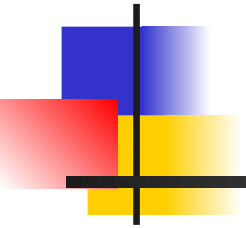
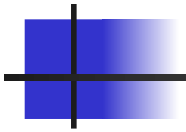


Computer Architecture, Networks, and Operating Systems (CANOS)

Lecture 16:
X86 (part 2)



Announcements

- Project 2 due Friday @ 11:59pm
- Remote class on Friday

8086 Instruction Example

```
mov [200h], 5h
mov cx, [200h]
mov ax, 1h
mov dx, 0h
mult:
mul cx
loop mult
mov [300h], ax
mov [301h], dx
```

Exercise

- Download Emu8086
- https://emu8086.en.lo4d.com/windows
- Write pseudocode for each line of Example 1.
- Use the following reference to help you:
- https://eecs.wsu.edu/~ee314/handouts/x86ref.pdf

8086 Instruction Encoding

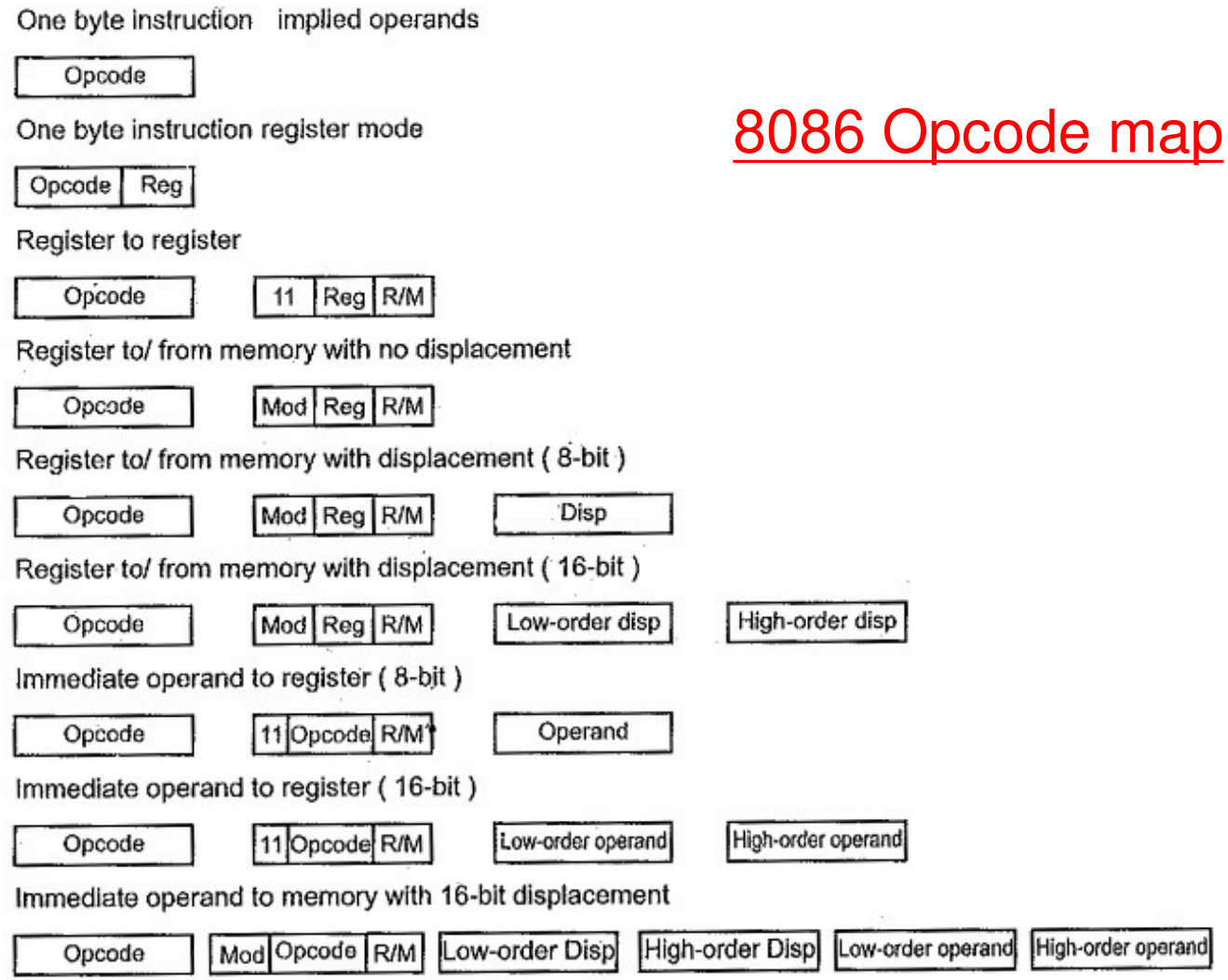
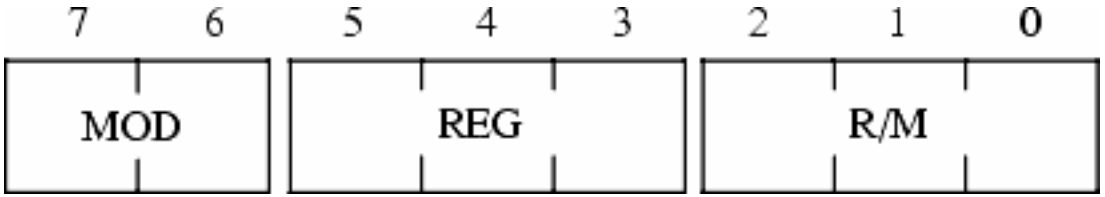


