#### **ARCOS Group**

#### uc3m Universidad Carlos III de Madrid

# L3: Fundamentals of assembler programming (3) Computer Structure

Bachelor in Computer Science and Engineering
Bachelor in Applied Mathematics and Computing
Dual Bachelor in Computer Science and Engineering and Business Administration



#### Contents

- Basic concepts on assembly programming
- RISC-V 32 assembly language, memory model and data representation
- Instruction formats, addressing modes and instruction sets
- Procedure calls and stack convention

#### Different language levels



```
temp = v[k];
 High-level language
                             v[k] = v[k+1];
 (e.g.: C, Python, ...)
                             v[k+1] = temp;
          Compiler
                                 t0, 0(x2)
                              lw
 Assembly language
                                 t1, 4(x2)
    (e.g.: RISC-V)
                                 t1, 0(x2)
                                   t0, 4(x2)
                              SW
          Assembler
                             0000 1001 1100 0110 1010 1111 0101 1000
Machine language
(e.g.: RISC-V in binary)
                             1010 1111 0101 1000 0000 1001 1100 0110
                             1100 0110 1010 1111 0101 1000 0000 1001
                             0101 1000 0000 1001 1100 0110 1010 1111
```

#### An assembly instruction corresponds to a machine instruction

**Example:** 

Assembly: add x5, x6, x2

Machine: 0x002302B3

# Instruction and pseudoinstruction RISC-V<sub>32</sub>



- A pseudo-assembler instruction corresponds to one or several machine instructions.
  - Example 1:

```
▶ The instruction: mv x2, x1
```

- It is equivalent to: add x2, zero, x1
- Example 2:
  - The instruction: li t1, 0x00800010
  - It does not fit in 32 bits, but it can be used as a pseudoinstruction.
  - lt is equivalent to:

```
□ lui t1, 0x00800
□ ori t1, t1, 0x010
```

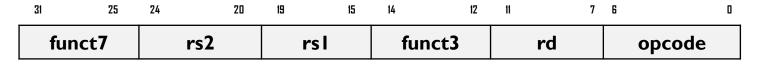
- An assembly instruction corresponds to a machine instruction
  - **Example:** 
    - Assembly: add x5, x6, x2
    - Machine: 0x002302B3

#### Instruction format



#### A machine instruction is coded in binary:

- Size fits one or more words
- An instruction is divided into fields
  - ▶ Each field encodes an element that includes the statement
  - ▶ There may be implicit elements
- Example of fields in a RISC-V instruction:



- ▶ The format specifies, for each field of the instruction:
  - The meaning of each field
  - **Encoding used** in each field
    - Binary, one's complement, two's complement, etc.
  - The **number of bits** in each field
    - The size of the fields limits the number of values to be encoded.

#### Instruction format



#### A machine instruction is self-contained and includes:

- Operation code
- Operands (value or location of value to use)
- Result (location to save)
- Address of the next instruction
  - ▶ Implicit: PC ← PC + '4' (point to the following 32-bit instruction)
  - ► Explicit: j 0x01004 (modifies the PC)

#### Usually:

- One architecture offers a few instruction formats.
  - Simplicity in the design of the control unit.
- Fields of the same type always of equal length.
- **Selection together** with the **operation code** (e.g. add, addi).
  - Usually the first field.

#### Format length

- The format length is number of bits to encode the instruction
  - The size of an instruction is usually one word (or multiples words)
  - In RISC-V<sub>32</sub> the size of all instructions is one word (32 bits)

#### Two types:

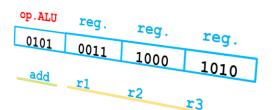
- ► Fixed/Unique length:
  - All instructions with the same size
  - **Examples:** 
    - ☐ MIPS32 (32 bits), PowerPC (32 bits), ...
- Variable length:
  - Different instructions can have different sizes.
  - ▶ How to know the instruction length?  $\rightarrow$  Op. code
  - **Examples:** 
    - □ IA32 (Intel processors): variable number of bytes

