

[New issue](#)[Jump to bottom](#)

[Bug Report] incorrect MISC_MEM decoder #900

[Closed](#)

Phantom1003 opened this issue on Jun 3 · 2 comments

Phantom1003 commented on Jun 3

Contributor

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

As discussed before [719](#), `fence` / `fence.i` should ignores immediate, rs1, rd field. We found the patch [724](#) does not fix this bug.

The checking after the patch still throws an exception for non-zero rd and rs1:

[cva6/core/decoder.sv](#)

Lines 238 to 239 in 909d85a

```
238     if (instr.stype.rs1 != '0 || instr.stype.imm0 != '0 || instr.instr[31:28] != '0)
239         illegal_instr = 1'b1;
```

According to the The RISC-V Instruction Set Manual Volume I: Unprivileged ISA:

FENCE: The unused fields in the FENCE instructions—rs1 and rd—are reserved for finer-grain fences in future extensions. For forward compatibility, base implementations shall ignore these fields, and standard software shall zero these fields.

FENCE.I: The unused fields in the FENCE.I instruction, imm[11:0], rs1, and rd, are reserved for finer-grain fences in future extensions. For forward compatibility, base implementations shall ignore these fields, and standard software shall zero these fields.

In the following test case, there is a valid `fence.i` at 0x80000194, whose rd field is 1, and a `fence` with non-zero rd at 0x80000198. cva6 still throws exceptions for them.

```
[cva6] Exception @      68600, PC: 0000000080000194, Cause: Illegal Instruction,
[cva6]                               tval: 000000000000120f
[spike] core   0: 0x0000000080000194 (0x0000120f) fence.i
[error] PC SIM 0000000080000194, DUT 0000000080000004
[error] INSN SIM 0000120f, DUT 34202f73
[CJ] Commit Failed
```

[cva6-4.zip](#)

@LuminaDCIX helps reproduce the problem

zarubaf commented on Jun 7

Contributor

Hm, based on the current spec it seems that:

[cva6/core/decoder.sv](#)

Lines 238 to 239 in 909d85a

```
238     if (instr.stype.rs1 != '0 || instr.stype.imm0 != '0 || instr.instr[31:28] != '0)
239         illegal_instr = 1'b1;
```

Is not needed anymore to preserve forward compatibility. I can't seem to find how `rd` is factored into the equation. Would you mind trying to delete the above lines and re-run the testcase?

Phantom1003 commented on Jun 7 • edited

Contributor

Author


I can't seem to find how `rd` is factored into the equation.

The fence instruction is I type, `instr.stype.imm0 != '0` will check the `rd` field.

  Phantom1003 mentioned this issue on Jun 23

fix fence(.i) decoder #923

 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