Fig. 6.8 Sample 8086 instruction formats

8086 Opcode map

8086 Instruction Encoding

- **Addressing mode byte:** specifies addressing mode



Page 17

MOD	Meaning
00	Register indirect addressing mode or SIB with no displacement (when R/M = 100) or Displacement only addressing mode (when R/M = 101).
01	One-byte signed displacement follows addressing mode byte(s).
10	Four-byte signed displacement follows addressing mode byte(s).
11	Register addressing mode.

Source

8086 Instruction Encoding

Table 2-1. 16-Bit Addressing Forms with the ModR/M Byte

r8(/r) / r16(/r) / r32(/r) / mm(/r) / xmm(/r) — Second operand registers if an instruction requires one			AL / AX / EAX / MM0 / XMM0	CL / CX / ECX / MM1 / XMM1	DL / DX / EDX / MM2 / XMM2	BL / BX / EBX / MM3 / XMM3	AH / SP / ESP / MM4 / XMM4	CH / BP[1] / EBP / MM5 / XMM5	DH / SI / ESI / MM6 / XMM6	BH / DI / EDI / MM7 / XMM7
(In decimal) /digit (Opcode)			0	1	2	3	4	5	6	7
(In binary) REG =			000	001	010	011	100	101	110	111
Effective Address	**Mod**	**R/M**	**Value of ModR/M Byte (in Hexadecimal)**							
[BX+SI]	00	000	00	08	10	18	20	28	30	38
[BX+DI]		001	01	09	11	19	21	29	31	39
[BP+SI]		010	02	0A	12	1A	22	2A	32	3A
[BP+DI]		011	03	0B	13	1B	23	2B	33	3B
[SI]		100	04	0C	14	1C	24	2C	34	3C
[DI]		101	05	0D	15	1D	25	2D	35	3D
disp16[2]		110	06	0E	16	1E	26	2E	36	3E
[BX]		111	07	0F	17	1F	27	2F	37	3F
[BX+SI]+disp8[3]	01	000	40	48	50	58	60	68	70	78
[BX+DI]+disp8		001	41	49	51	59	61	69	71	79
[BP+SI]+disp8		010	42	4A	52	5A	62	6A	72	7A
[BP+DI]+disp8		011	43	4B	53			6B	73	7B
[SI]+disp8		100	44	4C	54			6C	74	7C
[DI]+disp8		101	45	4D	55			6D	75	7D
[BP]+disp8		110	46	4E	56			6E	76	7E
[BX]+disp8		111	47	4F	57			6F	77	7F
[BX+SI]+disp16	10	000	80	88	90	98	A0	A8	B0	B8
[BX+DI]+disp16		001	81	89	91	99	A1	A9	B1	B9
[BP+SI]+disp16		010	82	8A	92	9A	A2	AA	B2	BA
[BP+DI]+disp16		011	83	8B	93	9B	A3	AB	B3	BB
[SI]+disp16		100	84	8C	94	9C	A4	AC	B4	BC
[DI]+disp16		101	85	8D	95	9D	A5	AD	B5	BD
[BP]+disp16		110	86	8E	96	9E	A6	AE	B6	BE
[BX]+disp16		111	87	8F	97	9F	A7	AF	B7	BF
EAX/AX/AL/MM0/XMM0	11	000	C0	C8	D0	D8	E0	E8	F0	F8
ECX/CX/CL/MM1/XMM1		001	C1	C9	D1	D9	E1	E9	F1	F9
EDX/DX/DL/MM2/XMM2		010	C2	CA	D2	DA	E2	EA	F2	FA
EBX/BX/BL/MM3/XMM3		011	C3	CB	D3	DB	E3	EB	F3	FB
ESP/SP/AHMM4/XMM4		100	C4	CC	D4	DC	E4	EC	F4	FC
EBP/BP/CH/MM5/XMM5		101	C5	CD	D5	DD	E5	ED	F5	FD
ESI/SI/DH/MM6/XMM6		110	C6	CE	D6	DE	E6	EE	F6	FE
EDI/DI/BH/MM7/XMM7		111	C7	CF	D7	DF	E7	EF	F7	FF

