生成对抗网络

摘要

我们提出了一个通过对抗过程来估计生成模型的新框架，其中我们同时训练两个模型：捕获数据分布的生成模型G和估计样本来自训练数据的概率的判别模型D G的训练过程是使D犯的概率最大化。 这个框架对应于一个极小的双人游戏。 在任意函数G和D的空间中，存在一个唯一的解，G随机地恢复训练数据分布，D等于1 2。 在G和D由多层感知器定义的情况下，整个系统可以用反向传播来训练。 在训练或生成样本期间，不需要任何马尔可夫链或展开的近似推理网络。 实验通过定性和定量评估生成的样本来证明框架的潜力。

1 引言

深度学习的承诺是发现丰富的层次模型[2]，它们表示人工智能应用中遇到的各种数据的概率分布，如自然图像，包含语音的音频波形和自然语言语料库中的符号。到目前为止，深度学习中最引人注目的成功涉及区分模型，通常是那些将高维度，丰富的感官输入映射到类标签的模型[14,22]。这些惊人的成功主要基于反向传播和丢失算法，使用分段线性单元[19,9,10]，它们具有特别良好的梯度。深层生成模型受到的影响较小，原因在于很难逼近极大似然估计和相关策略中出现的许多棘手的概率计算，以及难以在生成环境中利用分段线性单元的好处。我们提出了一个新的生成模型估计程序来回避这些困难。

在提出的敌对网络框架中，生成模型与敌手进行对抗：一个判别模型，用于判断样本是来自模型分布还是来自数据分布。 生成模式可以被认为是类似于造假者团队，试图产生假货币而没有被检测到，而鉴别模型类似于警察，试图检测假货币。 这场比赛的竞争促使两支球队改进他们的方法，直到假冒伪劣品从真品上无法辨认。

该框架可以产生针对多种模型和优化算法的特定训练算法。 在本文中，我们探讨了生成模型通过将随机噪声传递通过多层感知器产生样本的特殊情况，并且判别模型也是多层感知器。 我们把这个特例称为敌对网。 在这种情况下，我们可以仅使用高度成功的反向传播和丢失算法[17]来训练这两个模型，并且仅使用正向传播从生成模型中抽样。 没有近似的推理或马尔可夫链是必要的。

2 相关工作

带有潜在变量的定向图形模型的替代方法是具有潜在变量的无向图形模型，如限制玻尔兹曼机（RBMs）[27,16]，深玻尔兹曼机（DBMs）[26]及其众多变体。 这些模型中的相互作用被表示为未规范化的潜在函数的乘积，通过对随机变量的所有状态进行全局总和/积分来归一化。 这个数量（分配函数）及其梯度对于除了最微不足道的实例外都是难以处理的，虽然它们可以用马尔可夫链蒙特卡洛（MCMC）方法来估计。 混合构成依赖MCMC的学习算法的一个重要问题[3,5]。

深信念网络（DBN）[16]是包含单个无向层和多个有向层的混合模型。 虽然存在快速近似分层训练标准，但DBN会产生与无向和有向模型相关的计算困难。

也提出了不接近或限制对数似然的替代标准，如分数匹配[18]和噪声对比估计[13]。这两个要求学习的概率密度分析指定达到归一化常数。请注意，在许多具有多层潜在变量（如DBN和DBM）的有趣的生成模型中，甚至不可能推导出易处理的非标准化概率密度。一些模型，例如去噪自动编码器[30]和收缩自动编码器，其学习规则与应用于RBM的分数匹配非常相似。在NCE中，正如在这项工作中，采用了一种有区别的训练标准来适应生成模型。然而，生成模型本身不是用一个单独的判别模型来拟合，而是用来区分生成的数据与固定的噪声分布。由于NCE使用固定的噪声分布，所以在模型已经学习了观测变量的一小部分基本正确的分布之后，学习速度就会急剧下降。