## Example: instruction format for RISC-V

	31	25	24	20	19	15	14	12	11	7	6	0
R	funct7		rs2		rsl		funct3		rd		opcode	
I	imm[11:0]				rsl		funct3 rd			opcode		
UI							rd		opcode			
S	imm[11:5] rs2			rs l funct3			3	imm[4:0	ני	opcode		
В	[12] imm[10:5]		rs2		rsl		funct	3	imm[4:1]	[11]	opcode	
J	[20] imm[10:1]		[11]	imm[19:12]			rd		opcode			

- opcode (7 bits): partially indicates the type of instruction format.
  - Register, Immediate, Upper Immediate, Store, Branch, Jump
- funct7+funct3 (10 bits): together with opcode, describe the op. to perform.
- rs1 (5 bits): specifies the register as first operand.
- **rs2** (5 bits): specifies the register as second operand.
- rd (5 bits): specifies the target register.

#### Operation code

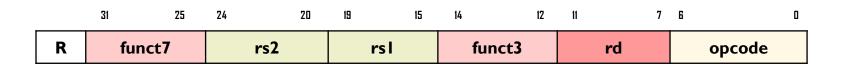


#### Fixed size:

- ▶ n bits  $\rightarrow$  2<sup>n</sup> operation codes
- ▶ m operation codes  $\rightarrow$   $\lceil \log_2 m \rceil$  bits.

#### Extension fields

- RISC-V (arithmetic-logic instructions)
- ▶ Op = 0; the instruction is encoded in funct X



#### Variable sizes:

More frequent instructions= shorter sizes

#### Locations of operands



I. In the instruction

li  $t0.0 \times 123$ 

2. In registers (processor)

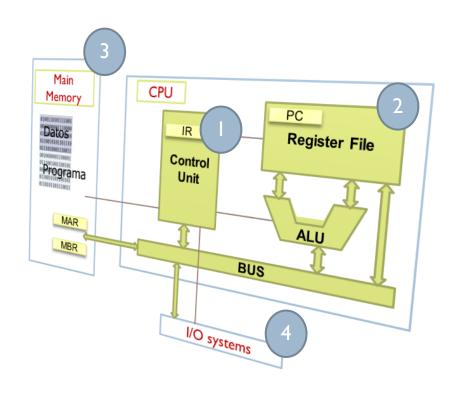
li t0 0×123

3. Main memory

lw t0 address(x0)

4. Input/output modules

in t0 0xFEB



#### Locations of operands



#### I. In the instruction

li t0 0x123



li t0.0x123

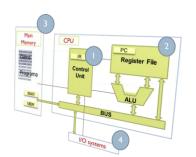
3. Main memory

lw t0 address(x0)

 num(registro): represents the address obtained by summing num with the address stored in the register

4. Input/output modules

in t0 0xFEB



# Example instruction and associated format in RISC-V

▶ add rd rs1 rs2

31	25	24	20	19	15	14	12	11	7	6		0
00000	00		rs2		rsl		000		rd		0110011	

#### Exercise

A 16-bit computer
 has an instruction set of 60 instructions and
 a register file of 8 registers.

The following is requested:

Define the format of this instruction: ADDx RI R2 R3, where RI, R2 and R3 are registers.

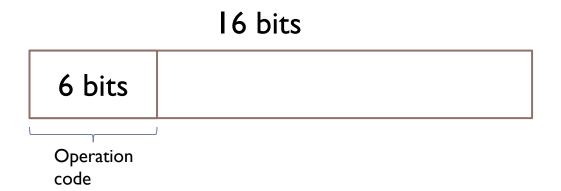
word-> 16 bits
60 instructions
8 registers (in RB)
ADDx RI(reg.), R2(reg.), R3(reg.)

I6-bit word defines the size of the instruction

I 6 bits

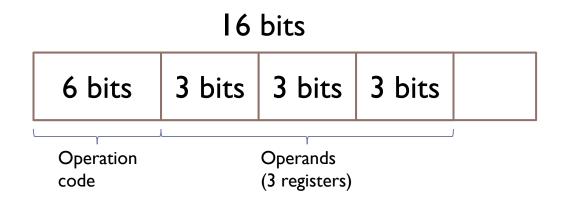
word-> 16 bits
60 instructions
8 registers (in RB)
ADDx R1(reg.), R2(reg.), R3(reg.)

