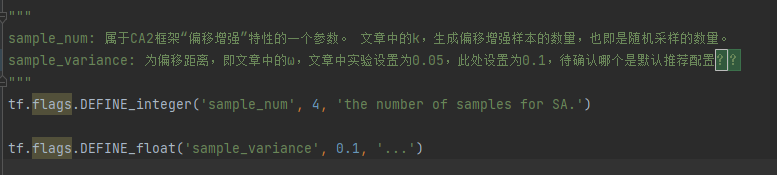
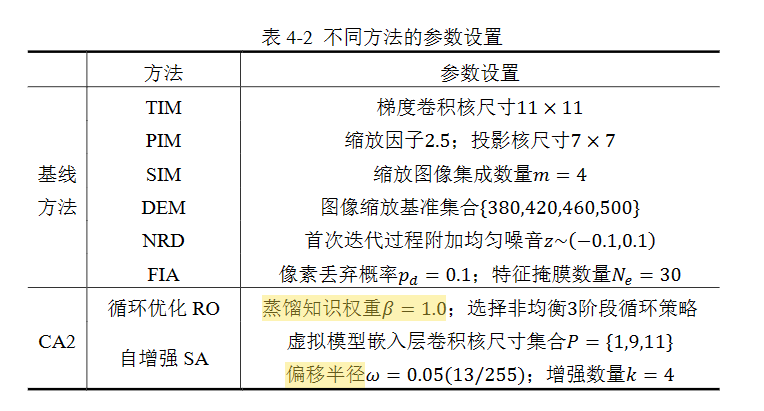
## 问题1

