简单理解与实验生成对抗网络GAN

原创

之前

GAN网络是近两年深度学习领域的新秀，火的不行，本文旨在浅显理解传统GAN，分享学习心得。现有GAN网络大多数代码实现使用python、torch等语言，这里，后面用matlab搭建一个简单的GAN网络，便于理解GAN原理。

GAN的鼻祖之作是2014年NIPS一篇文章：Generative Adversarial Net,可以细细品味。

- 分享一个目前各类GAN的一个**论文整理集合**
- 再分享一个目前各类GAN的一个**代码整理集合**

开始

我们知道GAN的思想是是一种二人零和博弈思想（two-player game），博弈双方的利益之和是一个常数，比如两个人掰手腕，假设总的空间是一定的，你的力气大一点，那你就得到的空间多一点，相应的我的空间就少一点，相反我力气大我就得到的多一点，但有一点是确定的就是，我两的总空间是一定的，这就是二人博弈，但是呢总利益是一定的。

引申到GAN里面就是可以看成，GAN中有两个这样的博弈者，一个人名字是生成模型（G），另一个人名字是判别模型（D）。他们各自有各自的功能。

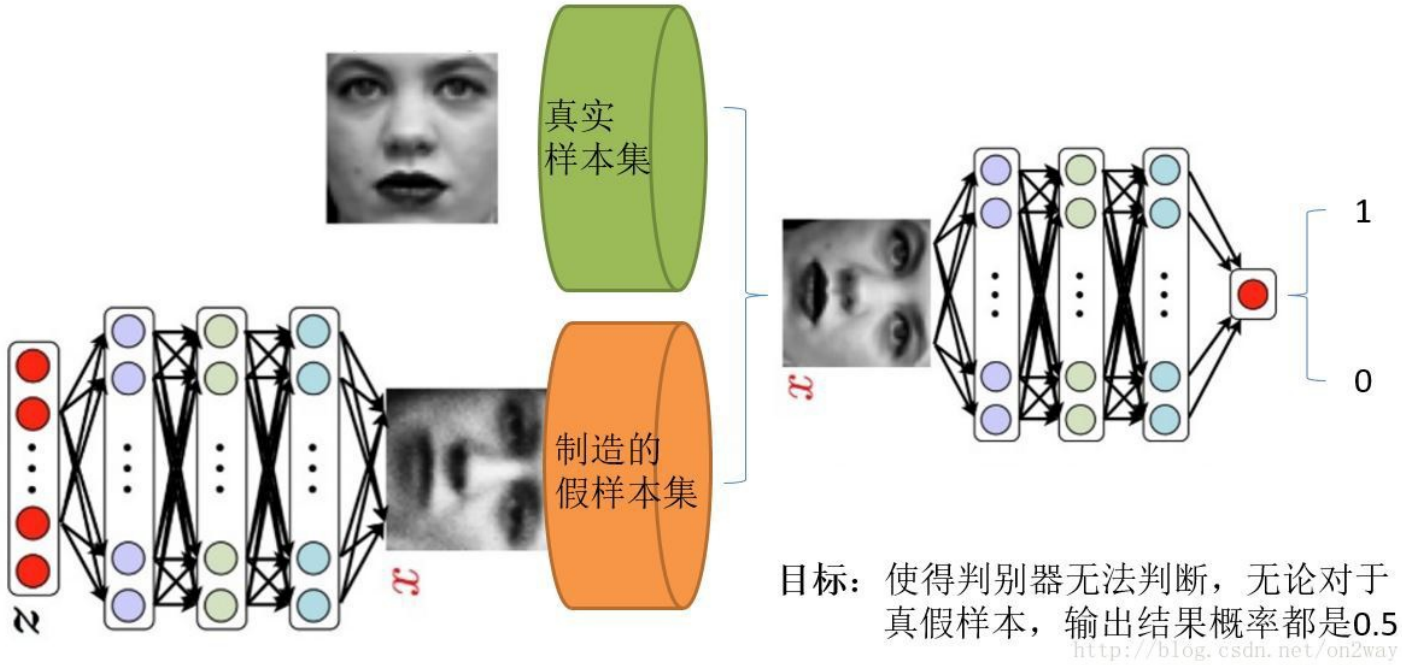
相同点是：

- 这两个模型都可以看成是一个黑匣子，接受输入然后有一个输出，类似一个函数，一个输入输出映射。

不同点是：

- 生成模型功能：比作是一个样本生成器，输入一个噪声/样本，然后把它包装成一个逼真的样本，也就是输出。
- 判别模型：比作一个二分类器（如同0-1分类器），来判断输入的样本是真是假。（就是输出值大于0.5还是小于0.5）；

直接上一张个人觉得解释的好的图说明：