▶ To encode 60 instructions, 6 bits are required for the operation code (minimum)



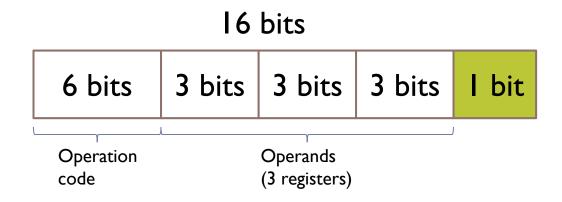
word-> 16 bits
60 instructions
8 registers (in RB)
ADDx R1(reg.), R2(reg.), R3(reg.)

For 8 registers, 3 bits are required (minimum)



word-> 16 bits
60 instructions
8 registers (in RB)
ADDx R1(reg.), R2(reg.), R3(reg.)

▶ I bit left over (16-6-3-3-3=1), used for padding



#### Contents

- Basic concepts on assembly programming
- RISC-V 32 assembly language, memory model and data representation
- Instruction formats, addressing modes and instruction sets
- Procedure calls and stack convention

## Addressing modes

 The addressing mode is a procedure for determining the location of an operand, a result or an instruction

- Implicit
- Immediate
- Directto registerto memory
- Indirectto registerto memory
- Relative
  to index register
  base register
  to PC
  to stack

#### Modos de direccionamiento en RISC-V

Immediate	value
Direct	
▶ To memory	address
▶ To register	xr
Indirect	
▶ To memory	
To register	(xr)
Relative to	
□ register	offset(xr)
□ stack	offset(sp)
	beq label l

## Addressing modes

The addressing mode is a procedure for determining the location of an operand, a result or an instruction

- Implicit
- Immediate
- Indirectto registerto memory
- Relative
  to index register
  base register
  to PC
  to stack

## Implicit addressing

Description	The operand is not coded in the instruction but is part of the instruction.					
Example	<pre>auipc a0 0x12345 &gt; a0 = PC + (0x12345 &lt;&lt; 12). &gt; a0 is one operand, PC is the other (implicit)  op</pre>					
(V/I) Advantages / Disadvantages	Fast: no need to access memory.  But it is only possible in a few cases.					

## Immediate addressing

Description	The operand is part of the instruction.						
Example	•		_		te value 0x4f5   .  mmediate field.  16 bits		
(V/I) Advantages / Disadvantages	<pre> ✓ It is fast: no need to access memory.  X Value does not always fit in a word:  It does not fit in 32-bits, it is equivalent to:    lui t1, 0x87654   ori t1, t1, 0x321</pre>						

