生成性对抗式主动学习

摘要
我们提出一种使用生成式对抗网络(GAN)的新的主动学习方法。与常规主动学习不同，我们自适应地合成用于查询的训练实例以提高学习速度。我们的方法优于在主动学习实验仅使用GAN的随机生成方式。与其他算法相比，我们证明了所提出算法在各种数据集中的有效性。据我们所知，这是使用GAN的第一个主动学习工作。

1.介绍

近年来最令人兴奋的机器学习突破之一是生成式对抗网络(GAN)(Goodfellow等，2014)。它通过发现一个双人对手游戏的纳什均衡训练一个生成模型。其在复杂域中生成样本的能力使得主动学习者能够根据需要合成训练样本的新的可能性，而不是依赖于从给定池中选择要查询的实例。
在分类设置中，给定未标记数据样本池和固定标签预算，主动学习算法通常从池中策略性地选择训练样本以最大化训练的分类器的准确性。这些算法的目的是降低标签复杂性。这样的方法称为基于池的主动学习。这种基于池的主动学习方法如图1(a)所示。
简而言之，我们建议使用生成式对抗网络来合成适应当前学习者的信息性培训实例。然后我们要求人的预测标记这些实例。将标记的数据添加回训练集以更新学习者。此协议迭代执行，直到达到标签预算。该过程如图1(b)所示。

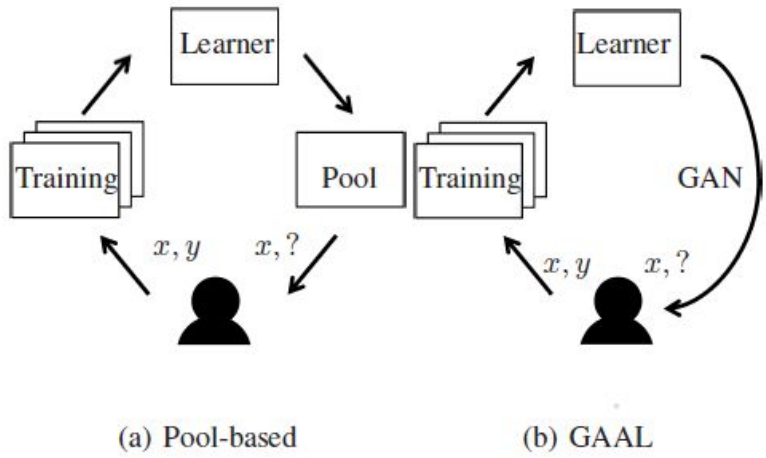


图1.(a)基于池的主动学习情景。学习者从给定的未标记池中选择用于查询的样本。(b)GAAL算法。学习者使用GAN合成用于查询的样本。

这项工作的主要贡献如下：
•据我们所知，这是使用深生成模型的第一个主动学习工作[1]。事实上，这是第一个工作，报告主动学习合成图像分类令人满意的结果。(Settles，2010;Lang和Baum，1992)。提出的框架可以为未来的GAN应用在主动学习奠定基础。
•因为我们不选择查询来自给定池的样本，所以我们活跃学习者的表现可能不受完全监督学习的表现的上限。通过训练的发生器的足够的容量，我们的方法允许我们对生成的实例进行控制，这些实例可能对以前的主动学习者是不可用的。虽然我们不声称我们的方法总是优于以前的主动学习者在准确性，在某些情况下，它产生的分类性能，即使通过一个完全监督的学习方案不可能实现。
•我们进行初步实验，比较我们的主动学习方法和自学教学学习。结果是有希望的。

2.相关工作

我们的工作涉及两个主题，主动学习和深生成模型。主动学习算法可以分为基于流的，基于池的和通过查询综合的学习。历史上，基于流和基于池的是主动学习的两种流行场景(Settles，2010)。

[1] (Papernot等人)的附录提到三个主动学习尝试，但没有报告数值结果。 我们的方法也不同于那些尝试。

我们的方法属于查询综合的类别。通过查询的早期主动学习仅在简单域(例如X={0,1}3，见(Angluin，1988;2001))中获得良好的结果。在(Lang和Baum，1992)中，作者合成学习查询，并使用人的预测训练一个神经网络来分类手写字符。
然而，他们报告了由于学习者产生的图像有时不能被人的预测识别的差的结果。我们将报告类似任务的结果，如区分5和7，显示我们主动学习计划的进步。图2比较了(Lang和Baum，1992)中的方法和我们的算法产生的图像样本。

