18-447 Lab B
MIPS ISA

Modified by Justin Meza
Based on slides by James C. Hoe
Instruction Set Architecture

• A stable platform, typically 15~20 years
  - guarantees binary compatibility for SW investments
  - permits adoption of foreseeable technology advances

• User-level ISA
  - program visible state and instructions available to user processes
  - single-user abstraction on top of HW/SW virtualization

• “Virtual Environment” Architecture
  - state and instructions to control virtualization (e.g., caches, sharing)
  - user-level, but not used by your average user programs

• “Operating Environment” Architecture
  - state and instructions to implement virtualization
  - privileged/protected access reserved for OS
Terminologies

• Instruction Set Architecture
  - the machine behavior as observable and controllable by the programmer
• Instruction Set
  - the set of commands understood by the computer
• Machine Code
  - a collection of instructions encoded in binary format
  - directly consumable by the hardware
• Assembly Code
  - a collection of instructions expressed in “textual” format
  - e.g. Add r1, r2, r3
  - converted to machine code by an assembler
  - one-to-one correspondence with machine code
  (mostly true: compound instructions, address labels ....)
What are specified/decided in an ISA?

• Data format and size
  - character, binary, decimal, floating point, negatives
• “Programmer Visible State”
  - memory, registers, program counters, etc.
• Instructions: how to transform the programmer visible state?
  - what to perform and what to perform next
  - where are the operands
• Instruction-to-binary encoding
• How to interface with the outside world?
• Protection and privileged operations
• Software conventions

Very often you compromise immediate optimality for future scalability and compatibility
MIPS R2000 Program Visible State

**Program Counter**
32-bit memory address of the current instruction

<table>
<thead>
<tr>
<th>M[0]</th>
</tr>
</thead>
<tbody>
<tr>
<td>M[1]</td>
</tr>
<tr>
<td>M[2]</td>
</tr>
<tr>
<td>M[3]</td>
</tr>
<tr>
<td>M[4]</td>
</tr>
<tr>
<td>M[N-1]</td>
</tr>
</tbody>
</table>

**General Purpose Register File**
32 32-bit words named r0...r31

<table>
<thead>
<tr>
<th><strong>Note</strong></th>
<th>r0=0</th>
</tr>
</thead>
<tbody>
<tr>
<td>r1</td>
<td></td>
</tr>
<tr>
<td>r2</td>
<td></td>
</tr>
</tbody>
</table>

**Memory**
$2^{32}$ by 8-bit locations (4 Giga Bytes)
32-bit address
(there is some magic going on)
Data Format

• Most things are 32 bits
  - instruction and data addresses
  - signed and unsigned integers
  - just bits
• Also 16-bit word and 8-bit word (aka byte)
• Floating-point numbers
  - IEEE standard 754
  - float: 8-bit exponent, 23-bit significand
  - double: 11-bit exponent, 52-bit significand
Big Endian vs. Little Endian
(Part I, Chapter 4, Gulliver’s Travels)

- 32-bit signed or unsigned integer comprises 4 bytes

- On a byte-addressable machine . . . . .

### Table: Big Endian vs. Little Endian

<table>
<thead>
<tr>
<th>MSB</th>
<th>LSB</th>
<th>MSB</th>
<th>LSB</th>
</tr>
</thead>
<tbody>
<tr>
<td>byte 0</td>
<td>byte 1</td>
<td>byte 3</td>
<td>byte 0</td>
</tr>
<tr>
<td>byte 4</td>
<td>byte 5</td>
<td>byte 6</td>
<td>byte 7</td>
</tr>
<tr>
<td>byte 8</td>
<td>byte 9</td>
<td>byte 10</td>
<td>byte 11</td>
</tr>
<tr>
<td>byte 12</td>
<td>byte 13</td>
<td>byte 14</td>
<td>byte 15</td>
</tr>
<tr>
<td>byte 16</td>
<td>byte 17</td>
<td>byte 18</td>
<td>byte 19</td>
</tr>
</tbody>
</table>

pointer points to the **big end**

### Diagram:

- MSB (most significant) vs. LSB (least significant)