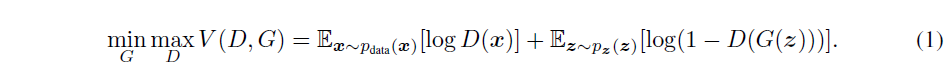
最后，一些技术不涉及明确定义概率分布，而是训练一个生成机器从所需的分布中抽取样本。这种方法的优点是这种机器可以设计成通过反向传播来训练。最近在这个领域的重要工作包括生成随机网络（GSN）框架[5]，它扩展了广义降噪自动编码器[4]：两者都可以被看作是定义一个参数化的马尔可夫链，即一个学习机器的参数执行生成马尔可夫链的一个步骤。与GSN相比，敌对网络框架不需要马尔可夫链进行抽样。因为敌对网络在生成过程中不需要反馈循环，所以它们能够更好地利用分段线性单元[19,9,10]，这可以提高反向传播的性能，但是当在反馈环路中使用时会遇到无限激活的问题。最近一些通过向后传播来生成生成机器的例子包括最近在自动编码变分贝叶斯[20]和随机反向传播[24]方面的工作。

3 对抗网络

当模型都是多层感知器时，敌对建模框架是最直接的应用。 为了学习发生器对数据x的分布pg，我们定义了一个先验输入噪声变量pz（z），然后代表到数据空间的映射为G（z;θg），其中G是由多层感知器表示的可微函数 参数θg。我们还定义了第二个多层感知器D（x; θd），输出单个标量。 D（x）表示x来自数据而不是pg的概率。 我们对D进行训练，以最大化将正确标签分配给训练样本和来自G的样本的概率。我们同时训练G以最小化

log（1-D（G（z）））：

换句话说，D和G发挥以下双值球员的极大极小游戏的价值函数V（G; D）：



在下一节中，我们提出了对抗网络的理论分析，基本上表明训练准则允许我们恢复数据生成分布，因为G和D被给予足够的容量，即在非参数极限。请参阅图1，对此方法进行较不正式的教学解释。在实践中，我们必须使用迭代的数值方法来实现游戏。在训练的内部循环中优化D以完成是计算禁止的，并且在有限的数据集上会导致过度拟合。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。这导致D维持在最佳解决方案附近，只要G足够慢地变化。这个策略类似于SML / PCD [31,29]训练的方式，从一个学习步骤到下一个学习步骤保持马尔可夫链的样本，以避免作为内部学习循环的一部分在马尔可夫链中燃烧。程序在算法1中正式提出。

在实践中，方程1可能不能提供足够的梯度让G学好。 在学习初期，当G很差时，D可以高信度地拒绝样本，因为它们与训练数据明显不同。 在这种情况下，log（1-D（G（z）））饱和。 我们可以训练G来最大化logD（G（z）），而不是训练G来最小化log（1-D（G（z）））。 这个目标函数导致了G和D动力学的相同的固定点，但在学习的早期提供了更强的梯度。