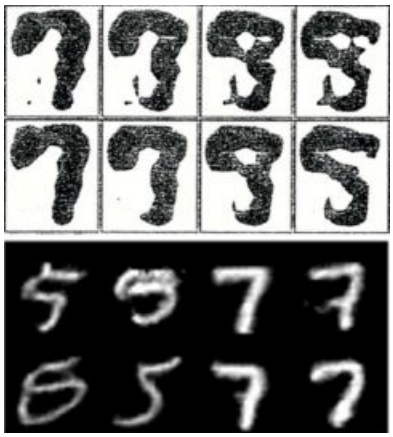


图2.(上)由神经网络合成的用于手写数字识别的图像查询。资料来源：(LangandBaum，1992)。(底部)通过我们的算法GAAL合成的图像查询。

来自(Tong和Koller，2002)的流行的SVMactive算法是用于SVM的高效的基于池的主动学习方案。他们的方案是我们也采用的不确定性抽样原则的一个特殊例子。
(Jain等人，2010)减少了通过SVMactive所采用的数据库的彻底扫描。我们的算法具有相同的优点，即不需要在每次主动学习迭代时测试数据库中的每个样本。
在半监督学习和主动学习中已经存在生成模型的一些应用。以前，(Nigam等人，2000)提出了一种基于生成模型的文本分类的半监督学习方法。(Hospedales等人，2013)将高斯混合模型应用于主动学习。在这项工作中，生成模型充当分类器。与这些方法相比，我们应用生成模型直接合成训练数据。这是一个更具挑战性的任务。据我们所知，这是使用深层的第一个主动学习工作生成模型。
我们的算法的一个组成部分是GAN模型的突破性工作(Goodfellow等人，2014)。我们的方法是GAN在主动学习中的应用。我们的方法也涉及到(Springenberg，2015)，研究了半监督设置的GAN。然而，我们的任务是主动学习，这不同于他们讨论的半监督学习。我们的工作与自学教学的学习算法(Raina等人，2007)共享共同的力量，两种方法使用未标记的数据来帮助任务。在5.4节中，我们将我们的算法与自学教学的学习算法进行比较。
据我们所知，使用GAN主动学习的唯一前面提到的是(Papernot等人)的附录。作者在其中讨论了三个减少查询数量的尝试。在第三次尝试中，他们生成合成样本，并通过信息内容排序，而我们通过解决优化问题自适应生成新查询。在这项工作中没有报告主动学习数值结果。

3.背景

我们简要介绍主动学习和生成式对抗网络中的一些重要概念。

3.1.主动学习

在PAC学习框架(Valiant和G.，1984)中，标签复杂度描述了找到具有误差a的假设所需的标记实例的数量。被动监督学习的标签复杂度，即使用所有标记的样本作为训练数据，是O(dǫ)(Vapnik和Vapnik，1998)，其中d是假设类H的VC维度。主动学习旨在减少标签复杂性通过选择最信息实例用于查询，同时获得低错误率。例如，(Hanneke，2007)证明了(Cohn等人，1994)的主动学习算法具有标签复杂度边界O(dǫlog1ǫ)，从而减少了被动实体所需的标记实例的数量的理论界限监督学习。理论上，主动学习算法的渐近精度不能超过监督学习算法的渐近精度。在实践中，如我们将在实验中证明的，在一些情况下，我们的算法可能能够实现比被动监督学习更高的准确度。
基于流的主动学习决定是否查询流入的实例。典型的方法包括(Beygelzimer等人，2008;Cohn等人，1994;Dasgupta等人，2007)。在这项工作中，我们将重点关注基于池的和

