

权利要求书

- 1、一种模型测试的方法，包括：
从测试样本集中获取样本；
将所述样本输入模型集包括的多个待测试模型中，以获得各个待测试模型的输出结果，其中，所述多个待测试模型包括至少一个神经网络模型；
根据所述输出结果确定测试结果，所述测试结果包括第一测试结果和第二测试结果中的至少一项，所述第一测试结果包括各个待测试模型的输出结果的准确性，所述第二测试结果包括所述至少一个神经网络模型的神经元覆盖率；
在所述测试结果未满足预定条件的情况下，按照预定规则，基于所述样本生成新样本，并将所述新样本加入所述测试样本集。
- 2、根据权利要求1所述的方法，其中，在所述测试结果包括第一测试结果的情况下，所述根据所述输出结果确定测试结果包括：
对所述多个待测试模型中包括的功能相同的待测试模型，投票确定正确输出结果，其中，票数最多的输出结果为正确输出结果；
确定输出结果为所述正确输出结果的待测试模型输出结果准确。
- 3、根据权利要求1所述的方法，其中，所述模型集中包括标准模型；以及
所述根据所述输出结果确定测试结果包括：
基于标准模型的输出结果，确定与所述标准模型功能相同的待测试模型的正确输出结果；
确定输出结果为所述正确输出结果的待测试模型的输出结果准确。
- 4、根据权利要求1所述的方法，其中，在所述测试结果包括第二测试结果的情况下，所述根据所述输出结果确定测试结果包括：
根据所述至少一个神经网络模型中各个神经元的输出是否满足输出条件，统计各个神经网络模型的神经元覆盖数，其中，所述神经元覆盖数包括，测试过程中满足过输出条件的神经元个数；
基于所述神经元覆盖数确定各个神经网络模型的神经元覆盖率，其中，所述神经元覆盖率和以下比值正相关：所述神经元覆盖数与总神经元个数的比值。
- 5、根据权利要求4所述的方法，其中，所述预定条件包括：
所述至少一个神经网络模型的神经元覆盖率均大于预设覆盖率阈值。
- 6、根据权利要求5所述的方法，其中，所述预定条件还包括：
所述多个待测试模型的输出结果准确度均大于预设准确度阈值。

7、根据权利要求 1 所述的方法，其中，按照预定规则，基于所述样本生成新样本包括：

获取所述样本中各个特征的设定范围；

基于各个特征的设定范围为所述样本添加随机扰动项，生成新样本。

5 8、根据权利要求 1 所述的方法，所述方法还包括以下中的一项或多项：

剔除模型集中测试结果满足所述预定条件的待测试模型；

在模型集中加入新的待测试模型。

9、一种模型测试的装置，包括：

获取单元，配置为从测试样本集中获取样本；

10 测试单元，配置为将所述样本输入模型集包括的多个待测试模型中，以获得各个待测试模型的输出结果，其中，所述多个待测试模型包括至少一个神经网络模型；

确定单元，配置为根据所述输出结果确定测试结果，所述测试结果包括第一测试结果和第二测试结果中的至少一项，所述第一测试结果包括各个待测试模型的输出结果的准确性，所述第二测试结果包括所述至少一个神经网络模型的神经元覆盖率；

15 生成单元，配置为在所述测试结果未满足预定条件的情况下，按照预定规则，基于所述样本生成新样本，并将所述新样本加入所述测试样本集。

10、根据权利要求 9 所述的装置，其中，在所述测试结果包括第一测试结果的情况下，所述确定单元包括：

20 结果确定模块，配置为对所述多个待测试模型中包括的功能相同的待测试模型，投票确定正确输出结果，其中，票数最高的输出结果为正确输出结果；

准确性确定模块，配置为确定输出结果为所述正确输出结果的待测试模型输出结果准确。

11、根据权利要求 9 所述的装置，所述模型集中包括标准模型，以及，

所述确定单元包括：

25 结果确定模块，配置为基于标准模型的输出结果，确定与所述标准模型功能相同的待测试模型的正确输出结果；

准确性确定模块，配置为确定输出结果为所述正确输出结果的待测试模型输出准确。

12、根据权利要求 9 所述的装置，其中，在所述测试结果包括第二测试结果的情况下，所述确定单元包括：

30 统计模块，配置为根据所述至少一个神经网络模型中各个神经元的输出是否满足输出条件，统计各个神经网络模型的神经元覆盖数，其中，所述神经元覆盖数包括，测试

过程中满足过输出条件的神经元个数;

覆盖率确定模块,配置为基于所述神经元覆盖数确定各个神经网络模型的神经元覆盖率,其中,所述神经元覆盖率和以下比值正相关:所述神经元覆盖数与总神经元个数的比值。

5 13、根据权利要求 12 所述的装置,其中,所述预定条件包括:

所述至少一个神经网络模型的神经元覆盖率均大于预设覆盖率阈值。

14、根据权利要求 13 所述的装置,其中,所述预定条件还包括:

所述多个待测试模型的输出结果准确度均大于预设准确度阈值。

15、根据权利要求 9 所述的装置,其中,所述生成模块进一步配置为:

10 获取所述样本中各个特征的设定范围;

基于各个特征的设定范围为所述样本添加随机扰动项,生成新样本。

16、根据权利要求 9 所述的装置,所述装置还包括以下中的一项或多项:

剔除单元,配置为剔除模型集中测试结果满足所述预定条件的待测试模型;

添加单元,配置为在模型集中加入新的待测试模型。

15 17、一种计算机可读存储介质,其上存储有计算机程序,当所述计算机程序在计算机中执行时,令计算机执行权利要求 1-8 中任一项的所述的方法。

18、一种计算设备,包括存储器和处理器,其特征在于,所述存储器中存储有可执行代码,所述处理器执行所述可执行代码时,实现权利要求 1-8 中任一项所述的方法。