

法律声明

■ 本课件包括演示文稿、示例、代码、题库、视频和声音等内容，北风网和讲师拥有完全知识产权；只限于善意学习者在本课程使用，不得在课程范围外向任何第三方散播。任何其他人或者机构不得盗版、复制、仿造其中的创意和内容，我们保留一切通过法律手段追究违反者的权利。

■ 课程详情请咨询

◆ 微信公众号：北风教育

◆ 官方网址：<http://www.ibeifeng.com/>



人工智能之深度学习

生成式对抗网络(GAN)

主讲人: Vincent Ying

上海育创网络科技有限公司



课程要求

■ 课上课下 “九字” 真言

- ◆ 认真听，善摘录，勤思考
- ◆ **多温故，乐实践**，再发散

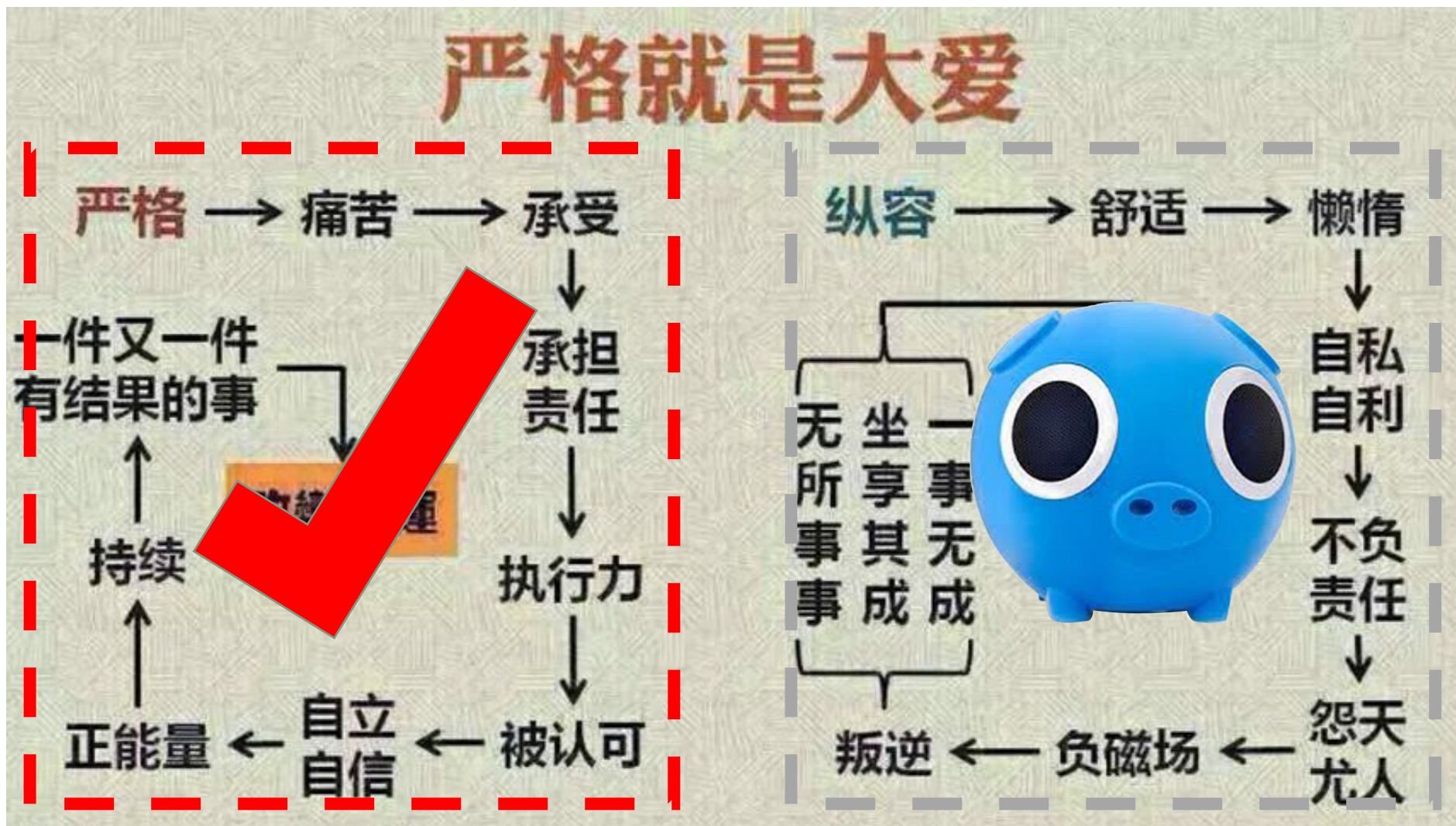
■ 四不原则

- ◆ **不懒散惰性，不迟到早退**
- ◆ **不请假旷课，不拖延作业**

■ 一点注意事项

- ◆ 违反 “四不原则” ， 不包就业和推荐就业

严格是大爱



寄语



做别人不愿做的事，
做别人不敢做的事，
做别人做不到的事。

课程内容

- 1、什么是生成式对抗网络
- 2、生成式对抗网络应用场景
- 3、Gans原理
- 4、Gans架构
- 5、DCGANS

什么是生成式对抗网络

- 生成式对抗网络（GAN）是一种深度学习模型，是近年来复杂分布上无监督学习最具前景的方法之一。模型通过框架中（至少）两个模块：生成模型（Generative Model）和判别模型（Discriminative Model）的互相博弈学习产生相当好的输出。原始 GAN 理论中，并不要求 G 和 D 都是神经网络，只需要是能拟合相应生成和判别的函数即可。但实用中一般均使用深度神经网络作为 G 和 D。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的判别模型D。G的训练程序是将D错误的概率最大化。

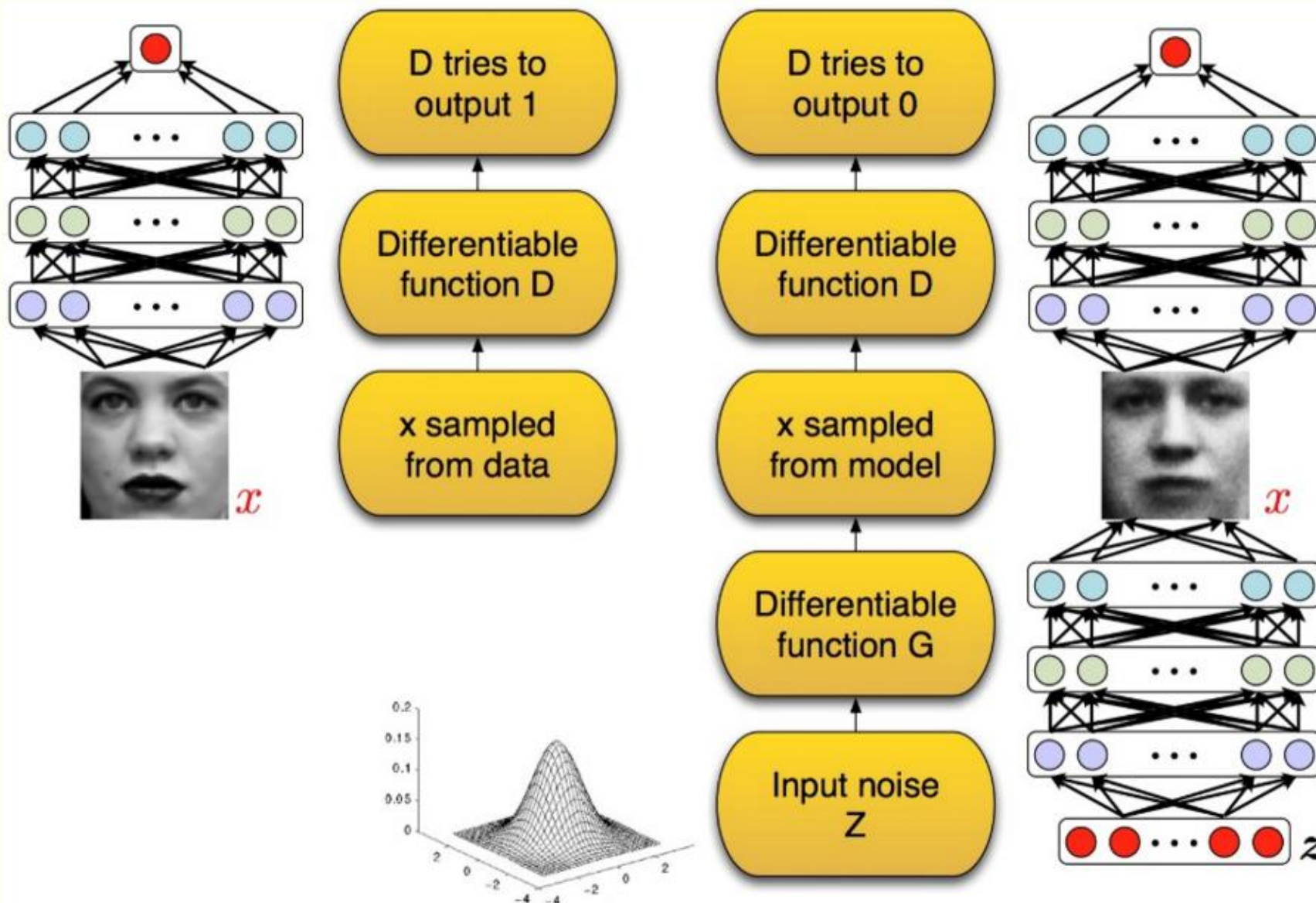
什么是生成式对抗网络

- 机器学习的模型可大体分为两类，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。如：
- 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）
- 生成式对抗网络将机器学习中的两大类模型，**Generative**和**Discriminative**给紧密地联合在了一起

