Stored Program Computers

- Instructions represented in binary, just like data
- Instructions and data stored in memory
- Programs can operate on programs
  - e.g., compilers, linkers, …
- Binary compatibility allows compiled programs to work on different computers
  - Standardized ISAs
The ISA

- Instruction Set Architecture
  - The ISA defines the CPU, or a CPU family (e.g. x86)
    - not only a collection of instructions,
    - includes the CPU view of memory, registers number and roles, etc.
  - The ISA is the **contract** between s/w and h/w

- ISA ≠ CPU architecture (µ-architecture)
  - E.g x86: Xeon ≠ Celeron, same ISA
MIPS ISA
The MIPS ISA

- Used as the example throughout the book
- Stanford MIPS commercialized by MIPS Technologies (www.mips.com)
- Large share of embedded core market
  - Applications in consumer electronics, network/storage equipment, cameras, printers, …
- Typical of many modern ISAs
  - See MIPS Reference Data tear-out card, and Appendixes B and E
MIPS ISA

- **Design principles**
  - small, regular & simple design ➔ fast
  - make the common case fast
  - good design requires good compromises

- **Features**
  - 32 32-bit registers, \( r_0 = 0 \) always
  - only *load* and *store* instructions access memory
  - 32-bit instructions, fixed size opcode, leftmost 6 bits
    - *fixed-field decoding*
  - all ALU operations are 3 address register operations
    - add \( r_1, r_2, r_3 \), meaning: \( r1 \leftarrow r2 + r3 \)
Representing Instructions

- Instructions are encoded in binary
  - Called machine code
- MIPS instructions
  - Encoded as 32-bit instruction words
  - Small number of formats encoding operation code (opcode), register numbers, ...
  - Regularity!
- Register numbers
  - $t0 – $t7 are reg’s 8 – 15
  - $t8 – $t9 are reg’s 24 – 25
  - $s0 – $s7 are reg’s 16 – 23

convention, used for code interoperability
MIPS R-format Instructions

<table>
<thead>
<tr>
<th>op</th>
<th>rs</th>
<th>rt</th>
<th>rd</th>
<th>shamt</th>
<th>funct</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>6 bits</td>
</tr>
</tbody>
</table>

- **Instruction fields**
  - **op**: operation code (opcode)
  - **rs**: first source register number
  - **rt**: second source register number
  - **rd**: destination register number
  - **shamt**: shift amount (00000 for now)
  - **funct**: function code (extends opcode)

- **Used only for ALU instructions**
R-format Example

<table>
<thead>
<tr>
<th>op</th>
<th>rs</th>
<th>rt</th>
<th>rd</th>
<th>shamt</th>
<th>funct</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>6 bits</td>
</tr>
</tbody>
</table>

add $r8$, $r17$, $r18$

<table>
<thead>
<tr>
<th>special</th>
<th>$r17$</th>
<th>$r18$</th>
<th>$r8$</th>
<th>0</th>
<th>add</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>17</td>
<td>18</td>
<td>8</td>
<td>0</td>
<td>32</td>
</tr>
</tbody>
</table>

| 000000 | 10001 | 10010 | 01000 | 00000 | 100000 |

$000000100011001001000000000100000_2 = 02324020_{16}$
Arithmetic Operations

- Add and subtract, three operands
  - Two sources and one destination
  `add a, b, c  # a gets b + c`
- All arithmetic operations have this form

*Design Principle 1*: Simplicity favours regularity

- Regularity makes implementation simpler
- Simplicity enables higher performance at lower cost
Arithmetic Example

- C code:
  \[ f = (g + h) - (i + j); \]
- Compiled MIPS code:
  ```
  add t0, g, h   # temp t0 = g + h
  add t1, i, j   # temp t1 = i + j
  sub f, t0, t1  # f = t0 - t1
  ```
Register Operands

- Arithmetic instructions use register operands
- MIPS has a 32 × 32-bit register file
  - Use for frequently accessed data
  - Numbered 0 to 31
  - 32-bit data called a “word”
- Assembler names
  - $t0, $t1, …, $t9 for temporary values
  - $s0, $s1, …, $s7 for saved variables
- *Design Principle 2*: Smaller is faster
  - c.f. main memory: millions of locations
Register Operand Example

- C code:
  \[ f = (g + h) - (i + j); \]
  - \( f, \ldots, j \) in \$s0, \ldots, \$s4

- Compiled MIPS code:
  - `add $t0, $s1, $s2`
  - `add $t1, $s3, $s4`
  - `sub $s0, $t0, $t1`
MIPS I-format Instructions

- Immediate arithmetic and load/store instructions
  - rt: destination or source register number
  - Constant: $-2^{15}$ to $(2^{15} - 1)$, used as immediate
  - Address: offset added to base address in rs

- Good design demands good compromises
  - Different formats complicate decoding, but allow 32-bit instructions uniformly
  - Keep formats as similar as possible
I-format Example: *load*

<table>
<thead>
<tr>
<th>op</th>
<th>rs</th>
<th>rt</th>
<th>immediate or offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>16 bits</td>
</tr>
</tbody>
</table>

\[ \text{lw} \ \$r8, \ 8(\$r17), \ \$r8 \leftarrow \text{Mem}[8+\$r17] \]

<table>
<thead>
<tr>
<th>lw</th>
<th>$r17</th>
<th>$r8</th>
<th>constant or address</th>
</tr>
</thead>
<tbody>
<tr>
<td>[35_{10}]</td>
<td>17</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>100011</td>
<td>10001</td>
<td>01000</td>
<td>0000000000001000</td>
</tr>
</tbody>
</table>

\[ 100011100010100000000000000001000_2 = 8E280008_{16} \]
**I-format Example: store**

<table>
<thead>
<tr>
<th>op</th>
<th>rs</th>
<th>rt</th>
<th>immediate or offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>16 bits</td>
</tr>
</tbody>
</table>

sw $r8, 8($r17), Mem[8+$r17] ← $r8

<table>
<thead>
<tr>
<th>op</th>
<th>$r17</th>
<th>$r8</th>
<th>constant or address</th>
</tr>
</thead>
<tbody>
<tr>
<td>sw</td>
<td>17</td>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>

\[
\begin{array}{llll}
10101110001010000000000000001000 & = AE280008_{16}
\end{array}
\]
### I-format Example: `addi`

<table>
<thead>
<tr>
<th>op</th>
<th>rs</th>
<th>rt</th>
<th>immediate or offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>16 bits</td>
</tr>
</tbody>
</table>

`addi $r8,$r17, 8   $r8 ← 8+$r17`

<table>
<thead>
<tr>
<th><code>addi</code></th>
<th><code>$r17</code></th>
<th><code>$r8</code></th>
<th>constant or address</th>
</tr>
</thead>
<tbody>
<tr>
<td>$8_{10}$</td>
<td>17</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>001000</td>
<td>10001</td>
<td>01000</td>
<td>00000000000001000</td>
</tr>
</tbody>
</table>

$001000100010100000000000000001000_2 = 22280008_{16}$
I-format Example: \textit{beq}