### What difference does it make?

- check out htonl(), ntohl() in in.h
Instruction Formats

- **3 simple formats**
  - **R-type**, 3 register operands
    - | 0 | rs | rt | rd | shamt | funct |
    - | 6-bit | 5-bit | 5-bit | 5-bit | 5-bit | 6-bit |
    - **I-type**, 2 register operands and 16-bit immediate
      - | opcode | rs | rt | immediate |
      - | 6-bit | 5-bit | 5-bit | 16-bit |
    - **J-type**, 26-bit immediate operand
      - | opcode | immediate |
      - | 6-bit | 26-bit |

- **Simple Decoding**
  - 4 bytes per instruction, regardless of format
  - must be 4-byte aligned (2 lsb of PC must be 2b’00)
  - format and fields readily extractable
(Not this R-Type)
Instruction Formats

- 3 simple formats
  - R-type, 3 register operands
    
    | 0 | rs | rt | rd | shamt | funct |
    |---|----|----|----|-------|-------|
    | 6-bit | 5-bit | 5-bit | 5-bit | 5-bit | 6-bit |

  - I-type, 2 register operands and 16-bit immediate
    
    | opcode | rs | rt | immediate |
    |--------|----|----|-----------|
    | 6-bit | 5-bit | 5-bit | 16-bit |

  - J-type, 26-bit immediate operand
    
    | opcode | immediate |
    |--------|-----------|
    | 6-bit | 26-bit |

- Simple Decoding
  - 4 bytes per instruction, regardless of format
  - must be 4-byte aligned (2 lsb of PC must be 2b’ 00)
  - format and fields readily extractable
ALU Instructions

- **Assembly** (e.g., register-register signed addition)
  \[
  \text{ADD } r_d, r_s, r_t
  \]

- **Machine encoding**
  \[
  \begin{array}{ccccccc}
  0 & rs & rt & rd & 0 & ADD \\
  6-bit & 5-bit & 5-bit & 5-bit & 5-bit & 6-bit \\
  \end{array}
  \]

- **Semantics**
  - \( \text{GPR}[r_d] \leftarrow \text{GPR}[r_s] + \text{GPR}[r_t] \)
  - \( \text{PC} \leftarrow \text{PC} + 4 \)

- **Exception on “overflow”**

- **Variations**
  - Arithmetic: \{signed, unsigned\} \times \{ADD, SUB\}
  - Logical: \{AND, OR, XOR, NOR\}
  - Shift: \{Left, Right-Logical, Right-Arithmetic\}
## Reg-Reg Instruction Encoding

What patterns do you see? Why are they there?
ALU Instructions

- Assembly (e.g., regi-immediate signed additions)
  \[
  \text{ADDI } r_t_{\text{reg}} \ r_s_{\text{reg}} \ i_{\text{mmediate}}_{16}
  \]
- Machine encoding

<table>
<thead>
<tr>
<th>ADDI</th>
<th>rs</th>
<th>rt</th>
<th>immediate</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-bit</td>
<td>5-bit</td>
<td>5-bit</td>
<td>16-bit</td>
</tr>
</tbody>
</table>

- Semantics
  - \( GPR[r_t] \leftarrow GPR[r_s] + \text{sign-extend} \) (immediate)
  - \( PC \leftarrow PC + 4 \)
- Exception on “overflow”
- Variations
  - Arithmetic: \{signed, unsigned\} x \{ADD, SUB\}
  - Logical: \{AND, OR, XOR, LUI\}
### Reg-Immed Instruction Encoding