什么是生成式对抗网络

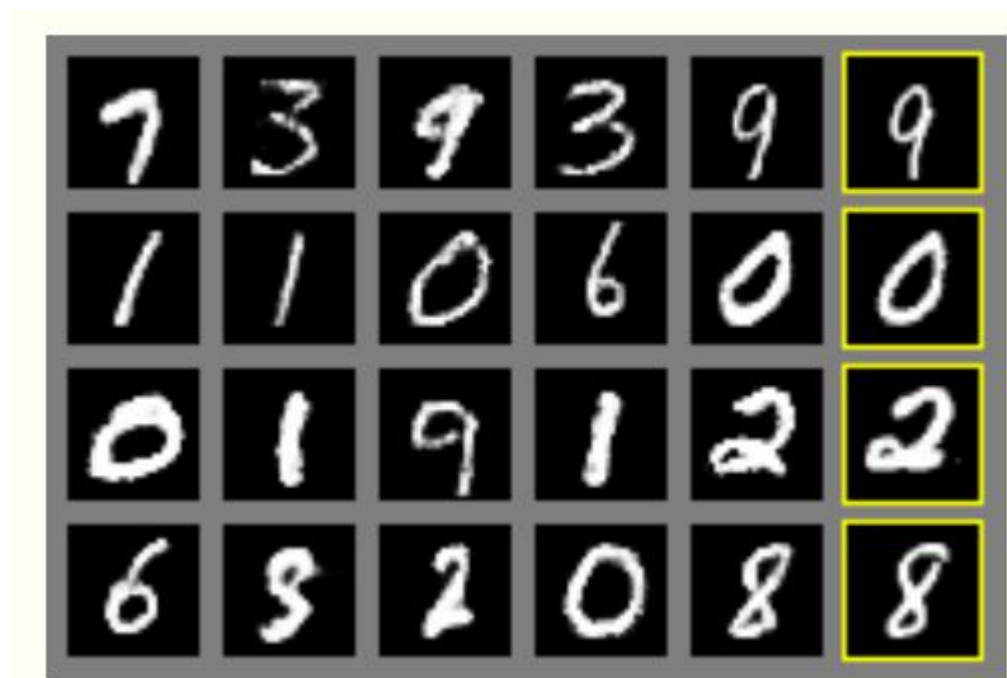
- 假设我们有两个网络，G（Generator）和D（Discriminator）。它们的功能分别是：
- G是一个生成图片的网络，它接收一个随机的噪声 z ，通过这个噪声生成图片，记做 $G(z)$ 。
- D是一个判别网络，判别一张图片是不是“真实的”。它的输入参数是 x ， x 代表一张图片，输出 $D(x)$ 代表 x 为真实图片的概率，如果为1，就代表100%是真实的图片，而输出为0，就代表不可能是真实的图片。
- 在训练过程中，生成网络G的目标就是尽量生成真实的图片去欺骗判别网络D。而D的目标就是尽量把G生成的图片和真实的图片分别开来。这样，G和D构成了一个动态的“博弈过程”。
- 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 $D(G(z)) = 0.5$ 。

什么是生成式对抗网络






什么是生成式对抗网络

- 一个例子：
- 最右边的一列是真实样本的图像，前面五列是生成网络生成的样本图像，可以看到生成的样本还是很像真实样本的，只是和真实样本属于不同的类，类别是随机的。



二 Gans应用 文本描述生成图片

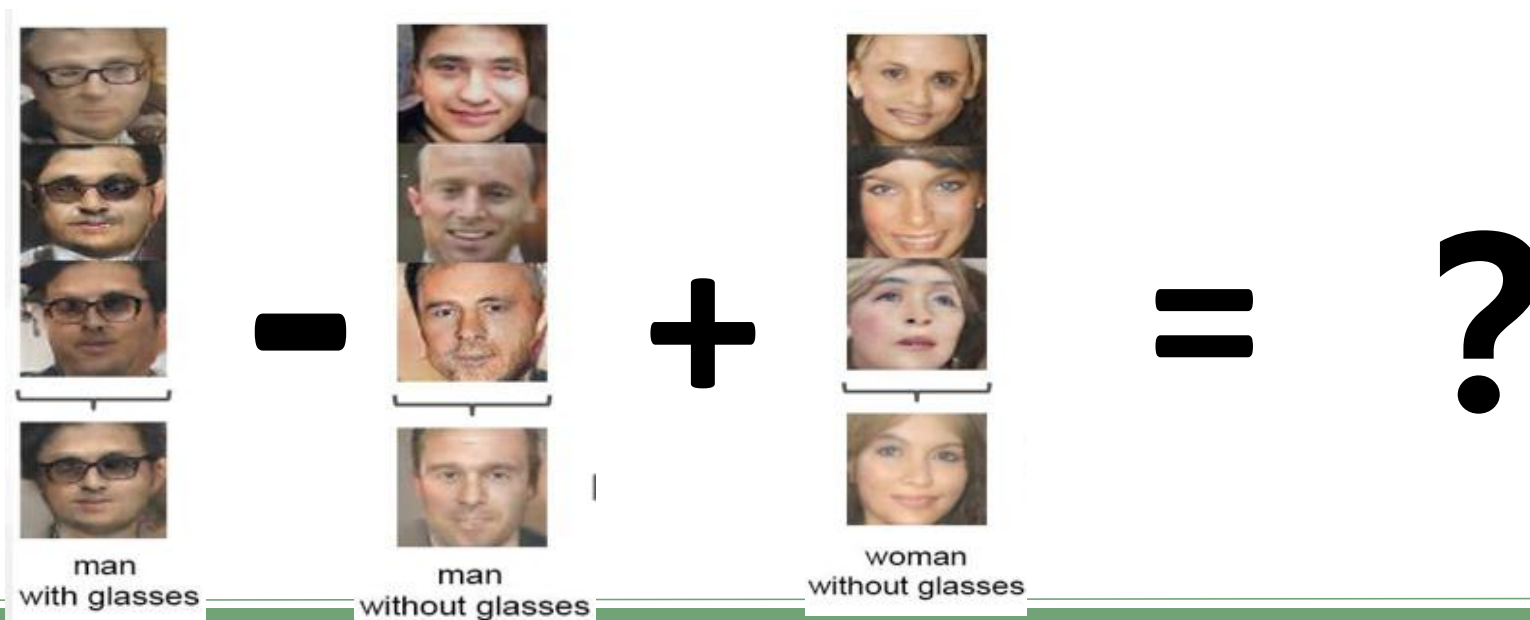
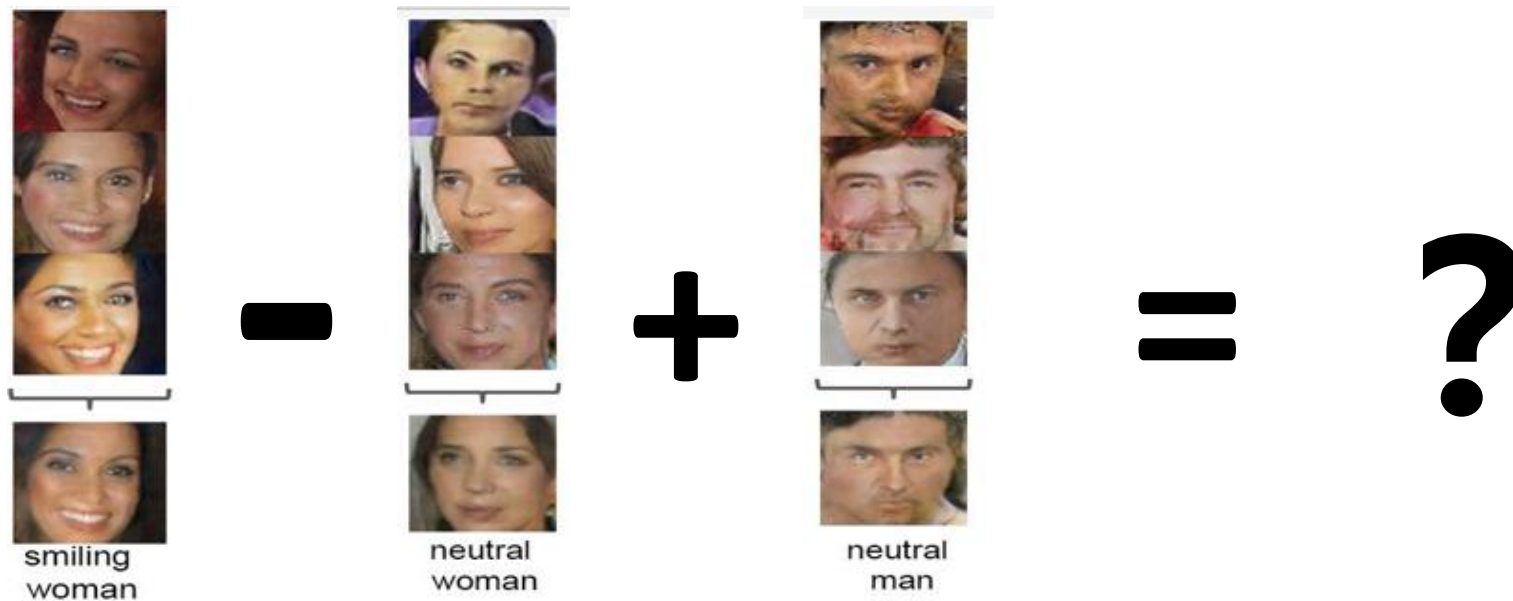
这只充满活力的**红色**小鸟有一个尖尖的**黑色**喙

