{T}}x}{\parallel W \parallel} \cdot \gamma + \beta \tag{13}$$

其中, W 是网络的权值, γ、β 为待学习的参数. 实验表明, 在 GAN 网络中使用 WN 可以取得比 BN 更好的效果[59].

除了在有监督学习中常用的 BN、WN 等方法, 有研究者还针对 GAN 提出了谱规范化 (Spectral normalization, SN)[43]. 该方法对判别器的各层施加操作

$$\bar{W}_{\text{SN}} = \frac{W}{\sigma(W)} \tag{14}$$

其中, $\sigma(W)$ 是权值的谱范数, 其值等于矩阵的最大奇异值. SN 可以极大地提高 GAN 的生成效果, SN-GANs 是少数几种可以使用单一网络生成 ImageNet 全部 1 000 类物体的 GAN 结构.

除此以外, 研究者还使用了 Minibatch discrimination[41] 的方法, 通过对批量生成样本 (区别于原始 GAN 对单个生成样本) 施加多样性约束以克服模式崩溃问题.

2.3 集成学习

集成学习 (Ensemble learning) 是通过构建并结合多个学习器来完成学习任务的一种方法[60−61], 一般分为两类. 一类是提升 (Boosting) 方法, 通过调整样本权重, 级联网络等方法将弱学习器提升为强学习器, 另一类则是使用多个同类学习器对数据的不同子集进行学习后, 再将学习结果通过某种方式整合 (Bagging) 起来.

基于 Boosting 思想的集成方法可以大致分为两类. 一类工作为同构网络合并. 此类的典型工作是 AdaGAN[62]. 该方法通过与 AdaBoost 类似的算法依次训练 T 个生成器模型. 在第 t 步训练过程中, 前一次未能成功生成的模式会被加大权重. 每次训练后输出的模型为 $G_t = (1-\beta_t)\,G_{t-1} + \beta_t G_t^c$, β_t 为一给定的超参数. 训练结束后得到一系列生成模型 $G_1, G_2, \cdots, G_T$ 及其相应权重 $\alpha_1, \alpha_2, \cdots, a_T$, $\sum_{i=0}^{T}\alpha_i = 1$. 最终的生成模型为

$$G = \sum_{i=0}^{T} \alpha_i G_i \tag{15}$$

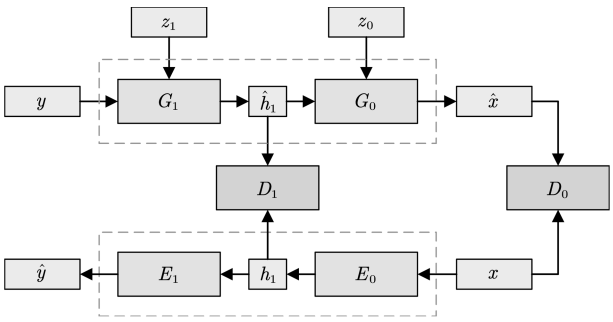


图 7 Stack GAN 的拓扑结构

Fig. 7 Schematic of stack GAN architecture

另一类工作的主要方法为网络叠加. 该类方法的主要模式是串联多个 GAN, 将上层生成器的输出作为隐变量输入下层生成器. Stack GAN[63] 是其中较为典型的工作. 如图 7 所示, 该模型的生成器由

多个子模型串联构成, 每级生成器 G_i 接受上一级生成器的输出 $\hat{h}_{i+1}$ 及一个随机变量 z_i 作为输入. 在训练时, 该方法同步训练一个编码器 E_i, 并使用其中间层的输出 h_i 和生成器的中间输出一起训练.

该类工作的另一种常见方式则通过叠加不同分辨率的生成器网络来实现. 以 LAP-GAN[64] 为例.

如图 8 所示, 该模型中上一层生成器的输出 I_{i+1} 在放大后 (记为 l_i) 与随机变量 z_i 一同输入下一层网络, 下一层的输出 $\tilde{h}_i$ 与 l_i 合并为 $\tilde{I}_i$, $\tilde{I}_i$ 经过放大后作为再下一层的输入.

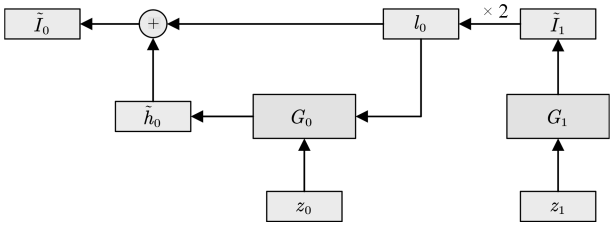


图 8　LAP-GAN 的拓扑结构

Fig. 8　Schematic of LAP-GAN architecture

后继的 PG-GAN (Progress growing of GANs)[65] 通过不断加深网络层数的方法改进了这一模式. 在训练过程中首先训练可输出低分辨率图像的浅层网络, 再在浅层网络上增加层数. 该方法可生成目前最高清晰度的图像.

基于 Bagging 思想的集成方法主要针对模式坍塌 (Mode collapse) 这一 GAN 训练中最常见的不收敛情况, 通过使用多个网络, 每个网络针对不同的模式进行训练, 之后再将这些网络的输出进行整合.

这类模型中较为典型的是 CoGAN[66] 与 MAD-GAN[67]. 两者均通过集成多个共享部分权值的生成器以实现生成多样性样本的目的. 两者的区别主要在于, CoGAN 使用了与生成器同样数量的判别器, 而 MAD-GAN 使用了多输出的单判别器, 通过判别目标函数和基于相似性的竞争性目标函数来引导生成器.

相较于基于 Boosting 的集成方法, 基于 Bagging 的 GAN 集成方法并没有在一般性的任务中取得显著效果. 但由于 Bagging 方法较为直接, 在个性化任务中能以较小的代价获得较大的提升.

2.4　优化算法

GAN 的优化算法是另一个重要的改进方向. GAN 使用同步梯度下降 (Simultaneous gradient ascent) 的方法优化网络, 一般可以定义两个效用函数 $f(\phi,\theta)$ 与 $g(\phi,\theta)$, 其中 $(\phi,\theta)\in\Omega_1\times\Omega_2$. 玩家 1 的目标是最大化效用函数 f, 玩家 2 的目标则是最大化效用函数 g. $\Omega_i\ (i=1,2)$ 为对应玩家的可能行动空间, 在 GAN 中, 它们对应着生成器与判别器的参数取值空间. GAN 博弈的相关梯度向量场 (Associated gradient vector field) 为

$$v(\phi,\ \theta)=\begin{pmatrix}\nabla_\phi f(\phi,\ \theta)\\ \nabla_\theta g(\phi,\ \theta)\end{pmatrix} \tag{16}$$

对于零和博弈, 有 $f(\phi,\theta)=-g(\theta,\phi)$. 在一些情况下, 如 $v(\phi,\theta)=\phi\cdot\theta$ 时, 使用同步梯度下降方法的参数轨迹为

$$\begin{cases}\theta(t)=\theta(0)\cos(t)-\phi(0)\sin(t)\\ \phi(t)=\theta(0)\sin(t)+\theta(0)\cos(t)\end{cases} \tag{17}$$

该式对应一个圆轨迹, 具有无穷小学习速率的梯度下降将在恒定半径处环绕轨道运行, 使用更大的学习率则轨迹有可能沿螺旋线发散. 在这种情况下, 同步梯度下降无法接近均衡点 $\theta=\phi=0$.

解决这一问题可以使用共识优化 (Consensus optimization)[68] 的方法.

定义 $L(x)=\frac{1}{2}\|v(x)\|^2$, 有修正的效用函数

$$\begin{cases}\tilde{f}(\phi,\theta)=f(\phi,\ \theta)-\gamma L(\phi,\ \theta)\\ \tilde{g}(\phi,\theta)=g(\phi,\ \theta)-\gamma L(\phi,\ \theta)\end{cases} \tag{18}$$

正则化因子 $L(\phi,\theta)$ 鼓励玩家间达成 “共识”, 这种方法较同步梯度下降方法具有更好的收敛性.

除了从优化方法的角度, 研究者还通过改变优化的形式对 GAN 加以改进. 最为常见的方法是使用强化学习中的策略梯度方法[69−70] 以实现生成离散变量的目的.