<table>
<thead>
<tr>
<th>0</th>
<th>SPECIAL</th>
<th>REGIMM</th>
<th>J</th>
<th>JAL</th>
<th>BEQ</th>
<th>BNE</th>
<th>BLEZ</th>
<th>BGTZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ADDI</td>
<td>ADDIU</td>
<td>SLTI</td>
<td>SLTIU</td>
<td>ANDI</td>
<td>ORI</td>
<td>XORI</td>
<td>LUI</td>
</tr>
<tr>
<td>2</td>
<td>COP0</td>
<td>COP1</td>
<td>COP2</td>
<td>*</td>
<td>BEQL</td>
<td>BNEL</td>
<td>BLEZL</td>
<td>BGTZL</td>
</tr>
<tr>
<td>3</td>
<td>DADDIε</td>
<td>DADDIUε</td>
<td>LDLε</td>
<td>LDRε</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>4</td>
<td>LB</td>
<td>LH</td>
<td>LWL</td>
<td>LW</td>
<td>LBU</td>
<td>LHU</td>
<td>LWR</td>
<td>LWUε</td>
</tr>
<tr>
<td>5</td>
<td>SB</td>
<td>SH</td>
<td>SWL</td>
<td>SW</td>
<td>SDLε</td>
<td>SDRε</td>
<td>SWR</td>
<td>CACHE δ</td>
</tr>
<tr>
<td>6</td>
<td>LL</td>
<td>LWC1</td>
<td>LWC2</td>
<td>*</td>
<td>LLDε</td>
<td>LDC1</td>
<td>LDC2</td>
<td>LDε</td>
</tr>
<tr>
<td>7</td>
<td>SC</td>
<td>SWC1</td>
<td>SWC2</td>
<td>*</td>
<td>SCDε</td>
<td>SDC1</td>
<td>SDC2</td>
<td>SDε</td>
</tr>
</tbody>
</table>

[MIPS R4000 Microprocessor User’s Manual]
Assembly Programming 101

• Break down high-level program constructs into a sequence of elemental operations

• E.g. High-level Code

\[ f = ( g + h ) - ( i + j ) \]

• Assembly Code
  - suppose \( f, g, h, i, j \) are in \( r_f, r_g, r_h, r_i, r_j \)
  - suppose \( r_{\text{temp}} \) is a free register

\[
\begin{align*}
\text{add } & \quad r_{\text{temp}} \quad r_g \quad r_h \quad \# \quad r_{\text{temp}} = g+h \\
\text{add } & \quad r_f \quad r_i \quad r_j \quad \# \quad r_f = i+j \\
\text{sub } & \quad r_f \quad r_{\text{temp}} \quad r_f \quad \# \quad f = r_{\text{temp}} - r_f
\end{align*}
\]
Load Instructions

• Assembly (e.g., load 4-byte word)
  \[ \text{LW } rt_{reg} \text{ offset}_{16} (\text{base}_{reg}) \]

• Machine encoding

<table>
<thead>
<tr>
<th></th>
<th>LW</th>
<th>base</th>
<th>rt</th>
<th>offset</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6-bit</td>
<td>5-bit</td>
<td>5-bit</td>
<td>16-bit</td>
</tr>
</tbody>
</table>

• Semantics
  - effective_address = sign-extend(offset) + GPR[base]
  - GPR[rt] ← MEM[ translate(effective_address) ]
  - PC ← PC + 4

• Exceptions
  - address must be “word-aligned”
    What if you want to load an unaligned word?
  - MMU exceptions
Data Alignment

- LW/SW alignment restriction
  - not optimized to fetch memory bytes not within a word boundary
  - not optimized to rotate unaligned bytes into registers
- Provide separate opcodes for the infrequent case

<table>
<thead>
<tr>
<th></th>
<th>byte-7</th>
<th>byte-6</th>
<th>byte-5</th>
<th>byte-4</th>
<th>byte-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

LWL  rd 6(r0)  
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>byte-6</td>
<td>byte-5</td>
<td>byte-4</td>
<td>D</td>
</tr>
</tbody>
</table>

