

CS220 – Logic Design AS02-The IA-32 Platform

- Outline
 - IA-32 History
 - 8086 Registers
 - Protected/Real Mode
 - IA-32 Registers
 - Development Tools
- References
 - Wikipedia: x86, IA-32, x86 assembly language

1

AS02-The IA-32 Platform Introduction

- Programming in assembly requires familiarity with the processor (CPU): How many registers? What is the size of each? What can each one do? What is each one called?
- We will be programming _____ processors (Intel Architecture – 32 bit, aka x86-32). This includes the 80386 through Pentium (and compatible) processors. It does NOT include the 8086, 80286 (16 bit) or Itanium (IA-64).

2

AS02-The IA-32 Platform History: 8088/8086

- The first IBM PC used an 8088. It is binary compatible with the 8086. It has several 16-bit registers: AX, BX, CX, DX, SI, DI, BP, SP, CS, DS, SS, ES, IP, and FLAGS.
- The 8088 had a 20-bit address bus and so could address up to 2^{20} bytes or 1 MB. However, the 16 bit registers could only address memory in 2^{16} or 64 KB segments.
- A modern Pentium CPU, operating in _____ mode, acts like a fast 8088 CPU.

3

AS02-The IA-32 Platform History: 80286

- The 80286 was used in the PC AT. It was backward compatible with the 8088/8086.
- It featured a new _____ mode (now called 16-bit protected mode) in which up to 16 MB of memory could be addressed. Protected mode could prevent one program from accessing memory used by another program.
- Memory still had to be accessed in 64 KB segments (just like real mode).

4

AS02-The IA-32 Platform History: 80386

- The 80386 was backward compatible with the 8088/8086 and the 80286.
- It featured a new 32-bit protected mode in which up to 4 GB of memory could be addressed (32 bit address bus). The internal registers were extended to 32 bits.
- In 32-bit protected mode memory could be accessed in _____ segments.

5

AS02-The IA-32 Platform History: Pentium

- From a programming standpoint there are few differences between the 80386 and the 80486, Pentium, Pentium Pro, Pentium MMX, Pentium II, Pentium III and Pentium IV CPUs. (Of course, they are much faster.)
- They are all backward compatible with the 8088 in real mode and the _____ in 32-bit protected mode. (32-bit protected mode is the standard mode for modern Oses such as Windows XP or Linux.)

6

AS02-The IA-32 Platform 8088/8086 Registers

- The 8088 had four 16-bit general purpose registers: AX, BX, CX, and DX. Each could be treated as two 8-bit registers. (The upper and lower bytes of AX are AH and AL.)



- There were two 16-bit index registers: SI and DI. These could not be broken into bytes.
- The 16-bit BP and SP registers are _____ registers.

7

AS02-The IA-32 Platform 8088/8086 Registers

- IP is the instruction pointer. It is used with CS to keep track of the address of the next instruction to be executed by the CPU.
- The _____ registers stores information about the results of a previous instruction.
- CS, DS, SS, and ES are 16-bit segment registers. They are, respectively, the code, data, stack and extra segment registers (also known as selector registers).

8

AS02-The IA-32 Platform 8088/8086 Registers

- Total memory was limited to 1 MB. Valid addresses range from 00000 to FFFFF. A _____ address is formed by combining a 16-bit segment register and a 16-bit offset.
- The segment value is multiplied by 16 (shifted left 4 bits) and added to the offset.
- This gives access to the entire 1 MB in 64 kB segments. Large programs would span segments, making programming awkward.

9

AS02-The IA-32 Platform 8088/8086 Registers

- For example, assume CS contains A47C and the IP contains 0048. The address can be written in segment:offset form as A47C:0048. The corresponding physical 20-bit address is:
$$A47C0 + 0048 = A4808$$
- Note that segmented addresses are not unique. The _____ address A4808 can be written as A47C:0048, or A47D:0038, or A480:0008, or

10

AS02-The IA-32 Platform Protected/Real Mode

- Even the very latest Pentium CPUs power up in real mode. In real mode an IA-32 acts just like an 8086. All modern OSes switch the CPU to protected mode when booting up.
- Two memory models are supported in protected mode – the flat memory model and the _____ memory model. Only the segmented memory model will be described. (This is the model used by modern OSes.)

