PDP-8 ISA Simulator

Deborah Denhart  
Jeremiah Franke

# Purpose

The purpose of this project was to familiarize ourselves with the instruction set architecture (ISA) for the PDP-8 processor by creating a PDP-8 simulator. This simulator is required to implement all of the PDP-8 instructions besides Microcode 3 and IO system calls. This project was to give us hands on demonstration of the ISA of a fairly simple processor so that we could better grasp the complexities that go along with implementing a RISC type ISA.

# Requirements

* Write an ISA level simulator for the PDP-8 architecture
* Generate a memory trace file with the format:
  + <type> <address>
  + <type> can be:
    - 0 for data read
    - 1 for data write
    - 2 for instruction fetch
  + <address> will be in octal format
  + The data that is read or written will not be displayed
* The different types of input can be:
  + Binary
  + ASCII hexadecimal
  + ASCII octal
* All instructions will be implemented
  + Except for I/O and group 3 microinstructions
    - Handled as NOPs
    - Has a clock cycle of 0
    - Print a warning
  + Must be clock accurate
  + Indirect addresses add 1cycle
  + Auto increment adds 2 cycles
  + Start at address 200 or assume the first address is the start
* Generate a summary at the end of execution
  + Total number of instructions executed
  + Total number of clock cycles consumed
  + Number of times each instruction type (by mnemonic) was executed

# Design

This simulator was designed to conform to the specifications provided by the many documentation resources for the ISA of the PDP-8. We very carefully tried to stay true to the original design of the PDP-8 architecture by emulating the framework that was used internally in the PDP-8 to fetch, execute, and decode instructions passed to it in a variety of programming formats. These assembly code formats were designed with the notion that the simulator needed to be able to accept binary, octal, and hexadecimal formatting for the proper instructions. This simulator is not designed to stop a user from running code that is correct but results in an incorrect final product, i.e. a forever loop. This simulator also features clock accuracy by way of simulating the time required to finish the different operations codes. This simulator does not currently have a graphic user interface, GUI, nor does it simulate the IO operations.

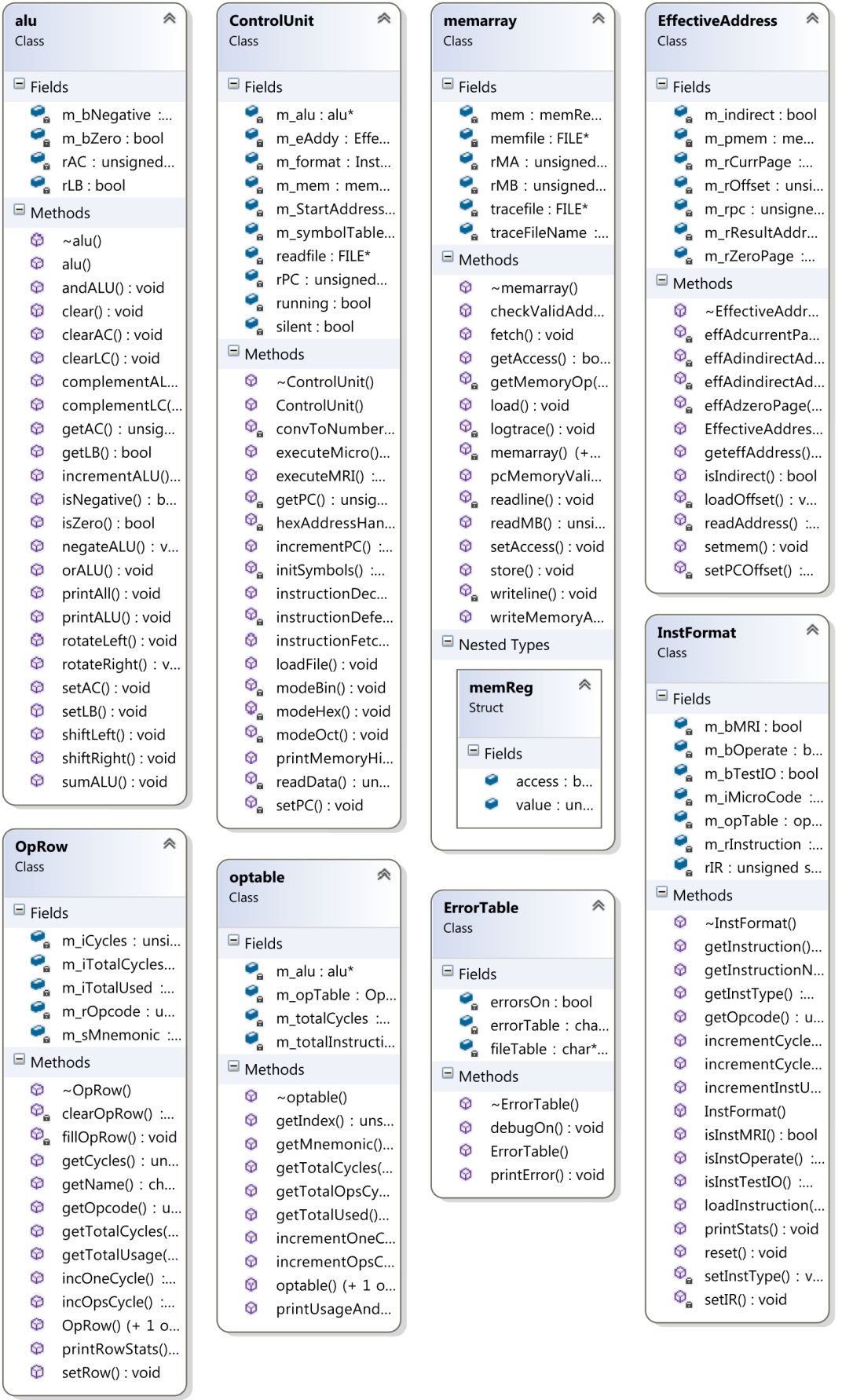
The simulator was designed in C++ with some libraries custom built for handling the conversion of the register values from octal to binary, strings, numerals, and two’s complement. The major libraries that handle this we implemented to make it easier to construct a GUI that would wrap around the command line code. The design also requires that conditional flags be used for choosing the correct input information type between octal, hex, and binary.