LWR  rd 3(r0)  
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>byte-6</td>
<td>byte-5</td>
<td>byte-4</td>
<td>byte-3</td>
</tr>
</tbody>
</table>

- LWL/LWR is slower but it is okay
- note LWL and LWR still fetch within word boundary
Store Instructions

• Assembly (e.g., store 4-byte word)
  \( SW \, rt_{\text{reg}} \, \text{offset}_{16} (\text{base}_{\text{reg}}) \)

• Machine encoding

<table>
<thead>
<tr>
<th>SW</th>
<th>base</th>
<th>rt</th>
<th>offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-bit</td>
<td>5-bit</td>
<td>5-bit</td>
<td>16-bit</td>
</tr>
</tbody>
</table>

• Semantics
  - effective_address = sign-extend(offset) + GPR[base]
  - MEM[ translate(effective_address) ] ← GPR[rt]
  - PC ← PC + 4

• Exceptions
  - address must be “word-aligned”
  - MMU exceptions
Assembly Programming 201

• E.g. High-level Code

\[ A[8] = h + A[0] \]

where \( A \) is an array of integers (4-byte each)

• Assembly Code
  - suppose \&A, h are in \( r_A, r_h \)
  - suppose \( r_{\text{temp}} \) is a free register

\[
\begin{align*}
\text{LW } r_{\text{temp}} & 0(r_A) & \# r_{\text{temp}} &= A[0] \\
\text{add } r_{\text{temp}} & r_h r_{\text{temp}} & \# r_{\text{temp}} &= h + A[0] \\
\text{SW } r_{\text{temp}} & 32(r_A) & \# A[8] &= r_{\text{temp}} \\
& & \# \text{note } A[8] \text{ is 32 bytes} \\
& & \# \text{ from } A[0]
\end{align*}
\]
Control Flow Instructions

- C-Code

```c
{ code A }
if X==Y then
  { code B }
else
  { code C }
{ code D }
```

These things are called basic blocks.
(Conditional) Branch Instructions

- Assembly (e.g., branch if equal)
  \[ \text{BEQ } r_{\text{reg}} \text{ rt}_{\text{reg}} \text{ immediate}_{16} \]
- Machine encoding
  \[
  \begin{array}{cccc}
  \text{BEQ} & \text{rs} & \text{rt} & \text{immediate} \\
  \text{6-bit} & \text{5-bit} & \text{5-bit} & \text{16-bit}
  \end{array}
  \]
- Semantics
  - \( \text{target} = \text{PC} + \text{sign-extend}(\text{immediate}) \times 4 \)
  - if \( \text{GPR}[\text{rs}] == \text{GPR}[\text{rt}] \) then \( \text{PC} \leftarrow \text{target} \)
  - else \( \text{PC} \leftarrow \text{PC} + 4 \)
- How far can you jump?
- Variations
  - BEQ, BNE, BLEZ, BGTZ

Why isn’t there a BLE or BGT instruction?
Jump Instructions

• Assembly
  J immediate_{26}

• Machine encoding
  
<table>
<thead>
<tr>
<th>J</th>
<th>immediate</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-bit</td>
<td>26-bit</td>
</tr>
</tbody>
</table>
  
  J-type

• Semantics
  - target = PC[31:28]x2^{28} | bitwise-or zero-extend(immediate)x4
  - PC ← target

• How far can you jump?

