3. More MIPS Instructions

What distinguishes a computer from a simple calculator is its ability to make decisions based on input data or values obtained during the computation

- ☐ In high-level programming languages, decision-making instruction:
 - o if statement
- ☐ In MIPS, decision-making instructions (or **conditional branches**):
 - O beq ('branch if equal'):
 - e.g. beq reg1, reg2, L1
 - go to statement labeled L1 if reg1 and reg2 have the same value
 - O bne ('branch if not equal'):
 - e.g. bne reg1, reg2, L1
 - go to statement labeled L1 if reg1 and reg2 do not have the same value

☐ In the following C code segment, **f**, **g**, **h**, **i**, and **j** are variables:

```
if (i == j) goto L1;
f = g + h;
L1: f = f - i;
```

Assuming that the five variables **f** through **j** correspond to five registers **\$s0** through **\$s4**, what is the compiled MIPS code?

□ Answer:

```
beq $s3, $s4, L1  # go to L1 if i==j
add $s0, $s1, $s2  # f = g + h (skipped if i==j)
L1: sub $s0, $s0, $s3  # f = f - i (always executed)
```

Notes:

L1 corresponds to the address of the **sub** instruction.

□ Compilers frequently create branches and labels where they do not appear in the programming language.

```
if (i != j) f = g + h;
f = f - i;
```

this code is another way to implement the previous example without using label **11**

- □ Avoiding the burden of writing explicit labels and branches is one benefit of writing in high-level programming languages and is one of the reasons why coding is faster at that level.
- ☐ Besides conditional branches, we also have **unconditional jumps**:
 - j ('jump'):
 - e.g. j L1
 - always go to statement labeled L1

□ Assume, as before, that the five variables **f** through **j** correspond to registers \$s0 through \$s4. What is the compiled MIPS code for this?

```
if (i == j)
  f = g + h;
else if (i == g)
  f = g - h;
else
  f = g + j
```

■ Answer:

■ Another Solution:

```
beq $s3, $s4, if_match
beq $s3, $s1, elseif_match
j else_match

if_match: add $s0, $s1, $s2
j exit

elseif_match: sub $s0, $s1, $s2
j exit

else_match: add $s0, $s1, $s4
exit:
```

- □ Although this solution is longer, it is more similar to C++ version & looks closer to a switch-case statement
- ☐ Could be easier to debug if you need to check for more conditions

- □ Decisions are important both for
 - choosing between two alternatives—found in if statement
 - iterating a computation—found in loops
- ☐ In **loops**, decisions are needed to determine when to stop looping
- □ Commonly used loop constructs in high-level programming languages
 - o while
 - o for

☐ Here is a traditional loop in C:

```
while (save[i] == k) i += 1;
```

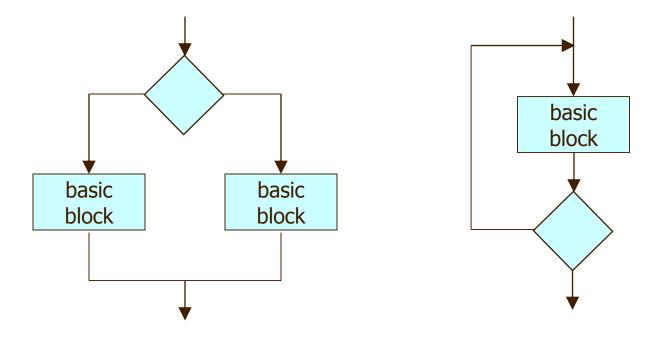
Assume that i and k correspond to registers \$3 and \$5 and the base of the array save is in \$6. What is the MIPS assembly code corresponding to this C Segment?

□ Answer:

```
Loop: sll $t1, $s3, 2  # Temp reg $t1 = 4 * i
  add $t1, $t1, $s6  # $t1 = address of save[i]
  lw $t0, 0($t1)  # Temp reg $t0 = save[i]
  bne $t0, $s5, Exit  # go to Exit if save[i]!= k
  addi $s3, $s3, 1  # i = i + 1
  j Loop

Exit:
```

□ A **basic block** is a sequence of instructions <u>without</u> branches and branch targets (except possibly at the end and at the beginning)



□ One of the first early phases of compilation is breaking the program into basic blocks.

