01-GAN公式简明原理之铁甲小宝篇

原创 bryant 机器学习与生成对抗网络 2019-11-27

声明：以下内容纯为形成笔记过程中，增加趣味性，无他。若有相关利益冲突/侵权，指出删。不当处，亦欢迎指正。

背景：《铁甲小宝》是我极其幼时、已记不起何时看的一部日本动画片，剧情忘了，但还记得在外婆家偷偷用黑白电视机看的场景。用到此处，想致敬这部动画片带来的回忆。可能读者没看过，故摘自百度百科介绍：《铁甲小宝》主角机器人“卡布达”和他的伙伴小让，每天都为了寻找“和平星”而努力，因为只要集齐13块“和平星”便可实现全人类的梦想与愿望，但几个未完成睡眠学习的机器人，蟑螂恶霸、鲨鱼辣椒、蜘蛛侦探，蝎子莱莱等，常常从中破坏。正义的卡布达及伙伴，经过一番斗智斗勇，合力对抗；通过努力经与和平星守护人S化敌为友，互相支持，拯救了全人类！

话说，卡布达、小让等人为了实现全人类的梦想和愿望，终于集齐了13颗和平星。然而，新的挑战可能即将到来！听说人工智能崛起了，不知道会不会危害世界和平！这日，卡布达决定研究一波AI里颇具盛名的GAN，也就是生成对抗网络！

1 GAN的目的

小让学习真是太菜了，在调研资料上他似乎帮不上什么忙，不过呢，他还是很清楚GAN这个东西居然本质上和卡布达的“变换形态”是差不多的！会变身就完事了！

GAN最原始的动机是**把一个高斯分布的噪声向量（用z表示）变成新的信息形态x**，也就是生成一个新的数据分布

$$p_G(x;\theta)$$

表示，可能是图像文本语音等，而其中的

$$\theta$$

是GAN神经网络的参数，它们是用来控制生成的信息长什么样的。但是，GAN它必须要有新形态的参照物、要事先知道生成的形态大概长什么样才行，比如想生成一堆假的鲨鱼辣椒的照片，那就需要提供GAN现实中已有的、真正的一堆鲨鱼辣椒的照片给他看了才行，这堆真正的照片数据分布用

$$p_{data}(x)$$

表示。

2 如何衡量生成的鲨鱼辣椒照片像不像鲨鱼辣椒?

进一步地，卡布达发现，一些数学公式可以衡量两个数据分布像不像，比如KL散度，通过计算它们之间的KL散度，值越小，就越相似了。

$$D_{KL}(P||Q) = \sum_i P(i) \log \frac{P(i)}{Q(i)}$$

$$D_{KL}(P||Q) = \int_{-\infty}^{\infty} p(x) \log \frac{p(x)}{q(x)} dx$$

第一，绝对不意气用事；第二，绝对不漏判任何一件坏事；第三，绝对裁判的公正漂亮，裁判机器人蜻蜓队长前来觐见！

3 GAN的构造

原来，卡布达发现，GAN为了达到目的，并不是孤军奋战欸，它是由两个神经网络组建的。一个是生成器G，一个判别器D，其中G是一个“形态变换器”负责把高斯噪声变换到假的“鲨鱼辣椒图像”，有着生成的功能；D去判别真的和假的“鲨鱼辣椒图像”之间的差距，然后告诉G说哪儿生成地还不行，G听了D的反馈又拼命地努力改进，有一种两相对抗的感觉。卡布达从蜻蜓队长那里得知：G和D之间的关系用一个公式联系起来：

$$V(G,D) = E_{x\sim P_{data}}[\log D(X)] + E_{x\sim P_G}[\log(1 - D(X))]$$

然后通过最优化手段：

$$G^* = \arg\min_G \max_D V(G,D)$$

小让才读完四年级啊，一脸懵，这公式啥玩意儿？这个公式居然能让G生成逼真的”鲨鱼辣椒“图像？？卡布达也不太明白这个公式，于是他们也决定让卡布达启动超级变换形态，提高智商，彻底搞懂GAN的这个公式原理！

4 启动超级变换形态

卡布达得知，G的生成和D的判别是交替进行的。比如在某一个阶段，G经过了一段时间的努力生成了一些“鲨鱼辣椒图像”，它就停止改进自己，轮到D来判别真假图像之间的差距。根据公式，D当然是想尽自己所能地判断出来，想让V(G,D)在固定G下取得最大值：

$$
\begin{aligned}
V &= E_{x\sim P_{data}}[\log D(X)] + E_{x\sim P_G}[\log(1-D(x))] \\
&= \int_x P_{data}(x)\log D(x)dx + \int_x p_G(x)\log(1-D(x))dx \\
&= \int_x [P_{data}(x)\log D(X)] + P_G(x)\log(1-D(x))]dx
\end{aligned}
$$

其中，+号左边一项里的

$$x\sim P_{data}$$

表示该项x是真正的“鲨鱼辣椒图像”，D（X）表示D认为这张真图像是真的概率，D当然希望给出的这个概率越高越准；+号右边一项里

$$x\sim P_G$$

表示该项x是G生成的假图像，（1-D（X））中的D（X）表示D认为这张假图像是真的概率，D当然希望给出的这个概率越低越好，所以反过来也就是（1-D（X））越大越好。从而上述式子里的

$$P_{data}(x)\log D(x)+P_G(x)\log(1-D(x))$$

越大越好。其中，

$$P_{data}(x)$$

是已有的/真正的“鲨鱼辣椒”图像，可以看作固定常量。而当前阶段G已经固定/不再改进自己了，所以

$$P_G(x)$$

也为固定的常量，分别用a, b表示，此时D开始改进自己，通过仔细观察真假图像来提升自己的判别力，D是一个变量，让自己最大化，求导有：

$$f(D)=a\log(D)+b\log(1-D)$$

$$\frac{df(D)}{dD}=a\times\frac{1}{D}+b\times\frac{1}{1-D}\times(-1)=0$$

$$a\times\frac{1}{D^*}=b\times\frac{1}{1-D^*}$$

$$\Leftrightarrow a\times(1-D^*)=b\times D^*$$

$$D^*(x)=\frac{P_{data}(x)}{P_{data}(x)+P_G(x)}$$

然后把它代回公式：

$$\max V(G,D) = V(G,D^*)$$
$$= E_{x\sim P_{data}}[\log \frac{P_{data}(x)}{P_{data}(x)+P_G(x)}] + E_{x\sim P_G}[\log \frac{P_G(x)}{P_{data}(x)+P_G(x)}]$$
$$= \int_x P_{data}(x)\log \frac{\frac{1}{2}P_{data}}{\frac{P_{data}(x)+P_G(x)}{2}}dx + \int_x P_G(x)\log \frac{\frac{1}{2}P_G(x)}{\frac{P_{data}(x)+P_G(x)}{2}}dx$$
$$= -2\log 2 + KL(P_{data}(x)||\frac{P_{data}(x)+P_G(x)}{2}) + KL(P_G(x)||\frac{P_{data}(x)+P_G(x)}{2})$$

“锁蝶斯涅！”小让恍然大悟，“原来最大化V(G,D)实际上就能导出KL散度的衡量形式，这个[max V（G,D）]就是真图像和假图像之间的距离，为了让它们看上去一样，以假乱真，只要让距离最小也就是min[maxV（G,D）]即可！”卡布达终于欣慰：“老铁，你这真是双击666啊。”