8 Reg/Opcode (Decimal/Binary)

24 Addressing mode

8 R/M

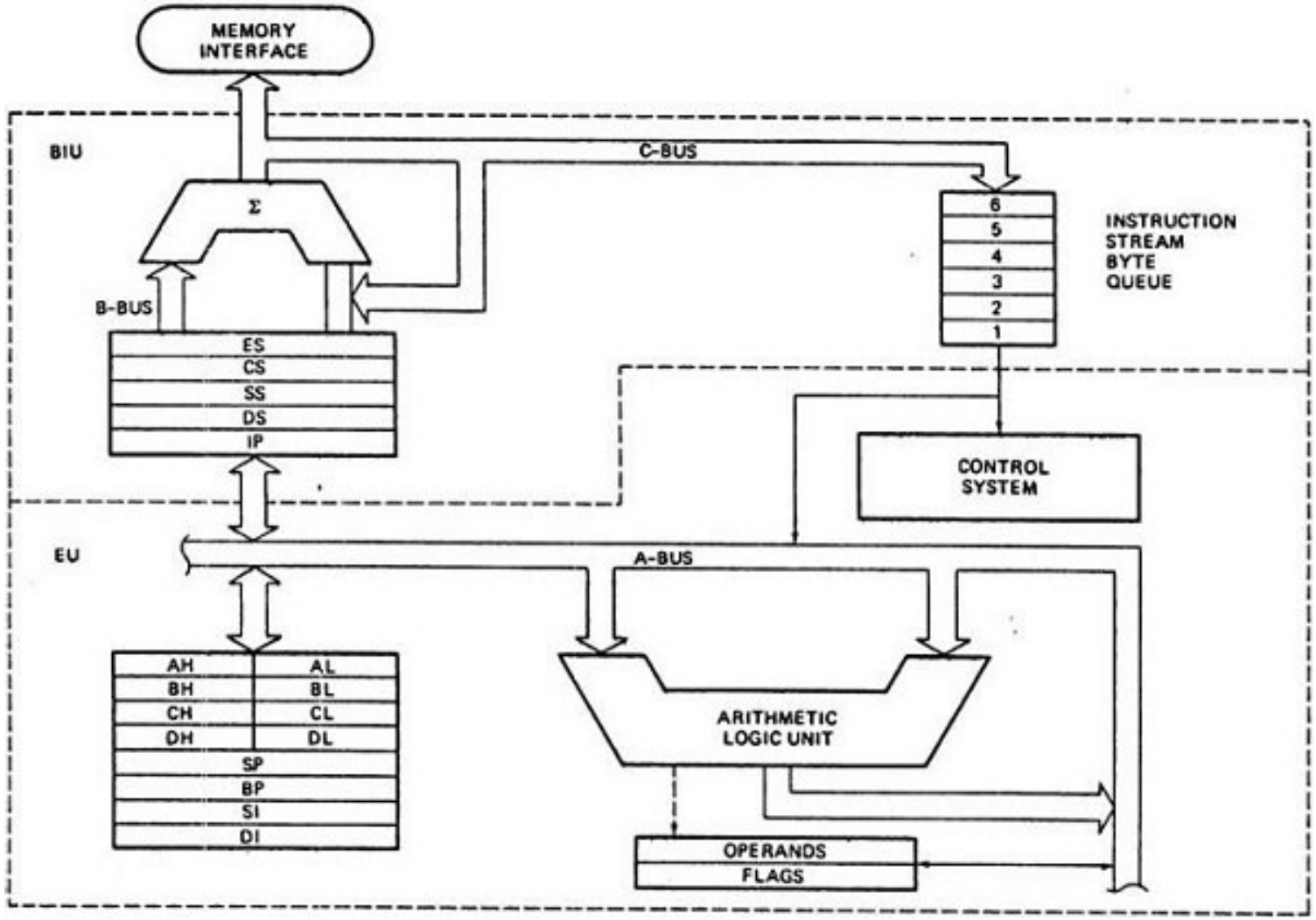
4 Mod