在之前，我们首先明白在使用GAN的时候的2个问题

- **我们有什么？**
  比如上面的这个图，我们有的只是真实采集而来的人脸样本数据集，仅此而已，而且很**关键的一点**是我们连人脸数据集的**类标签都没有**，也就是我们不知道那个人脸对应的是谁。
- **我们要得到什么**
  至于要得到什么，不同的任务得到的东西不一样，我们只说最原始的GAN目的，那就是我们想通过输入一个噪声，模拟得到一个人脸图像，这个图像可以非常逼真以至于以假乱真。

好了再来理解下GAN的两个模型要做什么。首先**判别模型**，就是图中右半部分的网络，直观来看就是一个简单的神经网络结构，输入就是一副图像，输出就是一个概率值，用于判断真假使用（概率值大于0.5那就是真，小于0.5那就是假），真假也不过是人们定义的概率而已。其次是**生成模型**，生成模型要做什么呢，同样也可以看成是一个神经网络模型，输入是一组随机数Z，输出是一个图像，不再是一个数值而已。从图中可以看到，会存在两个数据集，一个是真实数据集，这好说，另一个是假的数据集，那这个数据集就是有生成网络造出来的数据集。好了根据这个图我们再来理解一下GAN的目标是要干什么：

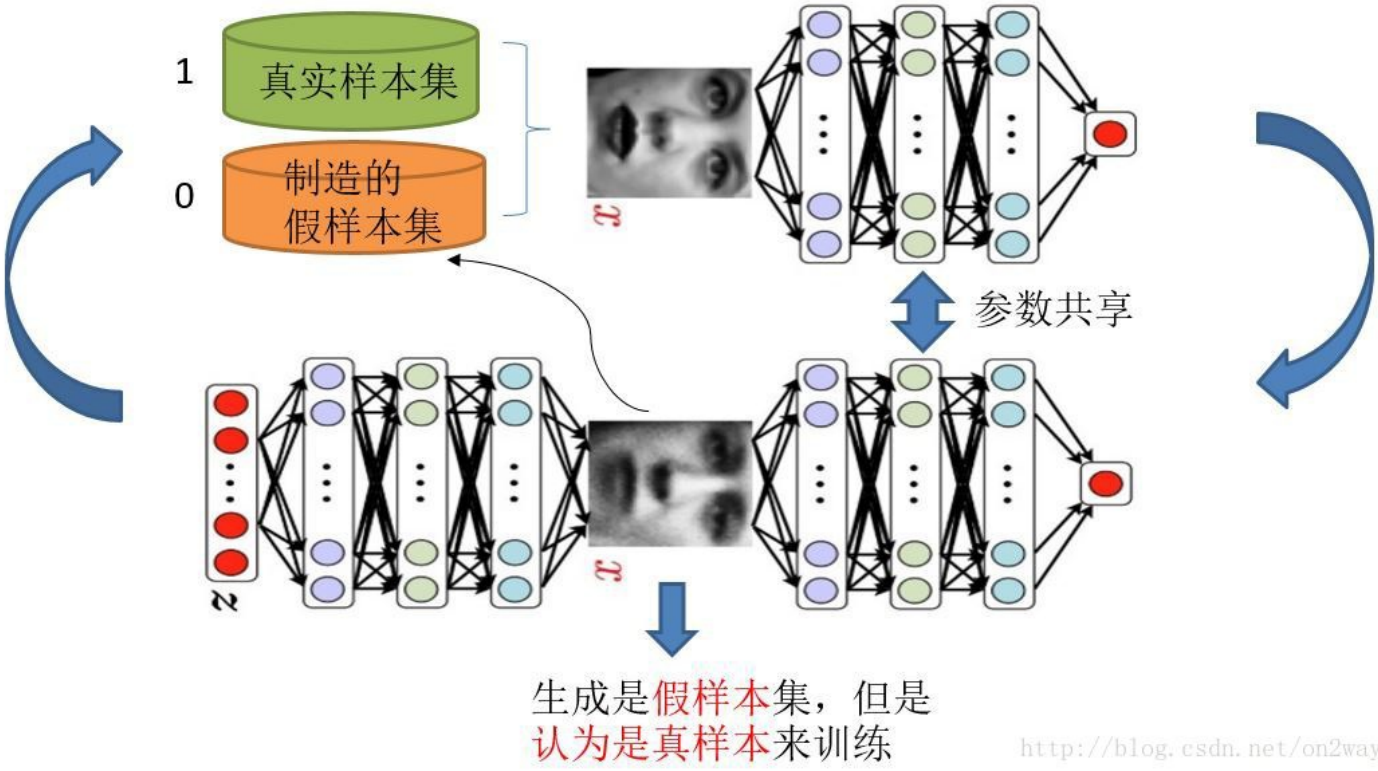
- 判别网络的目的：就是能判别出来属于的一张图它是来自真实样本集还是假样本集。假如输入的是真样本，网络输出就接近1，输入的是假样本，网络输出接近0，那么很完美，达到了很好判别的目的。
- 生成网络的目的：生成网络是造样本的，它的目的就是使得自己造样本的能力尽可能强，强到什么程度呢，你判别网络没法判断我是真样本还是假样本。

