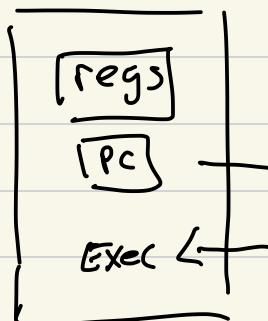


CS 631-02 RISC-V Emulation

RISC-V
Processor



Memory

STACK



HEAP

DATA

CODE

[emu]

[0x00B5058]

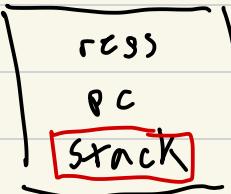
add a0 a0 a0 a1

RISC-V
Emulation
(code)

emu

Struct State

code



RISC-V Emulator Implementation

Incremental Development

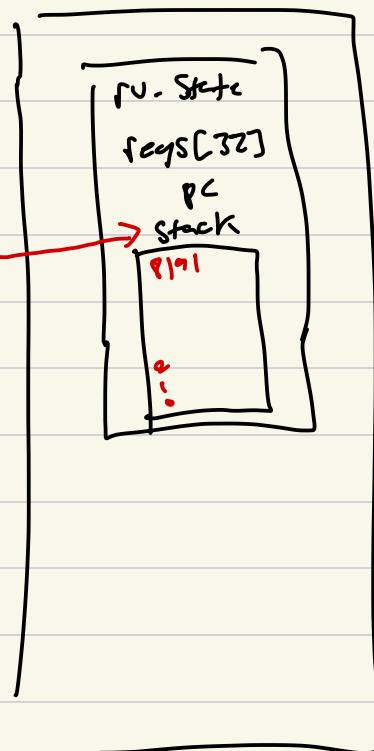
- ① Identify an instruction : ADDI
- ② Identify the instruction format
i-type
- ③ Implement or add to current implementation
- ④ Decode IW
get fields
- ⑤ Construct immediate
from IW
- ⑥ Update state
update rd
update memory
update PC

init Stack

emulated

SP

STACK



new instruction formats

immediates

jumps and branches

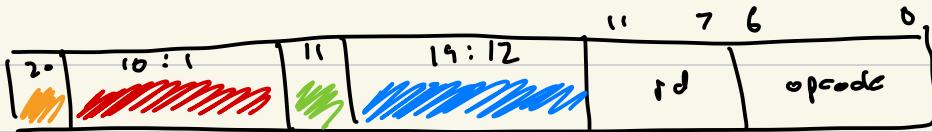
Memory

JAL

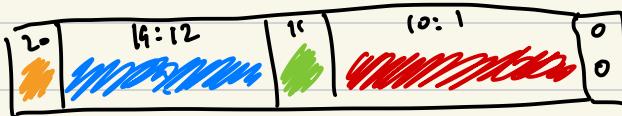
J-type PC immediate

j
jal
call

Iw



imm21



$$\text{int64_t} \text{ imm64} = \text{sign_ext}(\text{imm21}, \underline{\text{bit } 20})$$

B-type

beq rs1, rs2, lntc
↑↑

LW lw rd, offset(rs1)
base

$$\text{uint64_t} \text{ target_addr} = \text{base} + \text{offset}$$

$$\text{uint64_t} \text{ value} = *(\text{uint32_t}^* \text{ target_addr})^j$$