<table>
<thead>
<tr>
<th>op</th>
<th>rs</th>
<th>rt</th>
<th>offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>16 bits</td>
</tr>
</tbody>
</table>

\texttt{beq} \; \$r8,\$r17, \; 8 \quad \text{if} \; (\$r8==\$r17) \; \text{PC} \leftarrow \text{PC}+4+8

\begin{array}{|c|c|c|c|}
\hline
\text{beq} & \$r17 & \$r8 & \text{offset} \\
\hline
4_{10} & 17 & 8 & 8 \\
000100 & 10001 & 01000 & 000000000000010000 \\
\hline
\end{array}

00010010001010000000000000010002 = 12280008_{16}
Memory Operands

- Main memory used for composite data
  - Arrays, structures, dynamic data
- To apply arithmetic operations
  - Load values from memory into registers
  - Store result from register to memory
- Memory is byte addressed
  - Each address identifies an 8-bit byte
- Words are aligned in memory
  - Address must be a multiple of 4
- MIPS is Big Endian
  - Most-significant byte at least address of a word
  - c.f. Little Endian: least-significant byte at least address
Memory Operand Example 1

- C code:
  \[
g = h + A[8];
  \]
  - \(g\) in \(s1\), \(h\) in \(s2\), base address of \(A\) in \(s3\)

- Compiled MIPS code:
  - Index 8 requires offset of 32
    - 4 bytes per word
  
  ```
  lw  $t0, 32($s3)    # load word
  add $s1, $s2, $t0
  ```

offset

base register
Memory Operand Example 2

- C code:
  \[ A[12] = h + A[8]; \]
  - \( h \) in \$s2, base address of \( A \) in \$s3

- Compiled MIPS code:
  - Index 8 requires offset of 32
  
  \[
  \begin{align*}
  &\text{lw} \quad \$t0, \ 32(\$s3) \quad \# \text{ load word} \\
  &\text{add} \quad \$t0, \ \$s2, \ \$t0 \\
  &\text{sw} \quad \$t0, \ 48(\$s3) \quad \# \text{ store word}
  \end{align*}
  \]
Registers vs. Memory

- Registers are faster to access than memory
- Operating on memory data requires loads and stores
  - More instructions to be executed
- Compiler must use registers for variables as much as possible
  - Only spill to memory for less frequently used variables
  - Register optimization is important!
Immediate Operands

- Constant data specified in an instruction
  \[ \text{addi } s3, s3, 4 \]

- No subtract immediate instruction
  - Just use a negative constant
    \[ \text{addi } s2, s1, -1 \]

- Design Principle 3: Make the common case fast
  - Small constants are common
  - Immediate operand avoids a load instruction
32-bit Constants

- Most constants are small
  - 16-bit immediate is sufficient
- For the occasional 32-bit constant
  - \texttt{lui rt, constant}
    - Copies 16-bit constant to left 16 bits of \texttt{rt}
    - Clears right 16 bits of \texttt{rt} to 0

\texttt{li} $s0, 61 \quad \texttt{0000 0000 0111 1101 0000 0000 0000 0000}$
\texttt{ori} $s0, s0, 2304 \quad \texttt{0000 0000 0111 1101 0000 1001 0000 0000}$
The Constant Zero

- MIPS register 0 ($zero) is the constant 0
  - Cannot be overwritten
- Useful for common operations
  - E.g., move between registers
    add $t2, $s1, $zero
Character Data

- Byte-encoded character sets
  - ASCII: 128 characters
    - 95 graphic, 33 control
  - Latin-1: 256 characters
    - ASCII, +96 more graphic characters

- Unicode: 32-bit character set
  - Used in Java, C++ wide characters, ...
  - Most of the world’s alphabets, plus symbols
  - UTF-8, UTF-16: variable-length encodings
Byte/Halfword Operations

- Could use bitwise operations
- MIPS byte/halfword load/store
  - String processing is a common case
    - `lb rt, offset(rs)`  `lh rt, offset(rs)`
  - Sign extend to 32 bits in `rt`
    - `lbu rt, offset(rs)`  `lhu rt, offset(rs)`
  - Zero extend to 32 bits in `rt`
    - `sb rt, offset(rs)`  `sh rt, offset(rs)`
  - Store just rightmost byte/halfword
Conditional Operations

- Branch to a labeled instruction if a condition is true
  - Otherwise, continue sequentially
- `beq rs, rt, L1`
  - if \((rs == rt)\) branch to instruction labeled \(L1\);
- `bne rs, rt, L1`
  - if \((rs != rt)\) branch to instruction labeled \(L1\);
- `j L1`
  - unconditional jump to instruction labeled \(L1\)
Compiling If Statements

- **C code:**
  ```c
  if (i==j) f = g+h;
  else f = g-h;
  ```

- **Compiled MIPS code:**
  ```
  bne $s3, $s4, Else
  add $s0, $s1, $s2
  j Exit
  Else: sub $s0, $s1, $s2
  Exit: ...
  ```

Assembler calculates addresses
Compiling Loop Statements

- C code:
  ```c
  while (save[i] == k) i += 1;
  i in $s3, k in $s5, address of save in $s6
  ```

- Compiled MIPS code:
  ```mips
  Loop:  sll    $t1, $s3, 2
         add    $t1, $t1, $s6
         lw     $t0, 0($t1)
         bne    $t0, $s5, Exit
         addi   $s3, $s3, 1
         j      Loop
  Exit:  ...
  ```
Basic Blocks

- A basic block is a sequence of instructions with:
  - No embedded branches (except at end)
  - No branch targets (except at beginning)

- A compiler identifies basic blocks for optimization
- An advanced processor can accelerate execution of basic blocks
More Conditional Operations

- Set result to 1 if a condition is true
  - Otherwise, set to 0
- \texttt{slt rd, rs, rt}
  - if \((rs < rt)\) \(rd = 1;\) else \(rd = 0;\)
- \texttt{slti rt, rs, constant}
  - if \((rs < constant)\) \(rt = 1;\) else \(rt = 0;\)
- Use in combination with \texttt{beq, bne}
  - \texttt{slt $t0, $s1, $s2  \# if ($s1 < $s2)}
  - \texttt{bne $t0, $zero, L  \# branch to L}
Signed vs. Unsigned

- Signed comparison: `slt`, `slti`
- Unsigned comparison: `sltu`, `sltui`

### Example

- \$s0 = 1111 1111 1111 1111 1111 1111 1111 1111
- \$s1 = 0000 0000 0000 0000 0000 0000 0000 0001
- `slt $t0, $s0, $s1`  # signed
  - \(-1 < +1\) \(\Rightarrow\) \$t0 = 1
- `sltu $t0, $s0, $s1`  # unsigned
  - \(+4,294,967,295 > +1\) \(\Rightarrow\) \$t0 = 0
Branch Instruction Design

» Why not blt, bge, etc?

» Hardware for <, ≥, … slower than =, ≠
  » Combining with branch involves more work per instruction, requiring a slower clock
  » All instructions penalized!