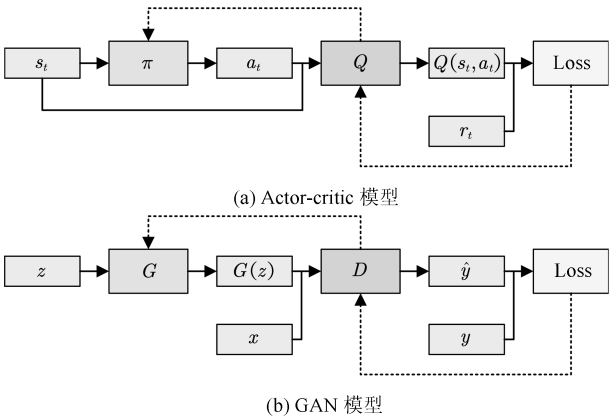


图 9　GAN 与 Actor-critic 模型

Fig. 9　GAN and actor-critic models

GAN 与强化学习领域的 Actor-critic 模型[70] 的关系引起了许多研究者的注意[71]. 强化学习 (Reinforcement learning)[72] 研究的问题是如何将状态映射为行动, 以最大化执行者的长期回报. Actor-critic 模型是强化学习中常用的建模方法, 在这一模

型中, 存在行动者 (Actor) 与批评家 (Critic) 两个子模型, 其中, 行动者根据系统状态做出决策, 评价者对行动者做出的行为给出估计. 如图 9 所示.

可以看出, GAN 模型与 Actor-critic 具有结构上的相似性, 两者均包含了一个由随机变量到另一空间的映射, 以及一个可学习的评价模型. 两者均通过迭代寻求均衡点的方式求解. Goodfellow 甚至认为 GAN 实质是一种使用 RL 技巧解决生成模型问题的方法, 两者的区别主要在于 GAN 中回报是策略的已知函数且可对行动求导[73].

Actor-critic 的优化方法主要是基于 REINFORCE 算法[74] 改进的策略梯度方法. 该方法的主要思想是: 行动者为一参数化的函数 $\pi(s;\theta)$, 每次行动的动作为 $a_t=\pi(s_t|\theta)$. 若一个动作可以获得较大的长期回报 $Q(s_t,a_t)$ 则提高该行动的出现几率, 否则降低该行动的出现几率. 长期回报一般由批评家给出. 每次行动后更新策略函数的参数:

$$\begin{aligned}&\theta\leftarrow\theta+\nabla\theta,\\&\nabla\theta=\hat{\mathrm{E}}\left[\nabla_\theta\log\pi_\theta(a_t|s_t)\,Q(s_t,a_t)\right]\end{aligned}\tag{19}$$

其中, $\nabla\theta$ 被称为策略梯度.

在原始 GAN 中, 生成器的学习依赖判别器回传的梯度. 由于离散取值的操作不可微, 原始 GAN 无法解决离散数据的生成问题. 通过借鉴 Actor-critic 模型的思想, 研究者提出了一系列基于策略梯度优化的 GAN 变体以解决这一问题.

SeqGAN[75] 是这一系列工作中较早出现的模型之一. 它的生成器结构及更新方式与用于图像生成的 GAN 类似. 其模型结构如图 10 所示:

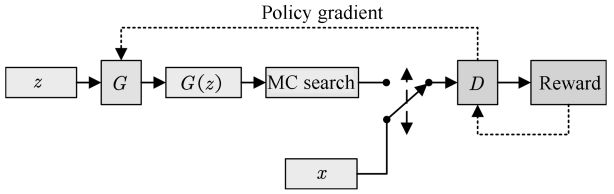


图 10 SeqGAN 的拓扑结构

Fig. 10 Schematic of SeqGAN architecture

SeqGAN 将序列生成问题视为序列决策问题进行处理, 使用 RNN 作为生成网络. 以已生成的语素 (Tokens) $Y_{1:t-1}$ 作为当前状态, 生成器输出的下一个词汇 y_t 为行为, 生成器网络为策略 π, 行为的回报 r_t 为判别器 D 对生成 Tokens 的置信概率. 为了提高对整句输出的判别准确度, SeqGAN 在每次生成一个 Token 后, 使用蒙特卡洛搜索 (Monte Carlo search, MC search) 的方法对句子进行补齐, 再将补齐后的句子输入判别器 D. SeqGAN 的值函数见式 (20), 每次更新的策略梯度见式 (21):

$$Q_{D_\phi}^{G_\theta}(s=Y_{1:t-1},a=y_t)=\begin{cases}\dfrac{1}{N}\sum_{n=1}^{N}D_\phi\left(Y_{1:T}^n,Y_{1:T}^n\in MC^{G_\beta}(Y_{1:t};N)\right), & \text{for } t<T\\ D_\phi\left(Y_{1:T}^n\right), & \text{for } t=T\end{cases}\tag{20}$$

$$\nabla_\theta J(\theta)=\mathrm{E}_{Y_{1:t-1}\sim G_\theta}\times\left[\sum_{y_t\in\mathcal{Y}}\nabla_\theta G_\theta(y_t|Y_{1:t-1})\cdot Q_{D_\phi}^{G_\theta}(Y_{1:t-1},y_t)\right]\tag{21}$$

通过这一方式, SeqGAN 克服了原始 GAN 无法生成离散数据序列的问题.

后续工作通过改进网络结构, 结合更丰富的数据类型等方法进一步强化了 GAN 的离散数据生成能力. 如 MaskGAN[76] 使用 Seq2Seq[7] 作为生成网络, 使得 GAN 具备了填词能力. SPIRAL[77] 使用艺术生成的序列数据作为样本, 可控制机械臂生成艺术图像.

3 GAN 判别机制的发展

如何合理选择目标函数是深度学习中至关重要的一个问题. 一个好的目标函数需要在刻画任务本质的同时, 提供良好的数值优化特性. 在 GAN 的训练过程中, 目标函数设计的主要目标是有效地定义可区分性, 并使得博弈过程可解[78−79].

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. 当判别器为最优判别器时, 生成器的损失函数等价于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 散度为一常数, 此时生成器的获得梯度为 0, 无法进一步学习[40].

有研究者认为, 这一问题的根源在于原始 GAN 假设了判别网络具有无限建模能力, 可以对于任意的样本分布进行判别. 然而对于一般的分布而言, 真实分布与生成分布不重叠的概率无限趋于 1[80]. 为了克服这一问题, 研究者提出对样本分布进行限制的方法, 通过假设样本服从某类特殊的函数族以避免梯度消失的问题.

3.1 Lipschitz 密度

一类较有代表性的限制是假设样本分布服从 Lipschitz 连续, 即其概率密度分布 $f(x)$ 服从

$$|f(a)-f(b)|\le K|a-b|\tag{22}$$

使不等式成立的最小 K 值被称为 Lipschitz 常数.

这类方法的典型代表是 Wasserstein GAN (WGAN)[81]. WGAN 使用 Wasserstein-1 距离 (又称 Earth-Mover (EM) 距离) 作为真实分布与生成分布相近度的度量. 定义如下:

$$W(P_r, P_g) = \inf_{\gamma \sim \Pi(P_r, P_g)} \mathrm{E}_{(x,\tilde{x})}\left[\|x - \tilde{x}\|\right] \tag{23}$$

其中, $\mathrm{E}_{(x,\tilde{x})\sim\gamma}\left[\|x-\tilde{x}\|\right]$ 相当于在真实与生成样本的联合分布 γ 的条件下, 将真实分布变换为生成分布所需要 "消耗" 的步骤. $W(P_r, P_g)$ 是这一 "消耗" 的最小值.

由于取下界的操作无法直接求解, 根据 Kantorovich-Rubinstein 对偶性[82], EM 距离被转化为如下的形式:

$$W(P_r, P_g) = \frac{1}{K} \sup_{\|f\|_L \le K} \mathrm{E}_{x\sim p_r}\left[f(x)\right] - \mathrm{E}_{x\sim p_g}\left[f(x)\right] \tag{24}$$

其中, $f(\cdot)$ 是一个满足 Lipschitz 连续条件的函数. 我们可以使用神经网络对 $f(\cdot)$ 进行拟合, 因此 WGAN 的目标函数为:

$$\min_G \max_C \mathrm{E}_{x\sim P_r}\left[C(x)\right] - \mathrm{E}_{\tilde{x}\sim P_r}\left[C(\tilde{x})\right] \tag{25}$$

其中评价函数 C 需要满足 Lipschitz 连续条件, 一般采用权值裁剪或软约束的方式保证. 在 WGAN 中, 判别器 (称为评价网络 C) 的目的是逼近 P_r 与 P_g 的 EM 距离, 生成器的目的则是最小化两者的 EM 距离. WGAN 的网络结构如图 11 所示.

