# Project plan for Mutation-Based Accuracy Improvements in Neural Networks using Spectrum-Based Fault Localization *Mutationsbasierte Genauigkeitsverbesserungen in neuronalen Netzwerken unter Nutzung spektrumbasierter Fehlerlokalisierung.*

Lennart Mühlhahn

November 8, 2023

## 1 Adapt DeepFault Functions

Adapting the needed DeepFault functions (excluding suspiciousness-guided input synthesis) from the DeepFault GitHub repo **eniser˙deepfault˙2019 eniser˙deepfault˙2023** to the new TensorFlow version. Furthermore, add a function to choose nodes at random.

## 2 Implement mutation functions

Functions for the following mutations:

- weight and bias mutations
  - random
  - by a fixed value
  - with a fixed value
- remove nodes
  - remove by slicing
  - set bias to zero
  - add a “sieve” layer

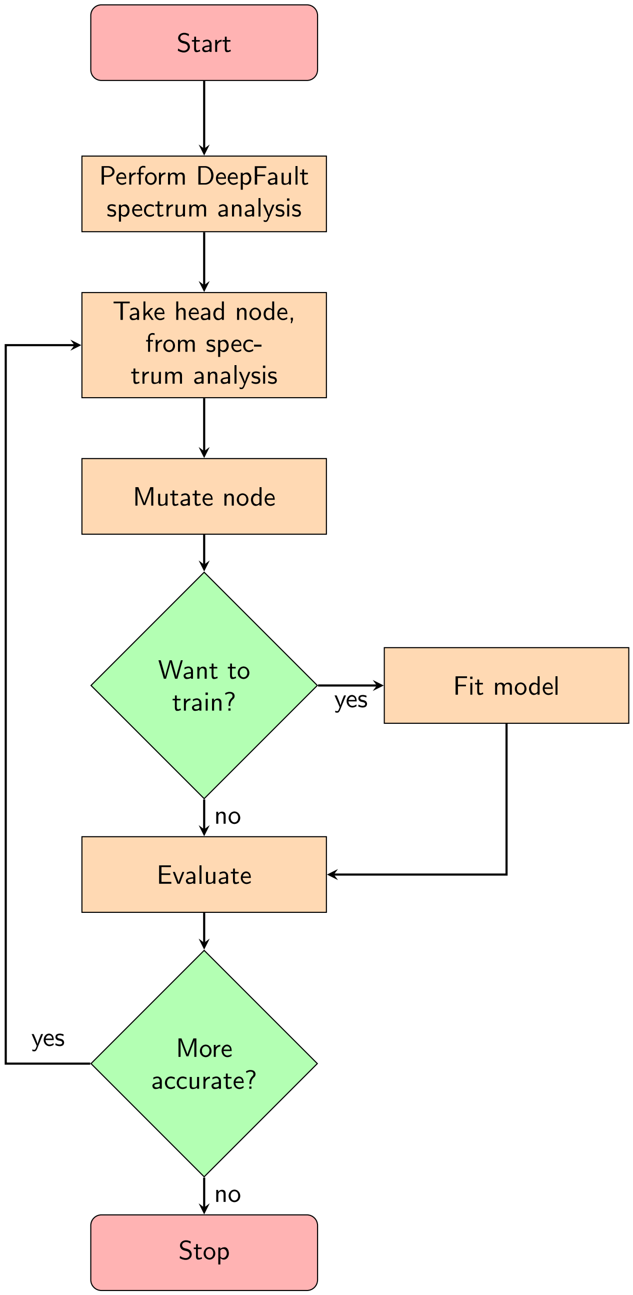
These functions need to be modified according to the findings of the DeepFault suspicious neuron identification.

# 3 Setup experiments

Implement a CNN and DNN based on the Fashion-MNIST dataset **xiao˙fashion-mnist˙2017** for experimenting. Create a container for conducting experiments.

# 4 Perform experiments

The experiments will try to modify suspicious nodes or delete suspicious nodes. I will try this until I get no more accuracy gains on the test data or a predefined number of modified nodes is reached. For the training one epoch will be performed and evaluated, but not used for further mutations, just for the evaluation.


Start
Perform DeepFault spectrum analysis
Take head node, from spectrum analysis
Mutate node
Want to train?
yes
Fit model
no
Evaluate
More accurate?
yes
no
Stop

# 5 Draft introduction

# 6 Draft main chapter

# 7 Draft background chapter

- Deep neural networks
- DNN testing and verification
- Mutation-based testing
- Spectrum analysis

# 8 Draft experimental results chapter

# 9 Draft conclusion

# 10 Revise chapters

# 11 Write abstract

# 12 Print Thesis

## Research Questions

RQ1. Could the mutation of faulty neurons improve the quality and reliability of a Deep Neural Network?

RQ2. Could the mutation of faulty neurons during training improve the quality and reliability of a Deep Neural Network?

RQ3. Which mutations are the most promising for improvement?

RQ4. Which combinations of mutations are the most promising?

RQ5. Which suspiciousness measure is the most promising for improving a Deep Neural Network?

RQ6. Are the suspiciousness measures more accurate than random choosing?

## Proposed Title