» beq and bne are the common case

» This is a good design compromise
Branch Addressing

- Branch instructions specify
  - Opcode, two registers, target address
- Most branch targets are near branch
  - Forward or backward

<table>
<thead>
<tr>
<th>op</th>
<th>rs</th>
<th>rt</th>
<th>constant or address</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>16 bits</td>
</tr>
</tbody>
</table>

- **PC-relative addressing**
  - Target address = PC + offset \( \times 4 \)
  - PC already incremented by 4 by this time
Jump Addressing

- Jump (j and jal) targets could be anywhere in text segment
- Encode full address in instruction

(Pseudo)Direct jump addressing

- Target address = PC\textsubscript{31...28} : (address \times 4)
Target Addressing Example

- Loop code from earlier example
- Assume Loop at location 80000

Loop: `sll $t1, $s3, 2` 80000

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>19</td>
<td>9</td>
<td>4</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

add $t1, $t1, $s6 80004

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>9</td>
<td>22</td>
<td>9</td>
<td>0</td>
<td>32</td>
<td></td>
</tr>
</tbody>
</table>

lw $t0, 0($t1) 80008

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>9</td>
<td>8</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

bne $t0, $s5, Exit 80012

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>8</td>
<td>21</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

addi $s3, $s3, 1 80016

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>19</td>
<td>19</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

j Loop 80020

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20000</td>
</tr>
</tbody>
</table>

Exit: ...

80024
Branching Far Away

- If branch target is too far to encode with 16-bit offset, assembler rewrites the code

Example

```
beq $s0,$s1, L1
↓
bne $s0,$s1, L2
j L1
L2:  ...
```
## MIPS ISA Register Names

<table>
<thead>
<tr>
<th>Name</th>
<th>Register number</th>
<th>Usage</th>
<th>Preserved on call?</th>
</tr>
</thead>
<tbody>
<tr>
<td>$zero</td>
<td>0</td>
<td>The constant value 0</td>
<td>n.a.</td>
</tr>
<tr>
<td>$v0–$v1</td>
<td>2–3</td>
<td>Values for results and expression evaluation</td>
<td>no</td>
</tr>
<tr>
<td>$a0–$a3</td>
<td>4–7</td>
<td>Arguments</td>
<td>no</td>
</tr>
<tr>
<td>$t0–$t7</td>
<td>8–15</td>
<td>Temporaries</td>
<td>no</td>
</tr>
<tr>
<td>$s0–$s7</td>
<td>16–23</td>
<td>Saved</td>
<td>yes</td>
</tr>
<tr>
<td>$t8–$t9</td>
<td>24–25</td>
<td>More temporaries</td>
<td>no</td>
</tr>
<tr>
<td>$gp</td>
<td>28</td>
<td>Global pointer</td>
<td>yes</td>
</tr>
<tr>
<td>$sp</td>
<td>29</td>
<td>Stack pointer</td>
<td>yes</td>
</tr>
<tr>
<td>$fp</td>
<td>30</td>
<td>Frame pointer</td>
<td>yes</td>
</tr>
<tr>
<td>$ra</td>
<td>31</td>
<td>Return address</td>
<td>yes</td>
</tr>
</tbody>
</table>
# MIPS Instruction Formats

<table>
<thead>
<tr>
<th>Name</th>
<th>Fields</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field size</td>
<td>6 bits</td>
<td>5 bits</td>
</tr>
<tr>
<td>R-format</td>
<td>op</td>
<td>rs</td>
</tr>
<tr>
<td>I-format</td>
<td>op</td>
<td>rs</td>
</tr>
<tr>
<td>J-format</td>
<td>op</td>
<td></td>
</tr>
</tbody>
</table>
Addressing Mode Summary

1. Immediate addressing
   \[ \text{op} \quad \text{rs} \quad \text{rt} \quad \text{Immediate} \]

2. Register addressing
   \[ \text{op} \quad \text{rs} \quad \text{rt} \quad \text{rd} \quad \ldots \quad \text{func} \]

3. Base addressing
   \[ \text{op} \quad \text{rs} \quad \text{rt} \quad \text{Address} \]

4. PC-relative addressing
   \[ \text{op} \quad \text{rs} \quad \text{rt} \quad \text{Address} \]

5. Pseudodirect addressing
   \[ \text{op} \quad \text{Address} \]

   \[ \text{op} \quad \text{PC} \]

   \[ \text{Memory} \]

   \[ \text{Byte} \quad \text{Halfword} \quad \text{Word} \]

   \[ \text{Memory} \]

   \[ \text{PC} \quad \text{Word} \]

   \[ \text{PC} \quad \text{Word} \]
Synchronization

- Two processors sharing an area of memory
  - P1 writes, then P2 reads
  - Data race if P1 and P2 don’t synchronize
    - Result depends on the order of accesses

- Hardware support required
  - Atomic read/write memory operation
  - No other access to the location allowed between the read and write

- Could be a single instruction
  - E.g., atomic swap of register ↔ memory
  - Or an atomic pair of instructions
Synchronization in MIPS

- Load linked: `ll rt, offset(rs)`
- Store conditional: `sc rt, offset(rs)`
  - Succeeds if location not changed since the `ll`
    - Returns 1 in rt
  - Fails if location is changed
    - Returns 0 in rt
- Example: atomic swap (to test/set lock variable)
  try: `add $t0,$zero,$s4` ;copy exchange value
  `ll $t1,0($s1)` ;load linked
  `sc $t0,0($s1)` ;store conditional
  `beq $t0,$zero,try` ;branch store fails
  `add $s4,$zero,$t1` ;put load value in $s4
PROCEDURE CALLING
Procedure Calling

Steps required
1. Place parameters in registers
2. Transfer control to procedure
3. Acquire storage for procedure
4. Perform procedure’s operations
5. Place result in register for caller
6. Return to place of call
Register Usage

- $a0 – $a3: arguments (reg’s 4 – 7)
- $v0, $v1: result values (reg’s 2 and 3)
- $t0 – $t9: temporaries
  - Can be overwritten by callee
- $s0 – $s7: saved
  - Must be saved/restored by callee
- $gp: global pointer for static data (reg 28)
- $sp: stack pointer (reg 29)
- $fp: frame pointer (reg 30)
- $ra: return address (reg 31)
Procedure Call Instructions

- Procedure call: jump and link
  \[ \text{jal } 	ext{ProcedureLabel} \]
  - Address of following instruction put in $ra
  - Jumps to target address

- Procedure return: jump register
  \[ \text{jr } $ra \]
  - Copies $ra to program counter
  - Can also be used for computed jumps
    - e.g., for case/switch statements
Leaf Procedure Example

- C code:
  ```c
  int leaf_example (int g, h, i, j)
  {
    int f;
    f = (g + h) - (i + j);
    return f;
  }
  ```

- Arguments g, ..., j in $a0, ..., $a3
- f in $s0 (hence, need to save $s0 on stack)
- Result in $v0
Leaf Procedure Example

- MIPS code:

```mips
leaf_example:
  addi $sp, $sp, -4
  sw $s0, 0($sp)  // Save $s0 on stack
  add  $t0, $a0, $a1
  add  $t1, $a2, $a3
  sub  $s0, $t0, $t1
  add  $v0, $s0, $zero
  lw   $s0, 0($sp)  // Restore $s0
  addi $sp, $sp, 4
  jr   $ra          // Return
```
Non-Leaf Procedures