有了这个理解我们再来看看为什么叫做对抗网络了。判别网络说，我很强，来一个样本我就知道它是来自真样本集还是假样本集。生成网络就不服了，说我也很强，我生成一个假样本，虽然我生成网络知道是假的，但是你判别网络不知道呀，我包装的非常逼真，以至于判别网络无法判断真假，那么用输出数值来解释就是，生成网络生成的假样本进去了判别网络以后，判别网络给出的结果是一个接近0.5的值，极限情况就是0.5，也就是说判别不出来了，这就是纳什平衡了。

由这个分析可以发现，生成网络与判别网络的目的正好是相反的，一个说我能判别的好，一个说我让你判别不好。所以叫做对抗，叫做博弈。那么最后的结果到底是谁赢呢？这就要归结到设计者，也就是我们希望谁赢了。作为设计者的我们，我们的目的是要得到以假乱真的样本，那么很自然的我们希望生成样本赢了，也就是希望生成样本很真，判别网络能力不足以区分真假样本位置。

再理解

知道了GAN大概的目的与设计思路，那么一个很自然的问题来了就是我们该如何用数学方法解决这么一个对抗问题。这就涉及到如何训练这样一个生成对抗网络模型了，还是先上一个图，用图来解释最直接：



需要注意的是生成模型与对抗模型可以说是完全独立的两个模型，好比就是完全独立的两个神经网络模型，他们之间没有什么联系。

好了那么训练这样的两个模型的大方法就是：**单独交替迭代训练**。

什么意思？因为是2个网络，不好一起训练，所以才去交替迭代训练，我们一一来看。
假设现在生成网络模型已经有了（当然可能不是最好的生成网络），那么给一堆随机数组，就会得到一堆假的样本集（因为不是最终的生成模型，那么现在生成网络可能就处于劣势，导致生成的样本就不咋地，可能很容易就被判别网络判别出来了说这货是假冒的），但是先不管这个，假设我们现在有了这样的假样本集，真样本集一直都有，现在我们人为的定义真假样本集的标签，因为我们希望真样本集的输出尽可能为1，假样本集为0，很明显这里我们就已经默认真样本集所有的类标签都为1，而假样本集的所有类标签都为0. 有人会说，在真样本集里面的人脸中，可能张三人脸和李四人脸不一样呀，对于这个问题我们需要理解的是，我们现在的任务是什么，我们是想分样本真假，而不是分真样本中那个是张三label、那个是李四label。况且我们也知道，原始真样本的label我们是不知道的。回过头来，我们现在有了真样本集以及它们的label（都是1）、假样本集以及它们的label（都是0），这样单就判别网络来说，此时问题就变成了一个再简单不过的**有监督的二分类问题**了，直接送到神经网络模型中训练就完事了。假设训练完了，下面我们来看生成网络。