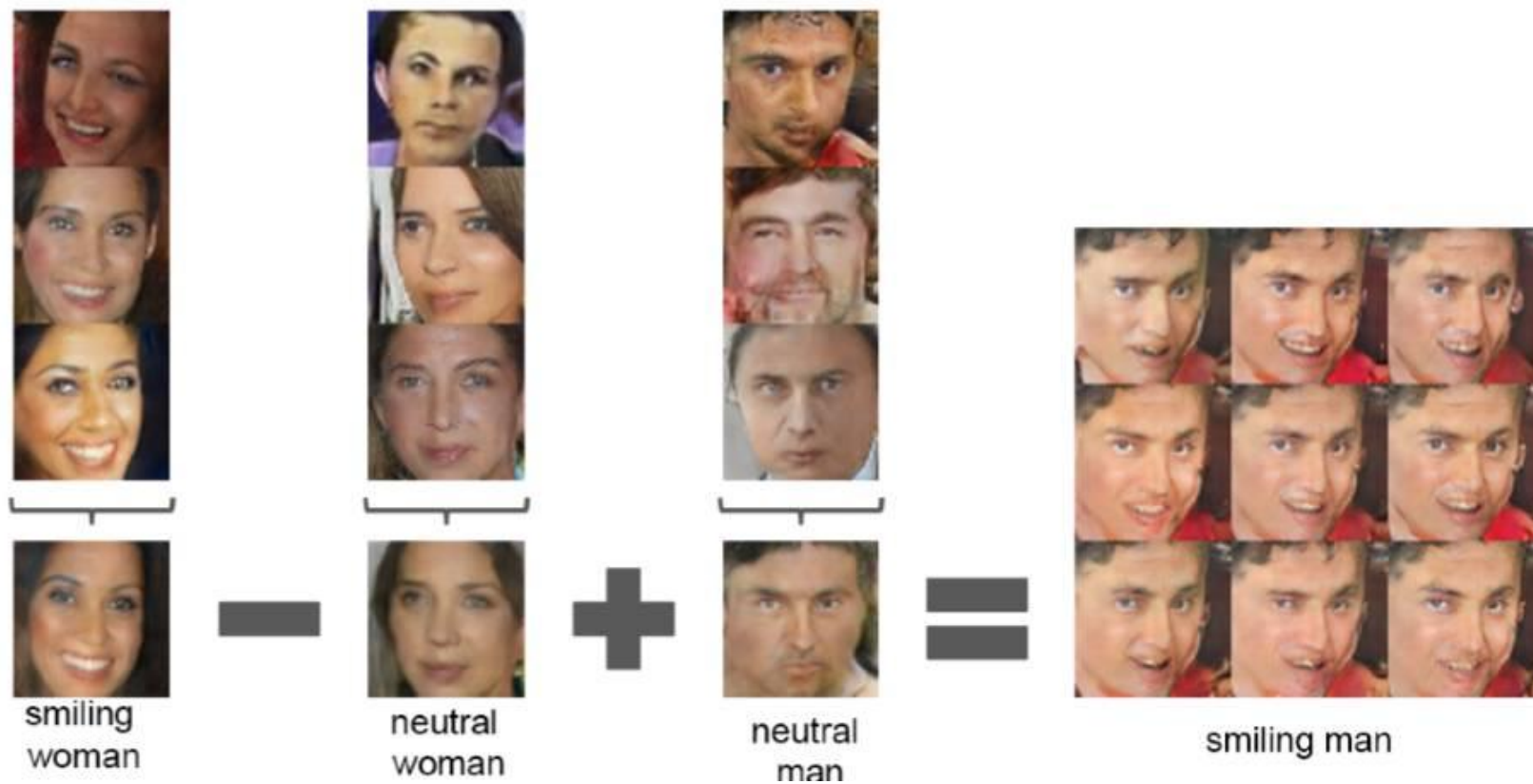
Caption	Image
this vibrant red bird has a pointed black beak	
this bird is yellowish orange with black wings	
the bright blue bird has a white colored belly	