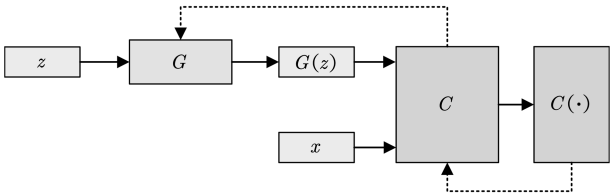


图 11　WGAN 的拓扑结构

Fig. 11　Schematic of WGAN architecture

WGAN 的可收敛性远强于原始 GAN, 一经提出就引起了极大的关注. 后继的改进版本 WGAN-GP 通过添加梯度惩罚的方式[83], 进一步提高了网络的稳定性, 在多种网络结构上都可实现收敛, 是目前性能最佳, 使用最广泛的 GAN 变种之一.

3.2　能量函数

除了使用 Lipschitz 连续假设对样本分布进行约束, 还可以使用非概率形式作为度量的 GAN 结构, 较为典型的是基于能量的 GAN (Energy-based GAN, EBGAN)[84]. EBGAN 将判别器 D 视为一个能量函数, 该函数得赋予真实样本较低的能量, 而赋予生成样本较高的能量. 其网络结构如图 12 所示.

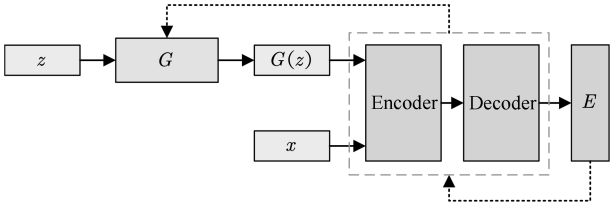


图 12　EBGAN 的拓扑结

Fig. 12　Schematic of EBGAN architecture

在论文中, EBGAN 使用了一个自动编码机作为判别网络, 并将自动编码机的重构误差作为样本的能量, 即:

$$D(x) = \|\mathrm{Decoder}\left(\mathrm{Encoder}\left(x\right)\right) - x\| \tag{26}$$

相应的损失函数为

$$J^{(D)} = D(x) + \left[m - D\left(G(z)\right)\right]^+ \tag{27}$$

$$J^{(G)} = D\left(G(z)\right) \tag{28}$$

其中 $[\cdot]^+ = \max(0, \cdot)$, m 是一个预定义的边界 (Margin), 主要作用在于避免判别器过强导致生成器无法获得有用的信息, 该参数也可以通过自适应的方式学习[85].

为了使得生成的样本具有更好的多样性, EBGAN 还提出了一种约束方法, 称为 Pulling-away term (PT), 其形式为

$$f_{\mathrm{PT}}(S) = \frac{1}{N(N-1)} \sum_i \sum_{j\neq i} \left(\frac{S_i^{\mathrm{T}} S_j}{\|S_i\|\|S_j\|}\right)^2 \tag{29}$$

其中, S 为判别器中编码层的输出. 通过增大 PT 值, EBGAN 可以有效地提升生成样本的多样性. EBGAN 为理解 GAN 提供了一种全新的视角.

4　GAN 的应用

GAN 在生成逼真图像上的性能远超以往, 一经提出便引起了极大的关注. 随着研究的深入, 研究者逐渐认识到其作为一种表征学习方式的潜力, 并进一步地发展了其对抗的思想, 将 GAN 的结构设计用于模仿学习与图像翻译等新兴领域.

一般而言, GAN 的应用遵循这样的设计模式: 首先定义一个模型用于将某一空间中的数据映射至另一空间, 再定义一个模型用于评估这一映射的质量. 通过迭代训练两模型得到理想的映射模型或评价模型. 本文将 GAN 的应用依据其映射的性质分

为三类: 数据生成与增强, 广义翻译模型, 以及广义生成模型.

4.1 数据生成与增强

作为生成模型, GAN 最为直接的作用是对训练数据进行增强. 根据增强后的数据性质, 这一类应用可以分为数据集内增强与数据集外增强两类. 前者是对训练集内数据进行填补, 清晰化, 变换等操作, 主要目的是增强数据集质量. 后者则主要是结合外部知识或无标签数据对数据集进行调整和猜测, 使其具备原数据集不具备的信息.

在有监督的深度学习训练中, 研究者常常要对原始数据进行平移、缩放、旋转等操作. 这些数据增强操作一方面扩大了数据集的样本量, 另一方面也有助于神经网络学到轮廓, 纹理等特征, 以收敛到更好的 (局部) 最优解[2].

数据集内提升是对这一工作的扩展. 典型的应用包括缺失数据填补[86−87]、超分辨率图像生成[88]、视频预测[89−90]、图像清晰化[91] 等. 该类工作的主要模式是将有缺陷的数据或历史数据输入生成器, 通过使用 GAN 的训练方式替代均方根误差 (Mean square error, MSE) 等人工设计的损失函数, 从而实现更好的修复或预测效果.

以缺失数据填补为例. 给定一个信息有缺失的数据, 如部分像素丢失的图像, 我们希望根据同类别的其他图像训练一个模型, 该模型可将丢失的信息补全. 如图 13 所示, 相比传统方法 (Image melding)[92], 基于 GAN 的数据填补可以更好地考虑图像的语义信息, 并填充符合当前场景的内容.

许多计算机视觉任务都可以通过 GAN 增强图像以提高性能. 除了图像分类, 目标检测等常用任务, GAN 也被用于对抗样本[93−94] 的生成[95] 与抵抗任务, 如 APE-GAN[96] 通过将对抗样本转化为可被目标模型正确识别的样本, Generative adversarial trainer[97] 使用 GAN 生成对抗性扰动 (Adversarial perturbation) 后将经过污染的样本与标记样本一起学习, 等等.

GAN 在数据集外扩展方面的工作, 主要集中在使用仿真数据扩大真实数据相关的工作. 在许多问题中, 真实数据的收集十分困难或缓慢, 但在仿真数据上训练的模型又无法很好地泛化以用于现实任务[98]. 研究者提出了 PixelDA[99]、SimGAN[100]、GraspGAN[101] 等模型以解决该问题. 该类模型的基本想法是通过使用 GAN 中的生成器作为精炼器 (Refiner), 对仿真数据进行修饰后, 使其与真实数据相接近. 该类方法使得以往需要大量样本的任务, 如人眼识别、自动驾驶、机械臂控制等, 现在通过少量真实样本与仿真环境即可完成训练[102−104].

GAN 还可以用于提升开放集分类 (Open-category classification, OCC, 即将与训练集内数据类型不一致的样本区分为单独一类) 问题的性能[105]. 通过生成接近集内数据但被判别器认为是集

图 13 GAN[86] 与传统方法[92] 的数据填补效果

Fig. 13 Image completion by GAN[86] and traditional method[92]

外数据的样本, GAN 可以较大地提升分类器在开放集分类问题上的性能.

数据生成与增强的工作往往与半监督学习相联系, 其目的在于提高后续的监督学习或强化学习性能. 一部分半监督学习方面工作还使用了 GAN 本身的结构特性. 如后文 IRGAN 对判别式信息检索 (Information retrieval, IR) 模型的提升, 使用 CGAN 模型中的判别器作为图像分类器[106], Professor forcing[107] 方法中使用 GAN 提高 RNN 的训练质量, 等等. 由于这部分研究尚不丰富, 限于篇幅本文不做详细介绍.

4.2　广义数据翻译

不同领域的数据往往具有各自不同的特征和作用. 如自然语言数据具有易获取, 具有较为明确的意义, 但缺乏细节信息的特点. 图像数据具有细节丰富, 但难以分析语义的特点. 同类数据间如何翻译, 不同类型的数据间如何转化, 不仅具有相当的实用价值, 而且对于提高神经网络的可解释性具有重要的意义. GAN 已被用于一些常见的数据翻译工作中, 如从语义图生成图像[108]、图文翻译[109] 等. 本节主要介绍一些 GAN 所特有或表现显著优于传统方法的应用.

根据用户修改自动对照片进行编辑和生成是一个极具挑战的任务. 研究人员提出了 iGAN 模型, 通过类似 InfoGAN 等模型调整隐变量改变输出样本的方法, 将用户输入作为隐变量, 实现了图像的自动修改与生成[110−111]. 效果如图 14 所示. 受该工作启发, 研究者提出了 “图对图翻译” 的新问题[112].

如图 15 所示, 许多常见的图像处理任务都可以看作是将一张图片 “翻译” 为另一张图片, 如将卫星图像转换为对应的路网图, 将手绘稿转换为照片, 将黑白图像转换为彩色图片等. Isola 等提出了一种名为 Pix2Pix[112] 的方法, 利用 GAN 实现了这种翻译, 模型结构如图 16 所示.