Exit:

41

```
Loop: sll $t1, $s3, 2
add $t1, $t1, $s6
lw $t0, 0($t1)
bne $t0, $s5, Exit
add $s3, $s3, 1
j Loop
```

42

```
bne $s3, $s4, ElsIf

add $s0, $s1, $s2

j Exit

ElsIf: bne $s3, $s1, Else

sub $s0, $s1, $s2

j Exit

Else: add $s0, $s1, $s4

Exit:
```

- ☐ Besides testing for equality or inequality, it is often useful to see if a variable is less than another variable.
 - o e.g., exit from a loop when the array index is less than a variable
- □ slt ('set on less than'):
 - O slt reg1, reg2, reg3
 - o register reg1 is set to 1 if the value in reg2 is less than the value in reg3; otherwise, register reg1 is set to 0
- □ slti ('set on less than immediate')
 - O slti \$t0, \$s2, 10 # \$t0=1 if \$s2 < 10

- ☐ MIPS compilers use beq, bne, slt, slti and the fixed value of 0 (always available by reading register \$zero) to create all comparison operations:
 - o equal
 - o not equal
 - o less than
 - less than or equal
 - o greater than
 - o greater than or equal

Give the MIPS code that tests if variable a (corresponding to register \$s0) is less than variable b (register \$s1) and then branch to label L if the condition holds.

□ Answer:

```
slt $t0, $s0, $s1 # $t0 gets 1 if $s0 < $s1
bne $t0, $zero, L # go to L if $t0 != 0</pre>
```

□ Remark:

 Instead of providing a separate 'branch if less than' instruction which will complicate the instruction set, the MIPS architecture chooses to do this operation using two faster MIPS instructions – similar for other conditional branches. Branch on greater than or equal to zero

 \square bgez \$s, label # if (\$s >= 0)

Branch on greater than zero

 \Box bgtz \$s, label # if (\$s > 0)

Branch on less than or equal to zero

□ blez \$s, label # if (\$s <= 0)

Branch on less than zero

 \Box bltz \$s, label # if (\$s < 0)

'Jump Register' Instruction

- Another unconditional jump instruction:
 - o jr ('jump register'):
 - e.g. jr reg
 - jump to address specified in register reg
- ☐ It is usually used for procedure call and case/switch statement

□ Consider the program below: What are the values stored in Array1 after the program is executed? (It depends on where 'jr' goes)

```
.data
Array1: .word 4 8 12 16 20
.text
.globl __start
  start:
la $t0, Array1
                          i) What are the values of t1 & t2 ?
lw $t1, 4($t0)
lw $t2, 8($t0)
                          ii) If the instruction add $t1, $t1, $t1
la $s0, Label1
                               stores at address 10000, what is the
add $s0, $s0, $t1
                               value of s0 & what jr $s0 does ?
ir $s0
Label1:
                           Store at address 10000
add $t1, $t1, $t1 ◆
add $t1, $t2, $t2
sw $t1, 12($t0)
                           iii) Where is this instruction stored ?
```

Array1: .word 4 8 12 16 20

la \$t0, Array1 Array1 → lw \$t1, 4(\$t0) lw \$t2, 8(\$t0)

i) So, t1 = 8, t2 = 12

la \$s0, Label1 add \$s0, \$s0, \$t1 jr \$s0

Address	Value	Array element
t0	4	Array1[0]
t0+4	8	Array1[1]
t0+8	12	Array1[2]
t0+12	16	Array1[3]
t0+16	20	Array1[4]

ii) s0 = 10000 after la \$s0, Labell is executed.

