面向神经网络的模糊测试优化算法及模糊器实现

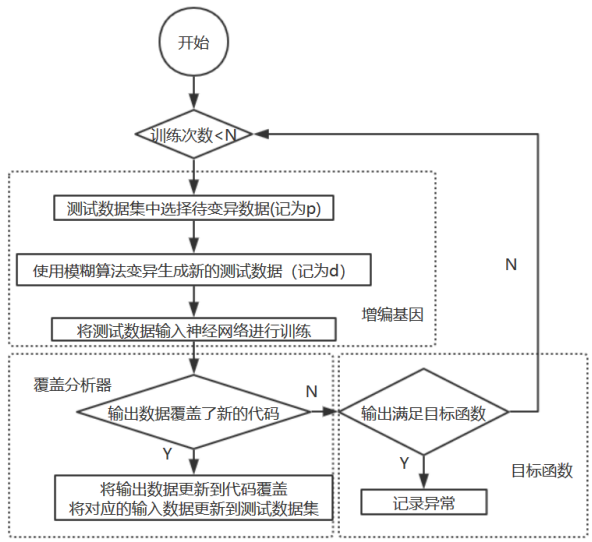
一. 成果完成人及所在单位：张晓云，光电与通信工程学院指导教师：熊飞兵 崔建峰

二. 成果简介：

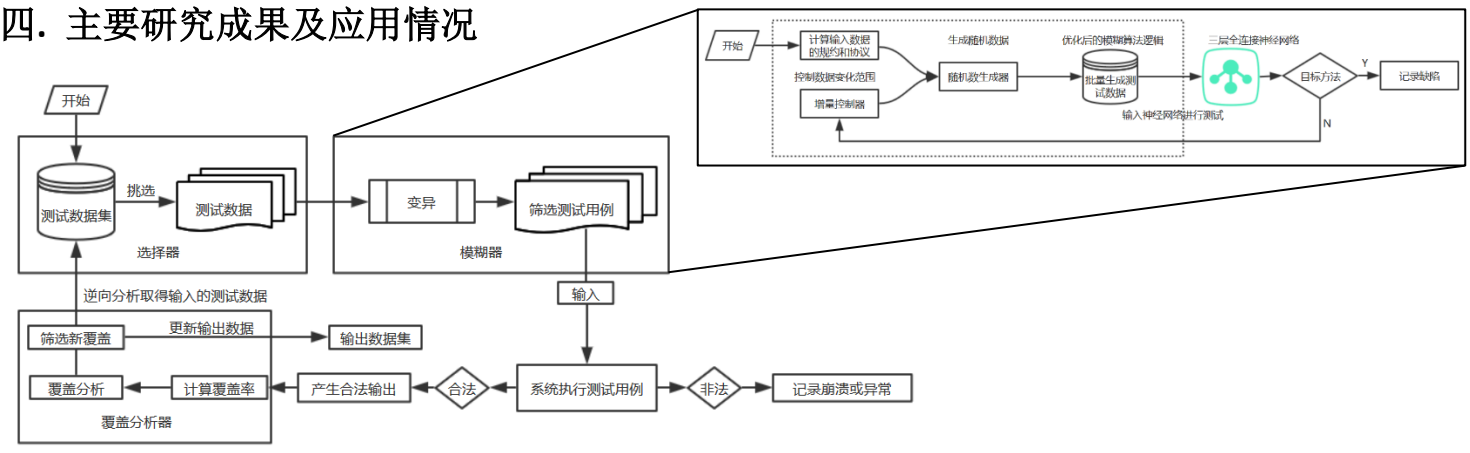
针对深度学习神经网络难以适配传统基于测试用例的测试方法这一情况，基于 TensorFuzz 神经网络测试框架的设计适用于测试神经网络的模糊算法，进而设计模糊器。TensorFuzz 是 2018 年 Google 发布的专门为神经网络检测缺陷框架，该框架在检测神经网络隐藏缺陷方面具有良好的效果，因此在发布后迅速成为最热门的神经网络模糊测试库。本研究针对该框架中测试流程进行研究，对最重要的部分模糊器的内部算法逻辑进行创新。通过对模糊数据产生过程进行高层次抽象，形成一种新的算法，并在此基础上实践出一种创新后的模糊器。对神经网络进行大量的训练和调优，通过测试结果逆向优化模糊算法，最终达到在神经网络中提高测试效率的目的。

三. 主要研究内容及创新点：

原始模糊器，首先将测试数据集作为输入，使用选择器在所构建好的新数据集中选择一个数据，传递到模糊器中进行变异，然后将变异后的数据输入神经网络执行训练，此时将输出结果分为两种情况。若输出结果满足了目标函数，即触发了崩溃或者检测到了异常，则说明模糊测试算法检测到了神经网络中存在的缺陷；若输出结果不满足目标函数，则通过覆盖分析器进行判断，是否覆盖了新的代码，并进一步确认是否更新测试数据集。优化后的模糊器，首先需要理解输入数据的规约和协议，在开始时通过随机数生成器和增量控制器生成测试数据，然后输入神经网络执行。此时也分为两种情况。若输出结果满足了目标函数，即触发了崩溃或检测到了异常，则记录该异常；若输出结果未满足目标函数，那么增量控制器会动态调整数据变化范围，生成一组新的测试用例，进行下一轮测试。在实际测试中，会多次改变增量控制器的参数使得生成的测试数据分布更加均匀。（图为：测试流程示意图）



四. 主要研究成果及应用情况



发表中文期刊：崔建峰,张晓云,陈金鑫.面向神经网络的模糊测试算法优化[J].厦门理工学院学报 2019,27(05):41-46

联系人：张晓云，　　电　话：15359262280　　E-mail：18030043877@163.com