查询合成方法。
在基于池的主动学习中，学习者基于某个标准从现有池中选择未标记的实例。一些基于池的算法通过使用聚类技术或最大化多样性度量来进行选择，例如，(Brinker;Xuetal。，2007;DasguptaandHsu，2008;NguyenandSmeulders;Yangetal。，2014;Hoietal。，2009)。另一种常用的基于池的主动学习原理是不确定性抽样。它相当于查询最不确定的实例。例如，(Tong和Koller，2002;Campbell等，2000)中的算法查询最接近支持向量机的决策边界的实例的标签。图3(a)示出了该选择过程。数学上，让P是未标记实例的池，并且f=Wϕ(x)+b是分离超平面。ϕ是由SVM内核引入的特征图。SVMactive算法(Tong和Koller，2002)通过最小化到超平面的距离(或其代理)来选择要查询的新实例

$$\min_{x\in P} \|W\phi(x)+b\|. \qquad (1)$$

这个公式可以通过在可分离情况下的版本空间理论(Tong和Koller，2002)或在不可分离情况下的其他分析来证明，例如(Campbell等人，2000;Bordes等人，2005)。这种简单有效的方法广泛应用于许多研究，例如(Goh等人，2004;Warmuth等人，2002)。

3.2. 生成对抗网络

生成式对抗网络(GAN)是由(Goodfellow等人，2014)发明的新颖的生成模型。它可以看作是发生器G和鉴别器D之间的以下双玩家最小最大游戏：

$$\min_{\theta_1}\max_{\theta_2}\left\{\mathbb{E}_{x\sim p_{\text{data}}}\log D_{\theta_1}(x)+\mathbb{E}_z\log(1-D_{\theta_1}(G_{\theta_2}(z)))\right\}, \qquad (2)$$

其中pdata是真实数据的基础分布，z是均匀分布的随机变量。D和G各自具有其自己的参数集合θ1和θ2。通过解决这个游戏，获得生成器G。在理想情况下，给定随机输入z，我们有G(z)～pdata。然而，发现这种纳什均衡在实践中是一个困难的问题。由于D和G的非凸性，不存在用于找到纳什均衡的理论保证。梯度下降型算法通常用于解决该优化问题。
自(Goodfellow等人，2014)以来已经提出了GAN的一些变体。(Radford等人，2015)的作者使用GAN与深度卷积神经网络结构在计算机视觉(DCGAN)中的应用。DCGAN产生良好的结果并且相对稳定。条件GAN(Gauthier，2014;Dosovitskiy等，2014;Mirza和Osindero，2014)是GAN的另一个变体，其中发生器和鉴别器可以受其他变量，例如图像的标签的影响。可以控制这样的发生器以从特定类别产生样品。(Chenetal。，2016)提出了使用无监督学习来学习解析表示的信息GAN。已经提出了一些更新的GAN模型。(Salimansetal。，2016)提出了一些改进的训练GAN的技术。Gan，WassersteinGAN的另一个潜在重要的改进已经由(Arjovsky等人，2017)提出。作者提出了一种替代训练GAN，可以避免不稳定性，如模式崩溃与理论分析。他们还提出了一个度量来评估这一代的质量，这对未来的GAN研究可能是有用的。WassersteinGAN对我们主动学习框架的可能应用留给未来的工作。
GAN的发明触发了各种新型应用。(Kadurin等人，2016)应用对抗自动编码器进行药物发现。(Yeh等人，2016)使用GAN在绘画任务中执行图像。(Zhuetal。，2016)提出iGAN将草图变成逼真的图像。(Ledig等人，2016)将GAN应用于单图像超分辨率。我们的研究是主动学习的第一个GAN应用程序。
对于GAN的综述，读者可参考(Goodfellow等，2016)。

4.生成对抗主动学习

在本节中，我们介绍称为生成对抗主动学习(GAAL)的主动学习方法。它结合查询综合与不确定性抽样原理。
我们的方法的直觉是生成当前学习者不确定的实例，即应用不确定性采样原理。为此，我们制定优化问题

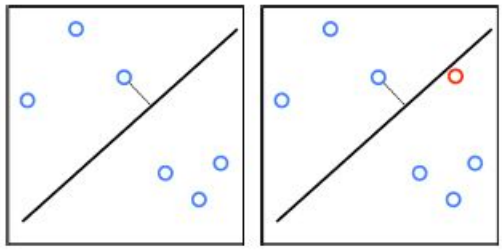
$$\min_z \left\{\mathrm{L}_{\text{active}}(G(z))+\mathrm{L}_{\text{reg}}(G(z))\right\}, \qquad (3)$$

