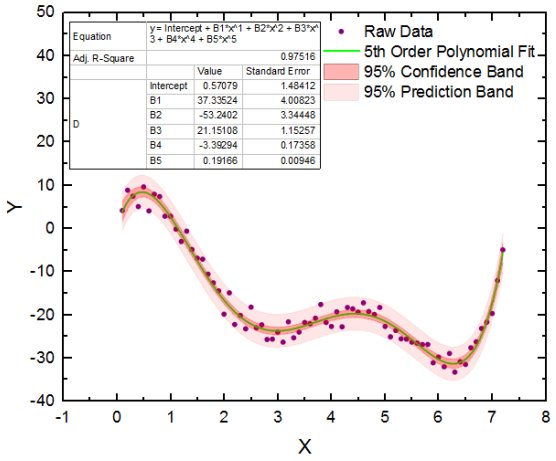
Function Fitting for Symbolic Execution

Advisor: **Masoud Ebrahimi**

Motivation

Have you tried Symbolic Execution?
It explodes when dealing with shared libraries!

In this project we want to tackle a arithmatic black-boxes that make symbolic execution almost impossible. Using a fitted curve we can enable symbolic executions to reveals bugs and vulnerabilites in software.



What is **symbolic execution**? a systematic and very effective approach to perform software testing.

What is a **black-box** and what is its **problem**? A black-box is a piece of software/hardware that you implement your software around it and it conceals parts of software execution paths, which makes systematic testing difficult (e.g., 3rd party libraries).

Can we **effectively** deal with **black-boxes**? Yes we can, we successfully used machine learning to this end. We already used automata learning to facilitate symbolic execution in the presence of black-box finite state machines [1].

Goals and Tasks

- Understand function fitting
- Fit a curve to an arithmatic black-box
- Get used to the existing framework (KLEE)
- Symbolically execute a fitted function

Literature

- B. K. Aichernig et al.
  Automata Learning
  for Symbolic Execution
  FMCAD'18

Schedule

- Reading related work and first steps
- Intermediate presentation or poster
- Implementing, experiments, …
- Writing thesis
- Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- Symbolic Execution
- WEKA is an Advantage
- Curve Fitting is an Advantage

Advisor / Contact

masoud.ebrahimi@iaik.tugraz.at