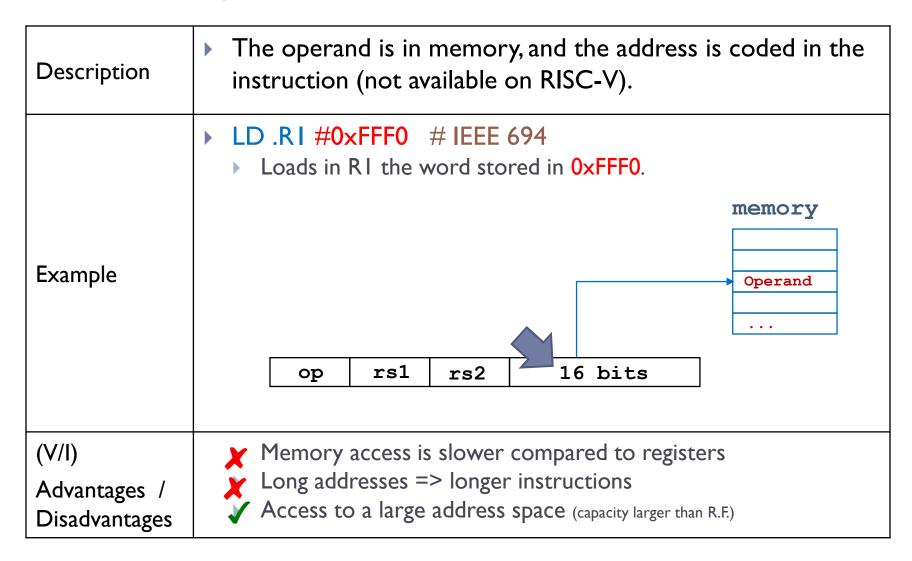
## Direct to register addressing

#### Register addressing

Description	Derand is in a register.					
Example	<ul> <li>mv a0 al</li> <li>Copies into register a0 the value in register al.</li> <li>The identifier of a0 and al is encoded in the instruction.</li> <li>op rs1 rs2 16 bits</li> <li>Operand</li> <li>Operand</li> <li>Register File</li> </ul>					
(V/I) Advantages / Disadvantages	<ul> <li>✗ The number of registers is limited</li> <li>✗ Access to registers is fast</li> <li>✗ The number of registers is small =&gt; few bits for encoding, shorter instructions</li> </ul>					

## Direct to memory addressing

#### Direct addressing

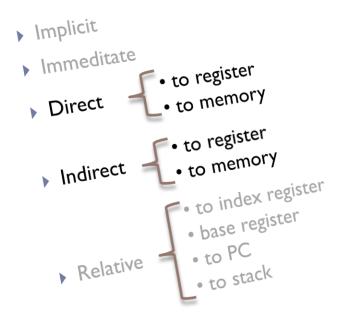


## Addressing modes

The addressing mode is a procedure for determining the location of an operand, a result or an instruction

Implicit
 Immediate
 Direct
 to register
 to memory
 Indirect
 to index register
 base register
 to PC
 to stack

## Direct vs. indirect addressing



- Direct addressing indicates where the operand is located:
  - In which register or in which memory position
- Indirect indicates where the address of the operand is located:
  - This address must be accessed in memory
  - A level (or several) of addressing is incorporated.

## Register indirect addressing

- The instruction has the register where the address is stored.
  Example: Iw a0 (al)
  Loads into a0 the value at the memory address stored in al.
  op rs rt 16 bits
- V/I
  - ✓ Wide address space, short instructions
  - Pseudo-instruction equivalent to lw a0 0(al)

## Indirect addressing

The instruction has the address where the operand address is stored (not available in RISC-V)
 Example: LD .RI [#DIR] # IEEE 694
 Loads into RI the value that is at the memory address that is stored in memory address #DIR.
 op rs rt 16 bits

- V/I
  - ✓ Large address space
  - ✓ Addressing can be nested, multilevel or cascading
    - Example: LD .R1 [[[.R1]]]
  - May require several memory accesses
  - x slower instructions to execute

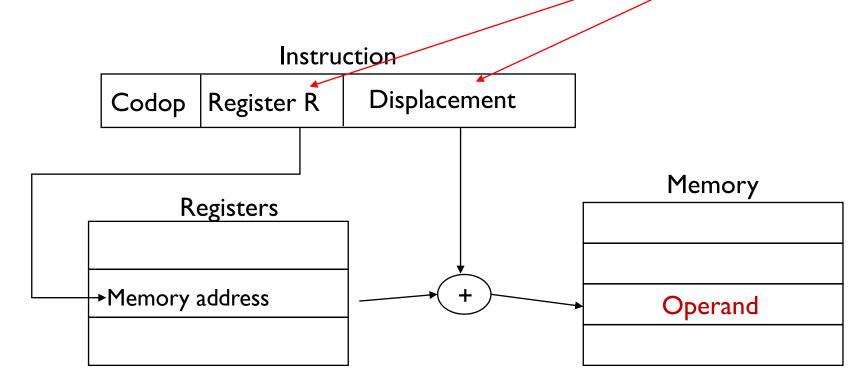
## Addressing modes

The addressing mode is a procedure for determining the location of an operand, a result or an instruction

Implicit
 Immediate
 to register
 to memory
 Indirect
 to register
 to memory
 to index register
 base register
 to PC
 to stack