其中z是潜在变量，G通过GAN算法获得。第一项Lactive(G(z))是用于生成信息性主动学习查询的损失函数。一个Lactive(G(z))的小值表示生成的实例G(z)对学习者是信息性的。第二项Lreg(G(z))是确保产生的样本的质量的正则化项。在上述对抗设置中，它惩罚低质量样本。

损失函数的一个特殊选择是基于3.1节的不确定性抽样。在这项工作中的不确定性抽样的这种具体适应可以更好地被创造为不确定性生成以指示它不是基于池的抽样方案。在具有判定函数f(x)=Wϕ(x)+b的分类器的设置中，到判定边界的(代理)距离是kw(x)+bk。类似于(1)的直觉，给定经训练的生成函数G，我们将主动学习合成作为以下优化问题进行公式化：

$$\min_z \left\{ \frac{1}{2} \|W^\top \phi(G(z)) + b\|^2 + \lambda \log(1 - D(G(z))) \right\}, \quad (4)$$

其中z是潜变量，λ是可调参数。图3(b)说明了GAAL的直觉。与图3(a)中的基于池的主动学习相比，我们希望它能够生成比现有池中可用的更多的信息实例。



(a)SVM活动　　(b)GAAL

图3.(a)SVM活动算法选择最接近边界的实例来查询预测。(b)GAAL算法合成对当前学习者有信息的实例。与现有池中的其他实例相比，合成的实例可能对学习者更有信息。

在被标记之后，该优化问题的解(G(z))将被用作下一次迭代的新训练数据。我们在算法1中概述我们的过程。

算法1　生成对抗主动学习(GAAL)

通过求解(2)训练用于所有未标记的数据的生成器G

通过随机抽取初始化标记的训练数据集S.

对一小部分数据进行标签

重复

根据当前学习者通过如下递减梯度求解优化问题(4)：

$$\nabla_z \{ \frac{1}{2} \|W^\top \phi(G(z)) + b\|^2 + \lambda \log(1 - D(G(z))) \}$$

使用解决方案{z1，z2，。。。}和G用于生成查询的实例

标签{G(z1)，G(z2)，...，。。。}为人的预测

将标记数据添加到训练数据集S并重新训练学习者，更新W，b

直到达到标签预算

函数(3)提供了使用其它损失术语的灵活性。例如，在逻辑回归作为选择分类器的情况下，主动学习中的不确定抽样原理对应于有效损失项选择

Lactive(z)=-h(G(z))logh(G(z))-(1-h(G(z)))log(1-h(G(z)))，其中 $h(x) = \frac{1}{1+e^{-\theta x}}$ 是分类器的参数，类似于(4)中的W，b。该公式的推导类似于(Joshi等人，2009)中的熵测量。

还可以使用现有技术的分类器，例如卷积神经网络。为此，我们用卷积神经网络的前馈函数替换函数(4)中的特征映射ϕ。在这种情况下，线性SVM将成为网络的输出层。

在训练GAN时，我们遵循(Radford等人，2015)提出的详细的程序。优化问题(4)是非凸的，可能有许多局部最小值。一个典型的目的是找到良好的局部最小值而不是全局最小值。我们使用具有动量的梯度下降算法来解决这个问题。我们还定期重新启动梯度下降以找到其他解决方案。使用反向传播计算D和G的梯度。

或者，我们可以最大化所生成的样本的多样性，而不是依赖于不确定性原理。一些主动学习方法依赖于最大化多样性度量，例如香农熵。在我们的例子中，我们可以用多样性量度替代目标函数(3)中的第一项，如(杨等人，2014;Hoi等人，2009)中提出的，从而最大化多样性。这种替代方法的评价留待未来工作。

5.实验

我们在MNIST，SVHN和CIFAR-10数据集的图像分类中执行主动学习实验。我们还比较了我们的自学教学方法，一种转移学习方法。在我们的实验中使用的GAN实现是对公开可用的Tenso Flow DCGAN实现的修改[2]。DCGAN的网络架构在(Radford等人，2015)中描述。
在我们的实验中，我们专注于二进制分类。虽然这可以推广到使用一对一或一对全方案的多个类(Joshi等人，2009)。我们使用线性SVM作为选择的分类器，尽管我们也测试了逻辑回归，其精度在大多数情况下略差。尽管可以使用具有更高精度的分类器(例如，卷积神经网络)，但是我们的目的不是实现绝对高精度，而是研究不同主动学习方案之间的相对性能。在我们的实验中比较以下方案。

