CS 33

Data Representation (Part 4)
Floating Point

- Single precision (float)
  
<table>
<thead>
<tr>
<th>s</th>
<th>exp</th>
<th>frac</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8-bits</td>
<td>23-bits</td>
</tr>
</tbody>
</table>
  
  - range: $\pm1.8\times10^{-38} - \pm3.4\times10^{38}$, ~7 decimal digits

- Double Precision (double)
  
<table>
<thead>
<tr>
<th>s</th>
<th>exp</th>
<th>frac</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11-bits</td>
<td>52-bits</td>
</tr>
</tbody>
</table>
  
  - range: $\pm2.23\times10^{-308} - \pm1.8\times10^{308}$, ~16 decimal digits
Floating Point in C

- **Conversions/casting**
  - casting between `int`, `float`, and `double` changes bit representation
  - `double/float → int`
    - truncates fractional part
    - like rounding toward zero
    - not defined when out of range or NaN: generally sets to TMin
  - `int → double`
    - exact conversion, as long as `int` has ≤ 53-bit word size
  - `int → float`
    - will round according to rounding mode
Quiz 1

Suppose \( f \), declared to be a float, is assigned the largest possible floating-point positive value (other than \( +\infty \)). What is the value of \( g = f+1.0 \)?

a) \( f \)
b) \( +\infty \)
c) NaN
d) 0
Float is not Rational ...

- Floating addition
  - commutative: \( a + f b = b + f a \)
    » yes!
  - associative: \( a + f (b + f c) = (a + f b) + f c \)
    » no!
      * \( 2 + f (1e38 + f -1e38) = 2 \)
      * \( (2 + f 1e38) + f -1e38 = 0 \)

Note that the floating-point numbers in this and the next two slides are expressed in base 10, not base 2.
Float is not Rational …

- **Multiplication**
  - commutative: \( a \times f b = b \times f a \)
    - yes!
  - associative: \( a \times f (b \times f c) = (a \times f b) \times f c \)
    - no!
      - \( 1e37 \times f (1e37 \times f 1e-37) = 1e38 \)
      - \( (1e37 \times f 1e37) \times f 1e-37 = +\infty \)
Float is not Rational …

• More …
  – multiplication distributes over addition:
    \[ a \times f (b + f c) = (a \times f b) + f (a \times f c) \]
    » no!
    » \( 1e38 \times f (1e38 + f -1e38) = 0 \)
    » \( (1e38 \times f 1e38) + f (1e38 \times f -1e38) = \text{NaN} \)
  – loss of significance:
    \( x = y + 1 \)
    \( z = 2/(x - y) \)
    \( z == 2? \)
    » not necessarily!
    • consider \( y = 1e38 \)
CS 33

Intro to Machine Programming
Generally we think of their being two sorts of memory: that containing instructions and that containing data. Programs, in general, don’t modify their own instructions on the fly. In reality, there’s only one sort of memory, which holds everything. However, we arrange so that memory holding instructions cannot be modified and that, usually, memory holding data cannot be executed as instructions.

Of course, programs such as compilers and linkers produce executable code as data, but they don’t directly execute it.
Processor: Some Details

- Execution engine
- Instruction pointer
- Condition codes
Processor: Basic Operation

while (forever) {
    fetch instruction IP points at
    decode instruction
    fetch operands
    execute
    store results
    update IP and condition code
}


## Instructions ...

<table>
<thead>
<tr>
<th>Op code</th>
<th>Operand1</th>
<th>Operand2</th>
<th>...</th>
</tr>
</thead>
</table>
Operands

- **Form**
  - immediate vs. reference
    - value vs. address
- **How many?**
  - 3
    - add a,b,c
      - c = a + b
  - 2
    - add a,b
      - b += a
Operands (continued)

- Accumulator
  - special memory in the processor
    » known as a register
    » fast access
  - allows single-operand instructions
    » add a
      • acc += a
    » add b
      • acc += b
Note we’re using the accumulator in two-operand instructions. The “%” makes it clear that “acc” is a register. The “$” indicates that what follows is an immediate operand; i.e., it’s a value to be used as is, rather than as an address or a register.
We have one set of arithmetic instructions that work with both unsigned and signed (two’s complement) interpretations of the bit values in a word.

The overflow flag is set when the result, interpreted as a two’s-complement value should be positive, but won’t fit in the word and thus becomes a negative number, or should be negative, but won’t fit in the word and thus becomes a positive number.