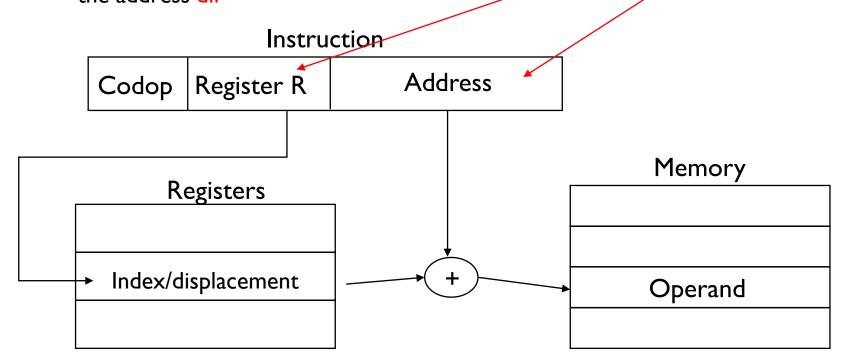
## Base-register addressing

- Example: lw a0 12(t1)
  - Loads into a0 the contents of the memory position given by tl + 12
  - Uses two fields of the instruction, tl has the base address



## Index-register addressing

- Example: lw a0 dir(tl)
  - Loads into a0 the contents of the memory position given by t1 + dir
  - It uses two fields: tl represents the displacement (index) with respect to the address dir



#### Utility: access to vectors

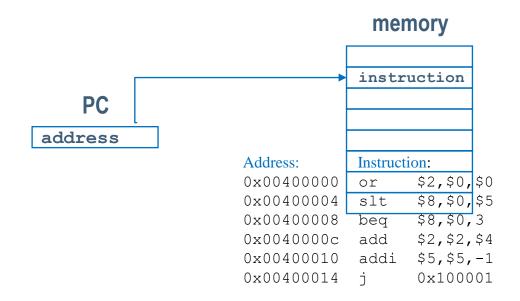
```
int v[5];
main ()
  v[3] = 5 ;
   v[4] = 8 ;
   v[1] = 3 ;
```

```
.data
 v: .zero 20 # 5_{int} * 4_{bytes/int}
.text
main:
        la t0 v
        li t1 5
        sw t1 12(t0)
        li
           t0 16
        li t1 8
        sw t1 v(t0)
        la t0 v
        addi t0 t0 4
        li t1 3
        sw t1 (t0)
```

#### PC-relative addressing

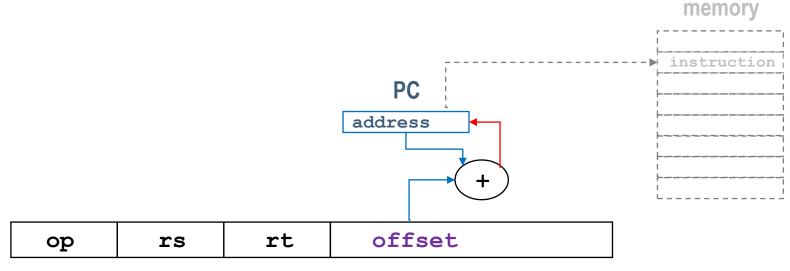


- Registers of 32 bits (4 bytes) in a 32-bits computer
- PC stores the address of the next instruction to be executed
  - Points to a word (4 bytes) in memory with the instruction to be executed
  - ▶ PC in a 32-bits computer is updated by default as PC = PC + 4



## PC-relative addressing

- ▶ Example: beq a0 x0 label
  - The label is encoded as the displacement from the memory address where this instruction is, to the memory position indicated in label.
    - ▶ Label encoded as offset (address -> number of instructions to jump)
  - If a0 is 0, then PC <= PC + "offset"</p>



## PC-relative addressing in RISC-V

The beq t0, x1, offset instruction is encoded in the machine instruction:

31 2	5 24 20	19	5 14 12	2 11 7	7 6 0
offset[12 10:5]	rs2	rs1	000	offset[4:1 11]	1100011

- Label must be encoded in the "offset" field as an offset relative to the beq instruction at the time of execution (PC points to the first byte of the following instruction)
  - The offset value can be positive or negative
- ▶ How is PC updated if t0 == xI?
  - If the condition is met:
    - ▶ PC = PC + offset
  - If the condition is not met:
    - ▶ PC = PC + 4

## PC-relative addressing in RISC-V

What is the value of fin when machine code is generated?