对于生成网络，想想我们的目的，是生成尽可能逼真的样本。那么原始的生成网络生成的样本你怎么知道它真不真呢？就是送到判别网络中，所以在训练生成网络的时候，我们需要联合判别网络一起才能达到训练的目的。什么意思？就是如果我们单单只用生成网络，那么想想我们怎么去训练？误差来源在哪里？细想一下没有，但是如果我们把刚才的判别网络串接在生成网络的后面，这样我们就知道真假了，也就有了误差了。所以对于生成网络的训练其实是对生成-判别网络串接的训练，就像图中显示的那样。好了那么现在来分析一下样本，原始的噪声数组Z我们有，也就是生成了假样本我们有，此时很关键的一点来了，我们要**把这些假样本的标签都设置为1**，也就是认为这些假样本在生成网络训练的时候是真样本。那么为什么要这样呢？我们想想，是不是这样才能起到迷惑判别器的目的，也才能使得生成的假样本逐渐逼近为正样本。好了，重新顺一下思路，现在对于生成网络的训练，我们有了样本集（只有假样本集，没有真样本集），有了对应的label（全为1），是不是就可以训练了？有人会问，这样只有一类样本，训练啥呀？谁说一类样本就不能训练了？只要有误差就行。还有人说，你这样一训练，**判别网络的网络参数不是也跟着变吗**？没错，这很关键，所以在训练这个串接的网络的时候，一个很重要的操作就是**不要判别网络的参数发生变化**，也就是不让它参数发生更新，只是把误差一直传，传到生成网络那块后更新生成网络的参数。这样就完成了生成网络的训练了。

在完成生成网络训练好，那么我们是不是可以根据目前新的生成网络再对先前的那些噪声Z生成新的假样本了，没错，并且训练后的假样本应该是更真了才对。然后又有了新的真假样本集（其实是新的假样本集），这样又可以重复上述过程了。我们把这个过程称作为单独交替训练。我们可以实现定义一个迭代次数，交替迭代到一定次数后停止即可。这个时候我们再去看一看噪声Z生成的假样本会发现，原来它已经很真了。

看完了这个过程是不是感觉GAN的设计真的很巧妙，个人觉得最值得称赞的地方可能在于这种**假样本在训练过程中的真假变换**，这也是博弈得以进行的关键之处。

进一步

文字的描述相信已经让大多数的人知道了这个过程，下面我们来看看原文中几个重要的数学公式描述，首先我们直接上原始论文中的目标公式吧：

$$\max_V$$

上述这个公式说白了就是一个最大最小优化问题，其实对应的也就是上述的两个优化过程。有人说如果不看别的，能达看到这个公式就拍案叫绝的地步，那就是机器学习的顶级专家，哈哈，真是前路漫漫。同时也说明这个简单的公式意义重大。

这个公式既然是最大最小的优化，那就不是一步完成的，其实对比我们的分析过程也是这样的，这里现优化D，然后在取优化G，本质上是两个优化问题，把拆解就如同下面两个公式：