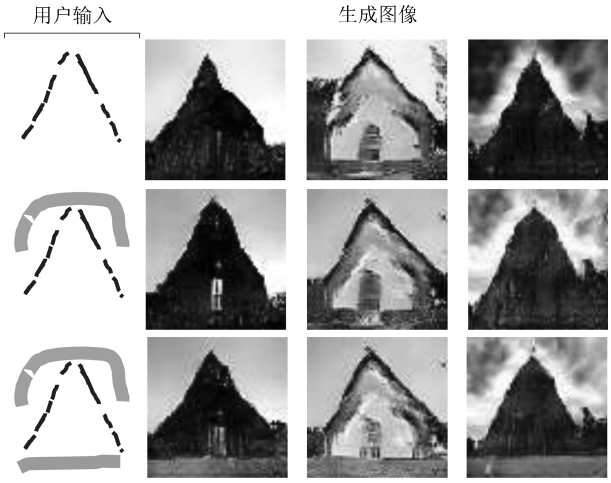


图 14　iGAN 的生成样例[110]

Fig. 14　Images generated by iGAN[110]

图 16 中 F 与 G 均为翻译器. Pix2Pix 需要成对的数据集 (x, y), 例如在卫星图像转换的任务中, x 是卫星图像, y 是对应的路网图像. 在 x 向 y 转换的过程中, 翻译器接受 x 的样本, 生成对应的样本 $\hat{y}$, 判别器 $D_{x:y}$ 判别 x 与 $\hat{y}$ 是否配对, 并将梯度回传给翻译器. y 向 x 的转换也照此进行.

Pix2Pix 取得了非常惊艳的效果, 后续的 Pix2PixHD[113] 等工作进一步提高了其生成样本的分辨率和清晰度. 不过, 该模型的训练必须有标注好的成对数据, 这限制了它的应用场景. 为了解决这一问题, 结合对偶学习[114], 研究者提出了 CycleGAN[115], 使得无须建立训练数据间一对一的映射, 也可以在源域和目标域之间实现转换. CycleGAN

图 15　图对图翻译举例[112]

Fig. 15　Examples of image to image translation[112]

的结构如图 17 所示.

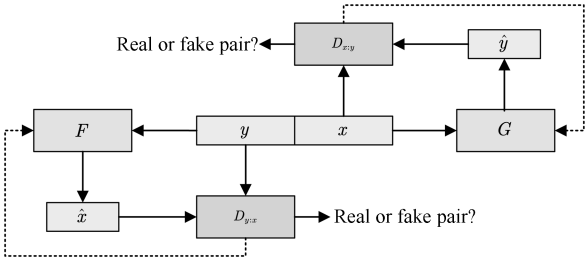


图 16 Pix2Pix 的拓扑结构

Fig. 16 Chematic of Pix2Pix architectur

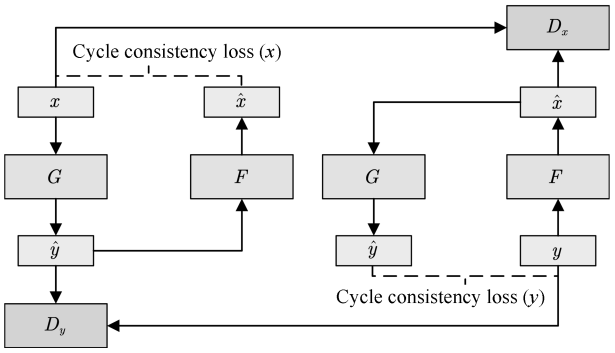


图 17 CycleGAN 的拓扑结构

Fig. 17 Schematic of CycleGAN architecture

为了使用非配对数据进行训练, CycleGAN 会首先将源域样本映射到目标域, 然后再映射回源域得到二次生成图像, 从而消除了在目标域中图像配对的要求. 为了保证经过 “翻译” 的图像是我们所期望的内容, CycleGAN 还引入了循环一致性的约束条件.

以 x 向 y 的转换为例, 翻译器 G 接受 x 的样本, 生成对应的样本 $\hat{y}$, 翻译器 F 再将 $\hat{y}$ 翻译为 $\hat{x}$. 判别器 D_y 接受样本 y 与 $\hat{y}$, 并试图判别其中的生成样本. $\hat{x}$ 应与 x 相似, 以保证中间映射有意义. 为此, 文中将循环一致性约束定义为

$$\begin{aligned}\mathcal{L}_{cyc}(G,F)=&\mathrm{E}_x\left[\|F(G(x))-x\|_1\right]+\\&\mathrm{E}_y\left[\|G(F(x))-y\|_1\right]\end{aligned}\tag{30}$$

在训练 GAN 的同时保证循环一致性约束最小化, CycleGAN 就可以通过非配对数据实现较好的映射效果. 该方法生成的图像与 Pix2Pix 十分接近. 除了用于数据增强任务外, 该模型也被广泛用于神经风格转换 (Neural style transfer)[116] 等艺术性工作中.

4.3 广义生成模型

以上讨论的工作主要关于图像, 自然语言等具体数据. 实际上, 我们可以考虑更为广义的数据, 如状态、行动、图网络等.

该类研究的典型工作之一为生成式模仿学习 (Generative adversarial imitation learning, GAIL)[117]. 模仿学习 (Imitation learning) 是强化学习中的一个重要课题, 其目的是解决如何从示教数据中学习专家策略的问题. 由于状态对行动的映射具有不确定性, 直接使用示教数据进行监督训练得到的策略模型往往不能很好地泛化. 研究者一般使用反向强化学习 (Inverse reinforcement learning, IRL)[118] 来解决这一问题. 通过学习一个代理回报函数 (Surrogate reward function) $\tilde{R}(s)$, 并期望该函数能最好地解释观察到的行为, 再由此从数据中习得类似的策略. IRL 成功解决了一系列的问题, 如预测出租车司机行为[119], 规划四足机器人的足迹[120] 等.

然而, IRL 算法的运算代价高昂, 且方法过于间接. 对于模仿学习而言, 真正的目的是使得 Agent 可以习得专家的策略, 内在的代价函数并非必要. 研究者从 GAN 的思想中得到启发, 提出了生成式模仿学习 (Generative adversarial imitation learning, GAIL)[117] 的方法. GAIL 的一般结构如图 18 所示.

与 GAN 类似, GAIL 的目的是训练一个策略网络 π_θ, 其输出的状态−行为对 $\mathcal{X}_\theta=\{(s_1,a_1),\cdots,(s_T,a_T)\}$ 可以欺骗判别器 D_ϕ, 使其无法区分 $\mathcal{X}_\theta$ 与由专家策略 π_E 输出的 $\mathcal{X}_E$. GAIL 的目标函数为

$$\begin{aligned}\max_{\phi}\min_{\theta}V(\theta,\phi)=&\mathop{\mathrm{E}}_{(s,a)\sim\mathcal{X}_E}\left[\log D_\phi(s,a)\right]+\\&\mathop{\mathrm{E}}_{(s,a)\sim\mathcal{X}_\theta}\left[\log\left(1-D_\phi(s,a)\right)\right]\end{aligned}\tag{31}$$

策略的代理回报函数为

$$\tilde{r}(s_t,a_t;\phi)=-\log\left(1-D_\phi(s_t,a_t)\right)\tag{32}$$

使用策略梯度方法更新行动者 π (生成器), 最终使得行动者的决策与专家的决策一致. 该方法被用于模仿驾驶员[121], 机械臂控制[122] 等任务中, 取得了较好的效果.

与 GAIL 相类似, IRGAN[123] 使用对抗方式提高信息检索 (Information retrieval, IR) 模型质量. 一般而言, IR 模型可分为两类. 一类为生成式模型, 其目标是学习一个查询 (Query) 到文档 (Document) 的关联度分布, 利用该分布对每个查询返回相关的检索结果. 另一类为判别式模型, 该模型可以区分有关联的查询对 $\langle query_r,\ doc_r\rangle$ 与无关联的查询对 $\langle query_f,\ doc_f\rangle$. 对于给定的查询对, 该模型可返回该查询对内元素的关联程度[124]. 由于这两类模型的对抗性质, IRGAN 将两个或多个生成式 IR 模型与判别式 IR 模型整合为一个 GAN 模型, 再通过

策略梯度优化的方式提升两类模型的检索质量.

