Abstract

我们提出了一个新的框架通过对抗过程来评估生成模型，在这个过程中，我们同时训练两个模型：一个模拟数据分布的生成模型G，一个评估样本是来自训练集还是由G生成的辨别模型D。对G的训练是为了使D出错的概率最大。这个模型的优化过程是一个“**二元极小极大博弈（minimax two-player game）**”问题。

（eg：A切蛋糕，B选蛋糕；A知道B肯定会选大的蛋糕，所以A将大蛋糕切得最小，这样对于A来说是最合理的。所以最终将蛋糕切为各一半）

在任意G 和D函数的空间中存在唯一的解，此时G模拟训练数据分布，并且D的判断正确概率每一处都是1/2。在G和D由多层感知器构成的情况下，整个系统可以用反向传播进行训练。在训练或生成样本时不需要任何马尔科夫链或展开的近似推理网络。

实验通过**对生成的样本定性和定量评估**来展示这个框架的潜力。

Introduction

深度学习的任务是发现丰富的层次模型，这些模型在人工智能领域里用来表达各种数据的概率分布，例如自然图像，包含语音的音频波形以及自然语言语料库中的符号等。到目前为止，在深度学习领域最为成功的模型就是判别式模型。成功的原因主要是基于反向传播和drop out算法，特别是具有良好梯度的分段线性单元。

而深度生成模型由于在最大似然估计和相关策略中会遇见许多难以解决的概率计算困难，而且在生成上下文时很难利用使用分段线性单元的好处，所以深度生成模型没有造成那么大的影响。

在本文提到的对抗网络框架中，生成模型对抗一个对手：一个通过学习去判别样本是来自模型分布还是数据分布的判别模型。

其中生成模型可以被认为是一个伪造团队，试图产生假货并在不被发现的情况下使用它，而判别模型类似于警察，试图检测假币。在这个游戏中的竞争驱使两个团队不断改进他们的方法，直到真假难分为止。

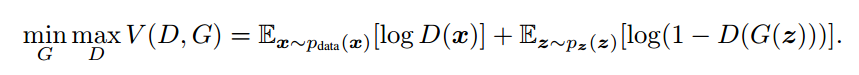
这个框架可以为多种多样的模型和优化算法提供具体的训练算法。在这篇文章中，探讨了生成模型通过将随机噪声传输到多层感知机来生成样本的例子，同时判别模型也是通过多层感知机实现的。我们称这个例子为对抗网络。这种情况下，我们只需要使用反向传播和drop out算法来同时训练两个模型，生成模型在生成样本时只使用前向传播算法，并且不需要近似推理或者是马尔科夫链。

Related work

与受限波兹曼机RBM和深度波兹曼机DBM和它们很多的变种、深度置信网络（DBN）、生成随机网络GSN等等模型相比，GAN不需要使用马尔科夫采样。并且由于对抗网络在生成阶段不需要循环反馈信息，它们能够更好的利用分段线性单元，这样可以提高反向传播的性能。

Adversarial nets

判别模型D和生成模型G的训练是关于值函数V(G, D)的极小化极大的二人博弈问题。（图灵测试）

[](https://ask.julyedu.com/uploads/questions/20170307/8c35593eb4897f1926735acb31ca9e5e.png)

（为了学习生成器关于数据x上的分布pg（生成器关于数据x上的分布），定义输入噪声的先验变量pz(z)，用G(z; θd）来代表数据空间的映射)。（这里的G是一个由含有参数θd的多层感知机表示的可微函数，另一个多层感知机D（x; θd）用来输出一个单独的标量，D(x)代表x来自于真实数据分布而不是pg的概率）训练D来最大化分配正确标签的概率，不管数据是来自于训练样例还是G生成的样例，我们同时训练G来最小化log(1-D(G(z))。换句话说，D和G的训练是关于值函数V(G，D)的极小极大二人博弈问题。

第四节中的理论分析，验证了基于训练准则可以恢复数据生成分布，当给予G和D足够的容量，即在非参数极限。

实现该训练过程时，要用迭代数值方法。并且在训练的内部循环中完成D的优化是禁止的，有限的数据集将导致过拟合。所以相反，我们在优化D的k个步骤和优化G的一个步骤之间交替。只要G变化足够慢，可以保证D保持其在最佳解附近。

实际上，方程1可能无法为G提供足够的梯度来学习。训练初期，当G的生成效果很差时，D会以高置信度来拒绝生成样本，因为它们与训练数据明显不同。

GAN的应用情境