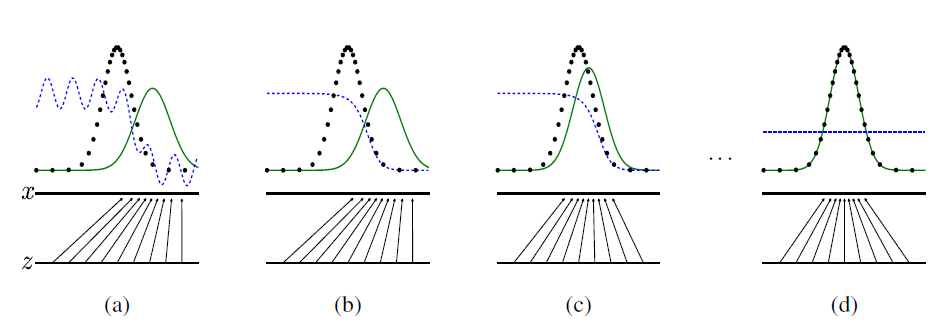


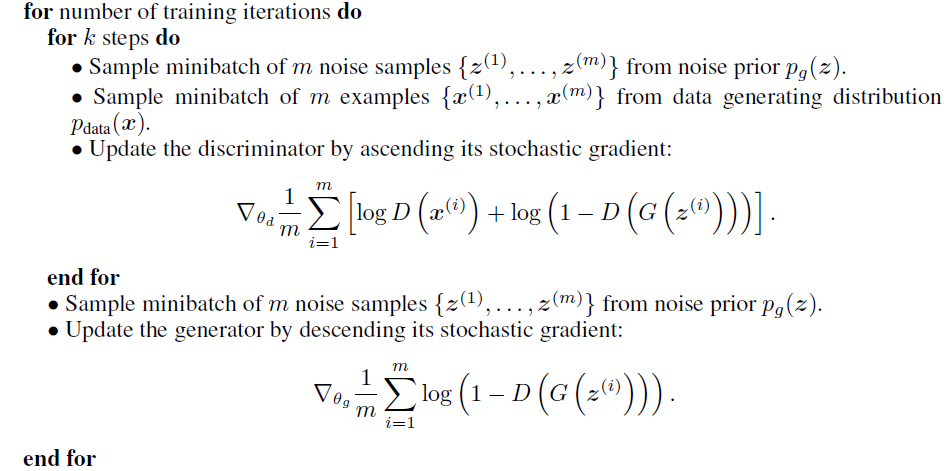
图1：通过同时更新判别分布（D，蓝色，虚线）来训练生成对抗网络，以便从生成分布pg（G）的数据生成分布（黑色，虚线）px中区分样本， （绿色，实线）。下面的水平线是从中采样z的区域，在这种情况下是均匀的。上面的水平线是x的域的一部分。向上的箭头显示映射x = G（z）如何在变换的样本上施加非均匀分布pg。 G在高密度区域收缩并在低密度区域扩大。 （a）考虑近似收敛的敌对配对：pg类似于pdata，D是部分准确的分类器（b）在算法D的内部循环中，训练样本与数据进行区分，收敛于D（x）= pdata （x）pdata（x）+ pg（x）。 （c）在更新到G之后，D的梯度已经引导G（z）流向更可能被分类为数据的区域。 （d）经过几个步骤的训练，如果G和D有足够的能力，他们将达到两个都不能提高的点，因为pg = pdata。鉴别器不能区分这两个分布，即D（x）= 12。

4 理论结果

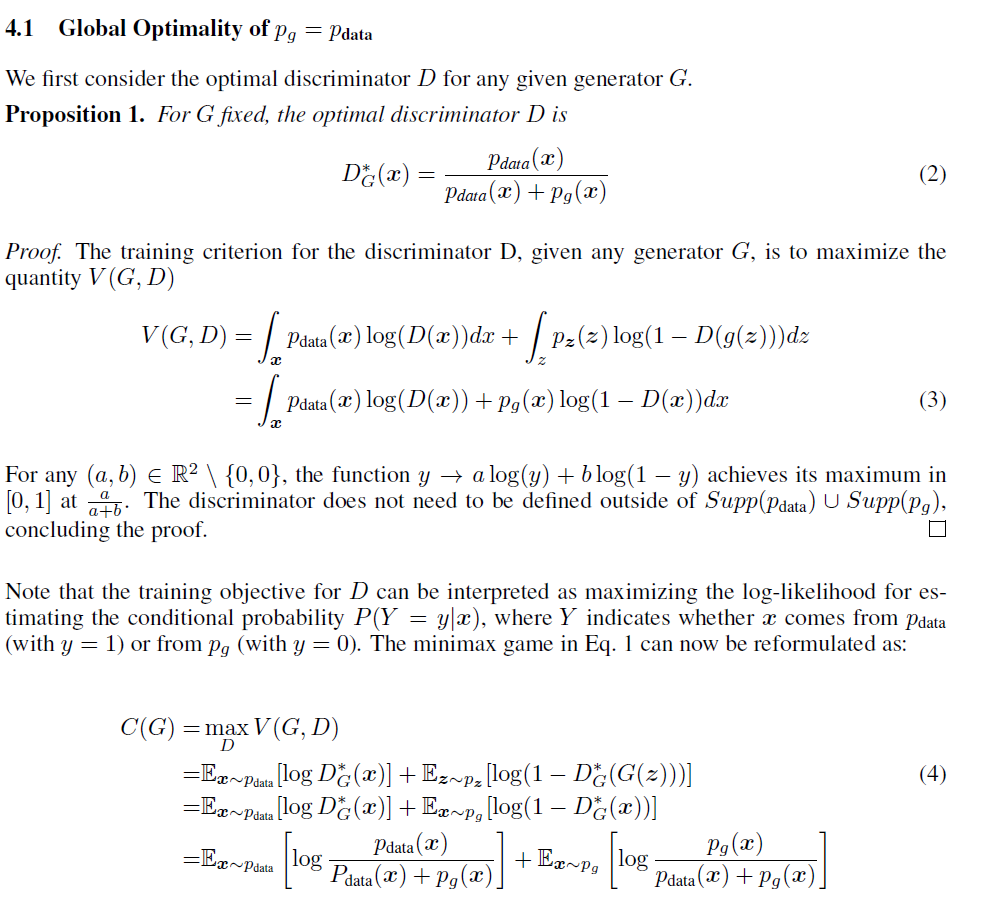
发生器G隐含地将概率分布pg定义为当z≥1时获得的样本G（z）的分布。PZ。 因此，如果给定足够的容量和训练时间，我们希望算法1收敛到一个好的pdata估计量。 本部分的结果是在非参数设置下完成的，例如， 我们通过研究概率密度函数空间中的收敛来表示具有无限容量的模型。

