Assembly Language:
Part 1
Context of this Lecture

First half lectures: “Programming in the large”
Second half lectures: “Under the hood”

<table>
<thead>
<tr>
<th>Starting Now</th>
<th>Afterward</th>
</tr>
</thead>
<tbody>
<tr>
<td>C Language</td>
<td>Application Program</td>
</tr>
<tr>
<td>Assembly Language</td>
<td>Operating System</td>
</tr>
<tr>
<td>Machine Language</td>
<td>Hardware</td>
</tr>
</tbody>
</table>

language levels tour

service levels tour
Goals of this Lecture

Help you learn:

• Language levels
• The basics of x86-64 architecture
  • Enough to understand x86-64 assembly language
• The basics of x86-64 assembly language
  • Instructions to define global data
  • Instructions to transfer data and perform arithmetic
## Lectures vs. Precepts

### Approach to studying assembly language:

<table>
<thead>
<tr>
<th>Precepts</th>
<th>Lectures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Study <strong>complete</strong> pgms</td>
<td>Study <strong>partial</strong> pgms</td>
</tr>
<tr>
<td>Begin with <strong>small</strong> pgms;</td>
<td>Begin with <strong>simple</strong> constructs; proceed to <strong>complex</strong> ones</td>
</tr>
<tr>
<td>proceed to <strong>large</strong> ones</td>
<td></td>
</tr>
<tr>
<td>Emphasis on <strong>writing</strong> code</td>
<td>Emphasis on <strong>reading</strong> code</td>
</tr>
</tbody>
</table>
Agenda

Language Levels

Architecture

Assembly Language: Defining Global Data

Assembly Language: Performing Arithmetic
High-Level Languages

Characteristics
- Portable
  - To varying degrees
- Complex
  - One statement can do much work
- Expressive
  - To varying degrees
  - Good (code functionality / code size) ratio
- Human readable

```
count = 0;
while (n>1)
{
    count++;
    if (n&1)
        n = n*3+1;
    else
        n = n/2;
}
```
Machine Languages

**Characteristics**

- Not portable
  - Specific to hardware
- Simple
  - Each instruction does a simple task
- Not expressive
  - Each instruction performs little work
  - Poor (code functionality / code size) ratio
- Not human readable
  - Requires lots of effort!
  - Requires tool support

```
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
9222 9120 1121 A120 1121 A121 7211 0000
0000 0001 0002 0003 0004 0005 0006 0007
0008 0009 000A 000B 000C 000D 000E 000F
0000 0000 0000 FE10 FACE CAFE ACED CEDE

1234 5678 9ABC DEF0 0000 0000 F00D 0000
0000 0000 EEEE 1111 EEEE 1111 0000 0000
B1B2 F1F5 0000 0000 0000 0000 0000 0000
```
Assembly Languages

Characteristics

• Not portable
  • Each assembly language instruction maps to one machine language instruction

• Simple
  • Each instruction does a simple task

• Not expressive
  • Poor (code functionality / code size) ratio

• Human readable!!!
Q: Why learn assembly language?

A: Knowing assembly language helps you:
   • Write faster code
     • In assembly language
     • In a high-level language!
   • Understand what’s happening “under the hood”
     • Someone needs to develop future computer systems
     • Maybe that will be you!
Why Learn x86-64 Assembly Lang?

Why learn x86-64 assembly language?

Pros
- X86-64 is popular
- CourseLab computers are x86-64 computers
  - Program natively on CourseLab instead of using an emulator

Cons
- X86-64 assembly language is big
  - Each instruction is simple, but…
  - There are many instructions
  - Instructions differ widely
We’ll study a popular subset
  • As defined by precept *x86-64 Assembly Language* document

We’ll study programs define functions that:
  • Do not use floating point values
  • Have parameters that are integers or addresses (but not structures)
  • Have return values that are integers or addresses (but not structures)
  • Have no more than 6 parameters

Claim: a reasonable subset
Agenda

Language Levels

Architecture

Assembly Language: Defining Global Data

Assembly Language: Performing Arithmetic
John Von Neumann (1903-1957)

In computing
- Stored program computers
  - Cellular automata
  - Self-replication

Other interests
- Mathematics
- Inventor of game theory
- Nuclear physics (hydrogen bomb)

Princeton connection
- Princeton Univ & IAS, 1930-1957

Known for “Von Neumann architecture (1950)”
- In which programs are just data in the memory
- Contrast to the now-obsolete “Harvard architecture”
Von Neumann Architecture

- CPU
- Control Unit
- ALU
- Registers
- Data bus
- RAM
Von Neumann Architecture

**RAM (Random Access Memory)**
Conceptually: large array of bytes

- Contains data
  (program variables, structs, arrays)
- and the program!