自增强策略中有一个参数ω（偏移距离），文章实验章节推荐配置为0.0.5，但是CA2 Github项目代码中配置为0.1。

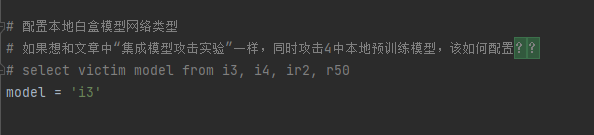
哪个是最终的推荐配？

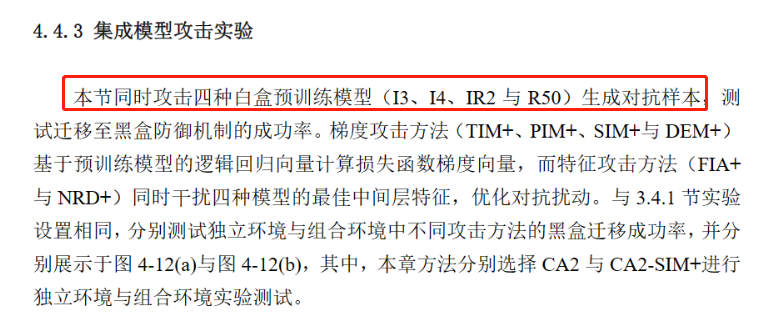




## 问题2

如果想和文章中“集成模型攻击实验”一样，同时攻击4中本地预训练模型，该如何配置？

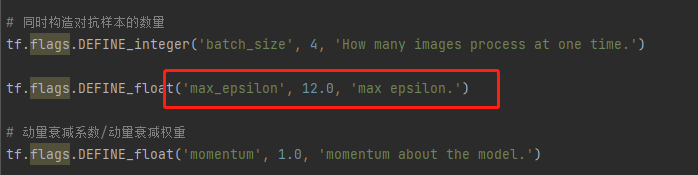


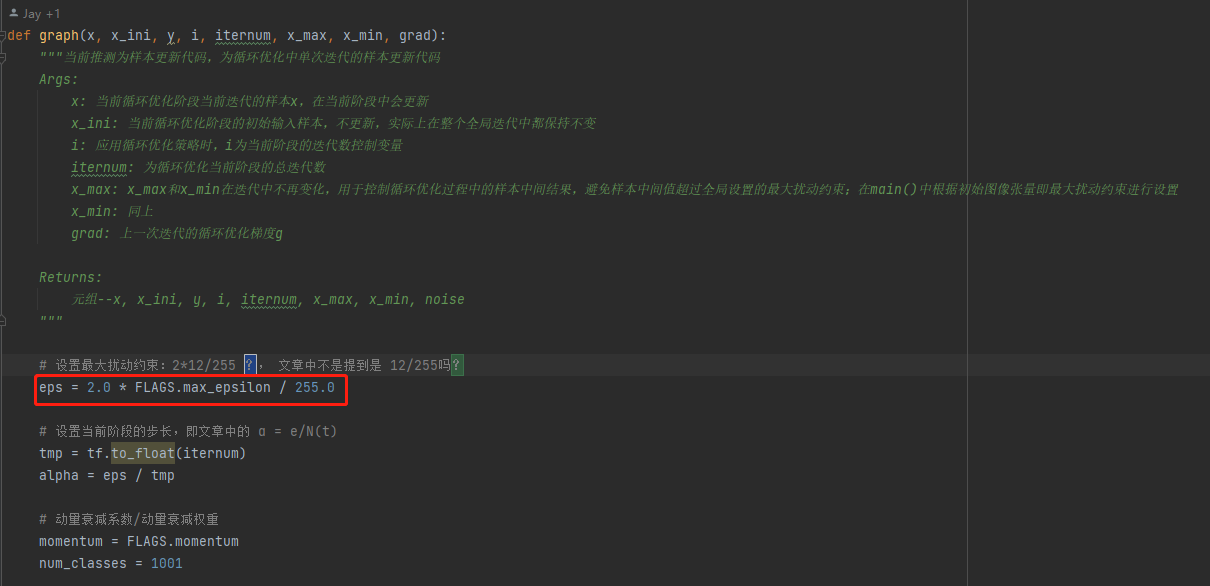


## 问题3

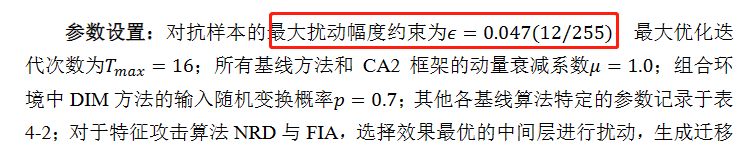
最大扰动幅度约束，文章中设置的为12/255，但是Github项目中graph()和main()的实现都把eps设置为24/255。

最终推荐设置是？



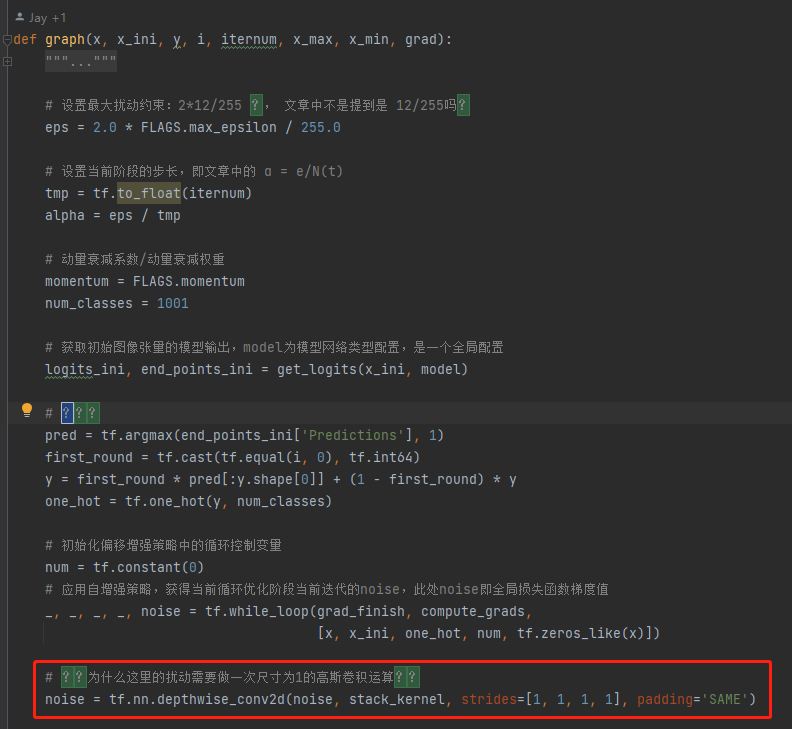






## 问题4

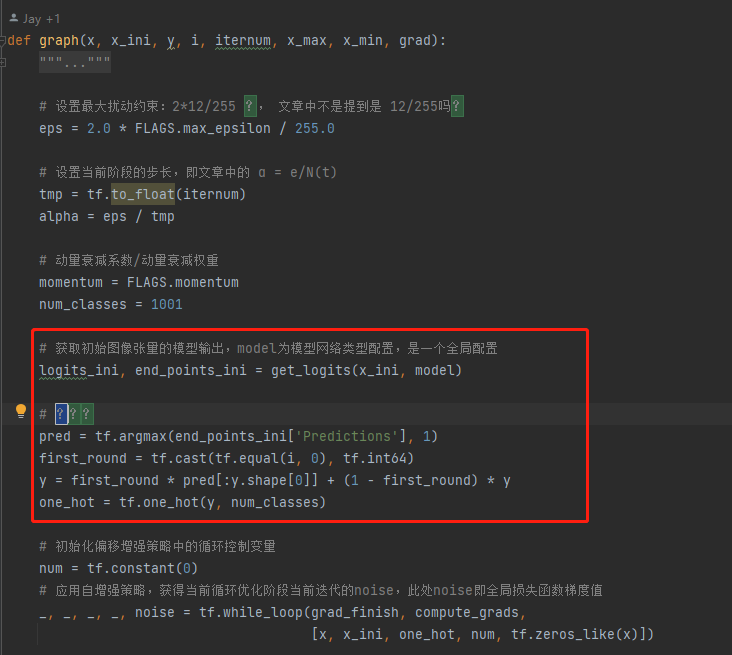
graph()的实现中，采用自增强策略计算得到损失函数梯度后，为什么需要进行一次卷积核尺寸为1的高斯卷积运算？ *//卷积核尺寸为1，计算后数值应该没有变化吧？*