这只鸟是**黄橙色**，**黑色**翅膀

这只明亮的**蓝色**小鸟有一个**白色**的肚子

二 Gans应用





二 Gans应用



自然图片+画家画作风格 生成一定画风的艺术图片

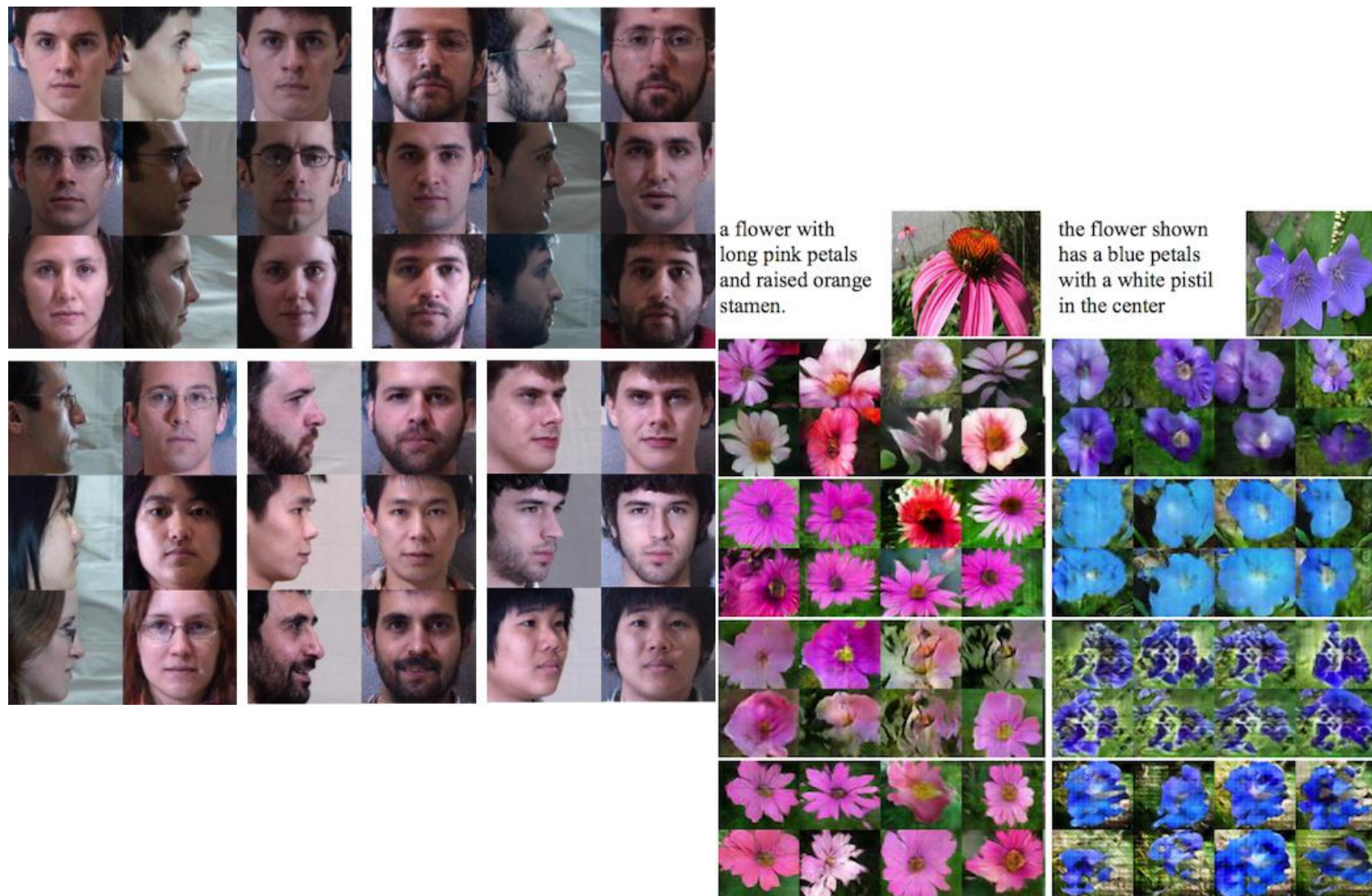
二 Gans应用



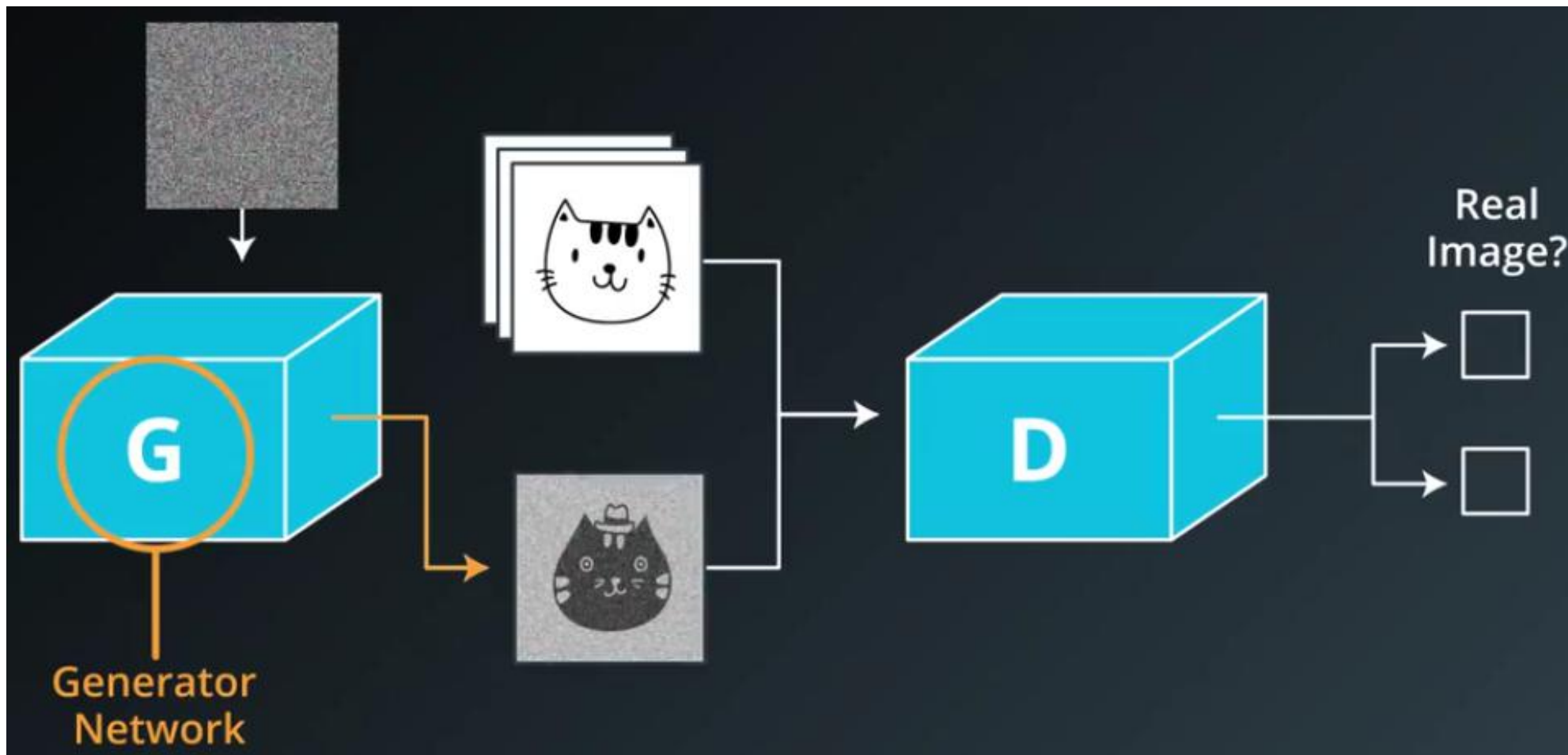
<https://github.com/junyanz/CycleGAN>

<https://affinelayer.com/pixsrv/>

- 图像生成，超分辨率
- 语义分割
- 文字生成
- 数据增强
- 聊天机器人
- 信息检索，排序



三 Gans运作原理



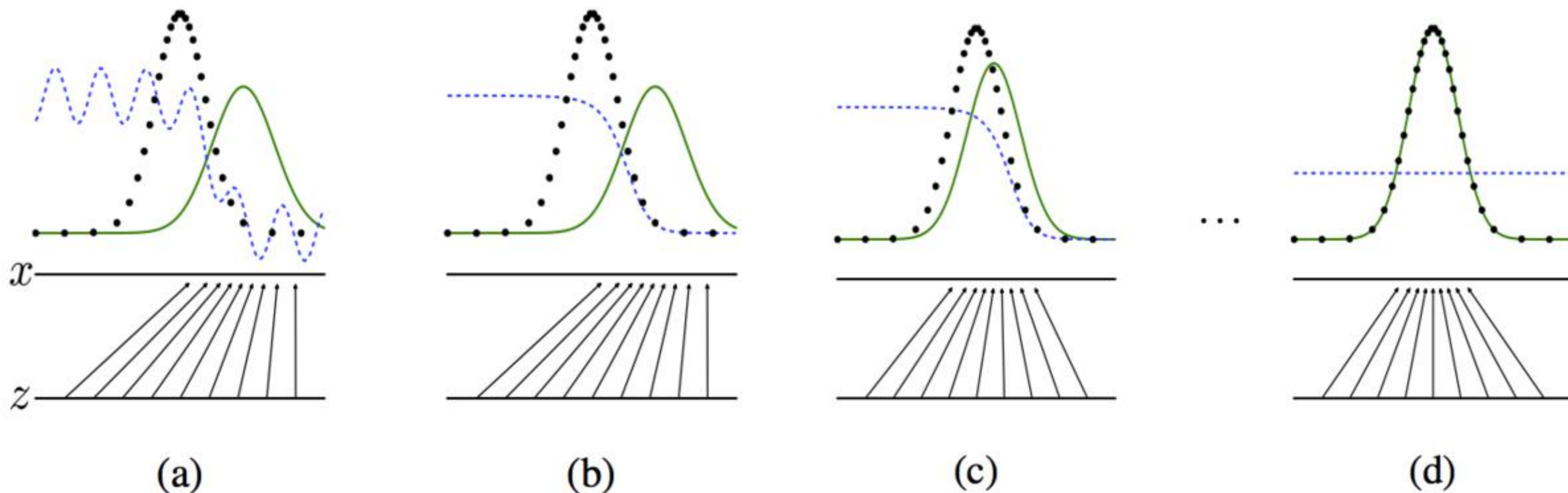
电影《逍遥法外》男主角制作伪造支票（G-net）；FBI警方(D-net)。

男主角（G-net）在FBI(D-net)逼迫下，不断提升伪造技术，最终伪造出“真”的支票。

三 Gans运作原理

■ GAN是什么，他是怎么对抗的？

- ◆ 生成式对抗网络包含一个**生成模型**（generative model, G）和一个**判别模型**（discriminative model, D）。
- ◆ 主要解决的问题shipping如何从训练样本中学习出新样本。
- ◆ 生成模型就是负责训练出样本的分布，判别模型是一个二分类器，用来判断输入样本时真实数据还是训练生成的样本。



图a,b,c,d. 黑色的点状线代表M所产生的一些数据，绿色的线代表我们自己模拟的分布G，蓝色的线代表着分类模型D。

a图表示初始状态，b图表示，保持G不动，优化D，直到分类的准确率最高。

c图表示保持D不动，优化G，直到混淆程度最高。d图表示，多次迭代后，终于使得G能够完全你和M产生的数据，从而认为，G就是M。

博弈

- 生成式对抗网络的优化是一个二元极小极大博弈 (minimax two-player game) 问题，它的目的是使生成模型的输出再输入给判别模型时，判别模型很难判断是真实数据还是虚假数据。
- 训练好的生成模型，有能力把一个噪声向量转化成和训练类似的样本
- **石头 剪刀 布 的例子。**

前向传播阶段

■ 可以有两种输入

- ◆ 1、我们随机产生一个随机向量作为生成模型的数据，然后经过生成模型后产生一个新的向量，作为Fake Image，记作 $D(z)$ 。
- ◆ 2、从数据集中随机选择一张图片，将图片转化成向量，作为Real Image,记作 x 。

■ 将由1或者2产生的输出，作为判别网络的输入，经过判别网络后输入值为一个0到1之间的数，用于表示输入图片为Real Image的概率，real为1，fake为0。

判别模型的损失函数

- 当输入的是从数据集中取出的real image 数据时，我们只需要考虑第二部分， $D(x)$ 为判别模型的输出，表示输入 x 为real 数据的概率，我们的目的是让判别模型的输出 $D(x)$ 的输出尽量靠近1。
- 当输入的为fake数据时，我们只计算第一部分， $G(z)$ 是生成模型的输出，输出的是一张Fake Image。我们要做的是让 $D(G(z))$ 的输出尽可能趋向于0。这样才能表示判别模型是有区分力的。
- **相对判别模型来说，这个损失函数其实就是交叉熵损失函数。计算loss，进行梯度反传。**这里的梯度反传可以使用任何一种梯度修正的方法。当更新完判别模型的参数后，我们再去更新生成模型的参数。

$$-((1-y)\log(1-D(G(z))) + y\log D(x))$$

生成模型的损失函数

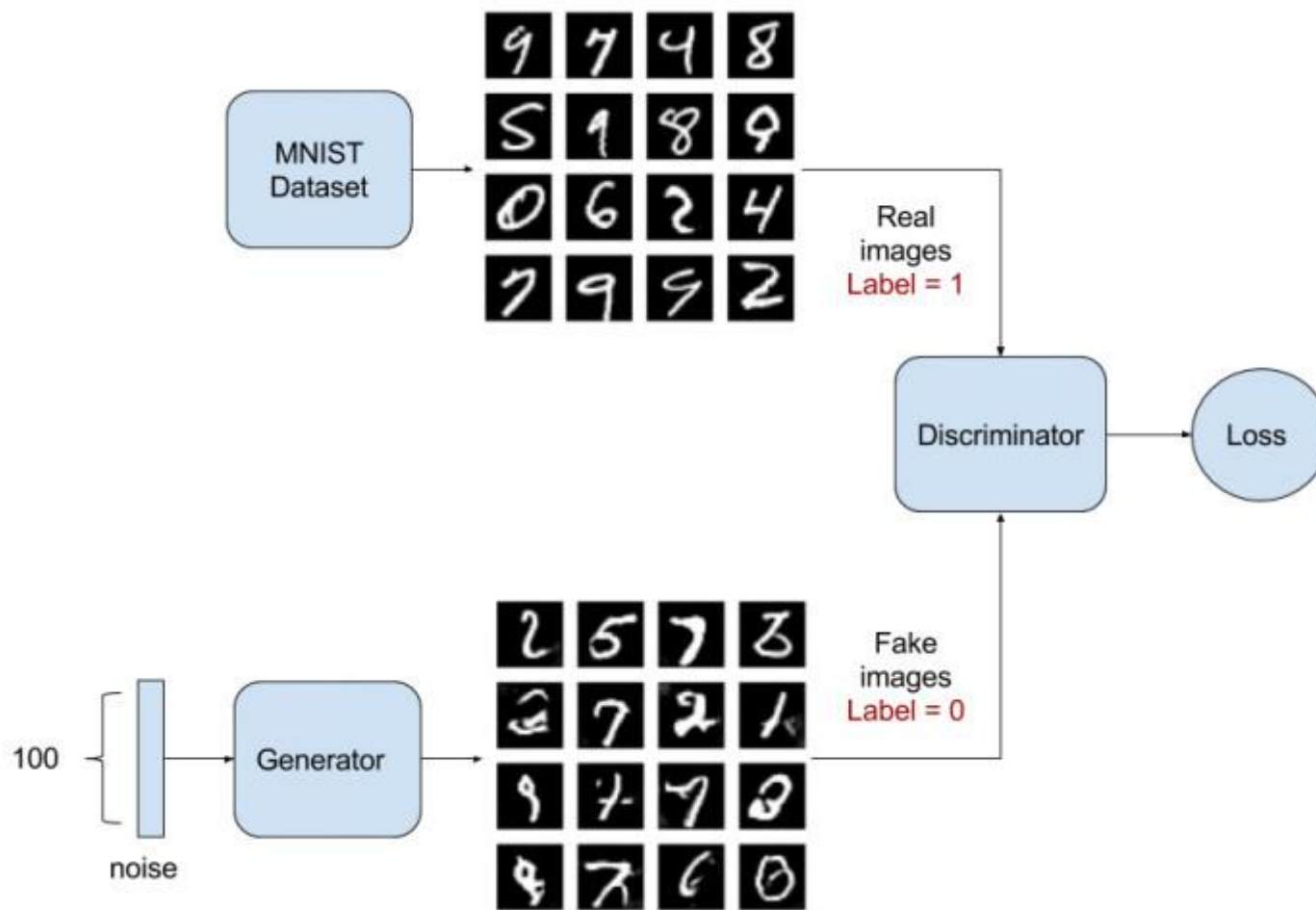
- 对于生成模型来说，我们要做的是让 $G(z)$ 产生的数据尽可能的和数据集中的数据一样。就是所谓的同样的数据分布。那么我们要做的就是最小化生成模型的误差，即只将由 $G(z)$ 产生的误差传给生成模型。
- 但是针对判别模型的预测结果，要对梯度变化的方向进行改变。当判别模型认为 $G(z)$ 输出为真实数据集的时候和认为输出为噪声数据的时候，梯度更新方向要进行改变。
- 其中 \bar{D} 表示判别模型的预测类别，对预测概率取整，为0或者1。用于更改梯度方向，阈值可以自己设置，或者正常的话就是0.5。

$$(1 - y) \log(1 - D(G(z))) (2 * \bar{D}(G(z)) - 1)$$

三 Gans网络架构核心 Vanilla-gans

- 一个最朴素的GAN模型，实际上是将一个随机变量（可以是高斯分布，或0到1之间的均匀分布），通过参数化的概率生成模型（通常是用一个**神经网络**模型来进行参数化），进行概率分布的逆变换采样，从而得到一个生成的概率分布。
- GAN的或者一般概率生成模型的训练目的，就是要使得生成的概率分布和真实数据的分布尽量接近，从而能够解释真实的数据。但是在实际应用中，我们完全没有办法知道真实数据的分布。我们所能够得到的只是从这个真实的数据分布中所采样得到的一些真实数据。

