OKR：2018年第二季度，神经元变异完成实验并投稿出去(NIPS，ddl：5月18号)，找数值误差最大的输入，把找到的bug都复现且提交给开发者留下bug号，基于CNN的模型架构搭建起来。

数据集minist，神经网络自己训练，选择从最简单的CNN做起。目前得到的模型准确率是98%，设定为低于90%说明模型被明显扰动了。

RQ1:单调(只有一种变异算子)变异体对模型的影响是什么？相对测试样本，变异模型的准确率(精确率和召回率)等指标明显下降吗？

RQ2:复合变异体的指标表现如何？

RQ3：如何挑选变异体，才能尽可能地保证变异测试的有效性，同时又能大幅降低资源消耗。如何度量有效性？是不是距离越远的变异体，能杀死它的测试集也最不同。

RQ4:我们的神经元变异方法是否有效？

研究、实验计划讨论：

(1)通过实验研究和验证，如何对深度学习模型(深度神经网络结构+参数list)进行变异，才会明显改变模型的性能(准确率明显下降低于90%)。

通过一个简单的程序去不断尝试确定这些比例。

    1、对多大比例的神经元进行扰动；

    2、对每个神经元的权重扰动的比例得多大；

    3、对每个神经元的偏移扰动的比例得多大；

    4、修改激活函数；

    5、修改输入的维数；

    6、神经元的增减；

(2)如何证明我们的变异是有效的。通过明显有优劣区别的测试集，来证明我们的变异体只有优秀的测试集才能杀死。

神经元变异导致模型性能明显下降的阈值表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 权重修改 | W\*1.1 | W\*1.5 | W\*2 | W\*5 | W\*10 |
| 相应需要修改的神经元的比例 |  |  |  |  |  |
| 偏移修改 | B\*1.1 | B\*1.5 | B\*2 | B\*5 | B\*10 |
| 相应需要修改的神经元的比例 |  |  |  |  |  |

注意：神经元的选择是随机选择，按一定比例选择，从百分之百开始(我相信百分之100应该肯定会变的)，然后往下遍历，准确率低于90%不是说只跑一次随机修改就可以，需要跑10次(暂定)，十次里面都低于90%就算性能明显下降。

算法：

for(所有比例)

for(所有权重比例)

for(所有偏移比例)

只改变激活函数

只修改输入维数

增减神经元：for(个数和比例)