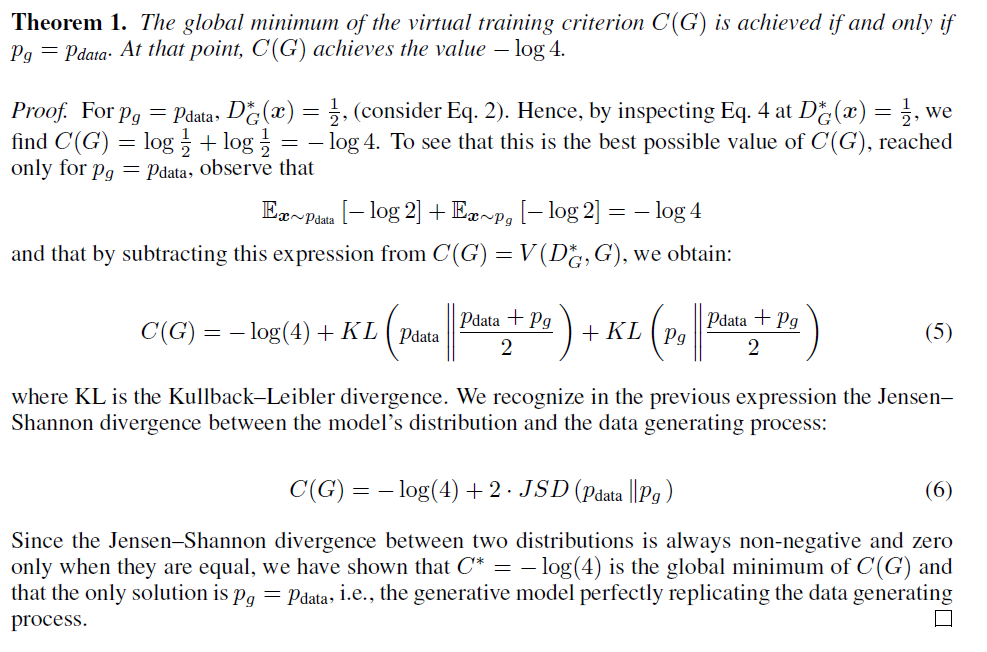
我们将在4.1节中展示这个minimax游戏对于pg = pdata有一个全局最优值。 然后，我们将在4.2节展示算法1优化公式1，从而获得期望的结果。