生成式对抗神经网络GAN-结构



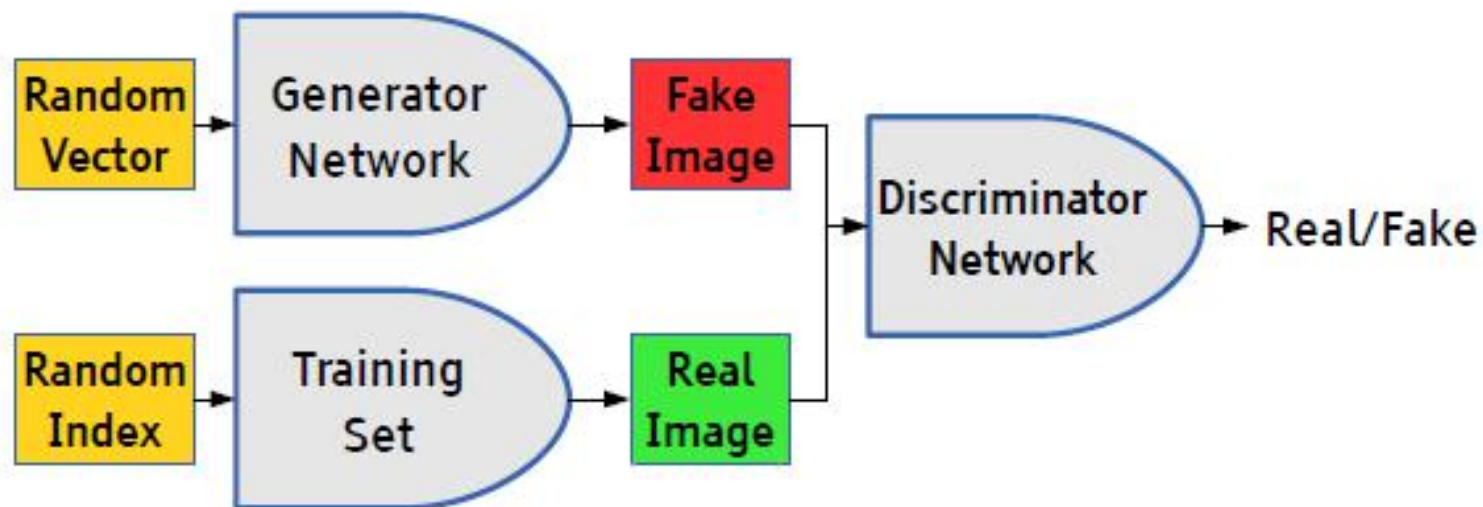
怎么定义损失

- 传统的生成模型，一般都采用数据的似然性来作为优化的目标，但**GAN创新性地使用了另外一种优化目标。**
- 首先，它引入了一个判别模型（常用的有支持向量机和多层神经网络）。
- 其次，它的优化过程就是在寻找生成模型和判别模型之间的一个纳什均衡。
- GAN所建立的一个学习框架，**实际上就是生成模型和判别模型之间的一个模仿游戏。**生成模型的目的，就是要尽量去模仿、建模和学习真实数据的分布规律；而判别模型则是要判别自己所得到的一个输入数据，究竟是来自于真实的数据分布还是来自于一个生成模型。通过这两个内部模型之间不断的竞争，从而提高两个模型的生成能力和判别能力。

详细实现过程

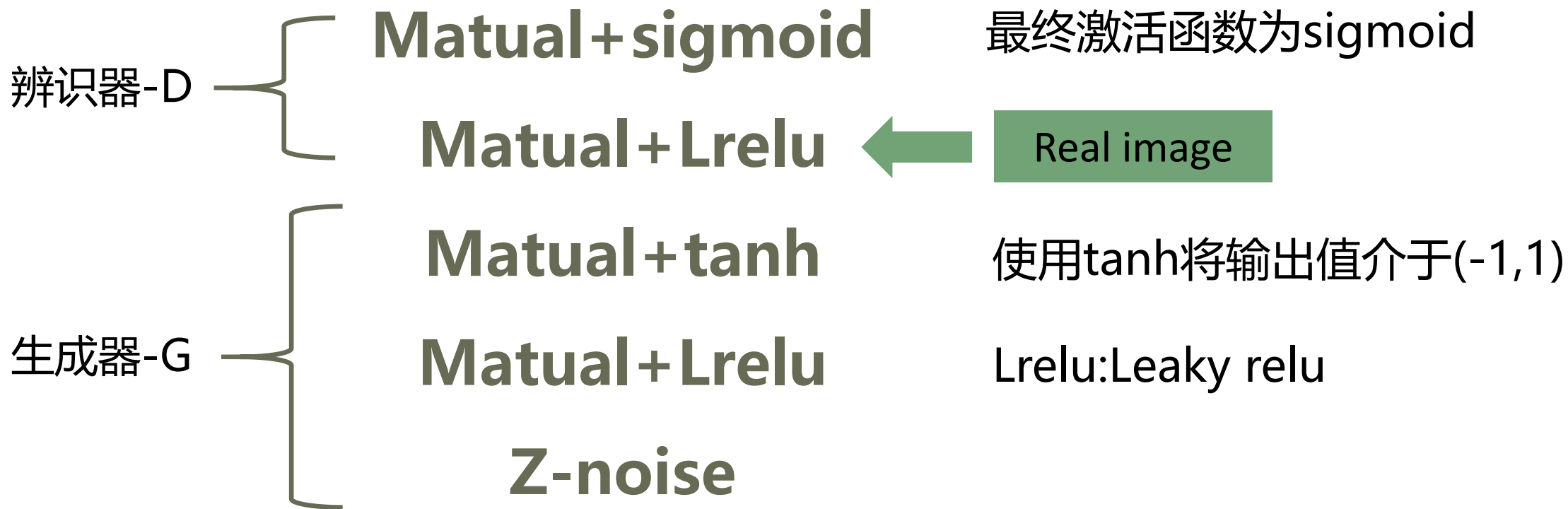
- 假设我们现在的数据集是手写体数字的数据集mnist。

初始化生成模型G、判别模型D（假设生成模型是一个简单的RBF，判别模型是一个简单的全连接网络，后面连接一层softmax）这些都是假设，对抗网络的生成模型和判别模型没有任何限制。

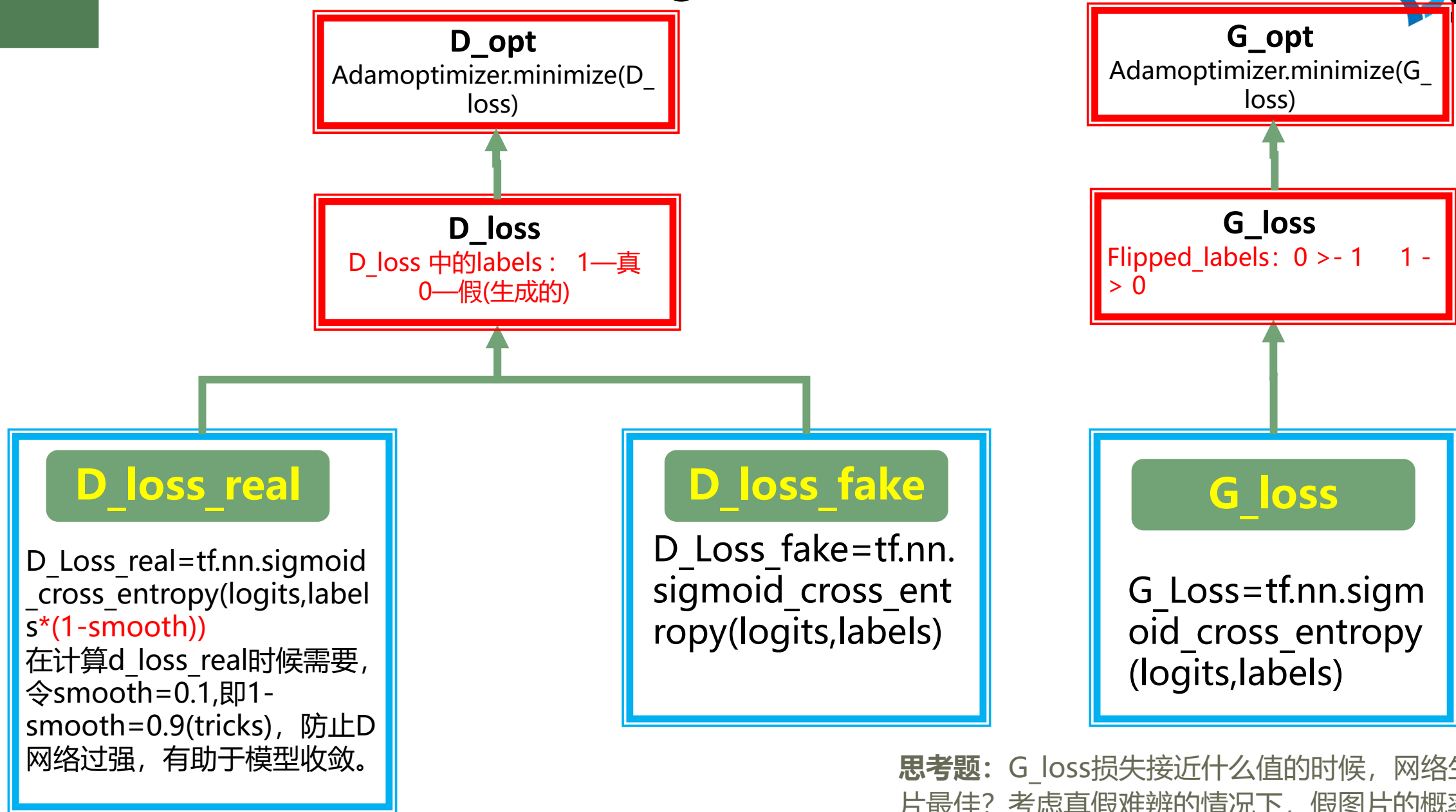


例子与训练

- 假设有一种概率分布 M ，它相对于我们是一个黑盒子。为了了解这个黑盒子中的东西是什么，我们构建了两个东西 G 和 D ， G 是另一种我们完全知道的概率分布， D 用来区分一个事件是由黑盒子中那个不知道的东西产生的还是由我们自己设的 G 产生的。
- 不断的调整 G 和 D ，直到 D 不能把事件区分出来为止。在调整过程中，需要：
- 优化 G ，使它尽可能的让 D 混淆。
- 优化 D ，使它尽可能的能区分出假冒的东西。
- 当 D 无法区分出事件的来源的时候，可以认为， G 和 M 是一样的。从而，我们就了解到了黑盒子中的东西。



思考题: 1、为什么用lrelu, 而不用relu; 2、判别器读入real image需要将值缩放到()区间?