• Variations
  - Jump and Link
  - Jump Registers
Branch Delay Slots
(FYI, not for your HW or lab)

• R2000 branch instructions also have an architectural latency of 1 instructions
  - the instruction immediately after a branch is always executed (in fact PC-offset is computed from the delay slot instruction)
  - branch target takes effect on the 2nd instruction

```
bne r_i r_j L1
  add r_e r_g r0
  j L2
L1:  add r_e r_h r0
L2:  add r_f r_e r0
...  ...
```
Strangeness in the Semantics

Where do you think you will end up?

\[
\begin{align*}
_s & : \ j \ L1 \\
    & : \ j \ L2 \\
    & : \ j \ L3 \\
L1 & : \ j \ L4 \\
L2 & : \ j \ L5 \\
L3 & : \ \text{foo} \\
L4 & : \ \text{bar} \\
L5 & : \ \text{baz}
\end{align*}
\]
Function Call and Return

• Jump and Link:  JAL offset_{26}
  - return address = PC + 8
  - target = PC[31:28]x2^{28} \mid_{\text{bitwise-or zero-extend}(\text{immediate})}x^{4}
  - PC ← target
  - GPR[r31] ← return address

On a function call, the callee needs to know where to go back to afterwards

• Jump Indirect:  JR \ rs_{\text{reg}}
  - target = GPR [rs]
  - PC ← target

PC-offset jumps and branches always jump to the same target every time the same instruction is executed
Jump Indirect allows the same instruction to jump to any location specified by rs (usually r31)
Assembly Programming 301

- ..... A \rightarrow \text{call} B \rightarrow \text{return} C \rightarrow \text{call} B \rightarrow \text{return} D ..... 
- How do you pass arguments between caller and callee?
- If A sets r10 to 1, what is the value of r10 when B returns to C?
- What registers can B use?
- What happens to r31 if B calls another function
Caller and Callee Saved Registers

• Callee-Saved Registers
  - Caller says to callee, “The values of these registers should not change when you return to me.”
  - Callee says, “If I need to use these registers, I promise to save the old values to memory first and restore them before I return to you.”

• Caller-Saved Registers
  - Caller says to callee, “If there is anything I care about in these registers, I already saved it myself.”
  - Callee says to caller, “Don’t count on them staying the same values after I am done.”
R2000 Register Usage Convention

- r0: always 0
- r1: reserved for the assembler
- r2, r3: function return values
- r4~r7: function call arguments
- r8~r15: “caller-saved” temporaries
- r16~r23: “callee-saved” temporaries
- r24~r25: “caller-saved” temporaries
- r26, r27: reserved for the operating system
- r28: global pointer
- r29: stack pointer
- r30: callee-saved temporaries
- r31: return address
R2000 Memory Usage Convention

- **Stack Pointer**: GPR[r29]
- **Stack Space**: Grows down
- **Free Space**: Grows up
- **Dynamic Data**
- **Static Data**
- **Text**
- **Reserved**

Memory usage convention:
- High address: Stack space, Free space, Dynamic data, Static data, Text, Binary executable
- Low address: Reserved

Diagram shows the memory allocation with decreasing addresses towards the high address and increasing addresses towards the low address.
# Calling Convention

1. caller saves caller-saved registers
2. caller loads arguments into r4~r7
3. caller jumps to callee using JAL
4. callee allocates space on the stack (dec. stack pointer)
5. callee saves callee-saved registers to stack (also r4~r7, old r29, r31)
6. callee loads results to r2, r3
7. callee restores saved register values
8. JR r31
9. caller continues with return values in r2, r3

......

**prologue**

**body of callee** (can “nest” additional calls) .......

**epilogue**
To Summarize: MIPS RISC

• Simple operations
  - 2-input, 1-output arithmetic and logical operations
  - few alternatives for accomplishing the same thing
• Simple data movements
  - ALU ops are register-to-register (need a large register file)
    - “Load-store” architecture
• Simple branches
  - limited varieties of branch conditions and targets
• Simple instruction encoding
  - all instructions encoded in the same number of bits
    - only a few formats

Loosely speaking, an ISA intended for compilers rather than assembly programmers
We’ll still learn about...

- Privileged Modes
  - User vs. supervisor
- Exception Handling
  - trap to supervisor handling routine and back
- Virtual Memory
  - Each user has 4-GBytes of private, large, linear and fast memory?
- Floating-Point Instructions