Instructions are fetched from RAM
So is data

Data bus

RAM

CPU

Control Unit

ALU

Registers
Von Neumann Architecture

Registers
- Small amount of storage on the CPU
- Much faster than RAM
- Top of the storage hierarchy
  - Above RAM, disk, …
### Registers (x86-64 architecture)

#### General purpose registers:

<table>
<thead>
<tr>
<th>Register</th>
<th>Big Endian (MSB)</th>
<th>Little Endian (LSB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAX</td>
<td>EAX</td>
<td>AX</td>
</tr>
<tr>
<td>RBX</td>
<td>EBX</td>
<td>BX</td>
</tr>
<tr>
<td>RCX</td>
<td>ECX</td>
<td>CX</td>
</tr>
<tr>
<td>RDX</td>
<td>EDX</td>
<td>DX</td>
</tr>
</tbody>
</table>
Registers (x86-64 architecture)

General purpose registers (cont.):

RSP is unique; see upcoming slide
## Registers (x86-64 architecture)

### General purpose registers (cont.):

<table>
<thead>
<tr>
<th>Register</th>
<th>R8D</th>
<th>R8W</th>
<th>R8B</th>
</tr>
</thead>
<tbody>
<tr>
<td>R8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R9</td>
<td>R9D</td>
<td>R9W</td>
<td>R9B</td>
</tr>
<tr>
<td>R10</td>
<td>R10D</td>
<td>R10W</td>
<td>R10B</td>
</tr>
<tr>
<td>R11</td>
<td>R11D</td>
<td>R11W</td>
<td>R11B</td>
</tr>
<tr>
<td>R12</td>
<td>R12D</td>
<td>R12W</td>
<td>R12B</td>
</tr>
<tr>
<td>R13</td>
<td>R13D</td>
<td>R13W</td>
<td>R13B</td>
</tr>
<tr>
<td>R14</td>
<td>R14D</td>
<td>R14W</td>
<td>R14B</td>
</tr>
<tr>
<td>R15</td>
<td>R15D</td>
<td>R15W</td>
<td>R15B</td>
</tr>
</tbody>
</table>
RSP Register

RSP (Stack Pointer) register
• Contains address of top (low address) of current function’s stack frame

Allows use of the STACK section of memory, and special-purpose stack manipulation instructions

(See Assembly Language: Function Calls lecture)
EFLAGS Register

Special-purpose register…

**EFLAGS (Flags) register**

- Contains **CC (Condition Code) bits**
- Affected by compare (**cmp**) instruction
  - And many others
- Used by conditional jump instructions

*(See Assembly Language: Part 2 lecture)*
RIP Register

Special-purpose register…

RIP (Instruction Pointer) register

- Stores the location of the next instruction
  - Address (in TEXT section) of machine-language instructions to be executed next
- Value changed:
  - Automatically to implement sequential control flow
  - By jump instructions to implement selection, repetition
Registers summary

16 general-purpose 64-bit pointer/long-integer registers, many with stupid names:
rax, rbx, rcx, rdx, rsi, rdi, \textcolor{red}{rbp, rsp}, r8, r9, r10, r11, r12, r13, r14, r15

sometimes used as a “frame pointer” or “base pointer”

“stack pointer”

If you’re operating on 32-bit “int” data, use these stupid names instead:
eax, ebx, ecx, edx, esi, edi, ebp, \textcolor{red}{rsp}, r8d, r9d, r10d, r11d, r12d, r13d, r14d, r15d

it doesn’t really make sense to put 32-bit ints in the stack pointer

2 special-purpose registers: \textcolor{red}{eflags, rip}

“condition codes” “program counter”
Typical pattern:

- **Load** data from RAM to registers
- **Manipulate** data in registers
- **Store** data from registers to RAM

Many instructions combine steps
ALU (Arithmetic Logic Unit)

- Performs arithmetic and logic operations

Diagram:
- ALU with inputs `src1`, `src2`, `operation`, and output `dest`.
- ALU connected to EFLAGS.
- ALU connected to CPU.
- ALU connected to Control Unit.
- ALU connected to Registers.
- ALU connected to RAM.
- ALU connected to Data bus.
Control Unit