Hence, the next instruction to be run after jr \$s0 is stored at 10000 + 8 = 10008th byte of the memory

Label1: add \$t1, \$t1, \$t1 add \$t1, \$t2, \$t2 sw \$t1, 12(\$t0)

	Address	Instruction			
Label1 →	10000	add \$t1, \$t1, \$t1			
	10004	add \$t1, \$t1, \$t2			
	10008	sw \$t1, 12(\$t0)			

iii) All MIPS instructions are fixed as 4 bytes long. So,
 sw \$t1, 12(\$t0) should be executed after jr \$s0
 (2 instructions skipped). Array1[3] = t1 = 8 at the end

4. Dealing with "Procedure"

- □ Procedures (also called subroutines) are necessary in any programming language
- ☐ They allow better structuring of programs
- ☐ Thus we need mechanisms that allow to **jump** to the procedure and to **return** from it

```
int    max(int k, int 1)
    if (k <= 1)
        return 1;
    else
        return k;
}</pre>
```

- Necessary steps for executing a procedure:
 - 1. Place the parameters in place where the procedure can get them
 - 2. Transfer control to the procedure
 - 3. Acquire the storage resources needed for the procedure
 - 4. Perform the desired task
 - 5. Place the result value in a place where the caller can access it
 - 6. Return control to the point of origin, since a procedure can be called from several points in a program

- Registers for procedure calling:
 - \$a0-\$a3: four **argument registers** for passing parameters
 - \$v0-\$v1: two value registers for returning values
 - \$ra: one return address register for returning to the point of origin
- **□ Program counter (PC) or instruction address register:**
 - Register that holds address of the current instruction being executed
 - It is updated after executing the current instruction
 - How?
 - PC = PC + 4 *or* PC = branch target address

- □ jal ('jump and link'):
 - O jal ProcedureAddress
 - Two things happen at the same time
 - 1. First, it save the address of the following instruction (i.e., PC + 4 as return address) to register \$ra
 - 2. Then, jump to address specified by ProcedureAddress
- ☐ jr ('jump register'):
 - O jr register
 - An unconditional jump to the address specified in a register
 - Can be used to return from a procedure
 - How?
 - jr \$ra (jumps to the address stored in register \$ra)

□ The calling program (caller)

- Passing parameters:
 - Puts the parameter values in \$a0 \$a3
 - Invokes jal x to jump to procedure X

□ Procedure X (callee)

- Performs the calculations
- O To return the results, place the results in \$v0 \$v1
- O Returns control to the caller using jr \$ra
- Caller picks up the result from \$v0 \$v1

```
What gets done here is
     12
         instruction1
     16
         instruction2
                                   ra = PC + 4 = 20 + 4 = 24
     20
          jal max
                                         = addr(max) = 60
                                   PC
          instruction3
     24
max: 60
         instruction5
         instruction6
    68
         instruction7
    72
         instruction8
    76
         jr $31
                                    It means "jr $ra"
```

```
12 instruction1
16 instruction2
20 jal max
24 instruction3
```

```
What gets done here is
```

```
$ra = PC + 4 = 20 + 4 = 24
PC = addr(max) = 60
```

```
max: 60 instruction5
64 instruction6
68 jal proc
72 instruction8
76 jr $31
```

What if we replace instruction 7 by another procedure call, say jal proc?