# Implementation

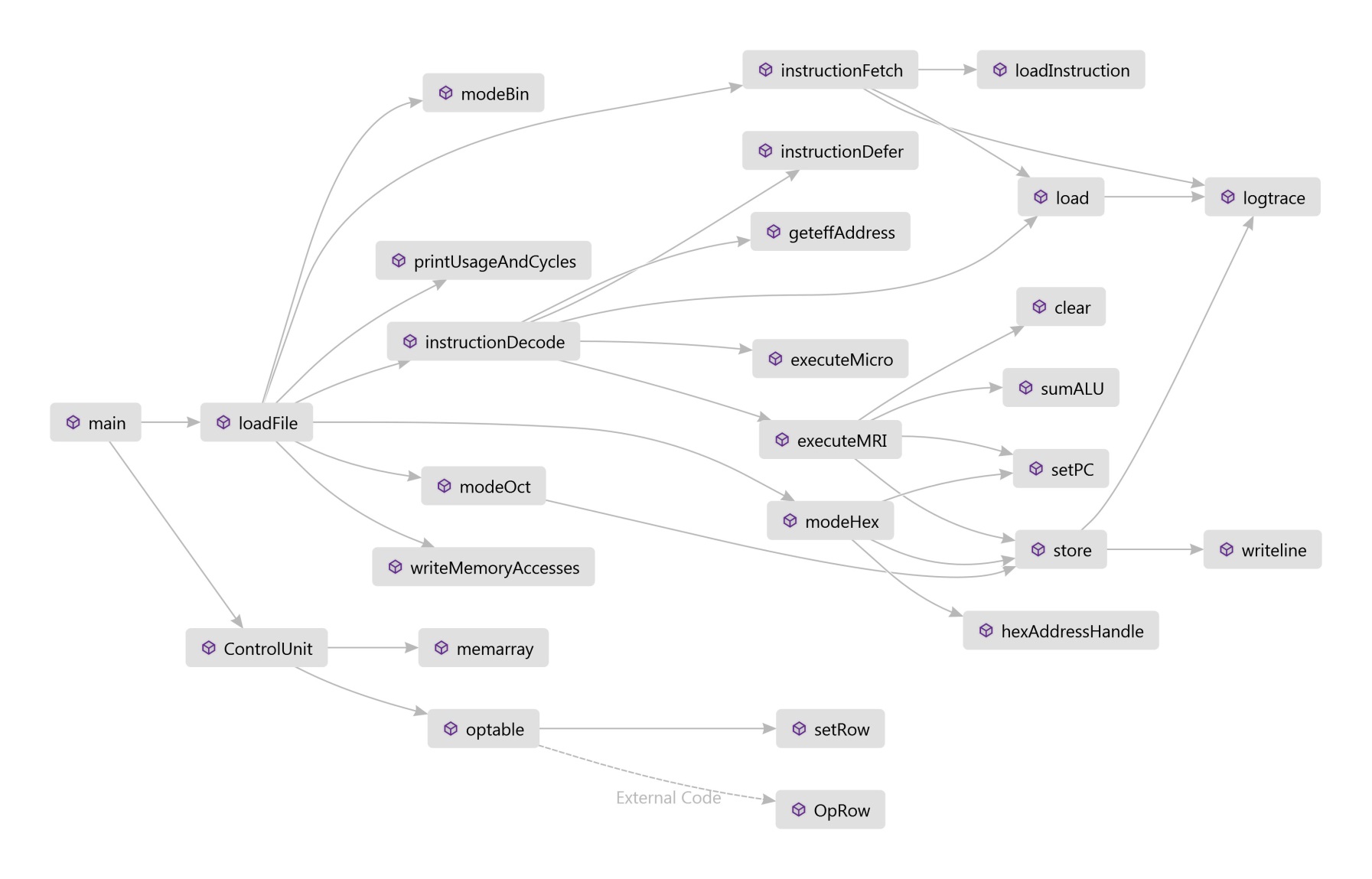
Figure 1 shows the class hierarchy of the PDP-8 simulator. The class memarray handles the paged memory file which is an array of the struct memReg, an unsigned short for register value and Boolean for access tracking. It’s subsystems handles access to and from the memory subsystem, including the only load and store methods. The alu class handles basic operations such as and, or, add, compliment, ect. The instFormat class takes in an instruction and parses it’s zero page and indirect bits, opcodes, statistic increment timing and printing. The effAddress calculates the effective address. The opRow class is a structure that holds opcodes names, cycles, total usage and total. The opTable class is an array of opRows that represents each opcode, indexing the table by that opcode. The error class prints errors in debug mode.