- Procedures that call other procedures
- For nested call, caller needs to save on the stack:
  - Its return address
  - Any arguments and temporaries needed after the call
- Restore from the stack after the call
Non-Leaf Procedure Example

C code:

```c
int fact (int n)
{
    if (n < 1) return 1;
    else return (n * fact(n - 1));
}
```

- Argument n in $a0
- Result in $v0
Non-Leaf Procedure Example

MIPS code:

```mips
fact:
    addi $sp, $sp, -8       # adjust stack for 2 items
    sw $ra, 4($sp)          # save return address
    sw $a0, 0($sp)          # save argument
    slti $t0, $a0, 1        # test for n < 1
    beq $t0, $zero, L1     # branch if n !< 0
    addi $v0, $zero, 1     # if n < 1, result is 1
    addi $sp, $sp, 8       # pop 2 items from stack
    jr $ra                  # and return
L1: addi $a0, $a0, -1    # else decrement n
    jal fact               # recursive call
    lw $a0, 0($sp)         # restore original n
    lw $ra, 4($sp)         # and return address
    addi $sp, $sp, 8       # pop 2 items from stack
    mul $v0, $a0, $v0     # multiply to get result
    jr $ra                 # and return
```

# adjust stack for 2 items
# save return address
# save argument
# test for n < 1
# branch if n != 0
# if n < 1, result is 1
# pop 2 items from stack
# and return
# else decrement n
# recursive call
# restore original n
# and return address
# pop 2 items from stack
# multiply to get result
# and return
Local Data on the Stack

- Local data allocated by callee
  - e.g., C automatic variables
- Procedure frame (activation record)
  - Used by some compilers to manage stack storage
Memory Layout

- Text: program code
- Static data: global variables
  - e.g., static variables in C, constant arrays and strings
  - $gp$ initialized to address allowing ±offsets into this segment
- Dynamic data: heap
  - E.g., malloc in C, new in Java
- Stack: automatic storage
String Copy Example

- C code (naïve):
  - Null-terminated string
  ```c
  void strcpy (char x[], char y[])
  {
    int i;
    i = 0;
    while ((x[i]=y[i])!='\0')
      i += 1;
  }
  ```
  - Addresses of x, y in $a0, $a1
  - i in $s0
String Copy Example

- **MIPS code:**

```mips
strcpy:
    addi $sp, $sp, -4        # adjust stack for 1 item
    sw  $s0, 0($sp)          # save $s0
    add  $s0, $zero, $zero  # i = 0

L1: add  $t1, $s0, $a1     # addr of y[i] in $t1
    lbu $t2, 0($t1)         # $t2 = y[i]
    add  $t3, $s0, $a0     # addr of x[i] in $t3
    sb  $t2, 0($t3)         # x[i] = y[i]
    beq $t2, $zero, L2     # exit loop if y[i] == 0
    addi $s0, $s0, 1       # i = i + 1
    j    L1                # next iteration of loop

L2: lw  $s0, 0($sp)        # restore saved $s0
    addi $sp, $sp, 4       # pop 1 item from stack
    jr  $ra                # and return
```
From high-level languages to ISAs

TRANSLATING PROGRAMS
Translation and Startup

Many compilers produce object modules directly

C program → Compiler → Assembly language program → Assembler

Object: Machine language module → Linker → Object: Library routine (machine language)

Executable: Machine language program → Loader → Memory

Static linking
Assembler Pseudoinstructions

- Most assembler instructions represent machine instructions one-to-one
- Pseudoinstructions: figments of the assembler’s imagination

- move $t0, $t1  →  add $t0, $zero, $t1
- blt $t0, $t1, L  →  slt $at, $t0, $t1
  bne $at, $zero, L

- $at (register 1): assembler temporary
Producing an Object Module

- Assembler (or compiler) translates program into machine instructions
- Provides information for building a complete program from the pieces
  - Header: described contents of object module
  - Text segment: translated instructions
  - Static data segment: data allocated for the life of the program
  - Relocation info: for contents that depend on absolute location of loaded program
  - Symbol table: global definitions and external refs
  - Debug info: for associating with source code
Linking Object Modules

- Produces an executable image
  1. Merges segments
  2. Resolve labels (determine their addresses)
  3. Patch location-dependent and external refs
- Could leave location dependencies for fixing by a relocating loader
  - But with virtual memory, no need to do this
  - Program can be loaded into absolute location in virtual memory space
Loading a Program

- Load from image file on disk into memory
  1. Read header to determine segment sizes
  2. Create virtual address space
  3. Copy text and initialized data into memory
     - Or set page table entries so they can be faulted in
  4. Set up arguments on stack
  5. Initialize registers (including $sp, $fp, $gp)
  6. Jump to startup routine
     - Copies arguments to $a0, … and calls main
     - When main returns, do exit syscall
Dynamic Linking

- Only link/load library procedure when it is called
  - Requires procedure code to be relocatable
  - Avoids image bloat caused by static linking of all (transitively) referenced libraries
  - Automatically picks up new library versions
Lazy Linkage

Indirection table

Stub: Loads routine ID, Jump to linker/loader

Linker/loader code

Dynamically mapped code

a. First call to DLL routine

b. Subsequent calls to DLL routine

Text

jal ...
lw jr ...

Data

Text

lj ... ID

Text

Dynamic linker/loader
Remap DLL routine

Text

Data/Text

DLL routine ...
jr

Text

DLL routine ...
jr
Starting Java Applications

Simple portable instruction set for the JVM

Java program

Class files (Java bytecodes)

Compiled Java methods (machine language)

Java Virtual Machine

Interprets bytecodes

Just In Time compiler

Java library routines (machine language)

Compiles bytecodes of “hot” methods into native code for host machine
C Sort Example

› Illustrates use of assembly instructions for a C bubble sort function

› Swap procedure (leaf)
  
  ```c
  void swap(int v[], int k)
  {
    int temp;
    temp = v[k];
    v[k] = v[k+1];
    v[k+1] = temp;
  }
  ```

› v in $a0, k in $a1, temp in $t0
The Procedure Swap

MIPS code:

```mips
swap:     sll $t1, $a1, 2    # $t1 = k * 4
          add $t1, $a0, $t1    # $t1 = v+(k*4)
                          # (address of v[k])
          lw $t0, 0($t1)       # $t0 (temp) = v[k]
          lw $t2, 4($t1)       # $t2 = v[k+1]
          sw $t2, 0($t1)       # v[k] = $t2 (v[k+1])
          sw $t0, 4($t1)       # v[k+1] = $t0 (temp)
          jr $ra               # return to calling routine
```
The Sort Procedure in C

- Non-leaf (calls swap)
  ```c
  void sort (int v[], int n)
  {
    int i, j;
    for (i = 0; i < n; i += 1) {
      for (j = i - 1;
           j >= 0 && v[j] > v[j + 1];
           j -= 1) {
        swap(v,j);
      }
    }
  }
  ```

