Class Announcements

1. Urmish’s office hours from 9-10 AM was cancelled. Alternated office hours details soon.

2. If you need alternate Midterm 1 email me with your name and the reason.

3. Questions about Prog.Assign. 1?

4. Details about hands-on intro to C Program. relevant to Prog.Assign. 1 soon.
Lecture Overview

- IEEE Floating Point
- ISA history and intro
- Assembly Intro, Disassembly
- IA32 Registers
- IA32 Operand forms
- IA32 Data Movement Instructions
- Assume a set of 4 chars. are in an integer-sized variable (X).
- Assume an instruction exists to print out the character all the way to the right...

\[
\begin{array}{cccc}
X & 'A' & 'B' & 'C' & 'D'
\end{array}
\]

\[
\text{putc } X \quad \text{(prints D)}
\]

- Invent instructions, and write code to print ABCD, without changing X.
Karen’s solution

```c
rotn X, 8 bits
putc X  # A
rotn X, 8 bits
putc X  # B
rotn X, 8 bits
putc X  # C
rotn X, 8 bits
putc X  # D
```
1. Fractional Binary Notation

\[ b_m b_{m-1} \ldots b_2 b_1 b_0 \cdot b_{-1} b_{-2} b_{-3} \ldots b_{-n+1} b_{-n} \]

\[ 2^m \quad 2^{m-1} \quad 2^{m-2} \quad \ldots \quad 2 \quad 1 \quad \frac{1}{2} \quad \frac{1}{4} \quad \frac{1}{8} \quad \ldots \quad \frac{1}{2^{n-1}} \quad \frac{1}{2^n} \]
IEEE Floating Point (Won’t be on exam)

• Limitations with binary Notation:
  • Can only exactly represent numbers of the form $x/2^k$
  • Just one setting of binary point within the $w$ bits

• IEEE Standard 754
  • Established in 1985 as uniform standard for floating point arithmetic
  • Nice standards for rounding, overflow, underflow
IEEE Floating Point (Won’t be on exam)

- Numerical Form:
  \[ (-1)^s \ M \ 2^E \]
  - \( s \) is sign bit: negative or positive
  - **Significand** \( M \) normally a fractional value in range \([0.0,2.0)\).
  - **Exponent** \( E \) weights value by power of two

- Encoding
  - MSB \( s \) is sign bit \( s \)
  - exp field encodes \( E \) (but is not equal to \( E \))
  - frac field encodes \( M \) (but is not equal to \( M \))
IEEE Floating Point (Won’t be on exam)

1. Normalized values: Exp neither all zeroes nor all ones)
   \[ E = \text{Exp} - \text{Bias} \text{ and } M = 1 + f \]

2. Denormalized values: Exp is all zeroes
   \[ E = 1 - \text{Bias} \text{ and } M = f \]

3. Special values: Exp is all ones: Inf, NaN

\( \text{Bias is } 2^{k-1} - 1 \), E.g. for \( k=4 \) bit exp field, Bias = 7
IEEE Floating Point (Won’t be on exam)

- **Single precision:** 32 bits
  - `s, exp, frac`
  - 1 8-bits 23-bits

- **Double precision:** 64 bits
  - `s, exp, frac`
  - 1 11-bits 52-bits

- **Extended precision:** 80 bits (Intel only)
  - `s, exp, frac`
  - 1 15-bits 63 or 64-bits
IEEE Floating Point (Won’t be on exam)