思考题: G_loss损失接近什么值的时候, 网络生成的假图片最佳? 考虑真假难辨的情况下, 假图片的概率是。

算法流程图

■ 下图是原文给的算法流程，noise 就是随机输入生成模型的值。

Algorithm 1 Minibatch stochastic gradient descent training of generative adversarial nets. The number of steps to apply to the discriminator, k , is a hyperparameter. We used $k = 1$, the least expensive option, in our experiments.

for number of training iterations **do**

for k steps **do**

- Sample minibatch of m noise samples $\{z^{(1)}, \dots, z^{(m)}\}$ from noise prior $p_g(z)$.
- Sample minibatch of m examples $\{x^{(1)}, \dots, x^{(m)}\}$ from data generating distribution $p_{\text{data}}(x)$.
- Update the discriminator by ascending its stochastic gradient:

$$\nabla_{\theta_d} \frac{1}{m} \sum_{i=1}^m \left[\log D(x^{(i)}) + \log (1 - D(G(z^{(i)}))) \right].$$

end for

- Sample minibatch of m noise samples $\{z^{(1)}, \dots, z^{(m)}\}$ from noise prior $p_g(z)$.
- Update the generator by descending its stochastic gradient:

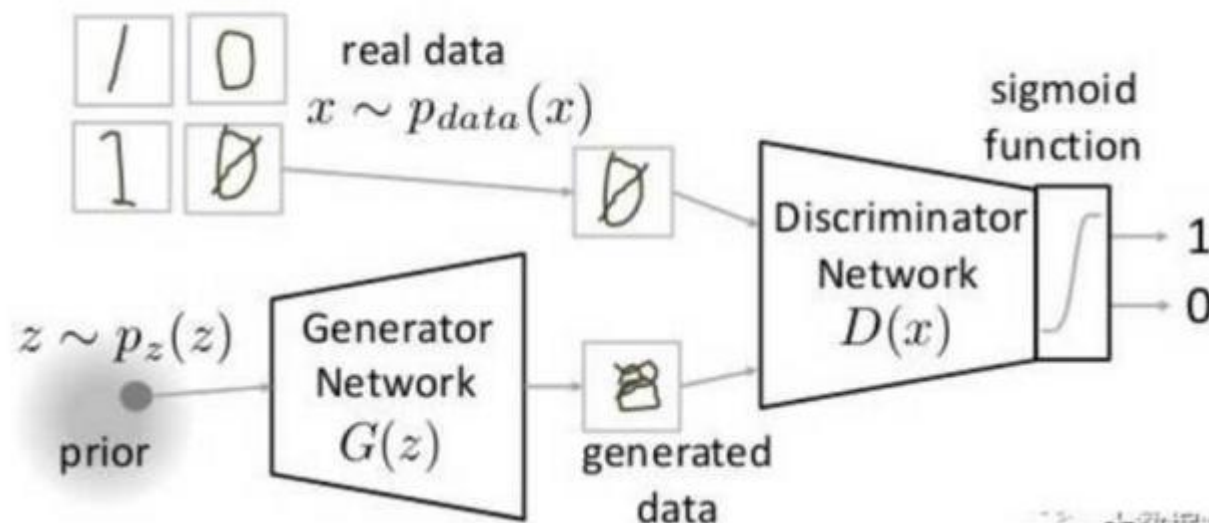
$$\nabla_{\theta_g} \frac{1}{m} \sum_{i=1}^m \log (1 - D(G(z^{(i)}))).$$

end for

The gradient-based updates can use any standard gradient-based learning rule. We used momentum in our experiments.

训练细节

- 训练阶段包括顺序完成的两个阶段
- **第一阶段：**训练鉴别器，冻结生成器（冻结意思是不训练，神经网络只向前传播，不进行Backpropagation反向传播）
- **第二阶段：**训练生成器，冻结鉴别器。



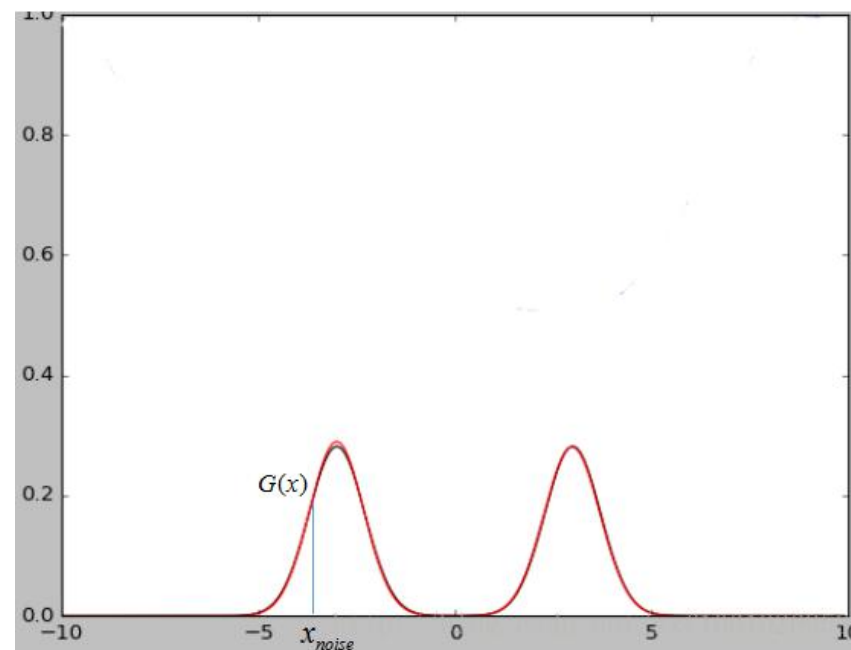
训练细节

■ 训练GAN的步骤

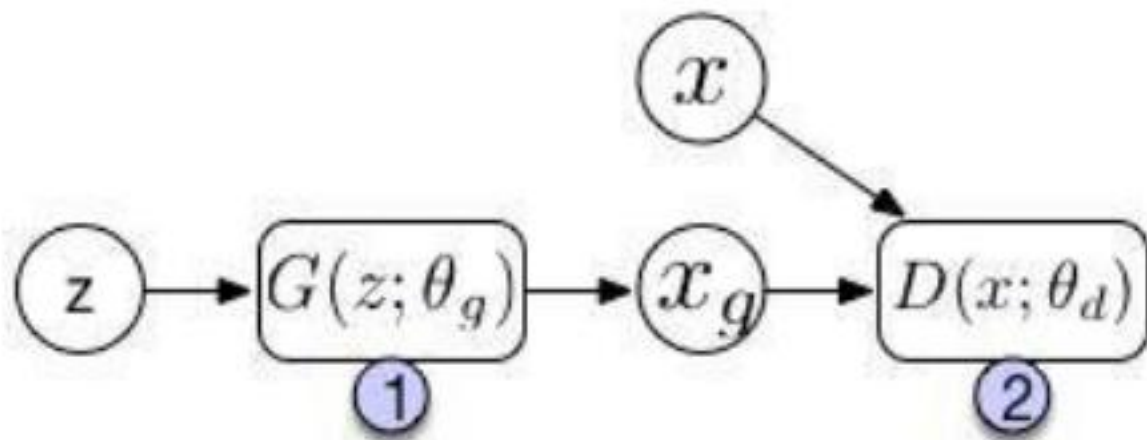
- **第1步：**定义问题。你想生成假的图像还是文字？你需要完全定义问题并收集数据。
- **第2步：**定义GAN的架构。GAN看起来是怎么样的，生成器和鉴别器应该是多层感知器还是卷积神经网络？这一步取决于你要解决的问题。
- **第3步：**用真实数据训练鉴别器N个epoch。训练鉴别器正确预测真实数据为真。这里N可以设置为1到无穷大之间的任意自然数。
- **第4步：**用生成器产生假的输入数据，用来训练鉴别器。训练鉴别器正确预测假的数据为假。
- **第5步：**用鉴别器的输出训练生成器。当鉴别器被训练后，将其预测值作为标记来训练生成器。训练生成器来迷惑鉴别器。
- **第6步：**重复第3到第5步多个epoch
- **第7步：**手动检查假数据是否合理。如果看起来合适就停止训练，否则回到第3步。这是一个手动任务，手动评估数据是检查其假冒程度的最佳方式。当这个步骤结束时，就可以评估GAN是否表现良好。

noise输入

- 假设我们现在的数据集是一个二维的高斯混合模型，那么这么noise就是x轴上我们随机输入的点，经过生成模型映射可以将x轴上的点映射到高斯混合模型上的点。当我们的数据集是图片的时候，那么我们输入的随机噪声其实就是相当于低维的数据，经过生成模型G的映射就变成了一张生成的图片 $G(x)$ 。
- 最终两个模型达到稳态的时候判别模型D的输出接近1/2，也就是说判别器很难判断出图片是真是假，这也说明了网络是会达到收敛的。