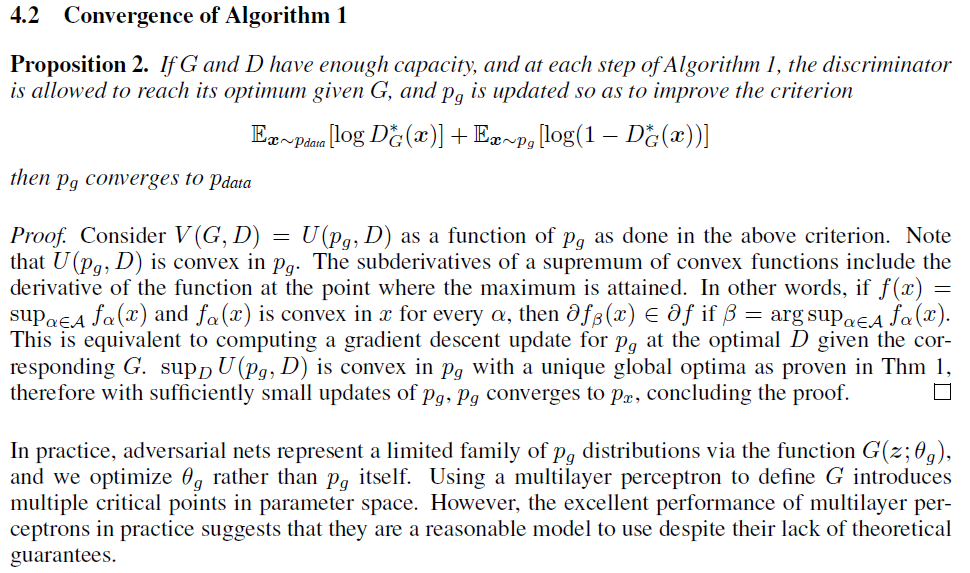
算法1生成敌对网络的Minibatch随机梯度下降训练。 应用于鉴别器的步数k是一个超参数。 在我们的实验中，我们使用k = 1，最便宜的选项。



基于渐变的更新可以使用任何标准的基于渐变的学习规则。 我们在实验中使用了动力







5 实验

我们训练了对抗网络的一系列数据集，包括MNIST [23]，多伦多人脸数据库（TFD）[28]和CIFAR-10 [21]。 发生器网络使用了整流器线性激活[19,9]和S形激活的混合，而鉴别器网络使用了maxout [10]激活。 辍学[17]被应用于训练鉴别网。 虽然我们的理论框架允许使用发电机中间层的压降和其他噪声，但是我们只使用噪声作为发电机网络最底层的输入。

我们通过拟合高斯Parzen窗口到G生成的样本并报告在这个分布下的对数似然估计测试集合数据在pg下的概率。 这个σ参数

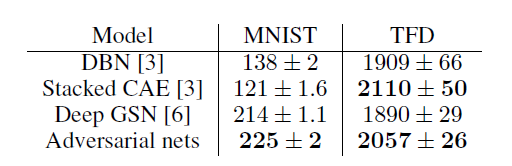


表1：Parzen基于窗口的对数似然估计。 在MNIST上报告的数字是样本在测试集合上的平均对数似然，跨越示例计算的平均值的标准误差。 在TFD上，我们计算了数据集折叠的标准误差， 使用每个折叠的验证集进行选择。 在TFD上？ 在每个倍数上进行交叉验证并计算每个倍数的平均对数似然。 对于MNIST，我们将其与实数值（而不是二元）版本的数据集的其他模型进行比较。

的高斯是通过验证集上的交叉验证获得的。 这个程序是在Breuleux等人介绍的。 [8]并用于各种生成模型，其确切的可能性是不容易的[25,3,5]。 结果报告在表1中。这种估计可能性的方法具有稍高的方差，并且在高维空间中表现不佳，但是这是我们所知道的最好的方法。 可以抽样但不估计可能性的生成模型的进展直接推动了如何评估这些模型的进一步研究。

在图2和图3中，我们显示了训练后从发生器网络中抽取的样本。 虽然我们没有声称这些样本比现有方法产生的样本更好，但我们认为这些样本至少与文献中更好的生成模型相竞争，并突出了对抗框架的潜力。

