# gan生成手写数字识别报告

## 一、实验环境

|  |  |  |
| --- | --- | --- |
| 实验平台 | 编程软件 | 编程语言 |
| Win11系统 | VSCODE | python |

## 二、网络以及选题介绍

### GAN网络介绍：

Ian J. Goodfellow等人于2014年10月在*Generative Adversarial Networks*中提出了一个通过对抗过程估计生成模型的新框架。框架中同时训练两个模型：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](https://baike.baidu.com/item/%E6%A6%82%E7%8E%87/828845" \t "_blank)的判别模型D。G的训练程序是将D错误的概率最大化。这个框架对应一个最大值集下限的双方对抗游戏。可以证明在任意函数G和D的空间中，存在唯一的解决方案，使得G重现训练数据分布，而D=0.5。在G和D由[多层感知器](https://baike.baidu.com/item/%E5%A4%9A%E5%B1%82%E6%84%9F%E7%9F%A5%E5%99%A8/10885549" \t "_blank)定义的情况下，整个系统可以用反向传播进行训练。在训练或生成样本期间，不需要任何[马尔可夫链](https://baike.baidu.com/item/%E9%A9%AC%E5%B0%94%E5%8F%AF%E5%A4%AB%E9%93%BE/6171383)或展开的近似推理网络。实验通过对生成的样品的定性和定量评估证明了本框架的潜力。

生成模型（Generative Model）和判别模型（Discriminative Model）。判别模型需要输入变量 ，通过某种模型来预测 。生成模型是给定某种隐含信息，来随机产生观测数据。举个简单的例子：

判别模型：给定一张图，判断这张图里的动物是猫还是狗

生成模型：给一系列猫的图片，生成一张新的猫咪（不在数据集里）

对于判别模型，损失函数是容易定义的，因为输出的目标相对简单。但对于生成模型，损失函数的定义就不是那么容易。我们对于生成结果的期望，往往是一个暧昧不清，难以数学公理化定义的范式。所以不妨把生成模型的回馈部分，交给判别模型处理。这就是Goodfellow他将机器学习中的两大类模型，Generative和Discrimitive给紧密地联合在了一起。

GAN的基本原理其实非常简单，这里以生成图片为例进行说明。假设我们有两个网络，G（Generator）和D（Discriminator）。正如它的名字所暗示的那样，它们的功能分别是：

G是一个生成图片的网络，它接收一个随机的噪声z，通过这个噪声生成图片，记做G(z)。

D是一个判别网络，判别一张图片是不是“真实的”。它的输入参数是x，x代表一张图片，输出D（x）代表x为真实图片的概率，如果为1，就代表100%是真实的图片，而输出为0，就代表不可能是真实的图片。

在训练过程中，生成网络G的目标就是尽量生成真实的图片去欺骗判别网络D。而D的目标就是尽量把G生成的图片和真实的图片分别开来。这样，G和D构成了一个动态的“博弈过程”。最后博弈的结果是什么？在最理想的状态下，G可以生成足以“以假乱真”的图片G(z)。对于D来说，它难以判定G生成的图片究竟是不是真实的，因此D(G(z)) = 1。这样我们的目的就达成了：我们得到了一个生成式的模型G，它可以用来生成图片。Goodfellow从理论上证明了该算法的收敛性，以及在模型收敛时，生成数据具有和真实数据相同的分布（保证了模型效果）。

### 手写数字生成选题介绍:

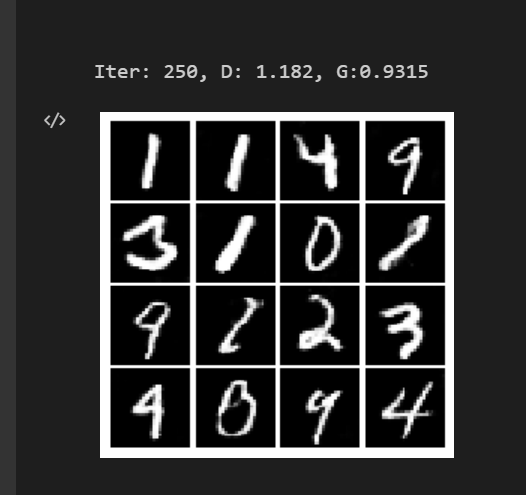
在介绍手写数字生成之前，我们首先来了解什么是手写数字以及手写数字识别。

图像识别（Image Recognition）是指利用计算机对图像进行处理、分析和理解，以识别各种不同模式的目标和对像的技术。 图像识别的发展经历了三个阶段：文字识别、数字图像处理与识别、物体识别。机器学习领域一般将此类识别问题转化为分类问题。手写识别是常见的图像识别任务。计算机通过手写体图片来识别出图片中的字，与印刷字体不同的是，不同人的手写体风格迥异，大小不一， 造成了计算机对手写识别任务的一些困难。 数字手写体识别由于其有限的类别（0~9共10个数字）成为了相对简单 的手写识别任务。DBRHD和MNIST是常用的两个数字手写识别数据集。

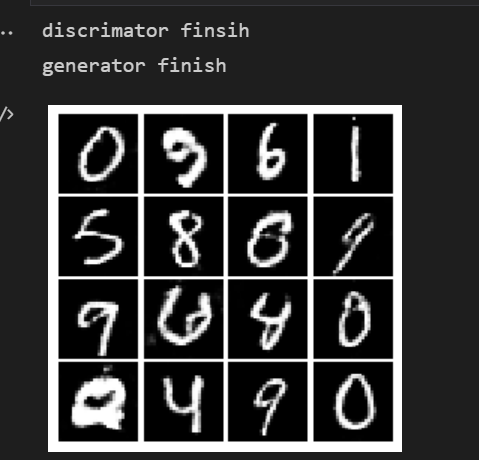
在此基础上我们需要更进一步的生成图像，这对神经网络来说是一巨大的挑战，gan网络为生成图像提供了可能。

## 三、结果截图

经过20个epoch训练，



生成网络与判别网络已经基本收敛一下是生成网络生成的图片。



## 四、总结

GAN有两个特点：

* 相比较传统的模型，存在两个不同的网络，训练方式为对抗式训练。
* G的梯度信息来自于判别器D，而不是样本数据。

GAN的优点：

* 相比于其他的生成模型，GAN只利用了反向传播，不需要复杂的马尔科夫链。而且可以生成更清晰真实的样本。
* GAN可以用到很多场景上，比如图片风格迁移、超分辨率、图像补全等等。

GAN的缺点：

* 训练需要达到纳什平衡，现在还没有一个很好的达到纳什平衡的方法。
* GAN不适合处理离散形式的数据。
* GAN存在训练不稳定、梯度消失、模式崩溃等问题。原因：GAN是采用对抗的训练方式，G的损失来自于D，因此G训练的效果的好坏与否是由D决定的。如果某一次G生成的样本可能并不是真是的，但是D还是给出了正确的评价，或者说G生成的结果中的某些特征得到了D的认可，那么G就认为自己生成的结果是正确的，这样子自我欺骗下去就会导致最终生成的额结果会丢失一些信息，特征不全。

后续有基于gan网络的新型结构例如DCGAN，WGAN，LSGAN等等，能更好的实现神经网络。