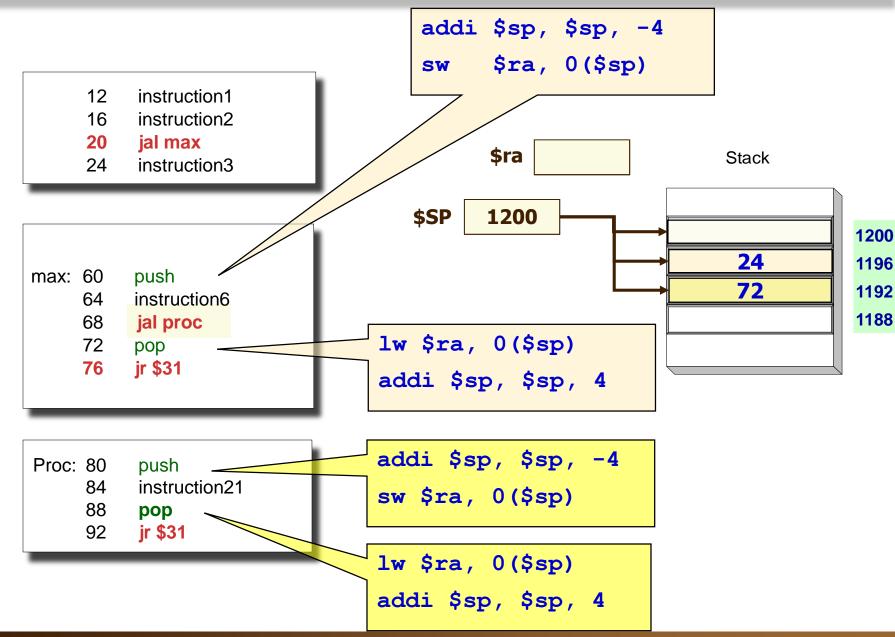
```
$ra = 72
PC = addr(proc) = 80
```

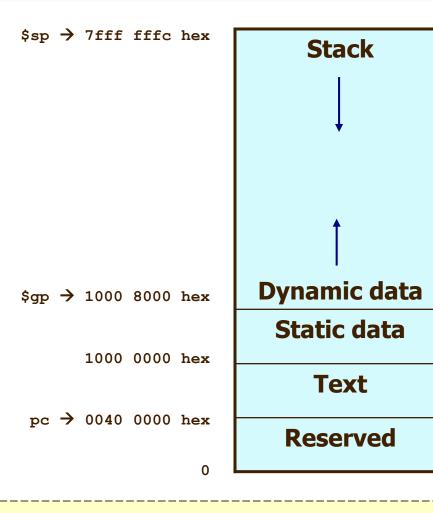
```
Proc: 80 instruction20
84 instruction21
88 ir $31
```

Oops! \$ra = 72!!!! Can't return to line 24

- □ Since **procedures** are like small programs themselves, they may **need to use the registers**, and they **may also call other procedures** (nested calls)
 - If we don't save some of the values stored in the registers, they will be wiped each time we call a new procedure
 - e.g. \$ra was wiped out in previous example in max(), and we have no way to return from nested procedure calls
- □ In MIPS, we need to save the registers by ourselves (some other ISAs would do it on your behalf)
 - The perfect place for this is called a <u>stack</u>
 - a memory accessible only from the top (Last In First Out, LIFO)
 - placing things on the stack is called push
 - removing them is called pop
 - push and pop are simply storing and loading words to and from a specific location in the memory pointed to by the stack pointer \$sp which always points to top of the stack

Using Stack to Deal with Nested Procedure





stack

For data structures that grow and shrink (e.g., linked lists) **heap**

For constant and other static variables static data segment

Home of MIPS machine code, or **text segment**

Heap operation:

- □ malloc() allocate space on the heap and returns a pointer to it
- ☐ **free()** releases space on the stack to which the pointer points

■ MIPS operands:

- 32 registers (32 bits each)
- 2³⁰ memory word locations (32 bits each)

□ MIPS instructions:

- O Arithmetic: add, sub, addi
- O Data transfer: 1w, sw
- O Logical: and, or, nor, andi, ori, sll, srl
- O Conditional branch: beg, bne, slt
- Unconditional jump: j, jr, jal

■ MIPS instruction formats:

O R-format, I-format (used by j and jal; to be explained later)

Name	Register number	Usage	Preserved on call?	
\$zero	0	constant value 0	n.a.	
\$at	1	reserved for assembler	n.a.	
\$v0-\$v1	2-3	values for results and expression evaluation	no	
\$a0-\$a3	4-7	arguments	no	
\$t0-\$t7	8-15	temporaries	no	
\$s0-\$s7	16-23	saved temporaries	yes	
\$t8-\$t9	24-25	more temporaries	no	
\$k0-\$k1	26-27	reserved for operating system kernel	n.a.	
\$gp	28	pointer to global area	yes	
\$sp	29	stack pointer	yes	
\$fp	30	frame pointer	yes	
\$ra	31	return address	yes	

Preserved on call means, the value of those registers should remain the same before and after the procedure is called

If any of those registers are modified inside the procedure, you should put them into stack before the procedure is actually executed

- ☐ Most computers use 8-bit (bytes) to represent characters
 - ASCII: American Standard Code for Information Interchange
 - Example:

ASCII value	Char- acter								
48	0	49	1	65	Α	66	В	90	Z
97	а	98	b	32	Space	35	#	42	*