<table>
<thead>
<tr>
<th>Description</th>
<th>Bit representation</th>
<th>e</th>
<th>E</th>
<th>f</th>
<th>M</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td>0 0000 000</td>
<td>0</td>
<td>-6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Smallest positive</td>
<td>0 0000 001</td>
<td>0</td>
<td>-6</td>
<td>1/8</td>
<td>1/8</td>
<td>1/512</td>
</tr>
<tr>
<td></td>
<td>0 0000 010</td>
<td>0</td>
<td>-6</td>
<td>2/8</td>
<td>2/8</td>
<td>2/512</td>
</tr>
<tr>
<td></td>
<td>0 0000 011</td>
<td>0</td>
<td>-6</td>
<td>3/8</td>
<td>3/8</td>
<td>3/512</td>
</tr>
<tr>
<td></td>
<td>0 0000 110</td>
<td>0</td>
<td>-6</td>
<td>6/8</td>
<td>6/8</td>
<td>6/512</td>
</tr>
<tr>
<td>Largest denorm.</td>
<td>0 0000 111</td>
<td>0</td>
<td>-6</td>
<td>7/8</td>
<td>7/8</td>
<td>7/512</td>
</tr>
<tr>
<td>Smallest norm.</td>
<td>0 0001 000</td>
<td>1</td>
<td>-6</td>
<td>0</td>
<td>8/8</td>
<td>8/512</td>
</tr>
<tr>
<td></td>
<td>0 0001 001</td>
<td>1</td>
<td>-6</td>
<td>1/8</td>
<td>9/8</td>
<td>9/512</td>
</tr>
<tr>
<td></td>
<td>0 0110 110</td>
<td>6</td>
<td>-1</td>
<td>6/8</td>
<td>14/8</td>
<td>14/16</td>
</tr>
<tr>
<td></td>
<td>0 0110 111</td>
<td>6</td>
<td>-1</td>
<td>7/8</td>
<td>15/8</td>
<td>15/16</td>
</tr>
<tr>
<td>One</td>
<td>0 0111 000</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>8/8</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>0 0111 001</td>
<td>7</td>
<td>0</td>
<td>1/8</td>
<td>9/8</td>
<td>9/8</td>
</tr>
<tr>
<td></td>
<td>0 0111 010</td>
<td>7</td>
<td>0</td>
<td>2/8</td>
<td>10/8</td>
<td>10/8</td>
</tr>
<tr>
<td></td>
<td>0 1110 110</td>
<td>14</td>
<td>7</td>
<td>6/8</td>
<td>14/8</td>
<td>224</td>
</tr>
<tr>
<td>Largest norm.</td>
<td>0 1110 111</td>
<td>14</td>
<td>7</td>
<td>7/8</td>
<td>15/8</td>
<td>240</td>
</tr>
<tr>
<td>Infinity</td>
<td>0 1111 000</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+∞</td>
</tr>
</tbody>
</table>
Focus: **x86 architecture**

- **1960s**: CISC
  System/360 (IBM), B5000 (Burroughs), Motorola 68000

- **1970s**: Large Scale Integration
  8008, 8080, 8086 (Intel), PDP-11, VAX (DEC)

- **1980s**: RISC, Instruction Level Parallelism, Pipelining
  80286, 80386, 80486 (Intel), Motorola 68020

- **1990s - today**: Multi-threading, Multi-Core, Open source processors
  Pentium, Pentium Pro, Intel Core (Intel), Athlon series (AMD)
Moore's Law

Number of Transistors per Integrated Circuit vs. Year

- Invention of the Transistor
- Doubles every 2.1 yrs

Process Technology (μm)


Intel Microprocessors

- Core i7
- Core 2 Duo
- Pentium 4
- Pentium II
- Pentium
entire architecture on 1 slide:

32-bit architecture
2-address instruction set
CISC (not RISC, load/store)
8 registers (depending on how we count)
uses condition codes for control instructions

IA 32
Assembly Programmer’s view

- **Programmer-Visible State**
  - **PC:** Program counter
    - Address of next instruction
    - Called “EIP” (IA32) or “RIP” (x86-64)
  - Register file
    - Heavily used program data
  - Condition codes
    - Store status information about most recent arithmetic operation
    - Used for conditional branching

- **Memory**
  - Byte addressable array
  - Code, user data, heap, (some) OS data
  - Includes stack used to support procedures
Assembly Language

• Why learn assembly?
  • Preferred for low level tasks: boot loaders, system calls
  • Less overhead than with HLL code
  • Helpful while debugging
  • Can access some new features of processor only through assembly until compilers add support.
  • One of the oldest tools in Programmers toolbox