- v in $a0, k in $a1, i in $s0, j in $s1
move $s2, $a0           # save $a0 into $s2
move $s3, $a1           # save $a1 into $s3
move $s0, $zero         # i = 0
for1tst: slt  $t0, $s0, $s3      # $t0 = 0 if $s0 ≥ $s3 (i ≥ n)
    beq  $t0, $zero, exit1  # go to exit1 if $s0 ≥ $s3 (i ≥ n)
    addi $s1, $s0, –1       # j = i − 1
for2tst: slti $t0, $s1, 0        # $t0 = 1 if $s1 < 0 (j < 0)
    bne  $t0, $zero, exit2  # go to exit2 if $s1 < 0 (j < 0)
    sll  $t1, $s1, 2        # $t1 = j * 4
    add  $t2, $s2, $t1      # $t2 = v + (j * 4)
    lw   $t3, 0($t2)        # $t3 = v[j]
    lw   $t4, 4($t2)        # $t4 = v[j + 1]
    slt  $t0, $t4, $t3      # $t0 = 0 if $t4 ≥ $t3
    beq  $t0, $zero, exit2  # go to exit2 if $t4 ≥ $t3
move $a0, $s2           # 1st param of swap is v (old $a0)
move $a1, $s1           # 2nd param of swap is j
jal   swap               # call swap procedure
addi $s1, $s1, –1       # j -= 1
j   for2tst              # jump to test of inner loop
exit2:   addi $s0, $s0, 1    # i += 1
j   for1tst              # jump to test of outer loop
The Full Procedure

sort:  

addi $sp,$sp, -20  # make room on stack for 5 registers

sw $ra, 16($sp)    # save $ra on stack
sw $s3, 12($sp)    # save $s3 on stack
sw $s2, 8($sp)     # save $s2 on stack
sw $s1, 4($sp)     # save $s1 on stack
sw $s0, 0($sp)     # save $s0 on stack

...  # procedure body

...  

exit1: lw $s0, 0($sp)  # restore $s0 from stack
lw $s1, 4($sp)        # restore $s1 from stack
lw $s2, 8($sp)        # restore $s2 from stack
lw $s3, 12($sp)       # restore $s3 from stack
lw $ra, 16($sp)       # restore $ra from stack
addi $sp,$sp, 20      # restore stack pointer
jr $ra                 # return to calling routine
Effect of Compiler Optimization

Compiled with gcc for Pentium 4 under Linux

- Relative Performance
- Instruction count
- Clock Cycles
- CPI
Effect of Language and Algorithm

**Bubblesort Relative Performance**

- C/none
- C/O1
- C/O2
- C/O3
- Java/int
- Java/JIT

**Quicksort Relative Performance**

- C/none
- C/O1
- C/O2
- C/O3
- Java/int
- Java/JIT

**Quicksort vs. Bubblesort Speedup**

- C/none
- C/O1
- C/O2
- C/O3
- Java/int
- Java/JIT
Lessons Learnt

- Instruction count and CPI are not good performance indicators in isolation
- Compiler optimizations are sensitive to the algorithm
- Java/JIT compiled code is significantly faster than JVM interpreted
  - Comparable to optimized C in some cases
- Nothing can fix a dumb algorithm!
Arrays vs. Pointers

- Array indexing involves
  - Multiplying index by element size
  - Adding to array base address

- Pointers correspond directly to memory addresses
  - Can avoid indexing complexity
### Example: Clearing an array

**clear1**

```c
int clear1(int array[], int size) {
    int i;
    for (i = 0; i < size; i += 1)
        array[i] = 0;
}
```

**clear2**

```c
int clear2(int *array, int size) {
    int *p;
    for (p = &array[0]; p < &array[size];
        p = p + 1)
        *p = 0;
}
```

**Assembly Code: clear1**

```
move $t0,$zero   # i = 0
loop1:  
sll $t1,$t0,2    # $t1 = i * 4
add $t2,$a0,$t1 # $t2 =
                #   &array[i]
sw $zero, 0($t2) # array[i] = 0
addi $t0,$t0,1  # i = i + 1
slt $t3,$t0,$a1 # $t3 =
                #   (i < size)
bne $t3,$zero,loop1 # if (...)   # goto loop1
```

**Assembly Code: clear2**

```
move $t0,$a0   # p = & array[0]
sll $t1,$a1,2   # $t1 = size * 4
add $t2,$a0,$t1 # $t2 =
                #   &array[size]
loop2:  
sw $zero, 0($t0) # Memory[p] = 0
addi $t0,$t0,4  # p = p + 4
slt $t3,$t0,$t2 # $t3 =
                #   (p<&array[size])
bne $t3,$zero,loop2  # if (...)
                # goto loop2
```
Comparison of Array vs. Ptr

- Multiply “strength reduced” to shift
- Array version requires shift to be inside loop
  - Part of index calculation for incremented i
  - c.f. incrementing pointer
- Compiler can achieve same effect as manual use of pointers
  - Induction variable elimination
  - Better to make program clearer and safer
ARM & MIPS ISA
## ARM & MIPS Similarities

- ARM: the most popular embedded core
- Similar basic set of instructions to MIPS

<table>
<thead>
<tr>
<th></th>
<th>ARM</th>
<th>MIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date announced</td>
<td>1985</td>
<td>1985</td>
</tr>
<tr>
<td>Instruction size</td>
<td>32 bits</td>
<td>32 bits</td>
</tr>
<tr>
<td>Address space</td>
<td>32-bit flat</td>
<td>32-bit flat</td>
</tr>
<tr>
<td>Data alignment</td>
<td>Aligned</td>
<td>Aligned</td>
</tr>
<tr>
<td>Data addressing modes</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>Registers</td>
<td>15 × 32-bit</td>
<td>31 × 32-bit</td>
</tr>
<tr>
<td>Input/output</td>
<td>Memory mapped</td>
<td>Memory mapped</td>
</tr>
</tbody>
</table>
# ISA Comparison