- Fetches and decodes each machine-language instruction
- Sends proper data to ALU
CPU (Central Processing Unit)

- Control unit
  - Fetch, decode, and execute
- ALU
  - Execute low-level operations
- Registers
  - High-speed temporary storage
Agenda

Language Levels
Architecture

Assembly Language: Defining Global Data
Assembly Language: Performing Arithmetic
Defining Data: DATA Section 1

```c
static char c = 'a';
static short s = 12;
static int i = 345;
static long l = 6789;
```

Note:

```c
.section " .data"

.c: .byte 'a'
.s: .word 12
.i: .long 345
.l: .quad 6789
```

- `.section` instruction (to announce DATA section)
- label definition (marks a spot in RAM)
- `.byte` instruction (1 byte)
- `.word` instruction (2 bytes)
- `.long` instruction (4 bytes)
- `.quad` instruction (8 bytes)
char c = 'a';
short s = 12;
int i = 345;
long l = 6789;

.note:
Can place label on same line as next instruction
.globl instruction
Defining Data: BSS Section

```c
static char c;
static short s;
static int i;
static long l;
```

```
.section "".bss"

c:
    .skip 1

s:
    .skip 2

i:
    .skip 4

l:
    .skip 8
```

Note:
- `.section` instruction (to announce BSS section)
- `.skip` instruction
Defining Data: RODATA Section

... "hello\n" ...;
...

.section " .rodata"
helloLabel:
.string "hello\n"

Note:
.section instruction (to announce RODATA section)
.string instruction
Agenda

Language Levels
Architecture
Assembly Language: Defining Global Data
Assembly Language: Performing Arithmetic
Instruction Format

Many instructions have this format:

\[
\text{name}\{b,w,l,q\} \ src, \ dest
\]

- **name**: name of the instruction (\text{mov}, \text{add}, \text{sub}, \text{and}, etc.)
- **byte** => operands are one-byte entities
- **word** => operands are two-byte entities
- **long** => operands are four-byte entities
- **quad** => operands are eight-byte entities
Instruction Format

Many instructions have this format:

\[ \text{name\{b,w,l,q\} src, dest} \]

- **src**: source operand
  - The source of data
  - Can be
    - **Register operand**: `%rax`, `%ebx`, etc.
    - **Memory operand**: `5` (legal but silly), `someLabel`
    - **Immediate operand**: `$5$, `$someLabel$`
Many instructions have this format:

[name{b,w,l,q}] src, dest

- **dest**: destination operand
  - The destination of data
  - Can be
    - **Register operand**: %rax, %ebx, etc.
    - **Memory operand**: 5 (legal but silly), someLabel
  - Cannot be
    - **Immediate operand**
Performing Arithmetic: Long Data

```c
static int length;
static int width;
static int perim;
...
perim =
    (length + width) * 2;
```

Note:
- **movl** instruction
- **addl** instruction
- **sall** instruction
- Register operand
- Immediate operand
- Memory operand
- `.section` instruction (to announce TEXT section)
Operands

Immediate operands

• $5 => use the number 5 (i.e. the number that is available immediately within the instruction)
• $i => use the address denoted by i (i.e. the address that is available immediately within the instruction)
• Can be source operand; cannot be destination operand

Register operands

• %rax => read from (or write to) register RAX
• Can be source or destination operand

Memory operands

• 5 => load from (or store to) memory at address 5 (silly; seg fault)
• i => load from (or store to) memory at the address denoted by i
• Can be source or destination operand (but not both)
• There’s more to memory operands; see next lecture
Performing Arithmetic: Byte Data

static char grade = 'B';
...
grade--;
Q: What would happen if we used `movl` instead of `movb`?

A. Would always work correctly
B. Would always work incorrectly
C. Would sometimes work correctly
D. *This* code would work, but something else might go wrong that would cause you sleepless nights of painful debugging

```
.section "data"
grade: .byte 'B'
...
.section "text"
...
# Option 1
movb grade, %al
subb $1, %al
movb %al, grade
...
# Option 2
subb $1, grade
...
# Option 3
decb grade
```
Q: What would happen if we used `subl` instead of `subb`?