优化D：

$$V$$

$$(D$$

优化G：

$$V$$

$$(D$$

可以看到，优化D的时候，也就是判别网络，其实没有生成网络什么事，后面的G(z)这里就相当于已经得到的假样本。优化D的公式的第一项，使的真样本x输入的时候，得到的结果越大越好，可以理解，因为需要真样本的预测结果越接近于1越好嘛。对于假样本，需要优化是的其结果越小越好，也就是D(G(z))越小越好，因为它的标签为0。但是呢第一项是越大，第二项是越小，这不矛盾了，所以呢把第二项改成1-D(G(z))，这样就是越大越好，两者合起来就是越大越好。 那么同样在优化G的时候，这个时候没有真样本什么事，所以把第一项直接却掉了。这个时候只有假样本，但是我们说这个时候是希望假样本的标签是1的，所以是D(G(z))越大越好，但是呢为了统一成1-D(G(z))的形式，那么只能是最小化1-D(G(z))，本质上没有区别，只是为了形式的统一。之后这两个优化模型可以合并起来写，就变成了最开始的那个最大最小目标函数了。

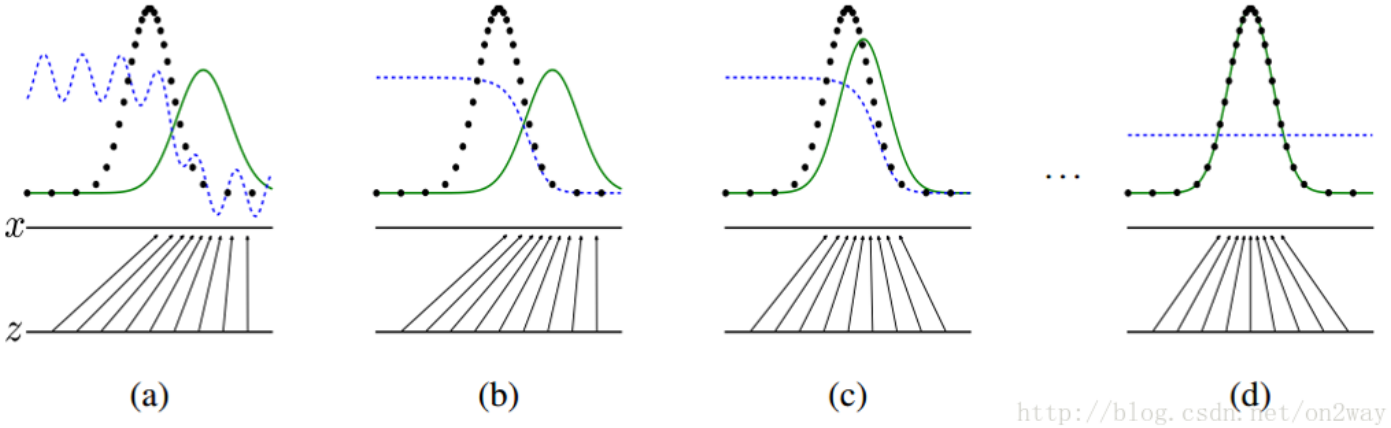
所以回过头来我们来看这个最大最小目标函数，里面包含了判别模型的优化，包含了生成模型的以假乱真的优化，完美的阐释了这样一个优美的理论。

再进一步

有人说GAN强大之处在于可以自动的学习原始真实样本集的数据分布，不管这个分布多么的复杂，只要训练的足够好就可以学出来。针对这一点，感觉有必要好好理解一下为什么别人会这么说。

我们知道，传统的机器学习方法，我们一般都会定义一个什么模型让数据去学习。比如说假设我们知道原始数据属于高斯分布呀，只是不知道高斯分布的参数，这个时候我们定义高斯分布，然后利用数据去学习高斯分布的参数得到我们最终的模型。再比如说我们定义一个分类器，比如SVM，然后强行让数据进行东变西变，进行各种高维映射，最后可以变成一个简单的分布，SVM可以很轻易的进行二分类分开，其实SVM已经放松了这种映射关系了，但是也是给了一个模型，这个模型就是核映射（什么径向基函数等等），说白了其实也好像是你事先知道让数据该怎么映射一样，只是核映射的参数可以学习罢了。所有的这些方法都在直接或者间接的告诉数据你该怎么映射一样，只是不同的映射方法能力不一样。那么我们再来看看GAN，生成模型最后可以通过噪声生成一个完整的真实数据（比如人脸），说明生成模型已经掌握了从随机噪声到人脸数据的分布规律了，有了这个规律，想生成人脸还不容易。然而这个规律我们开始知道吗？显然不知道，如果让你说从随机噪声到人脸应该服从什么分布，你不可能知道。这是一层层映射之后组合起来的非常复杂的分布映射规律。然而GAN的机制可以学习到，也就是说GAN学习到了真实样本集的数据分布。