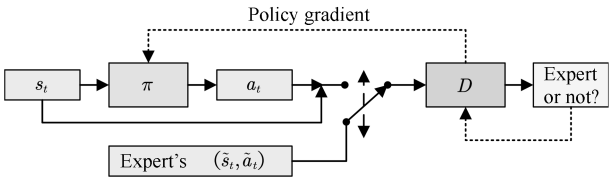


图 18　生成式模仿学习

Fig. 18　Generative adversarial imitation learnin

此外, GAN 还被用于专业领域数据的生成任务. 如用于生成恶意软件的 MalGAN[125] 模型, 用于生成 DNA 序列的 FBGAN[126], 用于学习图嵌入表示 (Graph embedding)[127] 的 GraphGAN 等. 限于篇幅, 本文不再详细介绍.

5　总结与展望

自 2014 年提出以来, 生成式对抗网络获得了极大的关注与发展. GAN 的相关工作越来越多地出现在机器学习的各类会议和期刊上, LeCun 甚至将其称为 "过去十年间机器学习领域中最让人激动的点子".

本文综述了 GAN 在理论与应用方面的成果, 总体来看可分为两个大的方向.

第一个研究方向集中在生成机制方面, 主要的问题是如何设计一个有效的结构, 以学习一个从隐变量到目标空间的映射. 在理论上主要包括了如何设计更好的网络结构和相应的优化方法以提高生成数据质量, 如何集成多模型以提高生成效率. 在应用上主要是考虑半监督学习问题以及复杂数据间的映射问题.

第二个研究方向集中在判别机制方面, 主要的问题是如何更好地将生成问题转化为一个较易学习的判别问题. 在理论上主要包括了如何设计博弈形式以提高学习效率, 在应用上主要是如何利用 GAN 中的判别模型辅助下游任务, 以及如何设计整体结构, 将其他问题转化为一个可判别的生成问题.

GAN 在数据生成, 半监督学习, 强化学习等多方面任务中起到了重要作用. 但也应看到, 该领域的发展仍处于早期阶段, 许多问题仍在制约 GAN 的发展. 最为突出的是 GAN 的评价与复现问题, 目前尚未有关于如何科学评价 GAN 的共识. 其次, GAN 的博弈与收敛机制背后的数学分析仍有待建立, 现有的研究主要是利用深度学习在有监督任务中积累的经验进行扩展. 最后, 大部分 GAN 的工作仍然缺乏实用价值, 仅可在特定的数据集上使用. 如何建立类似 ImageNet 等标准化任务以评价 GAN 方法; 如何建立和分析 GAN 的数学机制, 并在此基础上进一步实现 GAN 特有的, 与有监督学习任务不同的深度学习构件; 如何拓展 GAN 的应用范围; 这些问题仍有待研究者进一步探索.

从更高的角度看, GAN 的成功实质反映了人工智能的研究进入深水区, 研究的重点从视觉、听觉等感知问题向解决决策、生成等认知问题转移. 与机器感知问题相比, 这些新的问题往往人类也无法很好解决, 对这类问题的解决必须依赖新的研究方法.

这两类问题的区别可以使用强化学习中的 "探索与利用两难 (Explore and exploit dilemma)" 问题进行类比, 如图 19 所示. 对于感知问题, 我们有一个足够明确的目标以及目标临近域的数据, 所需要的是足够高效的利用方法. 然而, 对于认知问题, 我们只能通过比较局部目标的方法来定义问题, 且数据往往过于稀疏或处于局部最优点附近. 如在围棋 AI 的研究中发现, 使用人类数据训练的智能体会收敛到局部最优值, 反而无法胜过不学习人类经验的智能体[128]. 此时, 需要寻找一种方法充分探索可能性空间, 以更好地确定实际需要学习的目标.

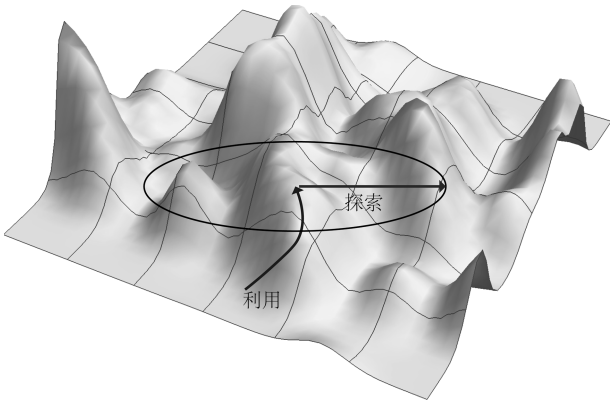


图 19　探索与利用

Fig. 19　Explore and exploit

实现这种探索的一个方式是将真实世界的互动机制引入模型. GAN 可以看作是这样的一个系统, 通过在生成模型上添加判别模型, GAN 模仿了现实世界中人类判断图片的机制, 进而将难以定义的样本差异转化为一个博弈问题. 与之类似的是 AlphaZero, 通过自我对弈的形式积累大量数据, 再从中探索出一个更优的策略. 在这一新的研究范式中, 模型从分析的工具变为了数据的 "工厂"[129].

这类方法的思路与国内学者提出的平行思想有很多相似之处. 平行思想是指, 通过将真实系统与人工系统融合, 在两个平行的系统中迭代实现对另一系统的描述、预测与引导[129]. 有研究者结合平行思想与机器学习提出了平行学习的概念[130]. 通过在平行系统中综合描述学习、预测学习与引导学习, 可以更好地提高机器学习方法的样本效率, 扩大学习的探索空间, 实现一条从小数据产生大数据, 再由大

数据炼成“小定律”的精准知识之路, 从而更好地分析和解决决策、生成等难以明确定义优化目标的问题. 目前, 平行学习已在自动驾驶中得到了成功的应用[131−132].

GAN 可被视为一个最简单且无引导学习功能的平行学习系统, 它用判别器逼近真实系统, 利用生成器逼近人工系统, 为虚实一体的智能“平行机”构造提供了一个例子[133]. GAN 为平行学习中的博弈提供了一个初步示例, 更为人工智能的下一步发展提供了一种全新的思路.

References

1 Murphy K P. *Machine Learning: A Probabilistic Perspective*. Cambridge: MIT Press, 2012.

2 Krizhevsky A, Sutskever I, Hinton G E. ImageNet classification with deep convolutional neural networks. In: Proceedings of the 25th International Conference on Neural Information Processing Systems. Lake Tahoe, Nevada, USA: ACM, 2012. 1097−1105

3 Farabet C, Couprie C, Najman L, LeCun Y. Learning hierarchical features for scene labeling. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2013, **35**(8): 1915−1929

4 Mikolov T, Deoras A, Povey D, Burget L, Cernocky J. Strategies for training large scale neural network language models. In: Proceedings of the 2011 IEEE Workshop on Automatic Speech Recognition and Understanding. Waikoloa, HI, USA: IEEE, 2011. 196−201

5 Hinton G, Deng L, Yu D, Dahl G E, Mohamed A R, Jaitly N, et al. Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups. *IEEE Signal Processing Magazine*, 2012, **29**(6): 82−97

6 Collobert R, Weston J, Bottou L, Karlen M, Kavukcuoglu K, Kuksa P. Natural language processing (almost) from scratch. *Journal of Machine Learning Research*, 2011, **12**: 2493−2537

7 Sutskever I, Vinyals O, Le Q V. Sequence to sequence learning with neural networks. In: Proceedings of the 27th International Conference on Neural Information Processing Systems. Montreal, Canada: MIT Press, 2014. 3104−3112

8 Hinton G E, Osindero S, Teh Y W. A fast learning algorithm for deep belief nets. *Neural Computation*, 2006, **18**(7): 1527−1554

9 Salakhutdinov R, Hinton G. Deep Boltzmann machines. In: Proceedings of the 12th International Conference on Artificial Intelligence and Statistics. Clearwater Beach, Florida, USA: AISTATS, 2009. 448−455

10 Smolensky P. Information processing in dynamical systems: Foundations of harmony theory. *Parallel Distributed Processing: Explorations in the Microstructure of Cognition*. Cambridge, MA, USA: MIT Press, 1986.