• We will use the ATT syntax and not the Intel syntax. Consider:
  Intel:       mov eax,1;       mov ebx,0ffh ;       int 80h
  AT&T:    movl $1,%eax;  movl $0xff,%ebx;   int $0x80
Characteristics of Assembly Programs: Data Types

1. Integer data of 1, 2, or 4 bytes (data values, addresses)
2. Floating point data of 4, 8, or 10 bytes
3. No aggregate types such as arrays or structures (Just contiguously allocated bytes in memory)
Characteristics of Assembly Programs: Operations

1. Arithmetic operations on memory or registers
2. Transfer data between memory and registers: Load and Store
3. Transfer control: Unconditional jumps, Conditional branches
Example Assembly Program

.include "defines.h"
.data
hw:
    .string "hello world\n"
.text
.globl main
main:
    movl $SYS_write,%eax
    movl $1,%ebx
    movl $hw,%ecx
    movl $12,%edx
    int $0x80
    movl $SYS_exit,%eax
    xorl %ebx,%ebx
    int $0x80
    ret
Generating Assembly Code from C

Example C Program and its assembly

```c
#include <stdio.h>
int a = 10, b = 20;
int main()
{
    int t = a;
    a = b;
    b = t;
    printf("%d %d\n", a, b);
    return 0;
}
```
Disassembly of Executables

1. objdump -S
2. gdb and then disassembly command
3. Compile with -g for source code info:
   man gcc says:
   -g Produce debugging information in the operating system's native format (stabs, COFF, XCOFF, or DWARF 2).
   GDB can work with this debugging information.
Registers

%eax
%ax
%ah
%al

%ecx
%cx
%ch
%cl

%edx
%dx
%dh
%dl

%ebx
%bx
%bh
%bl

“double word”
“word”
4 More Registers

\[
\begin{array}{cccc}
31 & 30 & \cdots & 15 & 14 & 0 \\
%esi & & & %si & & \\
%edi & & & %di & & \\
%esp & & & %sp & & \\
%ebp & & & %bp & & \\
\end{array}
\]
# Registers

1. `%esp`, `%ebp` : stack pointer, base pointer
2. `%eip` : instruction pointer
3. x86-64 : `%rax`, `%rbx` etc. (64 bits)

What to do when there are not enough registers?

**Answer:** Store temporarily in memory.
On to the instruction set. Our coverage will be of a small subset.

Classify instructions:

- data movement
- arithmetic
- logical (and shift)
- control
# Operands

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Addressing mode name</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Imm</td>
<td>immediate</td>
<td>value in machine code</td>
</tr>
<tr>
<td>%R</td>
<td>register</td>
<td>value in register R</td>
</tr>
<tr>
<td>Imm</td>
<td>absolute</td>
<td>address given by Imm</td>
</tr>
<tr>
<td>(%R)</td>
<td>register direct (incorrect in textbook)</td>
<td>address in %R</td>
</tr>
<tr>
<td>Imm (%R)</td>
<td>base displacement</td>
<td>address is Imm + %R</td>
</tr>
</tbody>
</table>
Some more operand formats in IA32

<table>
<thead>
<tr>
<th>Format</th>
<th>Expression</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>((E_b, E_i))</td>
<td>(M[R[E_b] + R[E_i]])</td>
<td>Indexed</td>
</tr>
<tr>
<td>(Imm(E_b, E_i))</td>
<td>(M[Imm + R[E_b] + R[E_i]])</td>
<td>Indexed</td>
</tr>
<tr>
<td>((E_i, s))</td>
<td>(M[R[E_i] \cdot s])</td>
<td>Scaled indexed</td>
</tr>
<tr>
<td>(Imm(E_i, s))</td>
<td>(M[Imm + R[E_i] \cdot s])</td>
<td>Scaled indexed</td>
</tr>
<tr>
<td>((E_b, E_i, s))</td>
<td>(M[R[E_b] + R[E_i] \cdot s])</td>
<td>Scaled indexed</td>
</tr>
<tr>
<td>(Imm(E_b, E_i, s))</td>
<td>(M[Imm + R[E_b] + R[E_i] \cdot s])</td>
<td>Scaled indexed</td>
</tr>
</tbody>
</table>