- 在算法1中提出的生成对抗主动学习(GAAL)算法。
- 使用常规GAN生成训练数据。我们称之为被动GAN。
- Tong＆Koller的SVM主动算法(Tong和Koller，2002)。
- 被动随机抽样，从随机抽样未标记池的实例。
- 被动监督学习，即使用池中的所有样本训练分类器。
- 自学教学(Rainaetal，2007)。我们用50个随机选择的样本初始化训练集。算法每次进行一批10个新样本。在我们的实验中，六个不同的人类贴标签者参与了标签工作。提供给贴标机的典型产生的样品示于图4中。

5.1.手写数字

MNIST数据集是具有60000个训练样本和10000个测试样本的著名的图像分类数据集。训练集和测试集遵循相同的分布。我们执行区分5和7的二进制分类实验，如(Lang和Baum，1992)。我们使用来自MNIST训练集的5和7的所有图像作为我们的未标记池来训练发生器G.与传统的主动学习不同，我们不在初始迭代之后从池中选择新的样本。相反，我们应用算法1来生成训练查询。对于生成器D和G，我们使用类似于(Goodfellow等人，2014;Radford等人，2015;Salimans等人，2016)的网络结构。我们使用线性SVM作为我们的分类器，尽管其他分类器也可以用于主动学习(Tong和Koller，2002;Schein和Ungar，2007;Settles，2010)。我们在一个测试集上测试训练分类器，其遵循不同分布作为训练集。目的是说明GAAL算法的自适应能力。为此，我们使用(LeCun等人，1989)的USPS数据集作为具有标准预处理的测试集。这个测试设置与我们在后面的实验中讨论的自学教学设置有关。

图4.GAAL生成的样本。(上)MNIST数据集。(底部)CIFAR-10数据集。

图5显示了测试算法的精度图。当使用完全训练集（11000训练图像）时，完全监督的精度在70.44%。随机抽样方案的准确性稳定地接近该水平。它接近于250个训练样本的监督精度。

[2] https://github.com/carpedm20/DCGAN-tensorflow

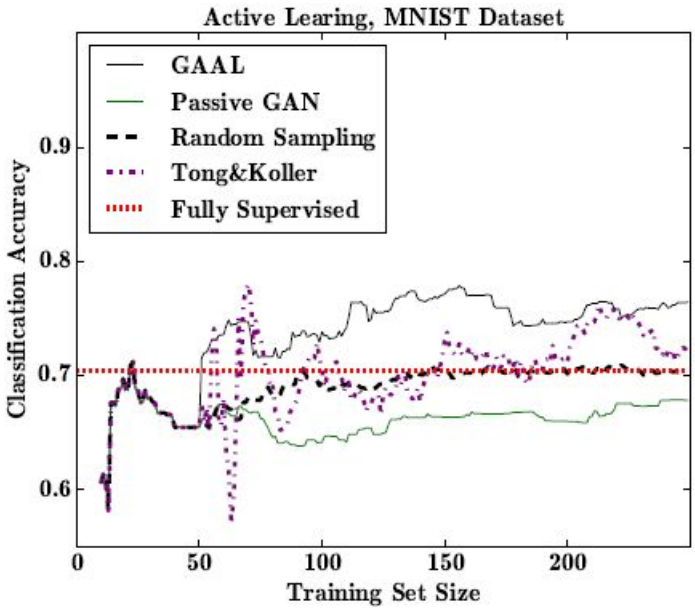


图5. MNIST数据集的主动学习结果，分类为5和7.结果在5次运行中取平均值。将完全监督的学习准确度绘制为水平线用于比较。

另一方面，GAAL能够实现比完全监督方案更好的精度。与250个训练样本，它达到大约76.42%的精度，提高超过监督学习。显然，Tong＆Koller和随机抽样的精度将最终收敛到完全监督学习的准确性。
注意，对于Tong＆Koller算法，通过训练池的穷尽扫描并不总是实用的。在大型数据集中，可以使用59的著名技巧(Smola和Sch¨olkopf，2000)。