#### ▶ The value of fin is:

- ▶ fin == 12
- When an instruction is executed, the PC points to the next one.
- ▶ 3 instructions ("addi", "j" and "mv") must be skipped.
- Each instruction to be skipped is 4 bytes

```
li t0 8
li t1 4
li t2 1
li t4 0
while: bge t4 t1 fin
mul t2 t2 t0
addi t4 t4 1
j while
fin: mv t2 t4
```

- end represents the address where the instruction my is stored
- while represents the address where the instruction bge is stored

	li	t0 8 t1 4 t2 1
while:	li bge	t4 0 t4 t1 <b>fin</b>
	addi	t2 t2 t0 t4 t4 1 while
fin:		t2 t4

#### Address Content 0x0000100 li t0 8 0x0000104 li t1 4 0x0000108 li t2 1 0x000010C li t4 0 0x0000110 t4 t1 fin bge 0x0000114 mul t2 t2 t0 0x0000118 addi t4 t4 1 0x000011C while

ΜV

t2 t4

0x0000120

	li	t0 8	
	li	t1 4	
	li	t2 1	
	li	t4 0	
while:	bge	t4 t1	fin
	mul	t2 t2	t0
	addi	t4 t4	1
	j	while	
fin:	mν	t2 t4	

#### Address

0x0000100

0x0000104

0x0000108

0x000010C

0x0000110

• end encoded as displacement relative to  $^{0\times0000114}$  current PC => 3

$$PC = PC + 3 * 4$$

• while encoded as displacement relative 0x000011c to current PC => -4

$$PC = PC + (-4)*4$$

#### Content

li	t0	8	
li	t1	4	
li	t2	1	
li	t4	0	
bge	t4	t1	fin
mul	t2	t2	t0
addi	t4	t4	1
j	whi	lle	
mv	t2	t	1

	li li	t0 8 t1 4	
	li	t2 1	
	li	t4 0	
while:	bge	t4 t1	fin
	mul	t2 t2	t0
	addi	t4 t4	1
	j	while	
fin:	mv	t2 t4	

#### Address

0x0000100

0x0000104

0x0000108

0x000010C

0x0000110

0x0000120

• end encoded as displacement relative to  $^{0\times0000114}$  current PC => 3

$$PC = PC + 3 * 4 = PC + 12$$

• while encoded as displacement relative 0x000011C to current PC => -4

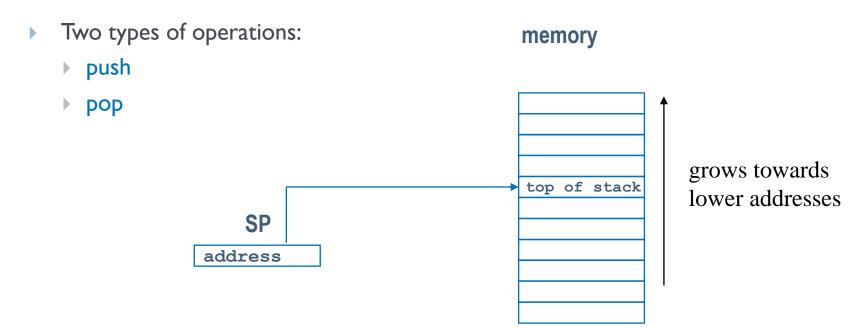
$$PC = PC + (-4)*4 = PC - 16$$

#### Content

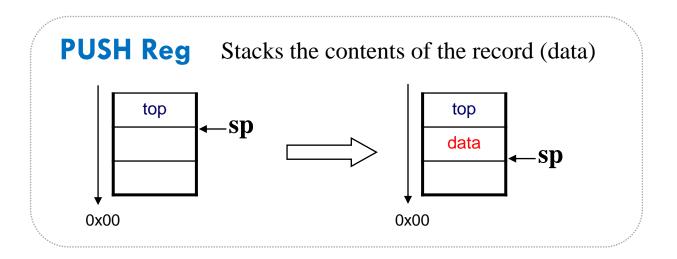
li	t0	8
li	t1	4
li	t2	1
li	t4	0
bge	t4	t1 12
mul	t2	t2 t0
addi	t4	t4 1
j	-1	6
mv	t2	t4

