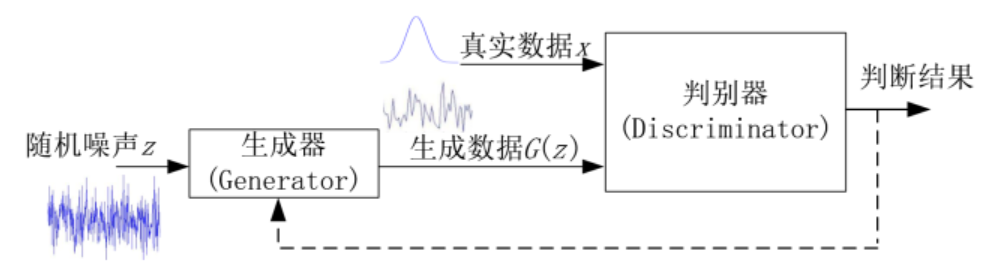
参考：

网站：<http://it.sohu.com/20161210/n475485860.shtml>

论文：[Generative Adversarial Nets](https://arxiv.org/abs/1406.2661)

有代码，见论文注释部分

1. 生成对抗网络（GAN）：靠数据和模型自己的内部对抗来实现无监督学习的模型。
2. 生成模型有两种应用：
3. 密度（概率）估计：在不了解事件概率分布的情况下，先假设随机分布，然后通过数据观测来确定真正的概率密度是怎样的。
4. 样本生成：提供训练样本数据分布，根据训练后模型来生成类似的样本分布。
5. 生成对抗模型的架构分成两个部分，分别是判别模型和生成模型。



其主要目的是判别器辅助生成器生成与真实数据分布一致的伪数据。生成器输入数据为随机噪声信号，通过生成器映射到一个新的数据空间中，同真实数据一起送入判别器进行判别，分别输出一个标量值，表示D对于输入数据是真实数据还是生成数据的置信度。最终D无法区分这两者时表示生成器达到最优。

1. 变量表示
2. 训练数据x，生成模型通过对x data的学习得到分布模型，输入的噪声变量；
3. 将噪声空间通过生成模型映射到data空间的函数，G是一个可微函数，参数为；
4. 判别模型的判别函数输入的值为x输入真实数据data的可能性，而不来自生成器空间；
5. 训练过程(Training Procedure)

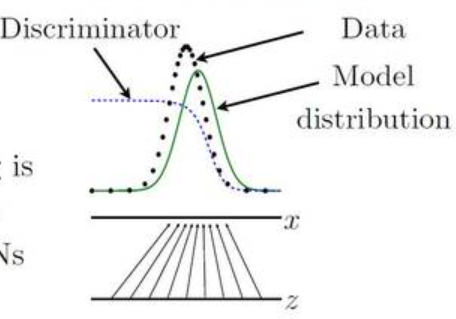
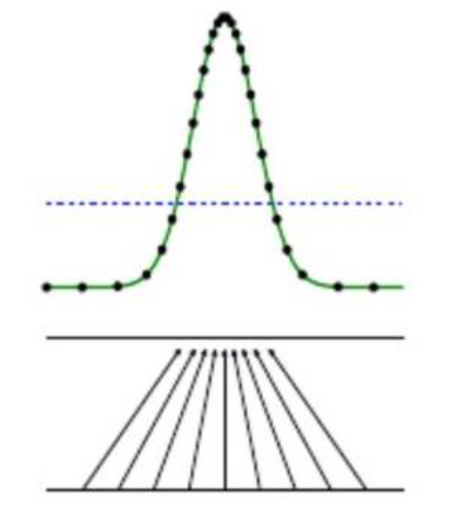
判别模型的目标是正确区分真实数据和伪造数据；生成模型的目标是最小化判别模型的准确率，使尽可能高，最小化。将训练转化为最大最小博弈问题(minimax game)，得到如下一个统一的优化公式：

公式的前半段表示判别模型评估的数据来源于data空间，即真实数据空间，值越大越好；公式后半段表示判别模型评估的数据来源于噪声空间，评估结果越小越好，但右半部分值越大越好；因此优化D，固定G时，向最大化方向发展；优化G，固定D时，向最小化方向发展。加入期望是因为生成器的目的是使伪造的数据与真实数据分布一致，但数据本身可以不同，使用期望来表示分布

很容易饱和因此可换用这段也不太明白，啥叫饱和？它到后边目标函数优化的时候仍然选择第一个式子作为生成模型的目标函数，所以这段话说得没啥意义。

真实数据分布（黑点）和模型生成的伪数据分布（绿线，model distribution，横轴表示数据，纵轴表示分布）如图所示，向上的箭头为z到x的映射，，分布差异D（蓝色虚线）表示为

训练网络的目的就是使生成模型伪造的数据分布与真实数据分布尽可能无差别，D会趋于，借此会训练出最优的生成模型。

1. 目标函数（objective function）优化

由于G和D都是可微网络，因此可选择任何类型的SGD方法做训练，在训练时使用两组数据：一组真实的训练数据，一组由生成模型生成的数据。D在训练的内部循环优化的代价很高，数据集有限的情况下会导致过度拟合，因此D每优化K次，G优化一次，只要G改变的足够慢，D可长时间保持在最优的状态左右。k是一个超参数。算法如下：

**for number of training iterations do**

**for k steps do**

sample minibatch of m noise samplesfrom noise prior

sample minibatch of m examplesfrom data generating distribution

Update the discriminator by ascending its stochastic gradient:

end for

sample minibatch of m noise samplesfrom noise prior

update te generator by descending its stochastic gradient:

**end for**

D的目标函数要往最大化方向发展，因此采用梯度上升求极大值的方法优化；G的目标函数要忘最小化方向发展，因此采用梯度下降求极小值的方法优化。

论文中4.1节证明在固定G，只优化D的情况下，当且仅当时V(G,D)达到最大值。证明的过程涉及到积分，条件概率，KL散度和香农熵，研究了半天也不太明白，先放下记着结论吧

论文中4.2节证明当D优化到最佳状态时，也会收敛于。用了凸函数和上确界的思想进行证明，也不太懂。

综上，在训练过程中，每轮迭代优先保证D在给定当前G下达到最优，再去更新G达到最优，如此循环。可真实训练中每隔k步才训练一回G，他不能保证一回G就训练成功了啊？

1. 优缺点

缺点：

1. 没有明确的式子来表示;
2. D和G的训练必须保持统一，(不能在D长久不更新的情况下只训练G，因为G会将许多噪声z映射到同一个真实数据点x上，使得G没有足够多样的训练数据训练)。

优点：

1. 生成模型不需马尔科夫链预测；
2. 在训练期间后推只用于计算梯度；？不理解
3. 许多不同类型的可微方程都可嵌入模型中（做目标函数？）；
4. 对抗模型可生成一些非常规的分布，马尔科夫链则不行；
5. 实验评估方式：Parzen window-based log-likelihood estimates，值越大越好。