<table>
<thead>
<tr>
<th>Instruction name</th>
<th>ARM</th>
<th>MIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Register-register</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>add</td>
<td>addu, addiu</td>
</tr>
<tr>
<td>Add (trap if overflow)</td>
<td>adds; swivs</td>
<td>add</td>
</tr>
<tr>
<td>Subtract</td>
<td>sub</td>
<td>subu</td>
</tr>
<tr>
<td>Subtract (trap if overflow)</td>
<td>subs; swivs</td>
<td>sub</td>
</tr>
<tr>
<td>Multiply</td>
<td>mul</td>
<td>mult, multu</td>
</tr>
<tr>
<td>Divide</td>
<td>—</td>
<td>div, divu</td>
</tr>
<tr>
<td>And</td>
<td>and</td>
<td>and</td>
</tr>
<tr>
<td>Or</td>
<td>orr</td>
<td>or</td>
</tr>
<tr>
<td>Xor</td>
<td>eor</td>
<td>xor</td>
</tr>
<tr>
<td>Load high part register</td>
<td>—</td>
<td>lui</td>
</tr>
<tr>
<td>Shift left logical</td>
<td>lsl¹</td>
<td>sliv, sll</td>
</tr>
<tr>
<td>Shift right logical</td>
<td>lsr¹</td>
<td>srlv, srl</td>
</tr>
<tr>
<td>Shift right arithmetic</td>
<td>asr¹</td>
<td>srav, sra</td>
</tr>
<tr>
<td>Compare</td>
<td>cmp, cmn, tst, teq</td>
<td>slt/i,slt/iu</td>
</tr>
<tr>
<td><strong>Data transfer</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load byte signed</td>
<td>ldrsb</td>
<td>lb</td>
</tr>
<tr>
<td>Load byte unsigned</td>
<td>ldrb</td>
<td>lbu</td>
</tr>
<tr>
<td>Load halfword signed</td>
<td>ldrsh</td>
<td>lh</td>
</tr>
<tr>
<td>Load halfword unsigned</td>
<td>ldrh</td>
<td>lhu</td>
</tr>
<tr>
<td>Load word</td>
<td>ldr</td>
<td>lw</td>
</tr>
<tr>
<td>Store byte</td>
<td>strb</td>
<td>sb</td>
</tr>
<tr>
<td>Store halfword</td>
<td>strh</td>
<td>sh</td>
</tr>
<tr>
<td>Store word</td>
<td>str</td>
<td>sw</td>
</tr>
<tr>
<td>Read, write special registers</td>
<td>mrs, msr</td>
<td>move</td>
</tr>
<tr>
<td>Atomic Exchange</td>
<td>swp, swpb</td>
<td>ll;sc</td>
</tr>
</tbody>
</table>
Compare and Branch in ARM

- Uses condition codes for result of an arithmetic/logical instruction
  - Negative, zero, carry, overflow
  - Compare instructions to set condition codes without keeping the result
- Each instruction can be conditional
  - Top 4 bits of instruction word: condition value
  - Can avoid branches over single instructions
Instruction Encoding

### Register-register

#### ARM

<table>
<thead>
<tr>
<th>31</th>
<th>28</th>
<th>27</th>
<th>20</th>
<th>19</th>
<th>16</th>
<th>15</th>
<th>12</th>
<th>11</th>
<th>4</th>
<th>3</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Op^4</td>
<td>Op^8</td>
<td>Rs1^4</td>
<td>Rd^4</td>
<td>Op^6</td>
<td>Rs2^4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### MIPS

<table>
<thead>
<tr>
<th>31</th>
<th>26</th>
<th>25</th>
<th>21</th>
<th>20</th>
<th>16</th>
<th>15</th>
<th>11</th>
<th>10</th>
<th>6</th>
<th>5</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Op^6</td>
<td>Rs1^6</td>
<td>Rs2^5</td>
<td>Rd^6</td>
<td>Const^8</td>
<td>Op^8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Data transfer

#### ARM

<table>
<thead>
<tr>
<th>31</th>
<th>28</th>
<th>27</th>
<th>24</th>
<th>23</th>
<th>20</th>
<th>19</th>
<th>16</th>
<th>15</th>
<th>12</th>
<th>11</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Op^4</td>
<td>Op^8</td>
<td>Rs1^4</td>
<td>Rd^4</td>
<td>Const^12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### MIPS

<table>
<thead>
<tr>
<th>31</th>
<th>26</th>
<th>25</th>
<th>21</th>
<th>20</th>
<th>16</th>
<th>15</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Op^6</td>
<td>Rs1^6</td>
<td>Rd^6</td>
<td>Const^16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Branch

#### ARM

<table>
<thead>
<tr>
<th>31</th>
<th>28</th>
<th>27</th>
<th>24</th>
<th>23</th>
<th>20</th>
<th>19</th>
<th>16</th>
<th>15</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Op^4</td>
<td>Op^8</td>
<td>Op^2</td>
<td>Const^24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### MIPS

<table>
<thead>
<tr>
<th>31</th>
<th>26</th>
<th>25</th>
<th>21</th>
<th>20</th>
<th>16</th>
<th>15</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Op^6</td>
<td>Rs1^6</td>
<td>Op^2 / Rs2^5</td>
<td>Const^16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Jump/Call

#### ARM

<table>
<thead>
<tr>
<th>31</th>
<th>28</th>
<th>27</th>
<th>24</th>
<th>23</th>
<th>20</th>
<th>19</th>
<th>16</th>
<th>15</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Op^4</td>
<td>Op^8</td>
<td>Op^2</td>
<td>Const^24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### MIPS

<table>
<thead>
<tr>
<th>31</th>
<th>26</th>
<th>25</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Op^6</td>
<td>Const^26</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# ARM & MIPS Addressing Modes

<table>
<thead>
<tr>
<th>Addressing mode</th>
<th>ARM</th>
<th>MIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register operand</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Immediate operand</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Register + offset (displacement or based)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Register + register (indexed)</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Register + scaled register (scaled)</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Register + offset and update register</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Register + register and update register</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>Autoincrement, autodecrement</td>
<td>X</td>
<td>—</td>
</tr>
<tr>
<td>PC-relative data</td>
<td>X</td>
<td>—</td>
</tr>
</tbody>
</table>
## ARM Arithmetic not in MIPS

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
<th>ARM</th>
<th>MIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load immediate</td>
<td>Rd = Imm</td>
<td>mov</td>
<td>addi $0,</td>
</tr>
<tr>
<td>Not</td>
<td>Rd = ~(Rs1)</td>
<td>mvn</td>
<td>nor $0,</td>
</tr>
<tr>
<td>Move</td>
<td>Rd = Rs1</td>
<td>mov</td>
<td>or $0,</td>
</tr>
<tr>
<td>Rotate right</td>
<td>Rd = Rs i &gt;&gt; i</td>
<td>ror</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rd_{0...i-1} = Rs_{31-i...31}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>And not</td>
<td>Rd = Rs1 &amp; ~(Rs2)</td>
<td>bic</td>
<td></td>
</tr>
<tr>
<td>Reverse subtract</td>
<td>Rd = Rs2 – Rs1</td>
<td>rsb, rsc</td>
<td></td>
</tr>
<tr>
<td>Support for multiword</td>
<td>CarryOut, Rd = Rd + Rs1 +</td>
<td>adcs</td>
<td></td>
</tr>
<tr>
<td>integer add</td>
<td>OldCarryOut</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for multiword</td>
<td>CarryOut, Rd = Rd – Rs1 +</td>
<td>sbcs</td>
<td></td>
</tr>
<tr>
<td>integer sub</td>
<td>OldCarryOut</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
INTEL X86 ISA
The Intel x86 ISA

- Evolution with backward compatibility
  - 8080 (1974): 8-bit microprocessor
    - Accumulator, plus 3 index-register pairs
  - 8086 (1978): 16-bit extension to 8080
    - Complex instruction set (CISC)
  - 8087 (1980): floating-point coprocessor
    - Adds FP instructions and register stack
  - 80286 (1982): 24-bit addresses, MMU
    - Segmented memory mapping and protection
  - 80386 (1985): 32-bit extension (now IA-32)
    - Additional addressing modes and operations
    - Paged memory mapping as well as segments
The Intel x86 ISA