GANs总结



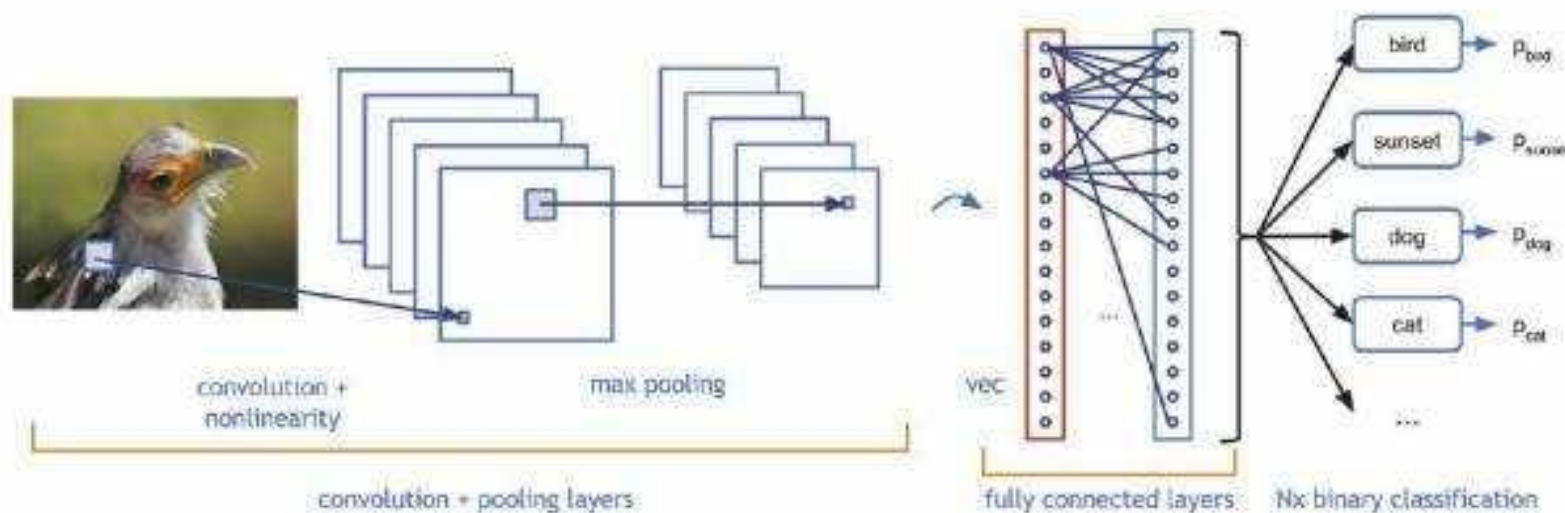
$$\min_G \max_D V(D, G) = \mathbb{E}_{\mathbf{x} \sim p_{\text{data}}(\mathbf{x})} [\log D(\mathbf{x})] + \mathbb{E}_{\mathbf{z} \sim p_z(\mathbf{z})} [\log(1 - D(G(\mathbf{z})))]$$

GANs总结

- 图中上半部分是GAN模型的基本架构。我们先从一个简单的分布中采样一个噪声信号 z （实际中可以采用 $[0, 1]$ 的均匀分布或者是标准正态分布），然后经过一个生成函数后映射为我们想要的分布 X_g （ z 和 X 都是向量）。生成的数据和真实数据都会输入一个识别网络 D 。识别网络通过判别，输出一个标量，表示数据来自真实数据的概率。
- 在实现上， G 和 D 都是可微分函数，都可以用多层神经网络实现。因此上面的整个模型的参数就可以利用backpropagation来训练得到。
- 图中的下半部分是模型训练中的目标函数。仔细看可以发现这个公式很像cross entropy，注意 D 是 $P(X_{data})$ 的近似。对于 D 而言要尽量使公式最大化（识别能力强），而对于 G 又想使之最小（生成的数据接近实际数据）。
- 整个训练是一个迭代过程，但是在迭代中，对 D 的优化又是内循环。所以每次迭代， D 先训练 k 次， G 训练一次。

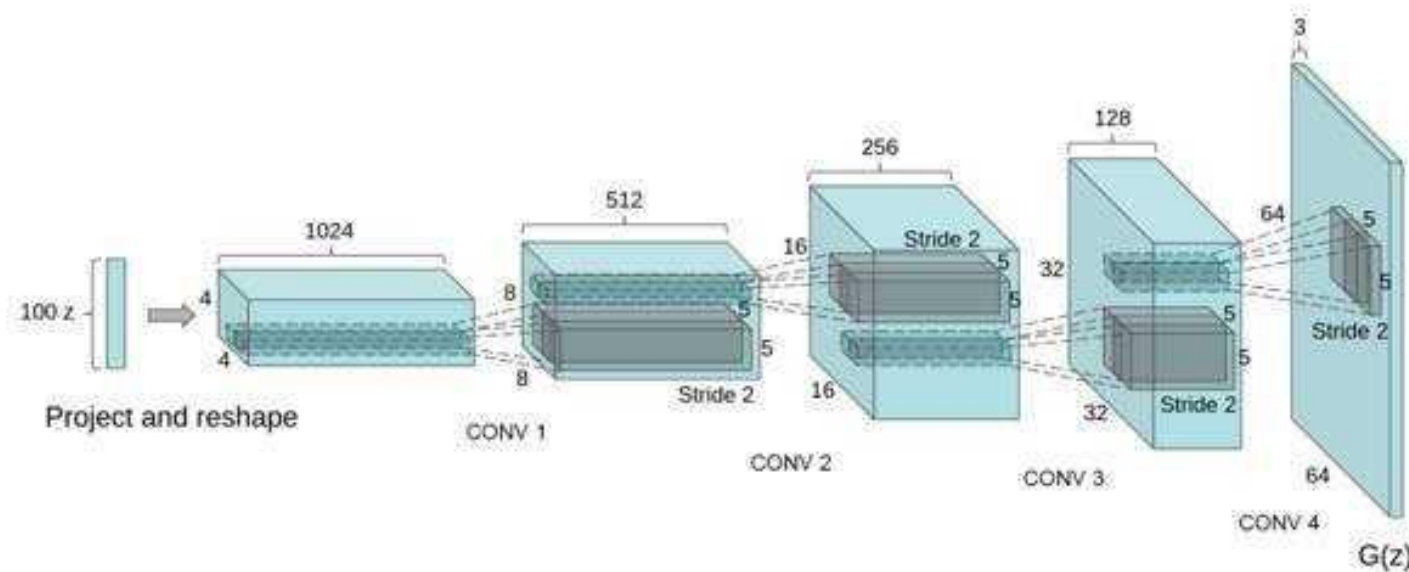
四 DCGAN

- 在图像生成过程中，如何设计生成模型和判别模型呢？深度学习里，对图像分类建模，刻画图像不同层次，抽象信息表达的最有效的模型是：CNN (convolutional neural network, 卷积神经网络)。



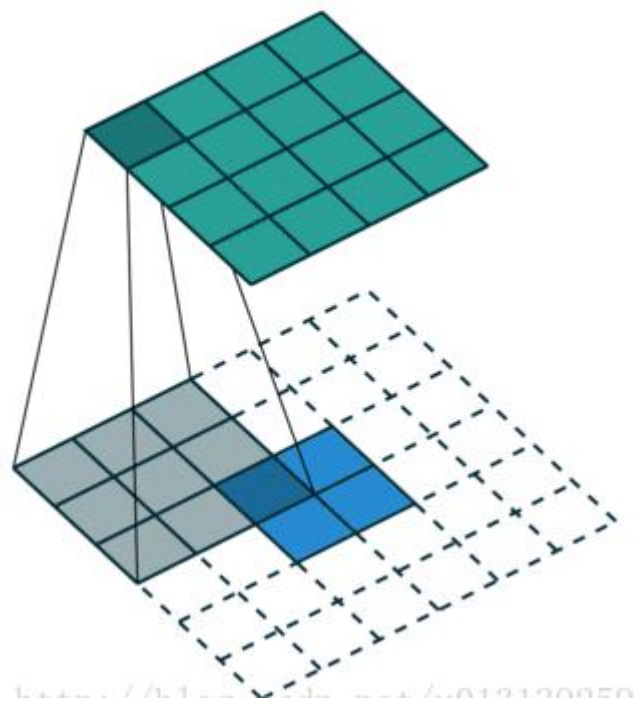
四 DCGAN

- 那么生成图像的模型应该是什么样子的呢？想想小时候上美术课，我们会先考虑构图，再勾画轮廓，然后再画细节，最后填充颜色，这事实上也是一个多层级的过程，就像是把图像理解的过程反过来，于是，人们为图像生成设计了一种类似反卷积的结构：Deep convolutional NN for GAN (DCGAN)



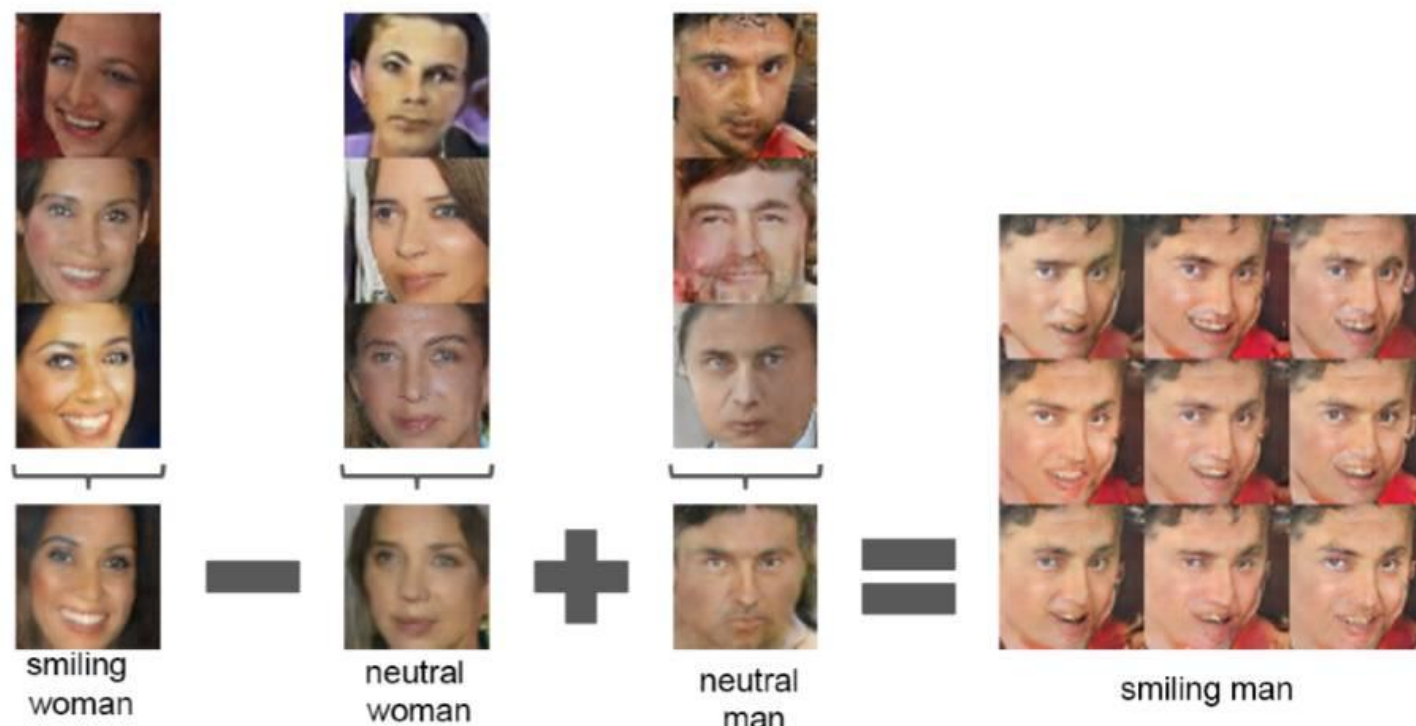
四 DCGAN

- 2x2的输入信号，经过3x3 的filters，产生了4x4的feature map。从小的维度产生大的维度，所以transposed-convolution又称为上采样卷积。