Cannot do memory to memory transfer with a single instruction
<table>
<thead>
<tr>
<th>Address</th>
<th>Value</th>
<th>Register</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x100</td>
<td>0xFF</td>
<td>%eax</td>
<td>0x100</td>
</tr>
<tr>
<td>0x104</td>
<td>0xAB</td>
<td>%ecx</td>
<td>0x1</td>
</tr>
<tr>
<td>0x108</td>
<td>0x13</td>
<td>%edx</td>
<td>0x3</td>
</tr>
<tr>
<td>0x10C</td>
<td>0x11</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operand</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>%eax</td>
<td></td>
</tr>
<tr>
<td>0x104</td>
<td></td>
</tr>
<tr>
<td>$0x108</td>
<td></td>
</tr>
<tr>
<td>(%eax)</td>
<td></td>
</tr>
<tr>
<td>4(%eax)</td>
<td></td>
</tr>
<tr>
<td>9(%eax,%edx)</td>
<td></td>
</tr>
<tr>
<td>260(%ecx,%edx)</td>
<td></td>
</tr>
<tr>
<td>0xFC(%ecx,%edx,4)</td>
<td></td>
</tr>
<tr>
<td>(%eax,%edx,4)</td>
<td></td>
</tr>
<tr>
<td>Operand</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>%eax</td>
<td>0x100</td>
</tr>
<tr>
<td>0x104</td>
<td>0xAB</td>
</tr>
<tr>
<td>$0x108</td>
<td>0x108</td>
</tr>
<tr>
<td>(%eax)</td>
<td>0xFF</td>
</tr>
<tr>
<td>4(%eax)</td>
<td>0xAB</td>
</tr>
<tr>
<td>9(%eax,%edx)</td>
<td>0x11</td>
</tr>
<tr>
<td>260(%ecx,%edx)</td>
<td>0x13</td>
</tr>
<tr>
<td>0xFC(,%ecx,4)</td>
<td>0xFF</td>
</tr>
<tr>
<td>(%eax,%edx,4)</td>
<td>0x11</td>
</tr>
</tbody>
</table>
# Data Movement Instructions

<table>
<thead>
<tr>
<th>Instruction</th>
<th>Source, Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>movb, movw, movl</td>
<td>S, D</td>
<td>nondestructive copy of S to D</td>
</tr>
<tr>
<td>movsbw, movsbl, movswl</td>
<td>S, D</td>
<td>sign-extended, nondestructive copy of S to D byte to word byte to double word word to double word</td>
</tr>
<tr>
<td>movzbow, movzbwl, movzwl</td>
<td>S, D</td>
<td>zero-extended, nondestructive copy of S to D byte to word byte to double word word to double word</td>
</tr>
<tr>
<td>pushl</td>
<td>S</td>
<td>push double word S onto the stack</td>
</tr>
<tr>
<td>popl</td>
<td>D</td>
<td>pop double word off the stack into D</td>
</tr>
<tr>
<td>Instruction</td>
<td>Source Type</td>
<td>Destination Type</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>movl $0x4050,%eax</td>
<td>Immediate--Register</td>
<td>4 bytes</td>
</tr>
<tr>
<td>movw %bp,%sp</td>
<td>Register--Register</td>
<td>2 bytes</td>
</tr>
<tr>
<td>movb (%edi,%ecx),%ah</td>
<td>Memory--Register</td>
<td>1 byte</td>
</tr>
<tr>
<td>movb $-17,(%esp)</td>
<td>Immediate--Memory</td>
<td>1 byte</td>
</tr>
<tr>
<td>movl %eax,-12(%ebp)</td>
<td>Register--Memory</td>
<td>4 bytes</td>
</tr>
</tbody>
</table>