- Further evolution…
  - i486 (1989): pipelined, on-chip caches and FPU
    - Compatible competitors: AMD, Cyrix, …
  - Pentium (1993): superscalar, 64-bit datapath
    - Later versions added MMX (Multi-Media eXtension) instructions
    - The infamous FDIV bug
    - New microarchitecture (see Colwell, The Pentium Chronicles)
  - Pentium III (1999)
    - Added SSE (Streaming SIMD Extensions) and associated registers
  - Pentium 4 (2001)
    - New microarchitecture
    - Added SSE2 instructions
The Intel x86 ISA

- And further…
  - AMD64 (2003): extended architecture to 64 bits
  - EM64T – Extended Memory 64 Technology (2004)
    - AMD64 adopted by Intel (with refinements)
    - Added SSE3 instructions
  - Intel Core (2006)
    - Added SSE4 instructions, virtual machine support
  - AMD64 (announced 2007): SSE5 instructions
    - Intel declined to follow, instead…
  - Advanced Vector Extension (announced 2008)
    - Longer SSE registers, more instructions
- If Intel didn’t extend with compatibility, its competitors would!
  - Technical elegance ≠ market success
Basic x86 Registers

<table>
<thead>
<tr>
<th>Name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAX</td>
<td>GPR 0</td>
</tr>
<tr>
<td>ECX</td>
<td>GPR 1</td>
</tr>
<tr>
<td>EDX</td>
<td>GPR 2</td>
</tr>
<tr>
<td>EBX</td>
<td>GPR 3</td>
</tr>
<tr>
<td>ESP</td>
<td>GPR 4</td>
</tr>
<tr>
<td>EBP</td>
<td>GPR 5</td>
</tr>
<tr>
<td>ESI</td>
<td>GPR 6</td>
</tr>
<tr>
<td>EDI</td>
<td>GPR 7</td>
</tr>
<tr>
<td>CS</td>
<td>Code segment pointer</td>
</tr>
<tr>
<td>SS</td>
<td>Stack segment pointer (top of stack)</td>
</tr>
<tr>
<td>DS</td>
<td>Data segment pointer 0</td>
</tr>
<tr>
<td>ES</td>
<td>Data segment pointer 1</td>
</tr>
<tr>
<td>FS</td>
<td>Data segment pointer 2</td>
</tr>
<tr>
<td>GS</td>
<td>Data segment pointer 3</td>
</tr>
<tr>
<td>EIP</td>
<td>Instruction pointer (PC)</td>
</tr>
<tr>
<td>EFLAGS</td>
<td>Condition codes</td>
</tr>
</tbody>
</table>
Basic x86 Addressing Modes

**Two operands per instruction**

<table>
<thead>
<tr>
<th>Source/dest operand</th>
<th>Second source operand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register</td>
<td>Register</td>
</tr>
<tr>
<td>Register</td>
<td>Immediate</td>
</tr>
<tr>
<td>Register</td>
<td>Memory</td>
</tr>
<tr>
<td>Memory</td>
<td>Register</td>
</tr>
<tr>
<td>Memory</td>
<td>Immediate</td>
</tr>
</tbody>
</table>

- **Memory addressing modes**
  - Address in register
  - \( \text{Address} = R_{\text{base}} + \text{displacement} \)
  - \( \text{Address} = R_{\text{base}} + 2^{\text{scale}} \times R_{\text{index}} \) (scale = 0, 1, 2, or 3)
  - \( \text{Address} = R_{\text{base}} + 2^{\text{scale}} \times R_{\text{index}} + \text{displacement} \)
x86 Instruction Encoding

- Variable length encoding
  - Postfix bytes specify addressing mode
  - Prefix bytes modify operation
  - Operand length, repetition, locking, …
x86 Addressing Modes not in MIPS

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
<th>Register restrictions</th>
<th>MIPS equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register indirect</td>
<td>Address is in a register.</td>
<td>Not ESP or EBP</td>
<td>lw $s0,0($s1)</td>
</tr>
<tr>
<td>Based mode with 8- or 32-bit displacement</td>
<td>Address is contents of base register plus displacement.</td>
<td>Not ESP</td>
<td>lw $s0,100($s1)# &lt;= 16-bit # displacement</td>
</tr>
<tr>
<td>Base plus scaled index</td>
<td>The address is Base + (2&lt;sup&gt;scale&lt;/sup&gt; x Index) where Scale has the value 0, 1, 2, or 3.</td>
<td>Base: any GPR Index: not ESP</td>
<td>mul $t0,$s2,4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>add $t0,$t0,$s1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>lw $s0,0($t0)</td>
</tr>
<tr>
<td>Base plus scaled index with 8- or 32-bit displacement</td>
<td>The address is Base + (2&lt;sup&gt;scale&lt;/sup&gt; x Index) + displacement where Scale has the value 0, 1, 2, or 3.</td>
<td>Base: any GPR Index: not ESP</td>
<td>mul $t0,$s2,4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>add $t0,$t0,$s1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>lw $s0,100($t0)# &lt;= 16-bit # displacement</td>
</tr>
</tbody>
</table>

FIGURE 2.38  x86 32-bit addressing modes with register restrictions and the equivalent MIPS code. The Base plus Scaled Index addressing mode, not found in ARM or MIPS, is included to avoid the multiplies by 4 (scale factor of 2) to turn an index in a register into a byte address (see Figures 2.25 and 2.27). A scale factor of 1 is used for 16-bit data, and a scale factor of 3 for 64-bit data. A scale factor of 0 means the address is not scaled. If the displacement is longer than 16 bits in the second or fourth modes, then the MIPS equivalent mode would need two more instructions: a lui to load the upper 16 bits of the displacement and an add to sum the upper address with the base register $s1. (Intel gives two different names to what is called Based addressing mode—Based and Indexed—but they are essentially identical and we combine them here.)
Implementing IA-32

- Complex instruction set makes implementation difficult
  - Hardware translates instructions to simpler micro-operations
    - Simple instructions: 1–1
    - Complex instructions: 1–many
  - Micro-engine is a RISC processor
  - Market share makes this economically viable

- Comparable performance to RISC
  - Compilers avoid complex instructions
FIGURE 2.43  Growth of x86 instruction set over time. While there is clear technical value to some of these extensions, this rapid change also increases the difficulty for other companies to try to build compatible processors.
CONCLUSION
Fallacies

- Powerful instruction => higher performance
  - Fewer instructions required
  - But complex instructions are hard to implement
    - May slow down all instructions, including simple ones
  - Compilers are good at making fast code from simple instructions
- Use assembly code for high performance
  - But modern compilers are better at dealing with modern processors
  - More lines of code => more errors and less productivity
Fallacies

- Backward compatibility $\Rightarrow$ instruction set doesn’t change
- But they do accrete more instructions

![Graph showing the increase in x86 instruction set over time from 1978 to 2008.]
Pitfalls

- Sequential words are not at sequential addresses
  - Increment by 4, not by 1!
- Keeping a pointer to an automatic variable after procedure returns
  - e.g., passing pointer back via an argument
  - Pointer becomes invalid when stack popped
Concluding Remarks