The program is written in C++ with custom classes and a custom library to control the data conversions. This is currently a command line program that requires flags for handling file input flow as well as debugging. The file input can be specified as a local path preceded by the –f flag. The input data type is the –o, -v flags. O is for octal, v is for hexadecimal and if no flag is given then binary is the default input type

## Figure 1 Class structure



## Figure 2 Example of Instruction Interaction Within the Classes



# Testing

## Op codes:

The op codes are plentiful in the PDP-8 , and the first six op codes are :

1. AND
   1. Bit by bit logical and of the accumulator and the contents of the effective address.
   2. DEBUG Execute: Memory Reference 0250 PC: 0204
   3. DEBUG opcode: 0, AND
   4. DEBUG offset: 412 Memory Reference
   5. DEBUG load instruction: Memory Reference
   6. DEBUG Execute: 0002
   7. DEBUG ALU: and is 0000
2. TAD
   1. Add the value pointed to by the effective address to the value in the accumulator
   2. Address 250 contains the value 2, Address 251 contains the value 3
   3. DEBUG Execute: Memory Reference 0250 PC: 0202
   4. DEBUG opcode: 1, TAD
   5. DEBUG offset: 412 Memory Reference
   6. DEBUG load instruction: Memory Reference
   7. DEBUG ALU: sum is 0002
   8. DEBUG Execute: Memory Reference 0251 PC: 0203
   9. DEBUG opcode: 1, TAD
   10. DEBUG offset: 412 Memory Reference
   11. DEBUG load instruction: Memory Reference
   12. DEBUG ALU: sum is 0005
3. ISZ
   1. Increment the contents of the effective address and skip the next instruction if the contents are zero.
   2. The contents of 253 are 7777 in octal which is -1. So the first run through it will skip the jump instruction beneath it.
   3. DEBUG Execute: Memory Reference 0253 PC: 0205
   4. DEBUG opcode: 2, ISZ
   5. DEBUG offset: 253 Memory Reference
   6. DEBUG load instruction: Memory Reference
4. DCA
   1. Deposit the value of the accumulator into memory and clear the accumulator
   2. The ALU was the value of 0005 in this test as the DCA was called after the two TAD ops.
   3. DEBUG opcode: 3, DCA
   4. DEBUG offset: 412 Memory Reference
   5. DEBUG load instruction: Memory Reference
   6. DEBUG ALU: clear is 0000
   7. DEBUG Execute: Memory Reference 0250 PC: 0204
5. JMS
   1. Jump to subroutine. Saves the return address at the jump destination address, then increments the pc to start on the instruction following the jump.
   2. DEBUG opcode: 4, JMS
   3. DEBUG offset: 300 Memory Reference
   4. DEBUG load instruction: Memory Reference
   5. DEBUG Execute: Memory Reference 0200 PC: 0200
6. JMP
   1. Direct jump with no return address. The effective address is the jump to address unless indirection is used.
   2. DEBUG opcode: 5, JMP
   3. DEBUG offset: 300 Memory Reference
   4. DEBUG load instruction: Memory Reference
   5. DEBUG Execute: Memory Reference 0200 PC: 0200
7. MicroInstructions:
   1. Vector of flags, each with different functionality. In some cases can be combined
   2. DEBUG: executing micro instruction: 7300, cla cll / clear AC and Link
   3. DEBUG: executing micro instruction: 7402, hlt / Halt program