A. Would always work correctly
B. Would always work incorrectly
C. Would sometimes work correctly
D. *This* code would work, but something else might go wrong that would cause you sleepless nights of painful debugging
More Arithmetic Instructions

<table>
<thead>
<tr>
<th>Instruction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add{q,l,w,b} srcIRM, destRM</td>
<td>dest += src</td>
</tr>
<tr>
<td>sub{q,l,w,b} srcIRM, destRM</td>
<td>dest -= src</td>
</tr>
<tr>
<td>inc{q,l,w,b} destRM</td>
<td>dest++</td>
</tr>
<tr>
<td>dec{q,l,w,b} destRM</td>
<td>dest--</td>
</tr>
<tr>
<td>neg{q,l,w,b} destRM</td>
<td>dest = -dest</td>
</tr>
</tbody>
</table>

Operand notation:
- src => source; dest => destination
- R => register; I => immediate; M => memory
Data Transfer Instructions

- `mov{q,l,w,b} srcIRM, destRM`  \( \text{dest} = \text{src} \)
- `movsb{q,l,w} srcRM, destR`  \( \text{dest} = \text{src} \) (sign extend)
- `movsw{q,l} srcRM, destR`  \( \text{dest} = \text{src} \) (sign extend)
- `movslq srcRM, destR`  \( \text{dest} = \text{src} \) (sign extend)
- `movzb{q,l,w} srcRM, destR`  \( \text{dest} = \text{src} \) (zero fill)
- `movzw{q,l} srcRM, destR`  \( \text{dest} = \text{src} \) (zero fill)
- `movzlq srcRM, destR`  \( \text{dest} = \text{src} \) (zero fill)
- `cqto`  \( \text{reg}[RDX:RAX] = \text{reg}[RAX] \) (sign extend)
- `cltd`  \( \text{reg}[EDX:EAX] = \text{reg}[EAX] \) (sign extend)
- `cwtl`  \( \text{reg}[EAX] = \text{reg}[AX] \) (sign extend)
- `cbtw`  \( \text{reg}[AX] = \text{reg}[AL] \) (sign extend)
## Signed multiplication and division instructions

<table>
<thead>
<tr>
<th>Instruction</th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>imulq srcRM</td>
<td>( \text{reg}[\text{RDX}:\text{RAX}] = \text{reg}[\text{RAX}]*\text{src} )</td>
</tr>
<tr>
<td>imull srcRM</td>
<td>( \text{reg}[\text{EDX}:\text{EAX}] = \text{reg}[\text{EAX}]*\text{src} )</td>
</tr>
<tr>
<td>imulw srcRM</td>
<td>( \text{reg}[\text{DX}:\text{AX}] = \text{reg}[\text{AX}]*\text{src} )</td>
</tr>
<tr>
<td>imulb srcRM</td>
<td>( \text{reg}[\text{AX}] = \text{reg}[\text{AL}]*\text{src} )</td>
</tr>
<tr>
<td>idivq srcRM</td>
<td>( \text{reg}[\text{RAX}] = \text{reg}[\text{RDX}:\text{RAX}]/\text{src} ) &lt;br&gt;( \text{reg}[\text{RDX}] = \text{reg}[\text{RDX}:\text{RAX}]%\text{src} )</td>
</tr>
<tr>
<td>idivl srcRM</td>
<td>( \text{reg}[\text{EAX}] = \text{reg}[\text{EDX}:\text{EAX}]/\text{src} ) &lt;br&gt;( \text{reg}[\text{EDX}] = \text{reg}[\text{EDX}:\text{EAX}]%\text{src} )</td>
</tr>
<tr>
<td>idivw srcRM</td>
<td>( \text{reg}[\text{AX}] = \text{reg}[\text{DX}:\text{AX}]/\text{src} ) &lt;br&gt;( \text{reg}[\text{DX}] = \text{reg}[\text{DX}:\text{AX}]%\text{src} )</td>
</tr>
<tr>
<td>idivb srcRM</td>
<td>( \text{reg}[\text{AL}] = \text{reg}[\text{AX}]/\text{src} ) &lt;br&gt;( \text{reg}[\text{AH}] = \text{reg}[\text{AX}]%\text{src} )</td>
</tr>
</tbody>
</table>

See Bryant & O’Hallaron book for description of signed vs. unsigned multiplication and division
# Multiplication and Division

