

Abstract本文会介绍一种全新的生成网络模型，这种模型是由对抗过程训练出来的，也就是我们会训 练两个模型：一个生成模型G能够有效捕获数据分布，另一个是判别模型D能够对G生成的数据与给定的训练数据进行比对估计。训练G的目的主要是想最大化D犯错的几率，这个过程就像是在玩双人对战游戏一样。在D与G的判别方程空间中一定存在最优解，这种情况下G生成的数据让D看起来处处都具有1/2的正确概率。由于G与D都是由多层感知器构成的，所以整个模型都可以被反向传播算法训练。在两个模型训练过程中都不需要添加马尔可夫链或者是近似推论。实验部分则演示了如何通过定性与定量评估来证明该模型的潜在实力。

1 Introduction

深度学习（Deepp Learning，DL）的承诺就是企图发现表现力更加丰富，且能表达更深层次信息的模型，这样的模型能为导入数据更有效率的表现其概率分布，从而能够让人们建立更强的人工智能程序，这样的程序可以处理很多非结构化数据，包含图像、声音与自然语言。直至今日，大多数的深度学习模型都在力争更加复杂的判别模型，通常这样的模型能够成功将大量的高维度感知数据映射到相应的类型标签。为了实现这样的优秀的模型，在本文发文时主要依靠反向传播技术（backpropagation）与随机丢弃技术（dropout），让网络使用分段结构的线性单元，这样对产生与处理梯度都很方便。深度生成模型（Deep generative models）的竞争就没有这么激烈，一方面是因为最大似然与相应策略所需要的基于概率的计算太过复杂了，另一方面就是这种分段线性结构不太能为生成模型帮上忙。于是乎我们就研究并且在本文提出了一种全新的生成模型，可以有效避免上述难题。

我们要描述的神经网络是一种对抗网络（adversarial nets）架构，生成模型需要与他的对手进行抗争，这个对手就是判别模型（discriminative model），判别模型会通过学习来尝试区分送到自己手中的数据到底是真实数据还是又生成模型瞎编的。你可以把生成模型看作一组印假钞的土匪，他们的目标就是让自己印出来的假钞十分逼真，让警察看了都认为是真钞。而判别模型就是警察，警察的目标就是自己对真钞越熟悉越好，而且能够最大程度区别真钞与假钞。两边相互竞争，一起提高水平，最终就训练出了非常厉害的GAN模型。

使用上述框架能够为许多模型与优化算法创造特定的训练方式。在这篇文章中，我们仅仅探索其中的一种方式，从随机噪声开始让生成模型通过多层神经网络来学习并生成数据，对应的判别模型也是一种多层神经网络。我们通过反向传播与随机丢弃来同时训练两个模型，然后仅通过生成模型的正向传播来生成数据。所以并不需要近似推论或马尔可夫链。

2 Related work

深度学习刚刚起步时，人们就发现了具有隐含变量的无向图方法可能会替代同类有向图方法，例如当时的限制型玻尔兹曼机（RBMs）、深度玻尔兹曼机（DBMs）以及其他相关的变种模型。这些模型中的内部作用表现为非标准化的函数乘积，通过对随机变量进行全局求和与积分来实现结果的泛化。尽管可以通过马尔可夫链蒙特卡罗（MCMC）方法进行估值计算，但计算结果及其梯度值对于除了典型的实例有效之外，其他所有实例都会产生较难处理的问题。混合性问题对于依赖MCMC的学习算法来说是一个难点。

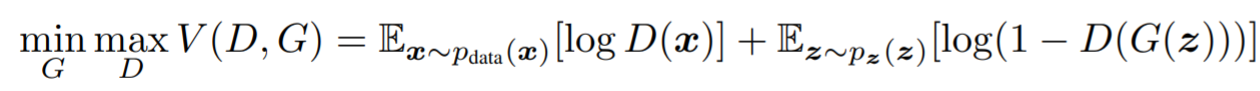
深度置信网络（DBN）是包含单个无向层和多个有向层的混合模型。虽然能够使用快速分层训练，但DBN会引起与无向和定向模型之间相关性的计算难题。

当时还存在其他算法，包括一些非估值算法与约束对数似然算法，例如得分匹配和噪声对比估计（NCE）算法，而这两者都需要将学习出来的概率密度解析为特定的归一化常数。请注意，在许多具有多层潜在变量（例如DBN和DBM）的有趣生成模型中，甚至不可能得出易处理的非标准化概率密度。像去噪自编码器和压缩自编码器这类模型，其学习规则与基于RBM的分数匹配算法非常相似，而NEC在这方面比较向本文要描述的GAN，它采用判别训练标准来拟合生成模型。不过生成模型本身不是用来拟合单独的判别模型，而是用于将生成的数据与样本区分为固定的噪声分布，因为NCE使用固定的噪声分布，所以在模型甚至在一小部分参数上学习了大致正确的分布后，学习速度会显着变慢。

最后，还有一些技术并不直接定义生成数据的概率分布，而是通过训练生成器，然后从所需分布中抽取样本，这样的实现方式具有的优点就是生成器可以被反向传播算法训练。最近期的杰出案例就是生成随机网络（GSN）框架了，它是对标准去噪自编码器的一种扩展：GSN与去噪自编码器都是由参数化的马尔可夫链定义，通过学习来不断采样出马尔可夫链的每一步。相比GSN，我们使用的对抗网络框架就完全不需要马尔可夫链进行采样了，这是因为对抗网络在采样生成时不需要经历一个完整的反馈循环，且更具备将线性单元进行分段描述的能力，这样的算法对反向传播过程进行了改良，但当其在单次反馈循环中的无界激活函数还是会出现问题。最近期的通过反向传播训练生成器的案例就是自编码变分贝叶斯和随机反向传播。

3 Adversarial nets

对抗模型的训练框架最常适配的就是让两个多层感知器相互对抗，这样它就能够通过数据学习生成模型产出的概率分布 。我们定义噪声变量 为先验输入，然后表示到数据空间的映射 ，其中G是由具有参数 加持的多层感知器表示的可微函数。同时我们再定义另一个多层感知器模型 来输出一个单独的标量。 的输出x是来自于数据还是 的差异性概率。我们训练D的目的就是最大化能够定义正确标签的概率，而这个概率既包含训练样本与正确标签的对应，也包含G的输出与正确标签对应。同一时刻我们训练G以最小化log(1-D(G(z)))，就如同下面这样。



下个小结我们就要讨论分析一下对抗网络了，从结果我们会看到只要G跟D容量足够，那么就能为人工智能赋予有效创造能力。