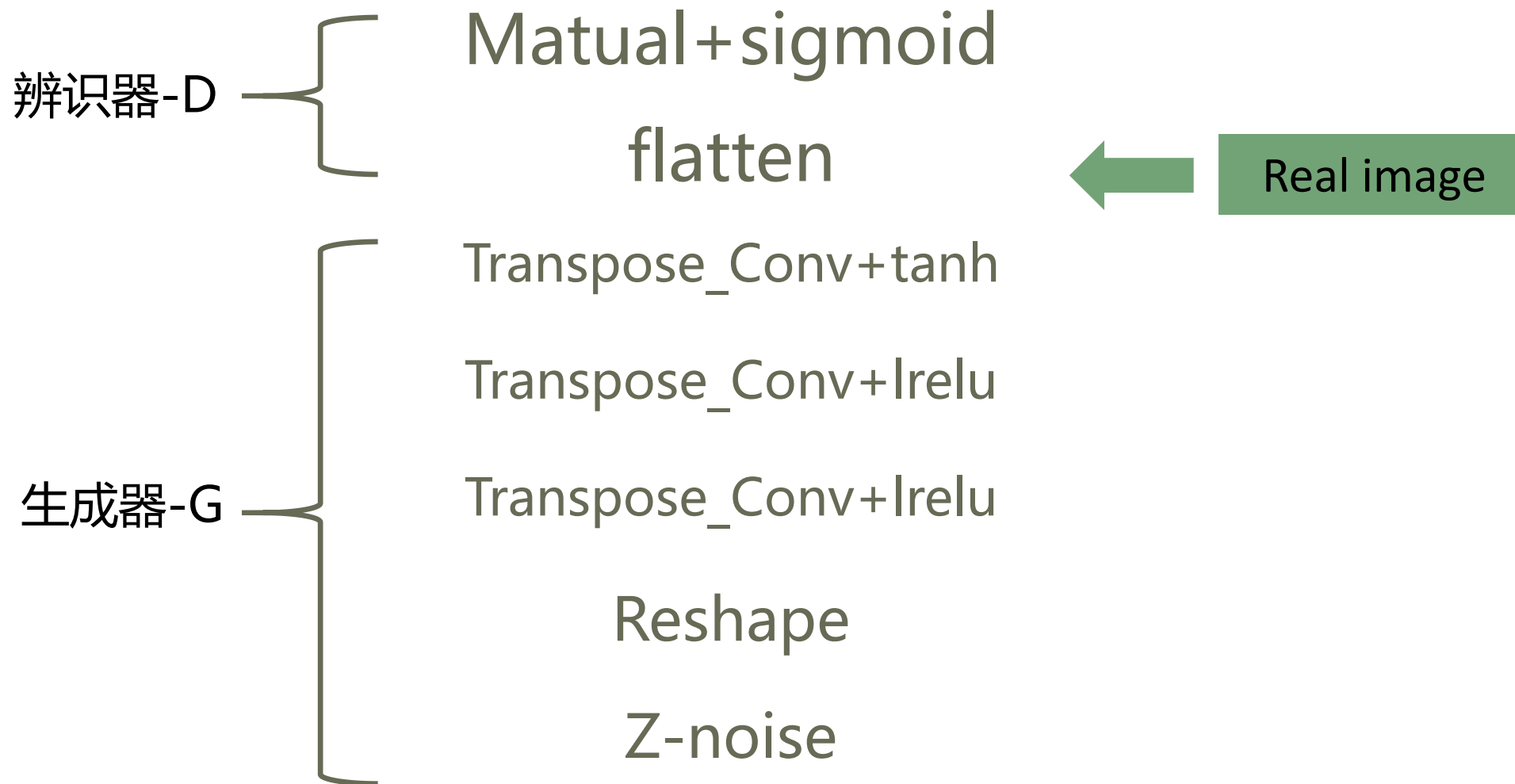


四 DCGAN

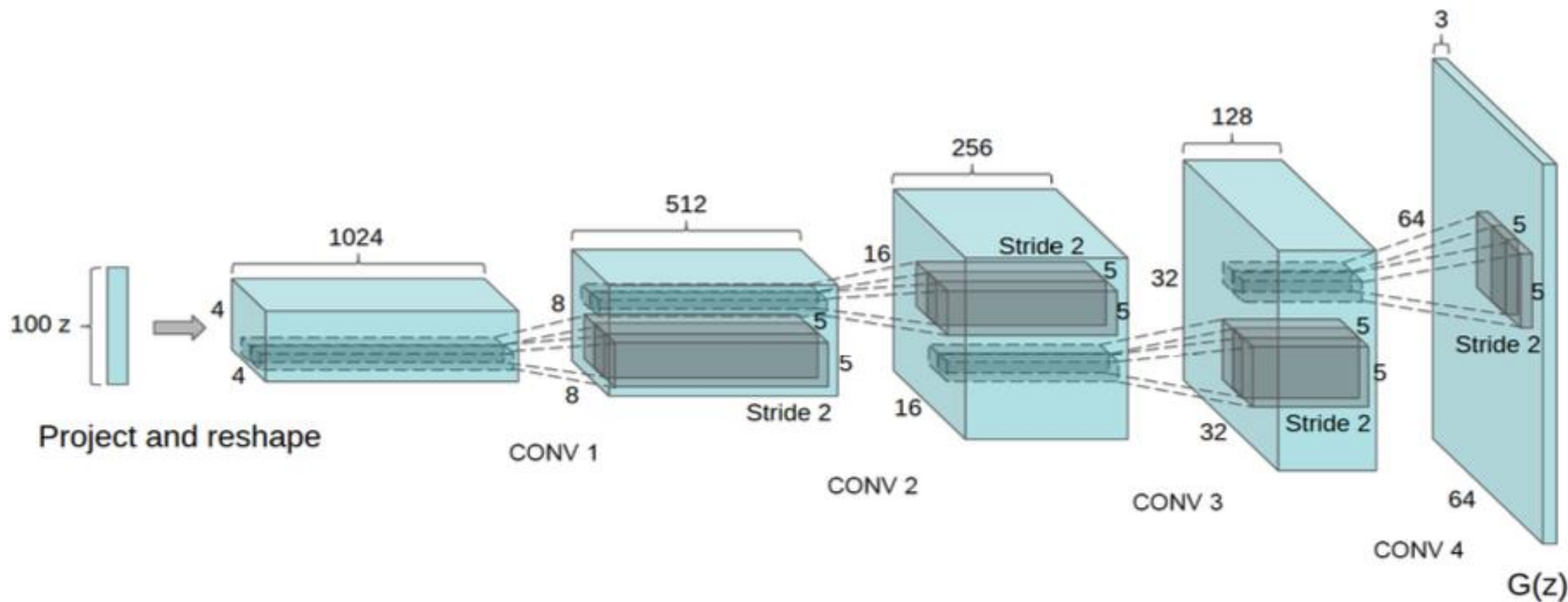
- DCGAN采用一个随机噪声向量作为输入，如高斯噪声。
- 输入通过与CNN类似但是相反的结构，将输入放大成二维数据。
- 通过采用这种结构的生成模型和CNN结构的判别模型，DCGAN在图片生成上可以达到相当可观的效果。



五 DCGans网络架构



五 生成器-G



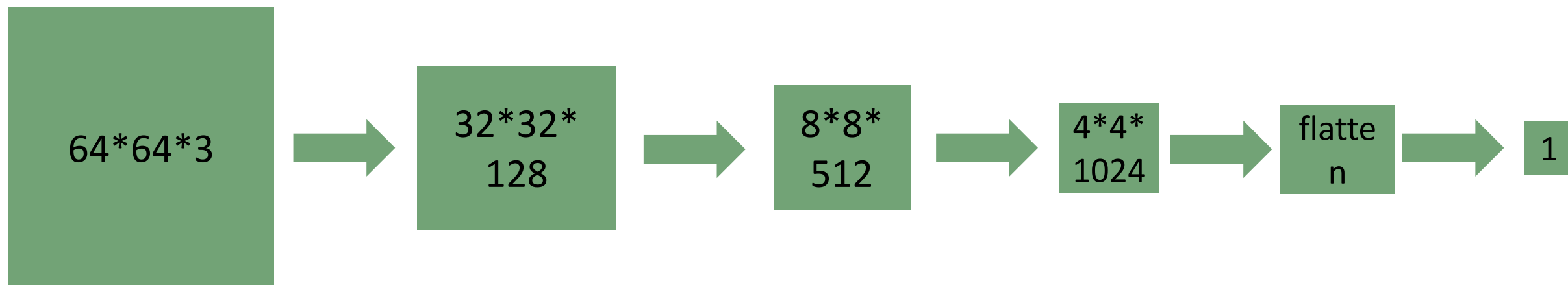
step1: Z向量($\text{len}(Z)=100$)-----4*4*1024 (FC) , 并重塑为4*4*1024的图片;

step2: 通过转置卷积 (conv2d_transpose) , 进行上采样 (upsampling) , 逐步减少深度, 增加高和宽;

step3: 最终生成shape和真图片shape一样的图片: 64*64*3。

备注: 1、隐藏层激活函数: Lrelu 2、无池化层 3、做批归一化

五 辨别器-D



- 1、隐藏层激活: Lrelu
- 2、无池化层
- 3、需要批归一化

GANs项目

- 01 生成手写数字集代码
- 02 DCgan手写数据集代码
- 03 人脸生成项目



THANK YOU

上海育创网络科技有限公司