11 Hinton G E, Zemel R S. Autoencoders, minimum description length and Helmholtz free energy. In: Proceedings of the 6th International Conference on Neural Information Processing Systems. Denver, Colorado, USA: Morgan Kaufmann Publishers Inc., 1994. 3−10

12 Bengio Y, Lamblin P, Popovici D, Larochelle H. Greedy layer-wise training of deep networks. In: Proceedings of the 21st Annual Conference on Neural Information Processing Systems. Vancouver, BC, Canada: MIT Press, 2007. 153−160

13 Goodfellow I J, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, et al. Generative adversarial nets. In: Proceedings of the 27th International Conference on Neural Information Processing Systems. Montreal, Canada: MIT Press, 2014. 2672−2680

14 Goodfellow I. NIPS 2016 tutorial: Generative adversarial networks. arXiv preprint arXiv: 1701.00160, 2016

15 Wang Kun-Feng, Gou Chao, Duan Yan-Jie, Lin Yi-Lun, Zheng Xin-Hu, Wang Fei-Yue. Generative adversarial networks: The state of the art and beyond. *Acta Automatica Sinica*, 2017, **43**(3): 321−332
(王坤峰, 苟超, 段艳杰, 林懿伦, 郑心湖, 王飞跃. 生成式对抗网络 GAN 的研究进展与展望. 自动化学报, 2017, **43**(3): 321−332)

16 LeCun Y, Bengio Y, Hinton G. Deep learning. *Nature*, 2015, **521**(7553): 436−444

17 Rumelhart D E, Hinton G E, Williams R J. Learning representations by back-propagating errors. *Nature*, 1986, **323**(6088): 533−536

18 Le Cun Y, Boser B, Denker J S, Howard R E, Habbard W, Jackel L D, et al. Handwritten digit recognition with a back-propagation network. In: Proceedings of the 1990 Advances in Neural Information Processing Systems. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1990. 396−404

19 Lecun Y, Bottou L, Bengio Y, Haffner P. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 1998, **86**(11): 2278−2324

20 Hochreiter S. Untersuchungen zu dynamischen neuronalen Netzen [Ph. D. dissertation], Technische Universitt München, München, Germany, 1991

21 Bengio Y, Simard P, Frasconi P. Learning long-term dependencies with gradient descent is difficult. *IEEE Transactions on Neural Networks*, 1994, **5**(2): 157−166

22 Hochreiter S, Schmidhuber J. Long short-term memory. *Neural Computation*, 1997, **9**(8): 1735−1780

23 Nair V, Hinton G E. Rectified linear units improve restricted Boltzmann machines. In: Proceedings of the 27th International Conference on Machine Learning. Haifa, Israel: Omni Press, 2010. 807−814

24 Srivastava N, Hinton G E, Krizhevsky A, Sutskever I, Salakhutdinov R. Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research*, 2014, **15**(1): 1929−1958

25 Kingma D P, Ba J. Adam: A method for stochastic optimization. arXiv preprint arXiv: 1412.6980, 2014

26 Chellapilla K, Puri S, Simard P. High performance convolutional neural networks for document processing. In: Proceedings of the 10th International Workshop on Frontiers in Handwriting Recognition. La Baule, France: Suvisoft, 2006.

27 Lacey G, Taylor G W, Areibi S. Deep learning on FPGAs: Past, present, and future. arXiv preprint arXiv: 1602.04283, 2016

28 Jouppi N P, Young C, Patil N, Patterson D, Agrawal G, Bajwa R, et al. In-datacenter performance analysis of a tensor processing unit. In: Proceedings of the 44th Annual International Symposium on Computer Architecture. Toronto, ON, Canada: ACM, 2017. 1−12

29 Dean J, Corrado G S, Monga R, Chen K, Devin M, Le Q V, et al. Large scale distributed deep networks. In: Proceedings of the 25th International Conference on Neural Information Processing Systems. Lake Tahoe, Nevada, USA: Curran Associates Inc., 2012. 1223−1231

30 Bergstra J, Bastien F, Breuleux O, Lamblin P, Pascanu R, Delalleau O, et al. Theano: Deep learning on GPUs with python. *Journal of Machine Learning Research*, 2011, **1**: 1−48

31 Collobert R, Kavukcuoglu K, Farabet C. Torch7: A Matlab-like environment for machine learning. In: BigLearn, NIPS Workshop. Martigny, Switzerland: Idiap Research Institute, 2011

32 Paszke A, Gross S, Chintala S, Chanan G. PyTorch: Tensors and dynamic neural networks in Python with strong GPU acceleration [Online], available: http://pytorch.org/, April 31, 2018

33 Abadi M, Agarwal A, Barham P, Brevdo E, Chen Z F, Citro C, et al. TensorFlow: Large-scale machine learning on heterogeneous distributed systems. arXiv preprint arXiv: 1603.04467, 2016

34 Li F F, Deng J. ImageNet: Where are we going? and where have we been?. In: Presented at the 2017 Conference on Computer Vision and Pattern Recognition [Online], available: https://www.youtube.com/watch?v=jYvBmJo7qjc, April 31, 2018

35 Hastie T, Tibshirani R, Friedman J. Unsupervised learning. *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. New York, NY, USA: Springer, 2009. 485−585

36 Bengio Y. Learning deep architectures for AI. *Foundations and Trends in Machine Learning*, 2009, **2**(1): 1−127

37 Werbos P J. Learning how the world works: Specifications for predictive networks in robots and brains. In: Proceedings of IEEE International Conference on Systems, Man and Cybernetics. New York, NY, USA: IEEE, 1987.

38 Opper M, Archambeau C. The variational Gaussian approximation revisited. *Neural Computation*, 2009, **21**(3): 786−792

39 Kingma D P, Welling M. Auto-encoding variational Bayes. arXiv preprint arXiv: 1312.6114, 2013

40 Arjovsky M, Bottou L. Towards principled methods for training generative adversarial networks. arXiv preprint arXiv: 1701.04862, 2017

41 Salimans T, Goodfellow I, Zaremba W, Cheung V, Radford A, Chen X. Improved techniques for training GANs. arXiv preprint arXiv: 1606.03498, 2016

42 Heusel M, Ramsauer H, Unterthiner T, Nessler B, Hochreiter S. GANs trained by a two time-scale update rule converge to a local Nash equilibrium. arXiv preprint arXiv: 1706.08500, 2017

43 Miyato T, Kataoka T, Koyama M, Yoshida Y. Spectral normalization for generative adversarial networks. arXiv preprint arXiv: 1802.05957, 2018

44 Papineni K, Roukos S, Ward T, Zhu W J. BLEU: A method for automatic evaluation of machine translation. In: Proceedings of the 40th Annual Meeting on Association for Computational Linguistics. Philadelphia, PA, USA: ACL, 2002. 311−318

45 Lucic M, Kurach K, Michalski M, Gelly S, Bousquet O. Are GANs created equal? A large-scale study. arXiv preprint arXiv: 1711.10337, 2017

46 Theis L, van den Oord A, Bethge M. A note on the evaluation of generative models. arXiv preprint arXiv: 1511.01844, 2015

47 Radford A, Metz L, Chintala S. Unsupervised representation learning with deep convolutional generative adversarial networks. arXiv preprint arXiv: 1511.06434, 2015

48 Zeiler M D, Taylor G W, Fergus R. Adaptive deconvolutional networks for mid and high level feature learning. In: Proceedings of the 2011 IEEE International Conference on Computer Vision. Barcelona, Spain: IEEE, 2011. 2018−2025

49 Mirza M, Osindero S. Conditional generative adversarial nets. arXiv preprint arXiv: 1411.1784, 2014

50 Odena A, Olah C, Shlens J. Conditional image synthesis with auxiliary classifier GANs. arXiv preprint arXiv: 1610.09585, 2016

51 Chen X, Duan Y, Houthooft R, Schulman J, Sutskever I, Abbeel P. Infogan: Interpretable representation learning by information maximizing generative adversarial nets. In: Proceedings of the 30th Conference on Neural Information Processing Systems. Barcelona, Spain: NIPS, 2016. 2172−2180

52 Larsen A B L, Sonderby S K, Larochelle H, Winther O. Autoencoding beyond pixels using a learned similarity metric. arXiv preprint arXiv: 1512.09300, 2015

53 Warde-Farley D, Bengio Y. Improving generative adversarial networks with denoising feature matching. In: International Conference on Learning Representations. 2017

54 Nguyen A, Clune J, Bengio Y, Dosovitskiy A, Yosinski J. Plug & play generative networks: Conditional iterative generation of images in latent space. In: Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition. Honolulu, Hawaii, USA: IEEE, 2017. 3510−3520

55 Rosca M, Lakshminarayanan B, Warde-Farley D, Mohamed S. Variational Approaches for auto-encoding generative adversarial networks. arXiv preprint arXiv: 1706.04987, 2017

56 Wu J J, Zhang C K, Xue T F, Freeman B, Tenenbaum J. Learning a probabilistic latent space of object shapes via 3D generative-adversarial modeling. In: Proceedings of the 30th Conference on Neural Information Processing Systems. Barcelona, Spain: NIPS, 2016. 82−90

57 Ioffe S, Szegedy C. Batch normalization: Accelerating deep network training by reducing internal covariate shift. In: Proceedings of the 32nd International Conference on Machine Learning. Lille, France: PMLR, 2015. 448−456

58 Salimans T, Kingma D P. Weight normalization: A simple reparameterization to accelerate training of deep neural networks. In: Proceedings of the 30th Conference on Neural Information Processing Systems. Barcelona, Spain: NIPS, 2016. 901−909

59 Xiang S T, Li H. On the effects of batch and weight normalization in generative adversarial networks. arXiv preprint arXiv: 1704.03971, 2017

60 Dietterich T G. Ensemble methods in machine learning. *Multiple Classifier Systems*. Berlin, Heidelberg, Germany: Springer, 2000. 1−15

61 Zhou Z H, Wu J X, Tang W. Ensembling neural networks: Many could be better than all. *Artificial Intelligence*, 2002, **137**(1): 239−263

62 Tolstikhin I, Gelly S, Bousquet O, Simon-Gabriel C J, Schölkopf B. AdaGAN: Boosting generative models. arXiv preprint arXiv: 1701.02386, 2017

63 Huang X, Li Y X, Poursaeed O, Hopcroft J, Belongie S. Stacked generative adversarial networks. In: Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition. Honolulu, HI, USA: IEEE, 2017.