## 问题5

还是关于graph()的实现，红框内的这段代码目的是为了计算one\_hot，没有搞明白。后面作为入参传递给compute\_grads()计算梯度。

one\_hot的含义和作用是什么？

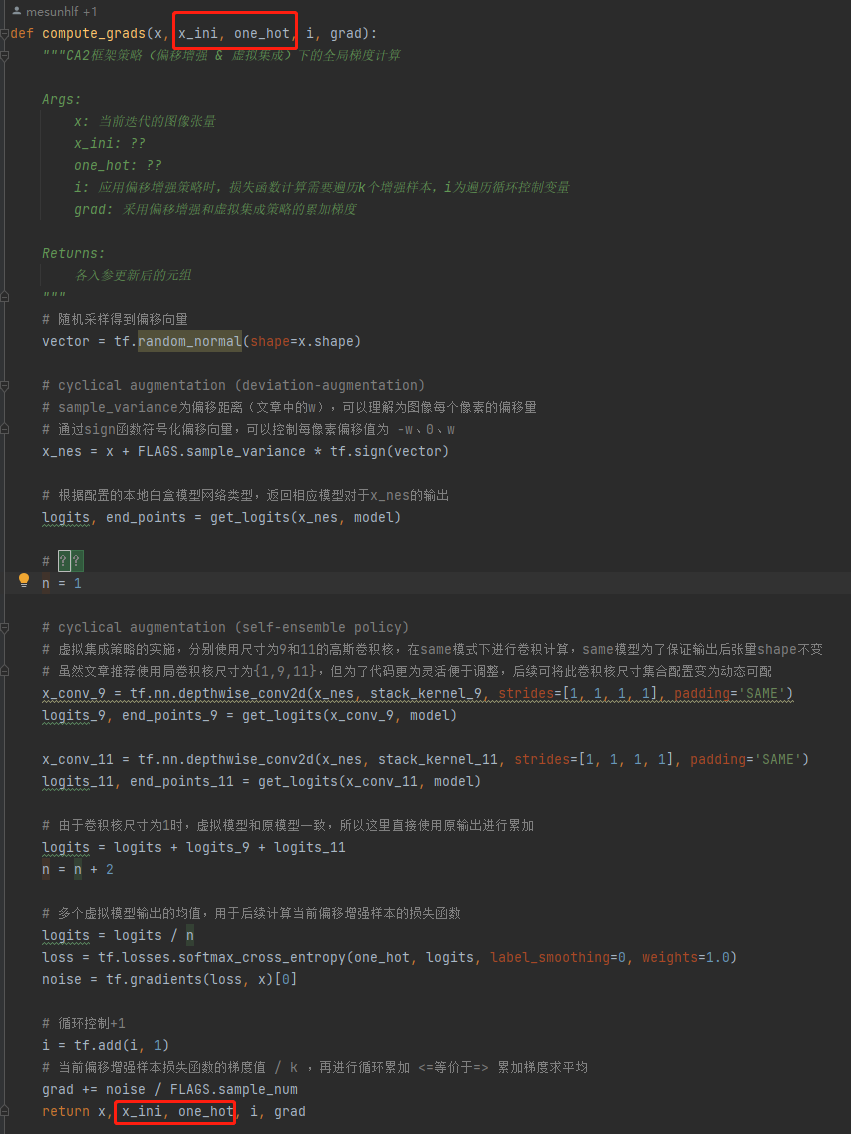


## 问题6

compute\_grads()的实现，入参x\_ini 和 one\_hot没搞明白作用。

x\_ini好像在return前没有变化，在自增强策略梯度计算的迭代中，起到的作用是？

one\_hot的疑问同上一个问题。



## 问题7

还是关于compute\_grads()的实现的问题：

文章中关于虚拟模型集成后的损失函数，定义为各个虚拟模型损失函数的累加和；

但是代码中是将各个虚拟模型的输出(logits)加和求平均后再计算交叉熵损失函数；

不太确认这里实现是否和文章定义是一致的？