## Add01:

### Assembly program:

\*0200 / start at address 0200

Main, cla cll / clear AC and Link

tad A / add A to Accumulator

tad B / add B

dca C / store sum at C

hlt / Halt program

jmp Main / To continue - goto Main

/

/ Data Section

/

\*0250 / place data at address 0250

A, 2 / A equals 2

B, 3 / B equals 3

C, 0

$Main / End of Program; Main is entry point

### Debug output:

DEBUG: writing at address 200 value 7300

DEBUG: writing at address 201 value 1250

DEBUG: writing at address 202 value 1251

DEBUG: writing at address 203 value 3252

DEBUG: writing at address 204 value 7402

DEBUG: writing at address 205 value 5200

DEBUG: writing at address 250 value 2

DEBUG: writing at address 251 value 3

DEBUG: writing at address 252 value 0

DEBUG: writing at address 253 value 775

DEBUG: reading address 200

DEBUG: fetching address 200

DEBUG: reading address 201

DEBUG: fetching address 201

DEBUG: reading address 250

DEBUG: sum alu rAC 2 = 2 + 0, rLB = 0

DEBUG: reading address 202

DEBUG: fetching address 202

DEBUG: reading address 251

DEBUG: sum alu rAC 5 = 3 + 2, rLB = 0

DEBUG: reading address 203

DEBUG: fetching address 203

DEBUG: reading address 252

DEBUG: writing at address 252 value 5

DEBUG: cleared rAC: 0 and rLB: 0

DEBUG: reading address 204

DEBUG: fetching address 204

-----------------------------------------------

Statistic Summary

-----------------------------------------------

Total instructions: 5 Total clock cycles: 8

-----------------------------------------------

AND: executed: 0 times consumed: 0 cycles

TAD: executed: 2 times consumed: 4 cycles

ISZ: executed: 0 times consumed: 0 cycles

DCA: executed: 1 times consumed: 2 cycles

JMS: executed: 0 times consumed: 0 cycles

JMP: executed: 0 times consumed: 0 cycles

IO : executed: 0 times consumed: 0 cycles

MIC: executed: 2 times consumed: 2 cycles

Halt...

## OR:

Assembly program to test indirect mode:

|  |  |  |
| --- | --- | --- |
| Loading program:  \*0200  Main, cla cll  TAD A  CMA  DCA C  TAD I B  CMA  AND C  CMA  DCA C  HLT  JMP Main  \*0310  A, 25  B, 313  C, 0  D, 45  $Main | / start at address 0200  / clear AC and Link  / load A to the alu  / complement alu  / store result to C  / load indirect B (D) to alu  / complement it  / and it with C  / complement result  / store result to C  / Halt program  / goto Main  / place data at address 0310  / A equals 25  / B equals indirect address D  / C holds saved result  / D equals 45 | DEBUG: writing at address 200 value 7300  DEBUG: writing at address 201 value 1310  DEBUG: writing at address 202 value 7040  DEBUG: writing at address 203 value 3312  DEBUG: writing at address 204 value 1711  DEBUG: writing at address 205 value 7040  DEBUG: writing at address 206 value 312  DEBUG: writing at address 207 value 7040  DEBUG: writing at address 210 value 3312  DEBUG: writing at address 211 value 7402  DEBUG: writing at address 212 value 5200  DEBUG: writing at address 310 value 25  DEBUG: writing at address 311 value 313  DEBUG: writing at address 312 value 0  DEBUG: writing at address 313 value 45 |
| cla cll | / clear AC and Link | DEBUG: fetching address 200  DEBUG: fetched: data: 7300  DEBUG: executing micro: instruction: 7300 |
| TAD A | / load A to the alu | DEBUG: fetching address 201  DEBUG: fetched data: 1310  DEBUG: offset: 110, pc offset: 200, indirect: 0  DEBUG: current page: 310  DEBUG: loading address: 310 data: 25  DEBUG: executing mri: opcode 1  DEBUG: sum alu rAC 25 = 25 + 0, rLB = 0 |
| CMA | / complement alu | DEBUG: fetching address 202  DEBUG: format loading instruction: 7040  DEBUG: executing micro: instruction: 7040  DEBUG: complemented rAC from 25 to 7752 |
| DCA C | / store result to C | DEBUG: fetching address 203  DEBUG: fetched: data: 3312  DEBUG: offset: 112, pc offset: 200, indirect: 0  DEBUG: current page: 312  DEBUG: loading address: 312 data: 0  DEBUG: executing mri: opcode 3  DEBUG: writing at address 312 value 7752  DEBUG: cleared rAC: 0 and rLB: 0 |
| TAD I B | / load indirect B (D) to alu | DEBUG: fetching address 204  DEBUG: fetched: data: 1711  DEBUG: offset: 111, pc offset: 200, indirect: 1  DEBUG: current page: 311  DEBUG: offset: 113, pc offset: 200, indirect: 0  DEBUG: current page: 313  DEBUG: loading address: 313 data: 45  DEBUG: sum alu rAC 45 = 45 + 0, rLB = 0 |
| CMA | / complement it | DEBUG: fetching address 205  DEBUG: fetched: data: 7040  DEBUG: executing micro: instruction: 7040  DEBUG: complemented rAC from 45 to 7732 |
| AND C | / and it with C | DEBUG: fetching address 206  DEBUG: fetched: data: 312  DEBUG: offset: 112, pc offset: 200, indirect: 0  DEBUG: current page: 312  DEBUG: loading address: 312 data: 7752  DEBUG: executing mri: opcode 0  DEBUG: and AC from 7732 to 7712 |
| CMA | / complement result | DEBUG: fetching address 207  DEBUG: fetched: data: 7040  DEBUG: executing micro: instruction: 7040  DEBUG: complemented rAC from 7712 to 65 |
| DCA C | / store result to C | DEBUG: fetching address 210  DEBUG: fetched: data: 3312  DEBUG: offset: 112, pc offset: 200, indirect: 0  DEBUG: current page: 312  DEBUG: loading address: 312 data: 7752  DEBUG: executing mri: opcode 3  DEBUG: writing at address 312 value 65  DEBUG: cleared rAC: 0 and rLB: 0 |
| HLT | / Halt program | DEBUG: fetching address 211  DEBUG: fetched: data: 7402  DEBUG: executing micro: instruction: 7402 |
| Main, cla cll  TAD A  CMA  DCA C  TAD I B  CMA  AND C  CMA  DCA C  HLT  JMP Main |  | -----------------------------------------------  Statistic Summary  -----------------------------------------------  Total instructions: 10 Total clock cycles: 16  -----------------------------------------------  AND: executed: 1 times consumed: 2 cycles  TAD: executed: 2 times consumed: 5 cycles  ISZ: executed: 0 times consumed: 0 cycles  DCA: executed: 2 times consumed: 4 cycles  JMS: executed: 0 times consumed: 0 cycles  JMP: executed: 0 times consumed: 0 cycles  IO : executed: 0 times consumed: 0 cycles  MIC: executed: 5 times consumed: 5 cycles  Halt... |

## Parsing different types of file input:

When the right file is run with the right flag ([default]/.bin, -o/.obj, -v/.mem), the three outputs should all be equal. Proper error handling should occur when a flag is incongruent with the data format within the file.

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Binary | Octal | Hexadecimal |
| Flag | [default] | -o | -v |
| File Input | -f add01.bin | -f add01.obj | -f add01.mem |
| -f add01.bin | DEBUG address: 0200  DEBUG address: 7300  DEBUG address: 1250  DEBUG address: 1251  DEBUG address: 3252  DEBUG address: 7402  DEBUG address: 5200  DEBUG address: 0250  DEBUG address: 0002  DEBUG address: 0003  DEBUG address: 0000 | ERROR: Invalid Address: 10000  Shutting down... | ERROR: Invalid Address: 10000  Shutting down... |
| -f add01.obj | ERROR: Invalid Address: 10000  Shutting down... | DEBUG address: 0200  DEBUG address: 7300  DEBUG address: 1250  DEBUG address: 1251  DEBUG address: 3252  DEBUG address: 7402  DEBUG address: 5200  DEBUG address: 0250  DEBUG address: 0002  DEBUG address: 0003  DEBUG address: 0000 | ERROR: Invalid Address: 10000  Shutting down... |
| -f add01.mem | ERROR: Invalid Address: 10000  Shutting down... | ERROR: Invalid Address: 10000  Shutting down... | DEBUG address: 0200  DEBUG address: 7300  DEBUG address: 1250  DEBUG address: 1251  DEBUG address: 3252  DEBUG address: 7402  DEBUG address: 5200  DEBUG address: 0250  DEBUG address: 0002  DEBUG address: 0003  DEBUG address: 0000 |