64 Denton E, Chintala S, Szlam A, Fergus R. Deep generative image models using a Laplacian pyramid of adversarial networks. In: Proceedings of the 29th Annual Conference on Neural Information Processing Systems. Montreal, Canada: Curran Associates, Inc., 2015. 1486−1494

65 Karras T, Aila T, Laine S, Lehtinen J. Progressive Growing of GANs for improved quality, stability, and variation. arXiv preprint arXiv: 1710.10196, 2017

66 Liu M Y, Tuzel O. Coupled generative adversarial networks. In: Proceedings of the 30th Conference on Neural Information Processing Systems. Barcelona, Spain: NIPS, 2016. 469−477

67 Ghosh A, Kulharia V, Namboodiri V, Torr P H S, Dokania P K. Multi-agent diverse generative adversarial networks. arXiv preprint arXiv: 1704.02906, 2017

68 Mescheder L, Nowozin S, Geiger A. The Numerics of GANs. arXiv preprint arXiv: 1705.10461, 2017

69 Sutton R S, McAllester D A, Singh S P, Mansour Y. Policy gradient methods for reinforcement learning with function approximation. In: Proceedings of the 12th International Conference on Neural Information Processing Systems. Denver, CO, USA: MIT Press, 1999. 1057−1063

70 Grondman I, Busoniu L, Lopes G A D, Babuska R. A survey of actor-critic reinforcement learning: Standard and natural policy gradients. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 2012, **42**(6): 1291−1307

71 Pfau D, Vinyals O. Connecting generative adversarial networks and actor-critic methods. arXiv preprint arXiv: 1610.01945, 2016

72 Sutton R S, Barto A G. *Reinforcement Learning: An Introduction*. Cambridge, UK: MIT Press, 1998.

73 Goodfellow I. AMA (Ask Me Anything) about the GANs (Generative Adversarial Nets) paper [Online], available: https://fermatslibrary.com/arxiv_comments?url=https%3A%2F%2Farxiv.org%2Fpdf%2F1406.2661.pdf, April 31, 2018

74 Williams R J. Simple statistical gradient-following algorithms for connectionist reinforcement learning. *Machine Learning*, 1992, **8**(3−4): 229−256

75 Yu L T, Zhang W N, Wang J, Yu Y. SeqGAN: Sequence generative adversarial nets with policy gradient. arXiv preprint arXiv: 1609.05473, 2016

76 Fedus W, Goodfellow I, Dai A M. MaskGAN: Better text generation via filling in the. arXiv preprint arXiv: 1801.07736, 2018

77 Ganin Y, Kulkarni T, Babuschkin I, Eslami S M A, Vinyals O. Synthesizing programs for images using reinforced adversarial learning. arXiv preprint arXiv: 1804.01118, 2018

78 Goodfellow I J. On distinguishability criteria for estimating generative models. arXiv preprint arXiv: 1412.6515, 2014

79 Arora S, Ge R, Liang Y Y, Ma T Y, Zhang Y. Generalization and equilibrium in generative adversarial nets (GANs). arXiv preprint arXiv: 1703.00573, 2017

80 Qi G J. Loss-sensitive generative adversarial networks on Lipschitz densities. arXiv preprint arXiv: 1701.06264, 2017

81 Arjovsky M, Chintala S, Bottou L. Wasserstein GAN. arXiv preprint arXiv: 1701.07875, 2017

82 Rachev S T, R M. *Duality Theorems For Kantorovich-Rubinstein And Wasserstein Functionals*. Warszawa: Instytut Matematyczny Polskiej Akademi Nauk, 1990.

83 Gulrajani I, Ahmed F, Arjovsky M, Dumoulin V, Courville A. Improved training of wasserstein GANs. arXiv preprint arXiv: 1704.00028, 2017

84 Zhao J B, Mathieu M, LeCun Y. Energy-based generative adversarial network. arXiv preprint arXiv: 1609.03126, 2016

85 Wang R H, Cully A, Chang H J, Demiris Y. MAGAN: Margin adaptation for generative adversarial networks. arXiv preprint arXiv: 1704.03817, 2017

86 Iizuka S, Simo-Serra E, Ishikawa H. Globally and locally consistent image completion. *ACM Transactions on Graphics*, 2017, **36**(4): Article No. 107

87 Li Y J, Liu S F, Yang J M, Yang M H. Generative face completion. In: Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition. Honolulu, Hawaii, USA: IEEE, 2017. 5892−5900

88 Ledig C, Theis L, Huszar F, Caballero J, Cunningham A, Acosta A, et al. Photo-realistic single image super-resolution using a generative adversarial network. arXiv preprint arXiv: 1609.04802, 2016

89 Lotter W, Kreiman G, Cox D. Unsupervised learning of visual structure using predictive generative networks. arXiv preprint arXiv: 1511.06380, 2015

90 Lotter W, Kreiman G, Cox D. Deep predictive coding networks for video prediction and unsupervised learning. arXiv preprint arXiv: 1605.08104, 2016

91 Kupyn O, Budzan V, Mykhailych M, Mishkin D, Matas J. DeblurGAN: Blind motion deblurring using conditional adversarial networks. arXiv preprint arXiv: 1711.07064, 2017

92 Huang J B, Kang S B, Ahuja N, Kopf J. Image completion using planar structure guidance. *ACM Transactions on Graphics*, 2014, **33**(4): Article No. 129

93 Goodfellow I J, Shlens J, Szegedy C. Explaining and harnessing adversarial examples. arXiv preprint arXiv: 1412.6572, 2014

94 Papernot N, Carlini N, Goodfellow I, Feinman R, Faghri F, Matyasko A, et al. cleverhans v2.0.0: An adversarial machine learning library. arXiv preprint arXiv: 1610.00768, 2016

95 Yang C F, Wu Q, Li H, Chen Y R. Generative poisoning attack method against neural networks. arXiv preprint arXiv: 1703.01340, 2017

96 Shen S, Jin G, Gao K, Zhang Y. APE-GAN: Adversarial Perturbation Elimination with GAN. arXiv preprint arXiv: 1707.05474, 2017.

97 Lee H, Han S, Lee J. Generative adversarial trainer: Defense to adversarial perturbations with GAN. arXiv preprint arXiv: 1705.03387, 2017

98 Johnson-Roberson M, Barto C, Mehta R, Sridhar S N, Rosaen K, Vasudevan R. Driving in the matrix: Can virtual worlds replace human-generated annotations for real world tasks? In: Proceedings of the 2017 IEEE International Conference on Robotics and Automation. Singapore: Institute of Electrical and Electronics Engineers Inc., 2017. 746−753

99 Bousmalis K, Silberman N, Dohan D, Erhan D, Krishnan D. Unsupervised pixel-level domain adaptation with generative adversarial networks. In: Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition. Honolulu, Hawaii, USA: IEEE, 2017. 95−104

100 Shrivastava A, Pfister T, Tuzel O, Susskind J, Wang W D, Webb R. Learning from simulated and unsupervised images through adversarial training. In: Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition. Honolulu, Hawaii, USA: IEEE, 2017. 2242−2251

101 Bousmalis K, Irpan A, Wohlhart P, Bai Y F, Kelcey M, Kalakrishnan M, et al. Using simulation and domain adaptation to improve efficiency of deep robotic grasping. arXiv preprint arXiv: 1709.07857, 2017