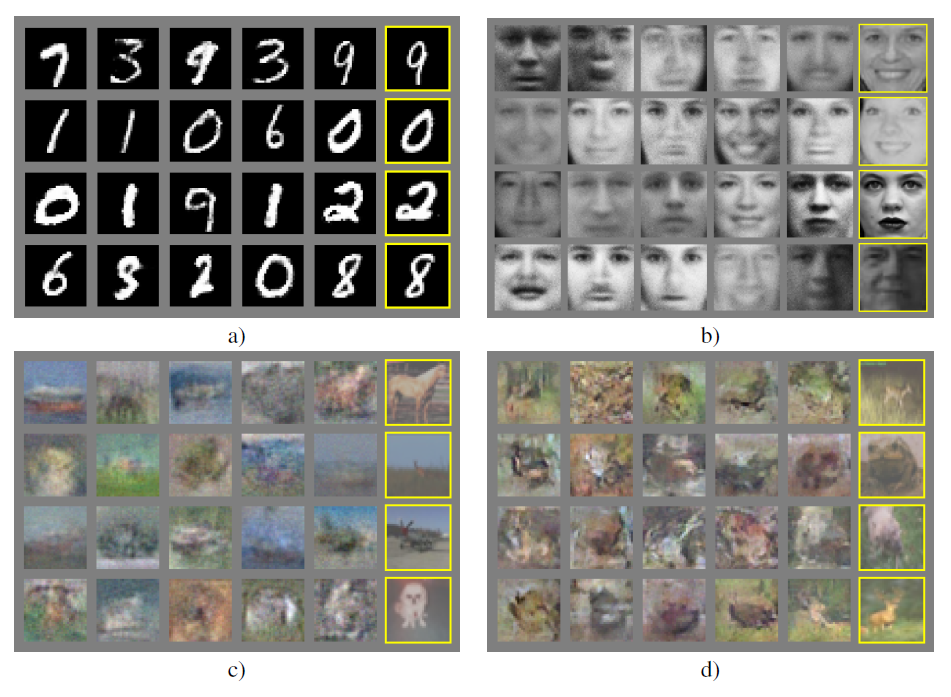


图2：来自模型的样本的可视化。 最右边的列显示了邻近样本的最近训练样本，以证明模型没有记住训练集。 样本是公平的随机抽签，而不是樱桃采摘。 与大多数其他深度生成模型的可视化不同，这些图像显示了模型分布的实际样本，而不是给定隐藏单元样本的条件均值。 此外，这些样本是不相关的，因为抽样过程不依赖于马尔可夫链混合。 a）MNIST b）TFD c）CIFAR-10（全连接模型）d）CIFAR-10（卷积鉴别器和“去卷积”发生器）