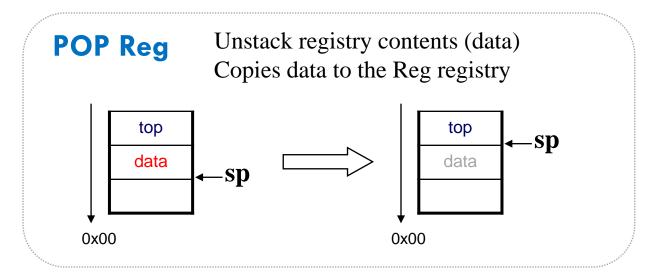
## Stack addressing

- ▶ The Stack Pointer (SP):
  - ▶ Is a 32-bits register (4 bytes) in RISC-V<sub>32</sub>
  - It stores the address of the top element on stack
    - Points to a word (4 bytes)



### Stack grows towards lower addresses



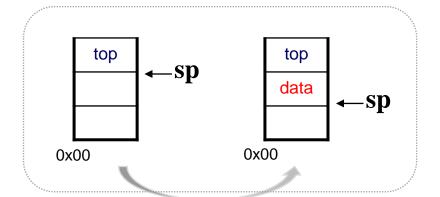


## Stack addressing in RISC-V

- RISC-V does not have PUSH or POP instructions.
- The stack pointer register (sp) is visible to the programmer.
  - It will be assumed that the stack pointer points to the last element on the stack

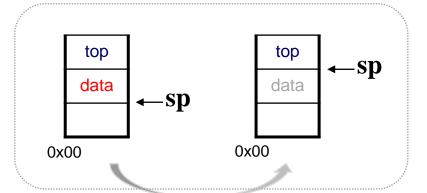
#### PUSH t0

addi sp, sp, -4 sw t0, 0(sp)



#### POP t0

lw t0, 0(sp)
addi sp, sp, 4



## PUSH action in RISC-V<sub>32</sub>

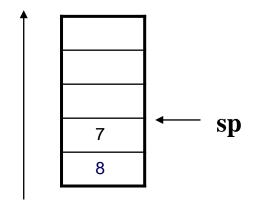
...

li t2, 9

addi sp, sp, -4

sw t2 0(sp)

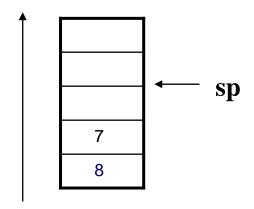
...



#### Initial state:

- The stack pointer register (sp) points to the last element at the top of the stack.
- The t2 register stores the value 9

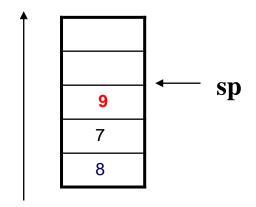
## PUSH action in RISC-V<sub>32</sub>



- ▶ 4 is subtracted from the stack pointer register in order to insert a new word on the stack
  - addi sp, sp, -4

## PUSH action in RISC-V<sub>32</sub>

```
...
li t2, 9
addi sp, sp, -4
sw t2 0(sp)
...
```



- ▶ The contents of register t2 are inserted at the top of the stack:
  - sw t2 0(sp)

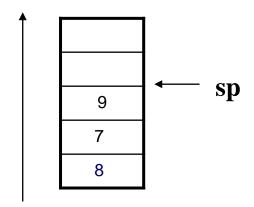
## POP action in RISC-V<sub>32</sub>

...

lw t2 0(sp)

addi sp, sp, 4

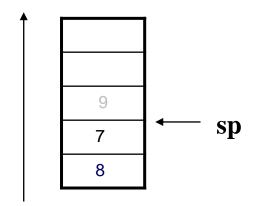
...



- ▶ The data stored at the top of the stack is copied to t2 (9)
  - lw t2 0(sp)

## POP action in RISC-V<sub>32</sub>

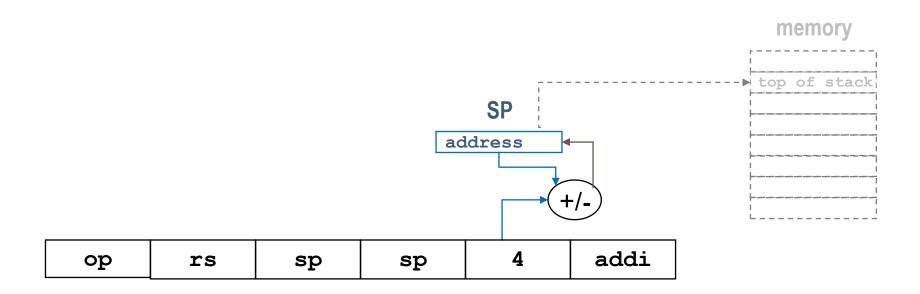
```
...
lw t2 0(sp)
addi sp, sp, 4
...
```



- The sp register is updated to point to the new top of the stack.
  - addi sp, sp, 4
- The unstacked data (9) is still in memory but will be overwritten in future PUSH (or similar memory access) operation.