## Unsigned multiplication and division instructions

<table>
<thead>
<tr>
<th>Instruction</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mulq srcRM</code></td>
<td><code>reg[RDX:RAX] = reg[RAX]*src</code></td>
</tr>
<tr>
<td><code>mull srcRM</code></td>
<td><code>reg[EDX:EAX] = reg[EAX]*src</code></td>
</tr>
<tr>
<td><code>mulw srcRM</code></td>
<td><code>reg[DX:AX] = reg[AX]*src</code></td>
</tr>
<tr>
<td><code>mulb srcRM</code></td>
<td><code>reg[AX] = reg[AL]*src</code></td>
</tr>
<tr>
<td><code>divq srcRM</code></td>
<td><code>reg[RAX] = reg[RDX:RAX]/src</code></td>
</tr>
<tr>
<td></td>
<td><code>reg[RDX] = reg[RDX:RAX]%src</code></td>
</tr>
<tr>
<td><code>divl srcRM</code></td>
<td><code>reg[EAX] = reg[EDX:EAX]/src</code></td>
</tr>
<tr>
<td></td>
<td><code>reg[EDX] = reg[EDX:EAX]%src</code></td>
</tr>
<tr>
<td><code>divw srcRM</code></td>
<td><code>reg[AX] = reg[DX:AX]/src</code></td>
</tr>
<tr>
<td></td>
<td><code>reg[DX] = reg[DX:AX]%src</code></td>
</tr>
<tr>
<td><code>divb srcRM</code></td>
<td><code>reg[AL] = reg[AX]/src</code></td>
</tr>
<tr>
<td></td>
<td><code>reg[AH] = reg[AX]%src</code></td>
</tr>
</tbody>
</table>

See Bryant & O’ Hallaron book for description of signed vs. unsigned multiplication and division.
Bitwise instructions

and\{q,l,w,b\} srcIRM, destRM  \quad dest = src \& dest
or\{q,l,w,b\} srcIRM, destRM  \quad dest = src | dest
xor\{q,l,w,b\} srcIRM, destRM  \quad dest = src \oplus dest
not\{q,l,w,b\} destRM  \quad dest = \neg dest
sal\{q,l,w,b\} srcIR, destRM  \quad dest = dest \ll src
sar\{q,l,w,b\} srcIR, destRM  \quad dest = dest \gg src (sign extend)
shl\{q,l,w,b\} srcIR, destRM  \quad (Same as sal)
shr\{q,l,w,b\} srcIR, destRM  \quad dest = dest \gg src (zero fill)
Summary

Language levels

The basics of computer architecture
  • Enough to understand x86-64 assembly language

The basics of x86-64 assembly language
  • Instructions to define global data
  • Instructions to perform data transfer and arithmetic

To learn more
  • Study more assembly language examples
    • Chapter 3 of Bryant and O’Hallaron book
  • Study compiler-generated assembly language code
    • gcc217 -S somefile.c
Appendix

Big-endian vs little-endian byte order
Byte Order

x86-64 is a **little endian** architecture

- **Least** significant byte of multi-byte entity is stored at lowest memory address
- “Little end goes first”

| 1000 | 00000101 |
| 1001 | 00000000 |
| 1002 | 00000000 |
| 1003 | 00000000 |

The int 5 at address 1000:

Some other systems use **big endian**

- **Most** significant byte of multi-byte entity is stored at lowest memory address
- “Big end goes first”

| 1000 | 00000000 |
| 1001 | 00000000 |
| 1002 | 00000000 |
| 1003 | 00000101 |

The int 5 at address 1000:
#include <stdio.h>
int main(void)
{
  unsigned int i = 0x003377ff;
  unsigned char *p;
  int j;
  p = (unsigned char *)&i;
  for (j=0; j<4; j++)
    printf("Byte %d: %2x\n", j, p[j]);
}
Byte Order Example 2

Note:
Flawed code; uses “b” instructions to manipulate a four-byte memory area

Note:
Flawed code; uses “b” instructions to manipulate a four-byte memory area

x86-64 is **little** endian, so what will be the value of grade?

What would be the value of grade if x86-64 were **big** endian?

```
.section " .data"
grade: .long 'B'
...

.section " .text"
...
# Option 1
movb grade, %al
subb $1, %al
movb %al, grade
...
# Option 2
subb $1, grade
```
Byte Order Example 3

Note:
Flawed code; uses “l” instructions to manipulate a one-byte memory area

What would happen?

```
.section ".data"
grade: .byte 'B'
...
.section ".text"
...
# Option 1
movl grade, %eax
subl $1, %eax
movl %eax, grade
...
# Option 2
subl $1, grade
```