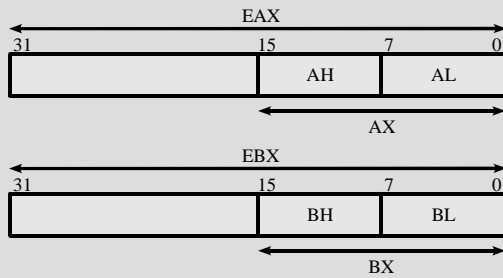
11

AS02-The IA-32 Platform IA-32 Registers

- In the _____ and later CPUs most of the 8088 registers were extended to 32 bits. For example, the 16-bit AX register was extended to the 32-bit EAX register. The names AX, AL and AH can still be used to access portions of the lower half of EAX.
- Most of the general-purpose registers can be used for holding any type of data, but some have acquired special uses (by either design or convention).

12

AS02-The IA-32 Platform IA-32 Registers



8/16/32-bit Register Names

13

AS02-The IA-32 Platform IA-32 Registers

| Name | Description |
|------|--|
| EAX | Accumulator for operands and results |
| EBX | Pointer to data in the data segment |
| ECX | Counter for string and loop operations |
| EDX | I/O Pointer |
| EDI | Data pointer for destination of string ops |
| ESI | Data pointer for source of string ops |
| ESP | Stack pointer |
| EBP | Stack data pointer |

IA-32 32-Bit General Purpose Registers

14

AS02-The IA-32 Platform IA-32 Registers

- The instruction pointer (EIP) is also a 32 bit register. The EIP is not manipulated directly. It is incremented automatically as code is executed or changed by **jump** instructions.
- The segment register values are used as indexes (selectors) into a _____ table. (The segment registers are still 16-bit registers.) An entry in a descriptor table describes a memory segment that may reside anywhere in physical memory.

15

AS02-The IA-32 Platform IA-32 Registers

- IA-32 added FS and GS segment registers:

| Name | Description |
|------|---------------|
| CS | Code segment |
| DS | Data segment |
| SS | Stack segment |
| ES | Extra segment |
| FS | Extra segment |
| GS | Extra segment |

IA-32 Segment Registers

16

AS02-The IA-32 Platform IA-32 Registers

- In protected mode (80386-Pentium) segments may be up to _____ in size. Because of the large segments, assembly programming in protected mode is simpler than in real mode.
- The IA-32 also has five control registers (CR0 – CR4) that determine the operating mode of the CPU. A 32-bit EFLAGS register contains status, control and system flags.

17

AS02-The IA-32 Platform Other Protected Mode Features

- In protected mode the IA-32 supports _____ memory (or paging). With paging enabled, an application uses addresses in a logical address space that may be mapped to any physical address. Each program can act as if it owns the entire 4 GB memory space.
- Paging also allows programs to allocate more memory than is physically available. The contents of individual 4 kB pages of memory can be stored on disk until needed.

18

AS02-The IA-32 Platform Development Tools - Assembler

- Assembly language source programs must be assembled to object code and then linked to produce an executable program.
- There are several assemblers for the IA-32 (MASM, NASM, gas, HLA). Each of these uses a slightly different assembly syntax.
- We will use _____, the GNU assembler. This will allow us to interface assembly routines with C/C++ routines compiled using gcc/g++.

19

AS02-The IA-32 Platform Development Tools - Assembler

- Assembly source code files should have a **.s** file name extension.
- The **gas** assembler is named _____. To assemble **test.s** to object file **test.o** invoke **gas** using:

```
as -o test.o test.s
```
- To create an assembly listing file:

```
as -o test.o -a=test.lst test.s
```

20

AS02-The IA-32 Platform Development Tools - Linker

- The object code files must be linked with _____ and library code to create an executable program.
- The GNU linker is named **ld**. Instead of invoking **ld** directly, it is simpler to use **gcc/g++** to call **ld** for us. This will ensure that **ld** is invoked with the correct arguments:

```
g++ -o test test.o
```

21

AS02-The IA-32 Platform Development Tools - Compiler

- A great way to _____ assembly is to look at assembly that corresponds to C/C++ code.
- The **-S** option to **g++** causes the compiler to generate assembly source. For example, to create a **test.s** assembly source file from a **test.cpp** C++ source file:

```
g++ -S test.cpp
```

22

AS02-The IA-32 Platform Other Development Tools

- **objdump** can be used to display the assembly mnemonics that correspond to the machine code in an object file:

```
objdump -d test.o
```
- _____ can be used to debug assembly (and C++) programs. You can set breakpoints, step through instructions, display register and variable values, etc.

23

AS02-The IA-32 Platform A Note On Assembly Syntax

- **gas** uses what is known as AT&T syntax. Most other assemblers for IA-32 use Intel syntax. There are a number of differences between AT&T and Intel syntax (see pg 49 of your text). One of the more obvious differences is the _____ order of source and destination operands:

```
movl $4, %eax # ATT (4 into EAX)
mov  eax, 4 # Intel(4 into EAX)
```

24