**一、GAN原理介绍**

说到GAN第一篇要看的paper当然是Ian Goodfellow大牛的Generative Adversarial Networks（arxiv：[https://arxiv.org/abs/1406.2661](https://link.zhihu.com/?target=https%3A//arxiv.org/abs/1406.2661" \t "_blank)），这篇paper算是这个领域的开山之作。

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：

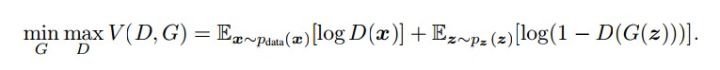
* G是一个生成图片的网络，它接收一个随机的噪声z，通过这个噪声生成图片，记做G(z)。
* D是一个判别网络，判别一张图片是不是“真实的”。它的输入参数是x，x代表一张图片，输出D（x）代表x为真实图片的概率，如果为1，就代表100%是真实的图片，而输出为0，就代表不可能是真实的图片。

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)) = 0.5。

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。

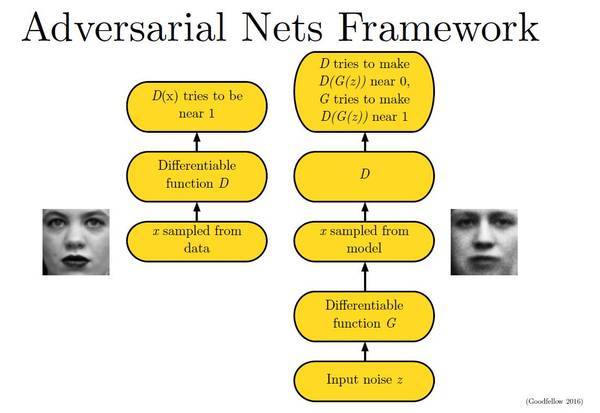
以上只是大致说了一下GAN的核心原理，如何用数学语言描述呢？这里直接摘录论文里的公式：



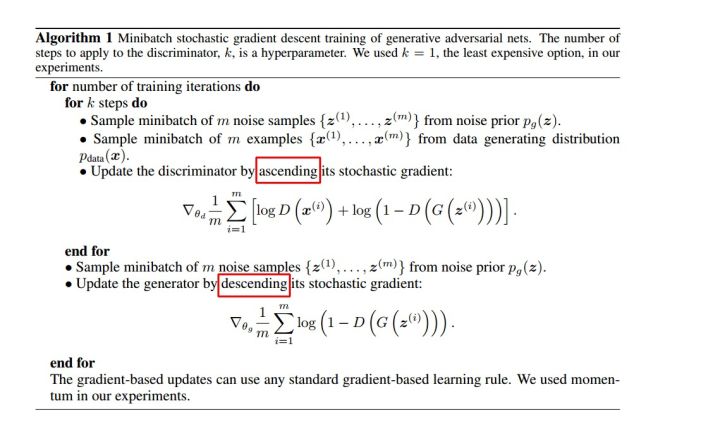
简单分析一下这个公式：

* 整个式子由两项构成。x表示真实图片，z表示输入G网络的噪声，而G(z)表示G网络生成的图片。
* D(x)表示D网络判断**真实图片是否真实**的概率（因为x就是真实的，所以对于D来说，这个值越接近1越好）。而D(G(z))是**D网络判断G生成的图片的是否真实的概率。**
* G的目的：上面提到过，D(G(z))是**D网络判断G生成的图片是否真实的概率**，G应该希望自己生成的图片“越接近真实越好”。也就是说，G希望D(G(z))尽可能得大，这时V(D, G)会变小。因此我们看到式子的最前面的记号是min\_G。
* D的目的：D的能力越强，D(x)应该越大，D(G(x))应该越小。这时V(D,G)会变大。因此式子对于D来说是求最大(max\_D)

下面这幅图片很好地描述了这个过程：



那么如何用随机梯度下降法训练D和G？论文中也给出了算法：

**这里红框圈出的部分是我们要额外注意的。**第一步我们训练D，D是希望V(G, D)越大越好，所以是加上梯度(ascending)。第二步训练G时，V(G, D)越小越好，所以是减去梯度(descending)。整个训练过程交替进行。

**二、DCGAN原理介绍**

我们知道深度学习中对图像处理应用最好的模型是CNN，那么如何把CNN与GAN结合？DCGAN是这方面最好的尝试之一（论文地址：[[1511.06434] Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks](https://link.zhihu.com/?target=https%3A//arxiv.org/abs/1511.06434" \t "_blank)）

DCGAN的原理和GAN是一样的，这里就不在赘述。它只是把上述的G和D换成了两个卷积神经网络（CNN）。但不是直接换就可以了，DCGAN对卷积神经网络的结构做了一些改变，以提高样本的质量和收敛的速度，这些改变有：

* 取消所有pooling层。G网络中使用转置卷积（transposed convolutional layer）进行上采样，D网络中用加入stride的卷积代替pooling。
* 在D和G中均使用batch normalization
* 去掉FC层，使网络变为全卷积网络
* G网络中使用ReLU作为激活函数，最后一层使用tanh
* D网络中使用LeakyReLU作为激活函数

DCGAN中的G网络示意：