## Stack addressing in RISC-V

- Example: push a0
  - addi sp sp -4 # SP = SP 4
  - $\triangleright$  sw a0 0(sp) # memory[SP] = a0



### Exercise

- Indicate the type of addressing used in the following instructions RISC-V:
  - I. li tl 4
  - 2. lw t0 4(a0)
  - 3. bne x0 a0 label

### Exercise (solution)

### 1. li tl 4

- tl -> direct to register
- 4 -> immediate

### I. Iw t0 4(a0)

- t0 -> direct to register
- 4(a0) -> relative to base register

#### I. bne x0 a0 label

- a0 -> direct to register
- label -> relative to program counter

## Examples of addressing modes

#### ▶ la t0 label immediate

- The second operand of the instruction is an address
- BUT this address is not accessed, the address itself is the operand

### Iw t0 label direct to memory (non-∃ on RV32)

- The second operand of the instruction is an address
- This address must be accessed in order to have the value to work with

### bne t0 t1 label relative to PC register

- The third operand of the instruction is offset with respect to PC
- label is encoded as a two's complement number representing the offset (as words) relative to the PC register

### Examples of instructions

- ▶ la t0, 0x0F000002
  - Direct to register + immediate.
     The 0x0F000002 value is loaded at t0
- ▶ lbu t0, label(x0)
  - Addresses direct to reg. + relative to base reg.
    The byte at memory address label is loaded at t0
- ▶ lb t0, 0(t1)
  - Addresses direct to reg. + relative to base reg.
     The byte in the memory position stored in t1+0 is loaded in t0

#### Contents

- Basic concepts on assembly programming
- RISC-V 32 assembly language, memory model and data representation
- Instruction formats, addressing modes and instruction sets
- Procedure calls and stack convention

### Instruction sets

### Queda definido por:

- Instruction set
- Instruction format
- Registers
- Addressing modes
- Data types and formats

### Instruction sets

- ▶ There are different ways for the classification of the instructions sets:
  - By complexity of the instruction set
    - CISC vs RISC
  - Execution modes
    - Stack

57

- Register
- ▶ Register-Memory, Memory-Register, ...

### CISC vs RISC

- Complex Instruction Set Computer
  - Many instructions
  - Complex instructions
    - More than one word
    - More complex control unit
    - Longer execution time
  - Irregular design

- About 20% of the instructions take up 80% of the total execution time of a program.
- ▶ 80% of the instructions are hardly ever used
- ▶ 80% of silicon underutilized, complex and costly

- Reduced Instruction Set Computer
  - Simple and orthogonal instructions:
    - Occupy one word
    - Instructions on registers
    - Use of the same addressing modes for all instructions (high degree of orthogonality)
  - More compact design:
    - Easier and faster control unit
    - Space left over for more registers and cache memory

### Execution modes

- The execution modes indicates the number of operands and the type of operands that can be specified in an instruction.
  - ▶ 0 addresses → Stack.
    - □ PUSH 5; PUSH 7; ADD
  - ► I address → Accumulator register.
    - □ ADD RI -> AC <- AC + RI
  - ▶ 2 addresses → Registers, Register-memory, Memory-memory.
    - $\square$  ADD .R0, .RI (R0 <- R0 + RI)
  - ▶ 3 addresses → Registers, Register-memory, memory-memory.
    - □ ADD .R0, .R1, .R2

#### **ARCOS Group**

### uc3m Universidad Carlos III de Madrid

# L3: Fundamentals of assembler programming (3) Computer Structure

Bachelor in Computer Science and Engineering
Bachelor in Applied Mathematics and Computing
Dual Bachelor in Computer Science and Engineering and Business Administration