再拿原论文中的一张图来解释：



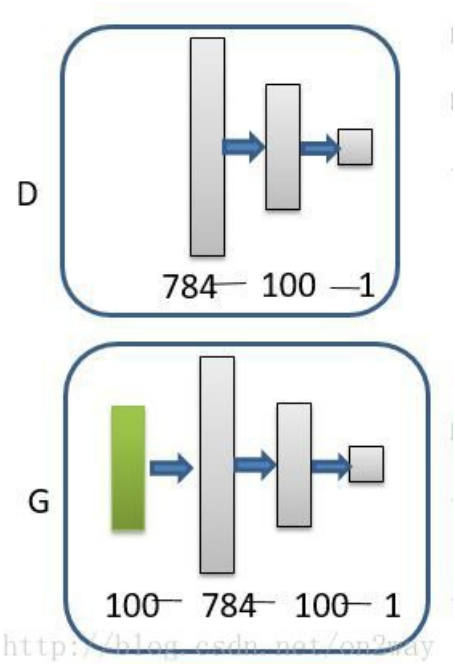
这张图表明的是GAN的生成网络如何一步步从均匀分布学习到正太分布的。原始数据x服从正太分布，这个过程你也没告诉生成网络说你得用正太分布来学习，但是生成网络学习到了。假设你改一下x的分布，不管什么分布，生成网络可能也能学到。这就是GAN可以自动学习真实数据的分布的强大之处。

还有人说GAN强大之处在于可以自动的定义潜在损失函数。 什么意思呢，这应该说的是判别网络可以自动学习到一个好的判别方法，其实就是等效的理解为可以学习到好的损失函数，来比较好或者不好的判别出来结果。虽然大的loss函数还是我们人为定义的，基本上对于多数GAN也都这么定义就可以了，但是判别网络潜在学习到的损失函数隐藏在网络之中，不同的问题这个函数就不一样，所以说可以自动学习这个潜在的损失函数。

开始做小实验

本节主要实验一下如何通过随机数组生成mnist图像。mnist手写体数据库应该都熟悉的。这里简单的使用matlab来实现，方便看到整个实现过程。这里用到了一个工具箱
DeepLearnToolbox,关于该工具箱的一些其他使用说明

