

New issue

[Jump to bottom](#)

[Bug Report] incorrect DRET decoder #899

✓ Closed Phantom1003 opened this issue on Jun 3 · 1 comment

Phantom1003 commented on Jun 3 • edited ▾

Contributor

Our co-simulation framework found the decoder has an incorrect behavior when execute a `dret` with non-zero `rd` field.

According to the Debug Specification Version 1.0.0:

To resume execution, the debug module sets a flag which causes the hart to execute a `dret`. `dret` is an instruction that only has meaning while in Debug Mode and not executing from the Program Buffer. Its recommended encoding is `0x7b200073`.

When modified `instr[11:7]` to `5'b00001`, `cva6` treats this invalid `dret` as normal `dret` as well. No exception occurred. The implementation is missing a check for this field.

In the following test case, there is an invalid `dret` at `0x8000019c`, whose `rd` field is 1, `cva6` execute it as normal instruction, while `spike` throws an exaption.

```
[spike] core 0: 0x000000008000019c (0x7b200273) unknown
[spike] core 0: exception trap_illegal_instruction, epc 0x000000008000019c
[spike] core 0: tval 0x000000007b200273
[spike] core 0: 0x0000000080000004 (0x00000f17) auipc t5, 0x0
[error] PC SIM 0000000080000004, DUT 000000008000019c
[error] INSN SIM 00000f17, DUT 7b200273
[CJ] Commit Failed
[cva6] 786ns 771 D 000000008000019c 0 7b200273 INVALID // CVA6 continues to execute
[cva6] 1068ns 1053 S 000000008000017c 0 0ff0000f fence // subsequent instructions
```

We believe is the debug mode checking reset the correct signal:

[cva6/core/decoder.sv](#)
Lines 134 to 135 in 909d85a

```
134 // check that we are in debug mode when executing this instruction
135 illegal_instr = (!debug_mode_i) ? 1'b1 : 1'b0;
```

[cva6-3.zip](#)

| @LuminaDCIX helps reproduce the problem

zarubaf commented on Jun 7

Contributor


Ah nice catch. Would you mind preparing a PR for that? This would be greatly appreciated. Thanks!



  Phantom1003 mentioned this issue on Jun 23

fix dret decoder #922

 Merged

 Phantom1003 closed this as completed on Jul 8

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