- □ Notice that character "a" and "A" are assigned with different values!
- ☐ Operation with byte: 1b (load byte), sb (store byte)
 - Example

```
1b $t0, 0($sp) # Read byte from source
sb $s0, 0($gp) # Write byte to destination
```

- □ Characters are normally combined into strings
- How to represent a string? Three choices are:
 - 1. First position of a string is reserved to give the length of a string
 - 2. An accompanying variable has the length of the string (as in a structure)
 - 3. The last position of a string is indicated by a character used to mark the end of a string
 - "C" uses the 3rd choice
 - "C" terminates a string with a byte whose value is 0
 (null in ASCII)
 - Example the string 'Cal' → ASCII 67,97,108,0

- ☐ Procedure strcpy() in "C" language
 - o copies string y to string x using the null byte termination convention

```
void strcpy (char x[], char y[])
{
    int i;

    i = 0;
    while ((x[i] = y[i])!='\0') /* copy & test byte */
        i += 1;
}
```

```
strcpy:
                               # adjust stack for 1 more item
  addi $sp, $sp, -4
                               # save $s0
  sw $s0, 0($sp)
  add $s0, $zero, $zero # i = 0 + 0
L1:
                               # address of y[i] in $t1
  add $t1, $s0, $a1
                               \# $t2 = y[i]
  lb $t2, 0($t1)▲
  add $t3, $s0, $a0
                               # address of x[i] in $t3
                               \# x[i] = $t2
  sb $t2, 0($t3)
                               # if y[i] = 0, go to L2
  beq $t2, $zero, L2
                               \# i = i + 1
  addi $s0, $s0, 1
                               # go to L1
       L1
                               \# y[i] == 0: end of string;
L2:
                               # restore old $s0
  lw $s0, 0($sp)
                               # pop 1 word off the stack
  addi $sp, $sp, 4
                               # return
  jr $ra
```

don't have to multiply i by 4 since x and y are arrays of bytes, not of words

- ☐ Constants are frequently short and fit into 16-bit field
- ☐ But sometimes they are bigger than 16 bits, e.g. 32-bit constant

Problem:

☐ With instruction learned so far, we cannot set registers' upper 16bits!

Solution:

- ☐ lui ("load upper immediate")
 - O e.g. lui reg, constant
 - o set the upper 16 bits of register **reg** to the **16**-bit value specified in **constant**
 - Set the lower 16 bits of register reg to zeros
 - o note that constant should not greater than 2¹⁶

- ☐ How to load the 32-bit constant below into register \$s0?
 ☐ 0000 0000 0011 1101 0000 1001 0000 0000₂ (0x003D0900)
- ☐ Solution: (assuming the initial value in \$s0 is 0)

```
lui $s0, 61  # 61_{10} = 0000 \ 0000 \ 0011 \ 1101_2  # value of $s0 becomes 0000 0000 0011 1101 0000 0000 0000 0000_2 ori $s0, $s0, 2304  # 2304_{10} = 0000 \ 1001 \ 0000 \ 0000_2  # now, we get the value desired into the register
```

5. Addressing Modes

- We have seen, so far three addressing modes of MIPS:
 - Immediate addressing: provides fast access of small constants
 e.g. addi \$t0, \$t0, 1023
 - 2. Register addressing: the operand is available in a register
 - e.g. add \$t0, \$t0, \$t1
 - 3. Base addressing: the operand is the sum of a **(base)** register and a **displacement**e.g. 1w \$t0, 1024 (\$t1)
- ☐ MIPS architecture provides <u>two more</u> ways of addressing

J-type or J-format

ор	address
6 bits	26 bits

- ☐ Also called pseudodirect addressing; the simplest addressing mode
- ☐ Used by instructions such as j ('jump') and jal ('jump and link')
 - O e.g. j L1 # go to instruction labeled L1
- □ 26-bit word address, corresponding to a 28-bit byte address, is concatenated with the 4 upper bits of the PC to form a 32-bit byte branch target address that corresponds to label L1

Example: 2 1100 0011 1000 0001 1111 0011 01

- \square If PC = 0100 1101 0111 0000 1100 0011 0000 1100
- □ Target L1 is: 0100 1100 0011 1000 0001 1111 0011 0100

Because,

□ All MIPS instructions are 4 bytes long

So,

- □ A branch target or offset can refer to number of words instead of number of bytes
- ⇒ essentially stretch the maximum possible branching distance by 4x

Questions:

- ☐ What is the range a 'j' and 'jal' can jump to?
 - O Within 256MB
- What if we want to jump beyond 256MB?