网络结构很简单，就定义成下面这样子：



将上述工具箱添加到路径，然后运行下面代码：

```
clc
clear
%% 构造真实训练样本 60000个样本 1*784维（28*28展开）
load mnist_uint8;

train_x = double(train_x(1:60000,:)) / 255;
% 真实样本认为为标签 [1 0]； 生成样本为[0 1];
train_y = double(ones(size(train_x,1),1));
% normalize
train_x = mapminmax(train_x, 0, 1);

rand('state',0)
%% 构造模拟训练样本 60000个样本 1*100维
test_x = normrnd(0,1,[60000,100]); % 0-255的整数
test_x = mapminmax(test_x, 0, 1);

test_y = double(zeros(size(test_x,1),1));
test_y_rel = double(ones(size(test_x,1),1));

%%
nn_G_t = nnsetup([100 784]);
nn_G_t.activation_function = 'sigm';
nn_G_t.output = 'sigm';

nn_D = nnsetup([784 100 1]);
nn_D.weightPenaltyL2 = 1e-4;  %  L2 weight decay
nn_D.dropoutFraction = 0.5;   %  Dropout fraction
nn_D.learningRate = 0.01;                %  Sigm require a lower learning rate
nn_D.activation_function = 'sigm';
nn_D.output = 'sigm';
% nn_D.weightPenaltyL2 = 1e-4;  %  L2 weight decay

nn_G = nnsetup([100 784 100 1]);
nn_G.weightPenaltyL2 = 1e-4;  %  L2 weight decay
```

```
nn_G.dropoutFraction = 0.5;   %  Dropout fraction
nn_G.learningRate = 0.01;                %  Sigm require a lower learning rate
nn_G.activation_function = 'sigm';
nn_G.output = 'sigm';
% nn_G.weightPenaltyL2 = 1e-4;  %  L2 weight decay

opts.numepochs =  1;        %  Number of full sweeps through data
opts.batchsize = 100;       %  Take a mean gradient step over this many samples
%%
num = 1000;
tic
for each = 1:1500
    %----------计算G的输出：假样本-------------------
    for i = 1:length(nn_G_t.W)   %共享网络参数
        nn_G_t.W{i} = nn_G.W{i};
    end
    G_output = nn_G_out(nn_G_t, test_x);
    %-----------训练D-----------------------------
    index = randperm(60000);
    train_data_D = [train_x(index(1:num),:);G_output(index(1:num),:)];
    train_y_D = [train_y(index(1:num),:);test_y(index(1:num),:)];
    nn_D = nntrain(nn_D, train_data_D, train_y_D, opts);%训练D
    %-----------训练G-----------------------------
    for i = 1:length(nn_D.W)  %共享训练的D的网络参数
        nn_G.W{length(nn_G.W)-i+1} = nn_D.W{length(nn_D.W)-i+1};
    end
    %训练G：此时假样本标签为1，认为是真样本
    nn_G = nntrain(nn_G, test_x(index(1:num),:), test_y_rel(index(1:num),:), opts);
end
toc
for i = 1:length(nn_G_t.W)
    nn_G_t.W{i} = nn_G.W{i};
end
fin_output = nn_G_out(nn_G_t, test_x);
```

函数nn_G_out为：

```
function output = nn_G_out(nn, x)
    nn.testing = 1;
    nn = nnff(nn, x, zeros(size(x,1), nn.size(end)));
    nn.testing = 0;
    output = nn.a{end};
end
```

看一下这个及其简单的函数，其实**最值得注意的就是中间那个交替训练的过程**，这里我分了三步列出来：

- 重新计算假样本（假样本每次是需要更新的，产生越来越像的样本）
- 训练D网络，一个二分类的神经网络；
- 训练G网络，一个串联起来的长网络，也是一个二分类的神经网络（不过只有假样本来训练），同时D部分参数在下一次的时候不能变了。

就这样调一调参数，最终输出在fin_output里面，多运行几次显示不同运行次数下的结果：

可以看到的是结果还是有点像模像样的。

实验总结

运行上述简单的网络我发现几个问题：

- **网络存在着不收敛问题；网络不稳定；网络难训练**；读过原论文其实作者也提到过这些问题，包括GAN刚出来的时候，很多人也在致力于解决这些问题，当你实验自己碰到的时候，还是很有意思的。那么这些问题怎么体现的呢，举个例子，可能某一次你会发现训练的误差很小，在下一代训练时，马上又出现极限性的上升的很厉害，过几代又发现训练误差很小，震荡太严重。
- 其次网络需要调才能出像样的结果。交替迭代次数的不同结果也不一样。比如每一代训练中，D网络训练2回，G网络训练一回，结果就不一样。
- 这是简单的无条件GAN，所以每一代训练完后，只能出现一个结果，那就是0-9中的某一个数。要想在一代训练中出现好几种结果，就需要使用到条件GAN了。

最后

现在的GAN已经到了五花八门的时候了，各种GAN应用也很多，理解底层原理再慢慢往上层扩展。GAN还是一个很厉害的东西，它使得现有问题从有监督学习慢慢过渡到无监督学习，而无监督学习才是自然界中普遍存在的，因为很多时候没有办法拿到监督信息的。要不Yann Lecun赞叹GAN是机器学习近十年来最有意思的想法。

福利

该节部分出了个视频版的讲解，详情请点击：http://www.mooc.ai/open/course/301
欢迎关注【微信公众号：AInewworld】了解更多。