The carry flag is set when computing the result, interpreted as an unsigned value, requires a borrow out of the most-significant bit (i.e., computing b-a when a is greater than b), or when it results in an overflow (e.g., for 32-bit unsigned integers, when the result should be greater than or equal to $2^{32}$ (but can't fit in a 32-bit word).
Examples (1)

- Assume 32-bit arithmetic

- x is 0x80000000
  - TMIN if interpreted as two's-complement
  - $2^{31}$ if interpreted as unsigned

- x-1 (0xffffffff)
  - TMAX if interpreted as two's-complement
  - $2^{31}$-1 if interpreted as unsigned
  - zero flag is not set
  - sign flag is not set
  - overflow flag is set
  - carry flag is not set
Examples (2)

- \textit{x is 0xffffffff}
  - -1 if interpreted as two’s-complement
  - UMAX (2^{32}-1) if interpreted as unsigned
- \textit{x+1 (0x00000000)}
  - zero under either interpretation
  - zero flag is set
  - sign flag is not set
  - overflow flag is not set
  - carry flag is set
Examples (3)

- \(x\) is 0xffffffff
  - -1 if interpreted as two's-complement
  - UMAX \((2^{32}-1)\) if interpreted as unsigned
- \(x+2\) \((0x00000001)\)
  - \((+)1\) under either interpretation
  - zero flag is not set
  - sign flag is not set
  - overflow flag is not set
  - carry flag is set
Quiz 2

- Set of flags giving status of most recent operation:
  - zero flag
    » result was zero
  - sign flag
    » for signed arithmetic interpretation: sign bit is set
  - overflow flag
    » for signed arithmetic interpretation
  - carry flag (generated by carry or borrow out of most-significant bit)
    » for unsigned arithmetic interpretation

- Set explicitly by compare instruction
  - cmp a,b
    » sets flags based on result of b-a

Which flags are set to one by “cmp 2,1”?

a) overflow flag only
b) carry flag only
c) sign and carry flags only
d) sign and overflow flags only
e) sign, overflow, and carry flags
Jump instructions cause the processor to start executing instructions at some specified address. For conditional jump instructions, whether to jump or not is determined by the values of the condition codes. Fortunately, rather than having to specify explicitly those values, one may use mnemonics as shown in the slide.

We'll see examples of their use in the next lecture, when we start looking at x86 assembler instructions.
In the C code above, the assignment to $a$ might be coded in assembler as shown in the box in the lower left. But this brings up the question, where are the values represented by $a$, $b$, $c$, and $d$? Variable names are part of the C language, not assembler. Let’s assume that these global variables are located at addresses 1000, 1004, 1008, and 1012, as shown on the right. Thus correct assembler language would be as in the middle box, which deals with addresses, not variable names. Note that “mov 1004,%acc” means to copy the contents of location 1004 to the accumulator register; it does not mean to copy the integer 1004 into the register!

Beginning with this slide, whenever we draw pictures of memory, lower memory addresses are at the bottom, higher addresses are at the top. This is the opposite of how we’ve been drawing pictures of memory in previous slides.
Here we rearrange things a bit. $b$ is a global variable, but $a$ is a local variable within `func`, and $c$ and $d$ are arguments. The issue here is that the locations associated with $a$, $c$, and $d$ will, in general, be different for each call to `func`. Thus we somehow must modify the assembler code to take this into account.
Note that both positive and negative offsets might be used.
Here we load the value 10,000 into the base register (recall that the “$” means what follows is a literal value; a “%” sign means that what follows is the name of a register), then store the value 10 into the memory location 10100 (the contents of the base register plus 100); the notation \( n(\% base) \) means the address obtained by adding \( n \) to the contents of the base register.
Here we return to our earlier example. We assume that, as part of the call to `func`, the base register is loaded with the address of the beginning of `func`'s current stack frame, and that the local variable `a` and the parameters `c` and `d` are located within the frame. Thus we refer to them by their offset from the beginning of the stack frame, which are assumed to be `-16`, `-8`, and `-12`. Since the stack grows from higher addresses to lower addresses, these offsets are negative. Note that the first assembler instruction copies the contents of location `1000` into `%acc.`
Quiz 3

Suppose the value in base is 10,000. What is the address of c?

a) 9992  
b) 9996  
c) 10,004  
d) 10,008

mov 1000,%acc
add -8(%base),%acc
mul -12(%base),%acc
mov %acc,-16(%base)
We’ve now seen four registers: the instruction pointer, the accumulator, the base register, and the condition codes. The accumulator is used to hold intermediate results for arithmetic; the base register is used to hold addresses for relative addressing. There’s no particular reason why the accumulator can’t be used as the base register and vice versa: thus they may be used interchangeably. Furthermore, it is useful to have more than two such dual-purpose registers. As we will see, the x86 architecture has eight such registers; the x86-64 architecture has 16.
Why do we make the distinction between registers and memory? Registers are in the processor itself and can be read from and written to very quickly. Memory is on separate hardware and takes much more time to access than registers do. Thus operations involving only registers can be executed very quickly, while significantly more time is required to access memory. Processors typically have relatively few registers (the IA-32 architecture has eight, the x86-64 architecture has 32; some other architectures have many more, perhaps as many as 256); memory is measured in gigabytes.

Note that memory access-time is mitigated by the use of on-processor caches, something that we will discuss in a few weeks.