0x0 0000000	
0x0 FFFFFF	
0x1 0000000	
•••	
0x1 FFFFFF	
0x2 0000000	J L1
•••	
0x2 FFFFFF	L1:
0x7 0000000	
•••	
0x7 FFFFFF	

0x0 0000000	
0x0 FFFFFF	
0x1 0000000	J L1
0x1 FFFFFF	
0x2 0000000	L1:
0x2 FFFFFF	
0x7 0000000	
•••	
0x7 FFFFFF	

What if the Jump target is more than 256 MB away?

We know that

- ☐ Conditional branch instructions (e.g., beq, bne) use I-format
- ☐ I-format can only specify 16-bit addresses

How to branch?

- □ PC-relative addressing
 - A branch offset is added to (PC+4) to obtain address to branch to
 - Branch offset is described in number of words. Why?
 - Branching within 2¹⁵ words before or after the current instruction is possible
 - This is good enough since conditional branches tend to branch to a nearby instruction

Notes:

While an instruction is being executed, the PC always points to the current instruction, i.e., address of current instruction

☐ Traditional loop in "C":

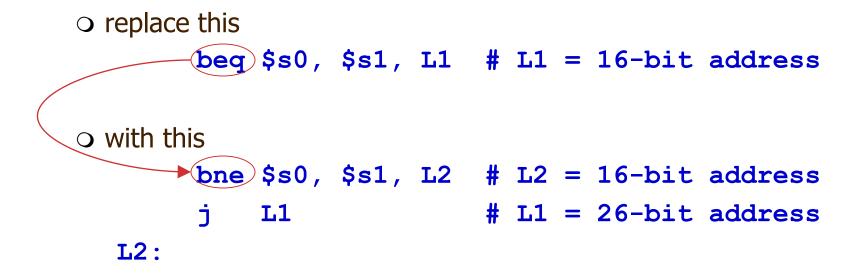
```
while (save[i] == k)
    i +=1 ;
```

- □ Assume \$s3 \rightarrow i, \$s6 \rightarrow save, \$s5 \rightarrow k, loop start at memory location 80000
- MIPS assembly code

Loop:				80000	0	0	19	9	2	0
sll	\$t1,	\$s3,	2	80004	θ_	9	22	9	0	32
add	\$t1,	\$t1,	\$s6	80008	35	9	8		0	
lw	\$t0,	0 (\$t	L)	80012	5	8	21		2	
bne	\$t0,	\$s5,	Exit	80016	8	19	19		1	
addi	\$s3,	\$s3,	1	80020	2		(20000		
Ċ	Loop			80024	Exit:					

Exit:

☐ From 16-bit word address to 26-bit word address:



Attention:

The tradeoff is longer program execution time

• i.e. need to execute two instructions rather than just one

1. Immediate addressing

• The operand is a constant within the instruction itself

2. Register addressing

The operand is a register

3. Base addressing or displacement addressing

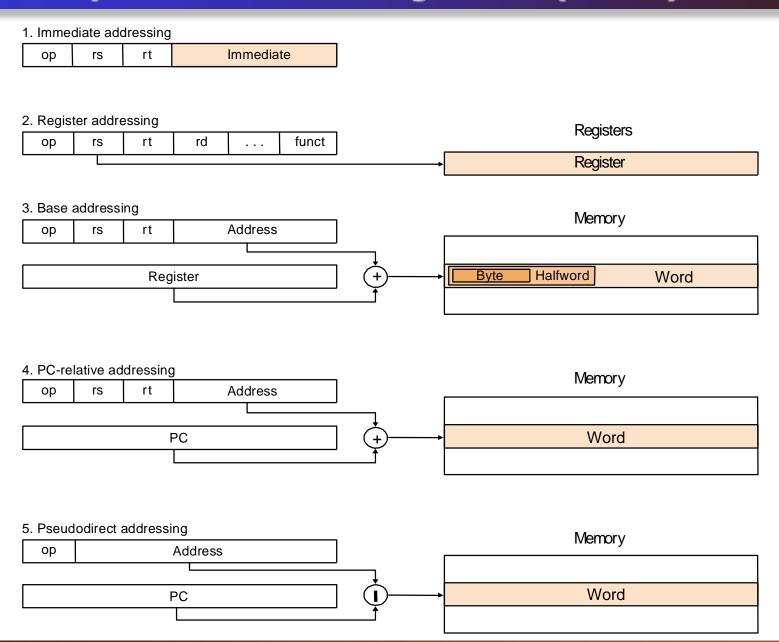
The operand is at the memory location with address= (register) + constant

