Symbolic Execution of Old Nintendo Games

Advisor: **Vedad Hadžić**

Motivation

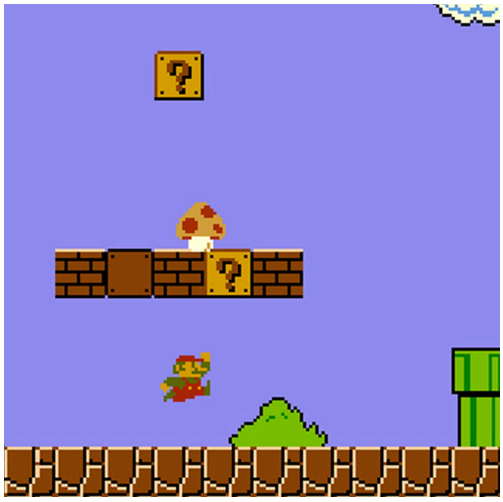
Symbolic execution is a program analysis technique that executes a program using symbolic inputs and constructs logic constraints that describe the execution paths taken by the program. Symbolic execution is used for everything from reverse-engineering and exploit development to test-generation and program coverage [2]. However, in this Bachelor thesis, you will use it to play games.

Nintendo has a long history of excellent games, arguably starting with the release of *Super Mario Bros.* in 1985. Since then, it has been played countless times and its machine code has been reverse-engineered [1]. Subsequently, speed-runners discovered many glitches and used them to achieve better world records.

Our goal is to use the knowledge of the disassembly, together with powerful symbolic execution engines [3], to beat the first level of this iconic game.

Goals and Tasks

- Become familiar with *angr* or *KLEE*
- Study the disassembly of SMB1
- Find a suitable emulator and modify it
- Perform symbolic execution with constraints
- Finish the first level in a semi-automated way



Literature

- doppelganger
  A Comprehensive Super Mario Bros. Disassembly
  https://gist.github.com/1wErt3r/4048722
- J. C. King
  Symbolic Execution and Program Testing
- Y. Shoshitaishvili et al.
  SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Good knowledge of Python, Logic, Assembly
- **(Bonus)** Familiarity with angr, KLEE, z3, MOS 6502 processors, emulators

Advisor / Contact

vedad.hadzic@iaik.tugraz.at