5.2.SVHN

街景房屋号码(SVHN)数据集包含超过600000个颜色32×32的房子号码图像。与MNIST数据集相比，由于其高尺寸，它显著更具挑战性。我们对SVHN数据集执行主动学习实验。图6显示了该实验的精确度图。

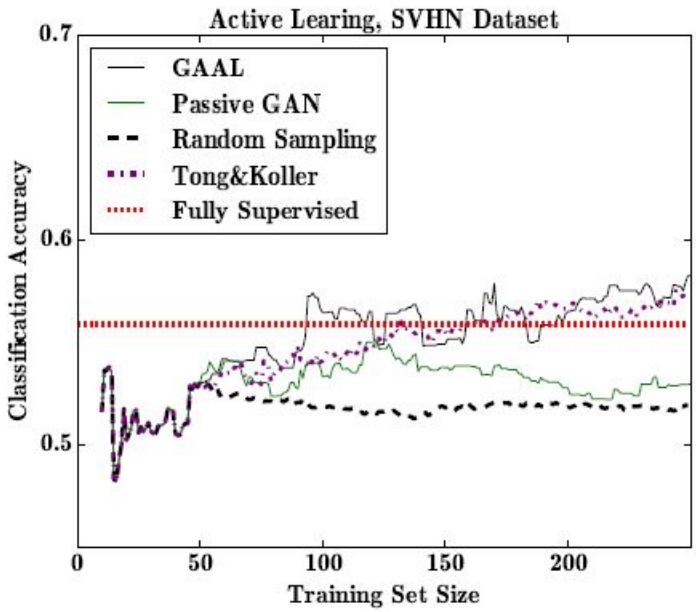


图6.SVHN数据集的主动学习结果，对5和7分类。

被动监督学习使用池中的所有数据实现56%的准确性，这略胜于随机猜测。GAAL方法能够实现比完全监督学习更高的精度，再次击败随机抽样和随机GAN生成。Tong＆Koller的算法达到与GAAL类似的精度，达到250个样本大小。然而，随着训练集大小的增加，其精度将

可预见地下降到被动监督学习。
GAAL算法没有证明在该实验中与在MNIST实验中一样大的改进。这可能是因为测试和训练集合遵循相同的分布。这激励了我们后来自学教学的学习实验。
在这个数据集(以及CIFAR-10数据集)中，我们的人类标记者注意到显著更高的生成失败的机会，例如，实例不能表示任一类别。这可能是因为尺寸明显高于MNIST数据集。因此，我们要求标签者只标记他们可以区分的样品。我们推测GAN最近的改进，例如(Salimans等人，2016;Arjovsky等人，2017)可以帮助减轻这个问题。解决这个限制将留待将来的研究。

5.3. CIFAR-10

CIFAR-10数据集的训练集包括来自10个类别的50000个32×32彩色图像。在主动学习环境中，人们可以推测通过对猫样狗或狗样猫的训练来区分猫和狗的可能性。在实践中，我们的人类标签者未能自信地识别大多数生成的猫和狗图像。图7显示了生成的样品。

图7.猫和狗类别中生成的样本。对于人类标签者来说，自信地识别这些图像是具有挑战性的。

为此，我们对汽车和马类进行二分类主动学习。对于人类贴标签者来说，识别汽车和马身体形状是相对容易的。图8显示了结果。在这个实验中，GAAL执行与随机抽样方案同等并且优于被动GAN方案。然而，它不能击败Tong＆Koller的主动学习算法。这可能是因为较高的维度需要更主动的学习迭代以使GAAL执行得更好。(Salimans等人，2016年)的作者报道了生成高分辨率的动物图像的尝试，但得到了错误的解剖结构。我们将此任务为今后的研究。可能具有改进的技术，例如(Arjovsky等人，2017)。

5.4与自学教学学习比较

GAAL和自学教学学习(雷纳等人，2007)的一个共同强项是，都利用了未标记的数据，以帮助与分类任务。正如我们在MNIST实验中看到的，我们的GAAL算法似乎能够适应学习者。本实验的结果是初步的，并不意味着作为综合评价。