102 Santana E, Hotz G. Learning a driving simulator. arXiv preprint arXiv: 1608.01230, 2016

103 Huang V, Ley T, Vlachou-Konchylaki M, Hu W F. Enhanced experience replay generation for efficient reinforcement learning. arXiv preprint arXiv: 1705.08245, 2017

104 Wang K F, Gou C, Zheng N N, Rehg J M, Wang F Y. Parallel vision for perception and understanding of complex scenes: Methods, framework, and perspectives. *Artificial Intelligence Review*, 2017, **48**(3): 299−329

105 Yu Y, Qu W Y, Li N, Guo Z M. Open-category classification by adversarial sample generation. arXiv preprint arXiv: 1705.08722, 2017

106 Odena A. Semi-supervised learning with generative adversarial networks. arXiv preprint arXiv: 1606.01583, 2016

107 Lamb A M, Goyal A, Zhang Y, Zhang S Z, Courville A, Bengio Y. Professor forcing: A new algorithm for training recurrent networks. In: Proceedings of the 29th Conference on Neural Information Processing Systems. Barcelona, Spain: NIPS, 2016. 4601−4609

108 Johnson J, Gupta A, Fei-Fei L. Image generation from scene graphs. arXiv preprint arXiv: 1804.01622, 2018

109 Reed S, Akata Z, Yan X C, Logeswaran L, Schiele B, Lee H. Generative adversarial text to image synthesis. arXiv preprint arXiv: 1605.05396, 2016

110 Zhu J Y, Krähenbühl P, Shechtman E, Efros A A. Generative visual manipulation on the natural image manifold. In: Proceedings of the 2016 European Conference on Computer Vision. Amsterdam, The Netherlands: Springer, 2016. 597−613

111 Brock A, Lim T, Ritchie J M, Weston N. Neural photo editing with introspective adversarial networks. arXiv preprint arXiv: 1609.07093, 2016

112 Isola P, Zhu J Y, Zhou T H, Efros A A. Image-to-image translation with conditional adversarial networks. arXiv preprint arXiv: 1611.07004, 2016

113 Wang T C, Liu M Y, Zhu J Y, Tao A, Kautz J, Catanzaro B. High-resolution image synthesis and semantic manipulation with conditional GANs. arXiv preprint arXiv: 1711.11585, 2017

114 He D, Xia Y, Qin T, Wang L W, Yu N H, Liu T Y, et al. Dual learning for machine translation. In: Proceedings of the 30th Conference on Neural Information Processing Systems. Barcelona, Spain: NIPS, 2016. 820−828

115 Zhu J Y, Park T, Isola P, Efros A A. Unpaired image-to-image translation using cycle-consistent adversarial networks. arXiv preprint arXiv: 1703.10593, 2017

116 Gatys L A, Ecker A S, Bethge M. A neural algorithm of artistic style. arXiv preprint arXiv: 1508.06576, 2015

117 Ho J, Ermon S. Generative adversarial imitation learning. arXiv preprint arXiv: 1606.03476, 2016

118 Ng A Y, Russell S J. Algorithms for inverse reinforcement learning. In: Proceedings of the 17th International Conference on Machine Learning. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2000. 663−670

119 Ziebart B D, Maas A L, Bagnell J A, Dey A K. Maximum Entropy Inverse Reinforcement Learning. In: Proceedings of the 23rd National Conference on Artificial Intelligence. Chicago, Illinois: AAAI, 2008. 1433−1438

120 Ratliff N D, Silver D, Bagnell J A. Learning to search: Functional gradient techniques for imitation learning. *Autonomous Robots*, 2009, **27**(1): 25−53

121 Kuefler A, Morton J, Wheeler T, Kochenderfer M. Imitating driver behavior with generative adversarial networks. In: Proceedings of the 2017 IEEE Intelligent Vehicles Symposium. Los Angeles, CA, USA: IEEE, 2017

122 Wang Z Y, Merel J, Reed S, Wayne G, de Freitas N, Heess N. Robust imitation of diverse behaviors. arXiv preprint arXiv: 1707.02747, 2017

123 Wang J, Yu L T, Zhang W N, Gong Y, Xu Y H, Wang B Y, et al. IRGAN: A minimax game for unifying generative and discriminative information retrieval models. In: Proceedings of the 40th International ACM SIGIR Conference on Research and Development in Information Retrieval. Shinjuku, Tokyo, Japan: ACM, 2017. 515−524

124 Frakes, W B, Baeza-Yates R, (Eds.). *Information Retrieval: Data Structures And Algorithms* (Vol. 331). Englewood Cliffs, New Jersey: prentice Hall, 1992.

125 Hu W W, Tan Y. Generating adversarial malware examples for black-box attacks based on GAN. arXiv preprint arXiv: 1702.05983, 2017

126 Gupta A, Zou J. Feedback GAN (FBGAN) for DNA: A novel feedback-loop architecture for optimizing protein functions. arXiv preprint arXiv: 1804.01694, 2018

127 Wang H W, Wang J, Wang J L, Zhao M, Zhang W N, Zhang F Z, et al. GraphGAN: Graph representation learning with generative adversarial nets. arXiv preprint arXiv: 1711.08267, 2017

128 Silver D, Schrittwieser J, Simonyan K, Antonoglou I, Huang A, Guez A, et al. Mastering the game of Go without human knowledge. *Nature*, 2017, **550**(7676): 354−359

129 Wang F Y, Zhang J J, Zheng X H, Wang X, Yuan Y, Dai X X, et al. Where does AlphaGo go: From church-turing thesis to AlphaGo thesis and beyond. *IEEE/CAA Journal of Automatica Sinica*, 2016, **3**(2): 113−120

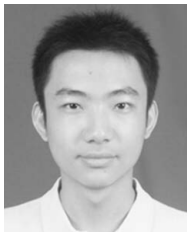
130 Li L, Lin Y L, Zheng N N, Wang F Y. Parallel learning: A perspective and a framework. *IEEE/CAA Journal of Automatica Sinica*, 2017, **4**(3): 389−395

131 Lin Y L, Li L, Dai X Y, Zheng N N, Wang F Y. Master general parking skill via deep learning. In: Proceedings of the 2017 IEEE Intelligent Vehicles Symposium. Los Angeles, CA, USA: IEEE, 2017.

132 Wang F Y, Zheng N N, Cao D P, Martinez C M, Li L, Liu T. Parallel driving in CPSS: A unified approach for transport automation and vehicle intelligence. *IEEE/CAA Journal of Automatica Sinica*, 2017, **4**(4): 577−587

133 王飞跃. 生成式对抗网络的研究进展与展望. 中国计算机学会通讯, 2017, **13**(11): 58−62

林懿伦 中国科学院自动化研究所复杂系统管理与控制国家重点实验室博士研究生. 主要研究方向为社会计算, 智能交通系统和智能汽车, 深度学习和强化学习.
E-mail: linyilun2014@ia.ac.cn
(**LIN Yi-Lun** Ph. D. candidate at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. His research interest covers social computing, intelligent transportation systems and intelligent vehicles, deep learning and reinforcement learning.)



戴星原 中国科学院自动化研究所复杂系统管理与控制国家重点实验室博士研究生. 主要研究方向为智能交通系统, 机器学习和深度学习.
E-mail: daixingyuan2015@ia.ac.cn
(**DAI Xing-Yuan** Ph. D. candidate at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. His research interest covers intelligent transportation systems, machine learning and deep learning.)

李 力 清华大学自动化系副教授. 主要研究方向为人工智能和机器学习, 智能交通系统和智能汽车. 本文通信作者.
E-mail: li-li@tsinghua.edu.cn
(**LI Li** Associate professor at the Department of Automation, Tsinghua University. His research interest covers artificial intelligence and machine learning, intelligent transportation systems and intelligent vehicles. Corresponding author of this paper.)

王 晓 中国科学院自动化研究所复杂系统管理与控制国家重点实验室助理研究员. 主要研究方向为社会计算, 社会网络结构分析及其内容挖掘, 知识自动化, 人工智能, 平行驾驶.
E-mail: x.wang@ia.ac.cn
(**WANG Xiao** Assistant researcher at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. Her research interest covers social computing, knowledge automation, artificial intelligence, and parallel driving.)

王飞跃 中国科学院自动化研究所复杂系统管理与控制国家重点实验室研究员. 国防科学技术大学军事计算实验与平行系统技术研究中心主任. 主要研究方向为智能系统和复杂系统的建模、分析与控制.
E-mail: feiyue.wang@ia.ac.cn
(**WANG Fei-Yue** Professor at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. Director of the Research Center for Computational Experiments and Parallel Systems Technology, National University of Defense Technology. His research interest covers modeling, analysis, and control of intelligent systems and complex systems.)