4. PC-relative addressing

 \circ The address is = (PC) + 4 + constant

5. Pseudodirect addressing

 The jump address is a constant in the instruction concatenated with the upper 4 bits of the PC



□ MIPS operands:

- 32 registers (32 bits each)
- 2³⁰ memory word locations (32 bits each)

■ MIPS instructions:

- O Arithmetic: add, sub, addi
- O Data transfer: lw, sw, lb, sb, lui
 - 1b and sb are similar to 1w and sw, but for transferring bytes instead of words
- O Conditional branch: beq, bne, slt, slti
- O Unconditional jump: j, jr, jal

■ MIPS instruction formats:

○ R-format, I-format, J-format

6. Other Issues

- MIPS is an example of RISC
 - Reduced Instruction Set Computer
 - Each instruction does one simple thing
 - Most existing processors are RISC since it is more promising
- □ Another approach is CISC
 - Complex Instruction Set Computer
 - One instruction may do multiple things, e.g. Intel's instruction set

	RISC	CISC
Number of instructions in a program	(–) more	(+) less
Time to execute the program	(+) usually less	(-) usually more
Hardware design	(+) simple	(–) complex

(+) means advantage, (-) means disadvantage

RISC	CISC			
Through quantitative measurements, choose only the most useful instructions and addressing modes.	Choose instructions and addressing modes that make the translation of high-level languages to assembly language simpler.			
With few instructions and addressing modes, we can directly execute them in hardware.	Since we can have many instructions and addressing modes, we need a microcode (or microprogrammed control) to execute them in hardware.			
A lot of chip space can be left for a large number of registers and cache memory.	We can have only few registers and small cache memory.			
Compilers are more difficult to write.	Compilers are easier to write.			
Assembly language programs are more difficult to write.	Assembly language programs are easier to write.			

Pseudoinstructions

□ Assembly language instructions that do not have corresponding machine instructions (i.e., they need not be implemented directly in hardware)

Why Pseudoinstructions?

☐ Their appearance in assembly language simplifies programming and translation, giving MIPS a richer set of assembly language instructions than those implemented by the hardware.

Cost of supporting Pesudoinstructions

☐ The only cost is reserving one register, \$at, for use by the assembler

□ move:

- O move \$t0, \$t1 # \$t0 gets value of \$t1
- The assembler converts this pseudoinstruction into the machine language equivalent of the following instruction:

```
add $t0, $zero, $t1  # $t0 gets 0 + value of $t1
```

□ Others:

- O blt ('branch on less than')
- O ble ('branch on less than or equal')
- o bgt ('branch on greater than')
- O bge ('branch on greater than or equal')

- ☐ The stored-program concept underlies today's digital computers
- □ An instruction specifies an operation and its corresponding operand(s)
- ☐ All MIPS instructions are 32 bits in length
 - To simplify the instruction set architecture
 - But, multiple instruction formats are supported
- Registers are fast temporary storage inside the processor
- ☐ Four design principles for ISA
 - Simplicity favors regularity
 - Smaller is faster
 - Make common case fast
 - Good design demands good compromises

- □ Program counter is a special register
 - Pointing to the current instruction to be fetched and executed
- Branch/jump instructions often require branch address calculation
- MIPS supports different addressing modes
 - 1. Register
 - 2. Displacement
 - 3. Immediate
 - 4. PC-relative
 - 5. Pseudodirect
- □ Pseudoinstructions extend the MIPS instruction set
 - To facilitate program development
- □ RISC and CISC are two very different design philosophies