Java X86 Structured Disassembler

Master thesis project for: Reinhard Umgeher
Student ID: 0555818
E-Mail: uni@myside.at

The output of a X86 disassembler usually is in an assembler source code format. While such an output is nice for humans to read, it is not a good representation for machines to process. The goal of this project is to adjust an existing Java X86 Disassembler to output a structured Java data structure instead of a String object for each instruction.

Example

Consider the following disassembled machine code:

```plaintext
mov [rax + 16], rdi
xor rax rax
cmp rax, rdi
```

The Java data structures built instead of the text should look similar to:

```
MOV
srcBase = rax
srcDisplacement = 16
dstReg = rdi
```

```
XOR
srcReg = rax
dstReg = rax
```

```
CMP
leftReg = rax
rightReg = rax
```

The output should serve as the input for any Java program that wants to process the machine code. It should also be possible to give it as an input to a Java assembler.

Maxine

The disassembler that this project should be done with is part of the Maxine project (more information at http://research.sun.com/projects/maxine/). In case of a successful implementation, the code changes may be contributed back to the project.

Contact: Dipl.-Ing. Thomas Wuerthinger (wuerthinger@ssw.jku.at)