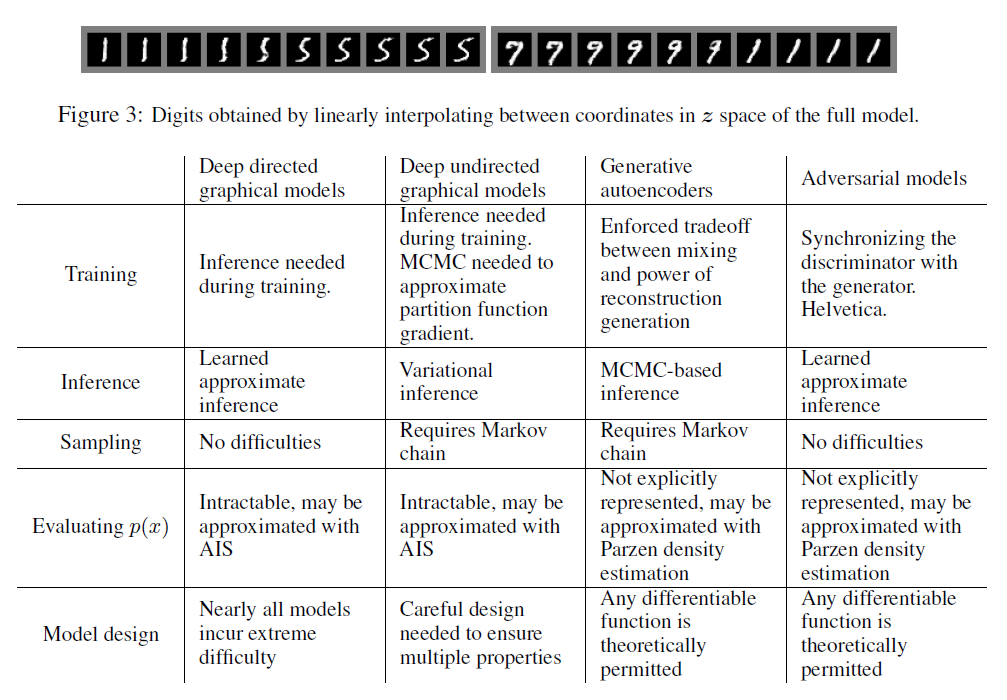


表2：生成建模方面的挑战：对涉及模型的每个主要操作的深度生成建模的不同方法所遇到的困难的总结。

6 优点和缺点

这个新的框架与先前的建模框架相比具有优点和缺点。 缺点主要是没有pg（x）的显式表示，并且D在训练过程中必须与G很好地同步（特别是，为了避免“Helvetica场景”，G不能被更新地训练得太多， 其中G将z的太多值坍缩到x的相同值以具有足够的多样性来对pdata进行建模），就像玻尔兹曼机器的负链必须在学习步骤之间保持最新一样。 它的优点是不需要马尔可夫链，只有反向传播被用来获得梯度，在学习过程中不需要推理，并且可以将各种各样的功能结合到模型中。 表2总结了生成敌对网与其他生成建模方法的比较。

上述优点主要是计算性的。 对冲模型也可以从发电机网络获得一些统计上的优点，而不是直接用数据例子更新，而只是通过鉴别器中流动的梯度。 这意味着输入的组件不会直接复制到生成器的参数中。 敌对网络的另一个优点是它们可以表示非常尖锐甚至退化的分布，而基于马尔可夫链的方法要求分布有些模糊，以便链能够在模式之间进行混合。

7 结论和未来的工作

这个框架承认了许多直接的扩展：

1.一个条件生成模型p（x j c）可以通过将c作为输入添加到G和D来获得。

2.学习近似推理可以通过训练一个辅助网络来预测给定的x。 这与唤醒算法[15]训练的推理网类似，但是其优点是可以在发电机网络完成训练之后对固定的发电机网络训练推理网络。

3.通过训练一系列共享参数的条件模型，可以对所有的条件p（xS j x6S）进行近似建模，其中S是x的下标的一个子集。 从本质上讲，可以使用敌对网络来实现确定性MP-DBM的随机扩展[11]。

4.半监督学习：当有限的标记数据可用时，来自鉴别器或推理网络的特征可以提高分类器的性能。

5.提高效率：通过分配更好的协调G和D的方法或从培训中确定样本z的更好的分布，可以大大加速培训。

本文已经证明了对抗建模框架的可行性，表明这些研究方向可能是有用的。

致谢

我们要感谢Patrice Marcotte，Olivier Delalleau，Kyunghyun Cho，Guillaume Alain和Jason Yosinski进行有益的讨论。 Yann Dauphin与我们分享了他的Parzen窗口评估代码。 我们要感谢Pylearn2 [12]和Theano [7,1]的开发者，特别是Fr'ed'eric Bastien，他特别为了这个项目而特意冲击了Theano特性。 Arnaud Bergeron为LATEX排版提供了急需的支持。 我们还要感谢CIFAR和加拿大研究会的资助，加拿大计算机学会和Calcul Qu'ebec提供计算资源。 伊恩·古德费洛（Ian Goodfellow）受到2013年深度学习谷歌奖学金的支持。 最后，我们要感谢Les Trois Brasseurs激发我们的创造力。