- Design principles
  1. Simplicity favors regularity
  2. Smaller is faster
  3. Make the common case fast
  4. Good design demands good compromises

- Layers of software/hardware
  - Compiler, assembler, hardware

- MIPS: typical of RISC ISAs
  - c.f. x86
Concluding Remarks

- Measure MIPS instruction executions in benchmark programs
- Consider making the common case fast
- Consider compromises

<table>
<thead>
<tr>
<th>Instruction class</th>
<th>MIPS examples</th>
<th>SPEC2006 Int</th>
<th>SPEC2006 FP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arithmetic</td>
<td>add, sub, addi</td>
<td>16%</td>
<td>48%</td>
</tr>
<tr>
<td>Data transfer</td>
<td>lw, sw, lb, lbu,</td>
<td>35%</td>
<td>36%</td>
</tr>
<tr>
<td></td>
<td>lh, lhu, sb, lui</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical</td>
<td>and, or, nor, andi,</td>
<td>12%</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>ori, sll, srl</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cond. Branch</td>
<td>beq, bne, slt,</td>
<td>34%</td>
<td>8%</td>
</tr>
<tr>
<td></td>
<td>slti, sltiu</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jump</td>
<td>j, jr, jal</td>
<td>2%</td>
<td>0%</td>
</tr>
</tbody>
</table>
this was covered in CS 61 or CS 120A

REVIEW SLIDES
Unsigned Binary Integers

Given an n-bit number

\[ x = x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \cdots + x_12^1 + x_02^0 \]

- Range: 0 to \(+2^n - 1\)
- Example
  - \(0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 1011_2\)
    - \(= 0 + \cdots + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0\)
    - \(= 0 + \cdots + 8 + 0 + 2 + 1 = 11_{10}\)
- Using 32 bits
  - 0 to \(+4,294,967,295\)
2s-Complement Signed Integers

- Given an n-bit number

\[ x = -x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \cdots + x_12^1 + x_02^0 \]

- Range: \(-2^{n-1}\) to \(+2^{n-1} - 1\)

- Example
  - 1111 1111 1111 1111 1111 1111 1111 1100₂
  - \(-1 \times 2^{31} + 1 \times 2^{30} + \ldots + 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0\)
  - \(-2,147,483,648 + 2,147,483,644 = -4_{10}\)

- Using 32 bits
  - \(-2,147,483,648\) to \(+2,147,483,647\)
2s-Complement Signed Integers

- Bit 31 is sign bit
  - 1 for negative numbers
  - 0 for non-negative numbers
- \(-(-2^{n-1})\) can’t be represented
- Non-negative numbers have the same unsigned and 2s-complement representation
- Some specific numbers
  - 0: 0000 0000 … 0000
  - –1: 1111 1111 … 1111
  - Most-negative: 1000 0000 … 0000
  - Most-positive: 0111 1111 … 1111
Signed Negation

- Complement and add 1
  - Complement means \(1 \rightarrow 0, \ 0 \rightarrow 1\)

\[
\begin{align*}
x + x &= 1111\ldots111_2 = -1 \\
x + 1 &= -x
\end{align*}
\]

Example: negate \(+2\)

- \(+2 = 0000\ 0000 \ldots \ 0010_2\)
- \(-2 = 1111\ 1111 \ldots \ 1101_2 + 1\)
  \[= 1111\ 1111 \ldots \ 1110_2\]
Sign Extension

- Representing a number using more bits
  - Preserve the numeric value
- In MIPS instruction set
  - `addi`: extend immediate value
  - `lb`, `lh`: extend loaded byte/halfword
  - `beq`, `bne`: extend the displacement
- Replicate the sign bit to the left
  - c.f. unsigned values: extend with 0s
- Examples: 8-bit to 16-bit
  - +2: 0000 0010 => 0000 0000 0000 0010
  - −2: 1111 1110 => 1111 1111 1111 1110
Hexadecimal

- **Base 16**
  - Compact representation of bit strings
  - 4 bits per hex digit

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>1000</th>
<th>1001</th>
<th>1010</th>
<th>1011</th>
<th>1100</th>
<th>1101</th>
<th>1110</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000</td>
<td>0001</td>
<td>0010</td>
<td>0011</td>
<td>0100</td>
<td>0101</td>
<td>0110</td>
<td>0111</td>
<td>1000</td>
<td>1001</td>
<td>1010</td>
<td>1011</td>
<td>1100</td>
<td>1101</td>
<td>1110</td>
<td>1111</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Example:** eca8 6420
  - 1110 1100 1010 1000 0110 0100 0010 0000
## Logical Operations

Instructions for bitwise manipulation

<table>
<thead>
<tr>
<th>Operation</th>
<th>C</th>
<th>Java</th>
<th>MIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shift left</td>
<td>&lt;&lt;</td>
<td>&lt;&lt;</td>
<td>sll</td>
</tr>
<tr>
<td>Shift right</td>
<td>&gt;&gt;</td>
<td>&gt;&gt;&gt;</td>
<td>srl</td>
</tr>
<tr>
<td>Bitwise AND</td>
<td>&amp;</td>
<td>&amp;</td>
<td>and, andi</td>
</tr>
<tr>
<td>Bitwise OR</td>
<td></td>
<td></td>
<td>or, ori</td>
</tr>
<tr>
<td>Bitwise NOT</td>
<td>~</td>
<td>~</td>
<td>nor</td>
</tr>
</tbody>
</table>

- Useful for extracting and inserting groups of bits in a word
**Shift Operations**

- **shamt**: how many positions to shift
- **Shift left logical**
  - Shift left and fill with 0 bits
  - \( sll \) by \( i \) bits multiplies by \( 2^i \)
- **Shift right logical**
  - Shift right and fill with 0 bits
  - \( srl \) by \( i \) bits divides by \( 2^i \) (unsigned only)
AND Operations

- Useful to mask bits in a word
  - Select some bits, clear others to 0

and $t0$, $t1$, $t2$

| $t2$ | 0000 0000 0000 0000 0000 1101 1100 0000 |
| $t1$ | 0000 0000 0000 0000 0011 1100 0000 0000 |
| $t0$ | 0000 0000 0000 0000 0000 1100 0000 0000 |
OR Operations

- Useful to include bits in a word
  - Set some bits to 1, leave others unchanged

or $t0, $t1, $t2

| $t2  | 0000 0000 0000 0000 0000 0000 1101 1100 0000 |
| $t1  | 0000 0000 0000 0000 0011 1100 0000 0000 |
| $t0  | 0000 0000 0000 0000 0011 1101 1100 0000 |
NOT Operations

- Useful to invert bits in a word
  - Change 0 to 1, and 1 to 0
- MIPS has NOR 3-operand instruction
  - $a$ NOR $b$ == NOT ($a$ OR $b$)

```assembly
nor $t0, $t1, $zero
```

<table>
<thead>
<tr>
<th>Register 0: always read as zero</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t1</td>
</tr>
<tr>
<td>$t0</td>
</tr>
</tbody>
</table>