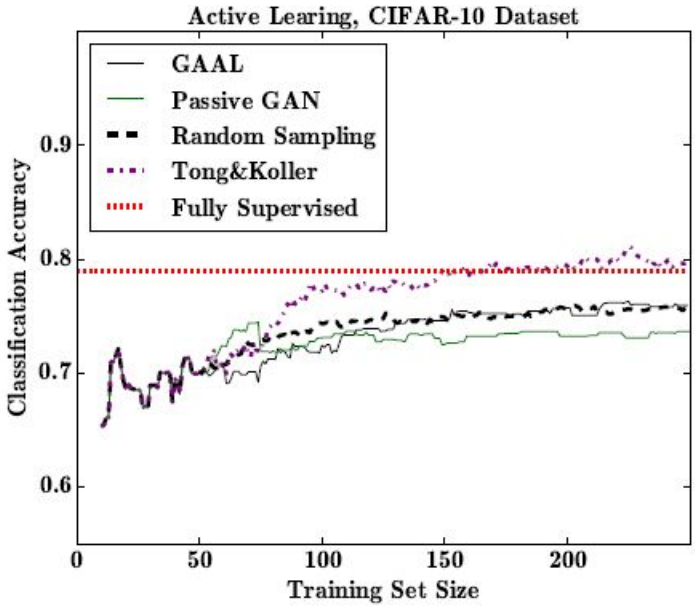


图8.CIFAR-10数据集的主动学习结果，分类汽车和马。

转移学习涉及训练域Ptr(x，y)的分布与目标域Pte(x，y)的分布不同的情况。在我们的例子中，训练域大多是未标记的。因此，我们比较的方法是自学教学学习(Raina等人，2007)。类似于(Le等人)中的算法，我们使用具有卷积层和汇集层的重建独立分量分析(RICA)模型。RICA类似于稀疏自动编码器。遵循标准的自学教学程序，我们首先训练未标记的池数据集。然后我们使用训练的RICA作为特征提取器从随机选择的MNIST图像获得更高级别的特

征。然后我们将特征与原始图像数据连接以训练分类器。最后，我们测试USPS数据集上的训练分类器。我们测试250,500,1000,2000和5000的训练大小。这样做的原因是已知深度学习型技术在丰富的训练数据中蓬勃发展。在主动学习场景中，它们可能在有限数量的训练数据下表现得相对较差。我们运行实验100次并取平均结果。我们使用与第5.1节中相同的GAAL算法设置。我们使用的分类器是线性SVM。表1显示出了GAAL、自学教学学习和对原始图像数据的常规监督学习的分类准确度。在原始特征上使用GAAL比具有相同训练大小250的自学教学学习的精度更高。实际上，当标记数据不足时，自学教学的表现比常规监督学习更差。这对于自动编码器类型算法是可能的。然而，当我们增加训练的规模，自学教学学习开始表现更好。有5000个训练样本，自学成绩的学习优于GAAL250个训练样本。

ALGOIRTHM	TRAINING SET SIZE	ACCURACY
GAAL	**250**	**76.42%**
SELF-TAUGHT	250	59.68%
SUPERVISED	250	67.87%
SELF-TAUGHT	500	65.53%
SUPERVISED	500	69.22%
SELF-TAUGHT	1000	71.96%
SUPERVISED	1000	69.58%
SELF-TAUGHT	2000	75.84%
SUPERVISED	2000	70.06%
SELF-TAUGHT	**5000**	**78.08%**
SUPERVISED	5000	72.00%

表1.GAAL和自学教学的比较

基于这些结果，我们怀疑GAAL也有潜力被用作自学的算法3。在实践中，GAAL算法也可以应用在由自学教学算法提取的特征之上。而对更先进的自学教学学习方法和更深层结构的综合比较，超出了这项工作的范围。

6.讨论和未来工作

在这项工作中，我们提出了一种新的主动学习方法，采用生成式对抗网络。虽然我们不声称我们的方法总是优于传统的基于池的方法在这个阶段，我们的实验显示有希望的结果。这项工作的结果足以激发未来对深度生成模型在主动学习中的研究。然而，工作仍然在建立理论保证。GAAL与自学教学的比较是特别有趣，值得进一步调查。我们还计划调查在我们的框架中使用Wasserstein GAN的可能性，例如，以解决第5.2节中提到的问题。