256 ModR/M possible values

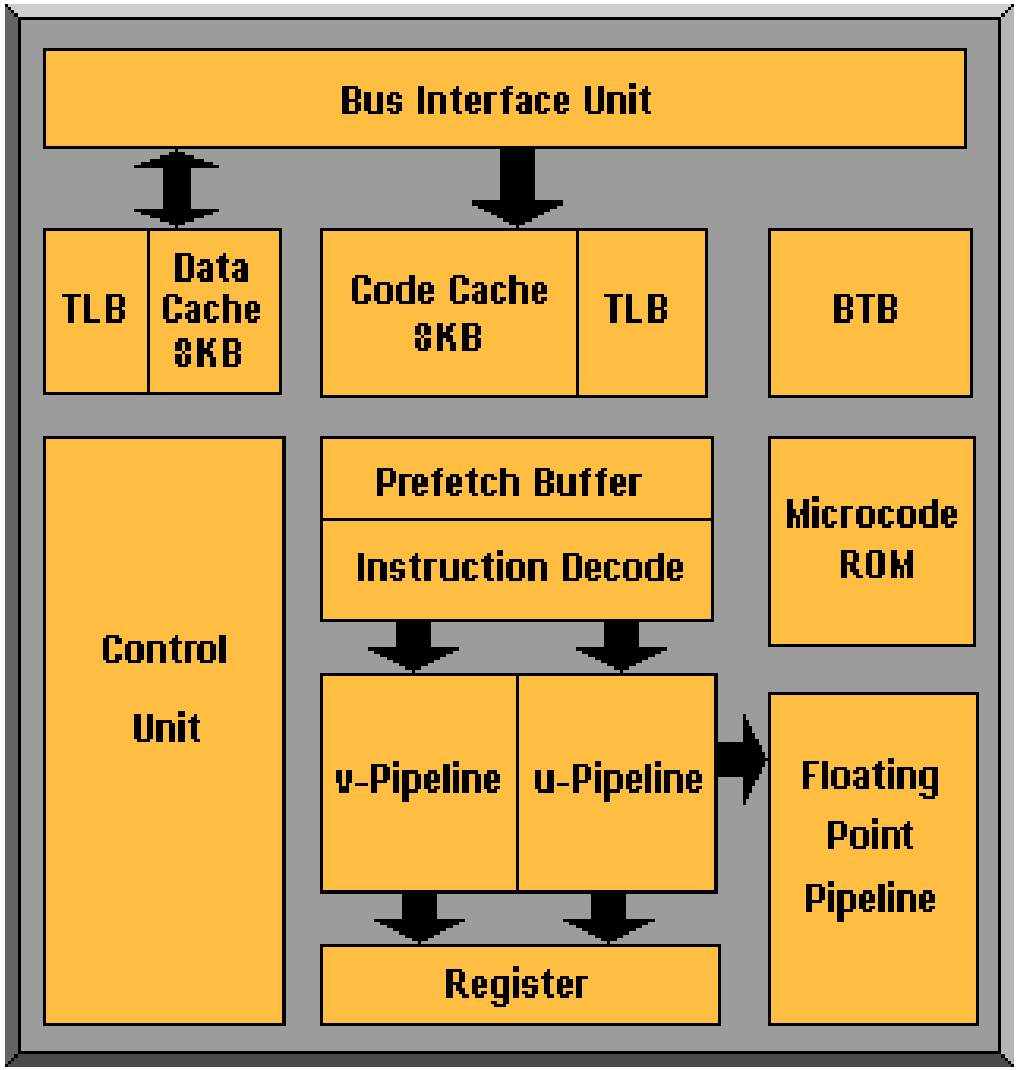
8 registers

Source: datacademia

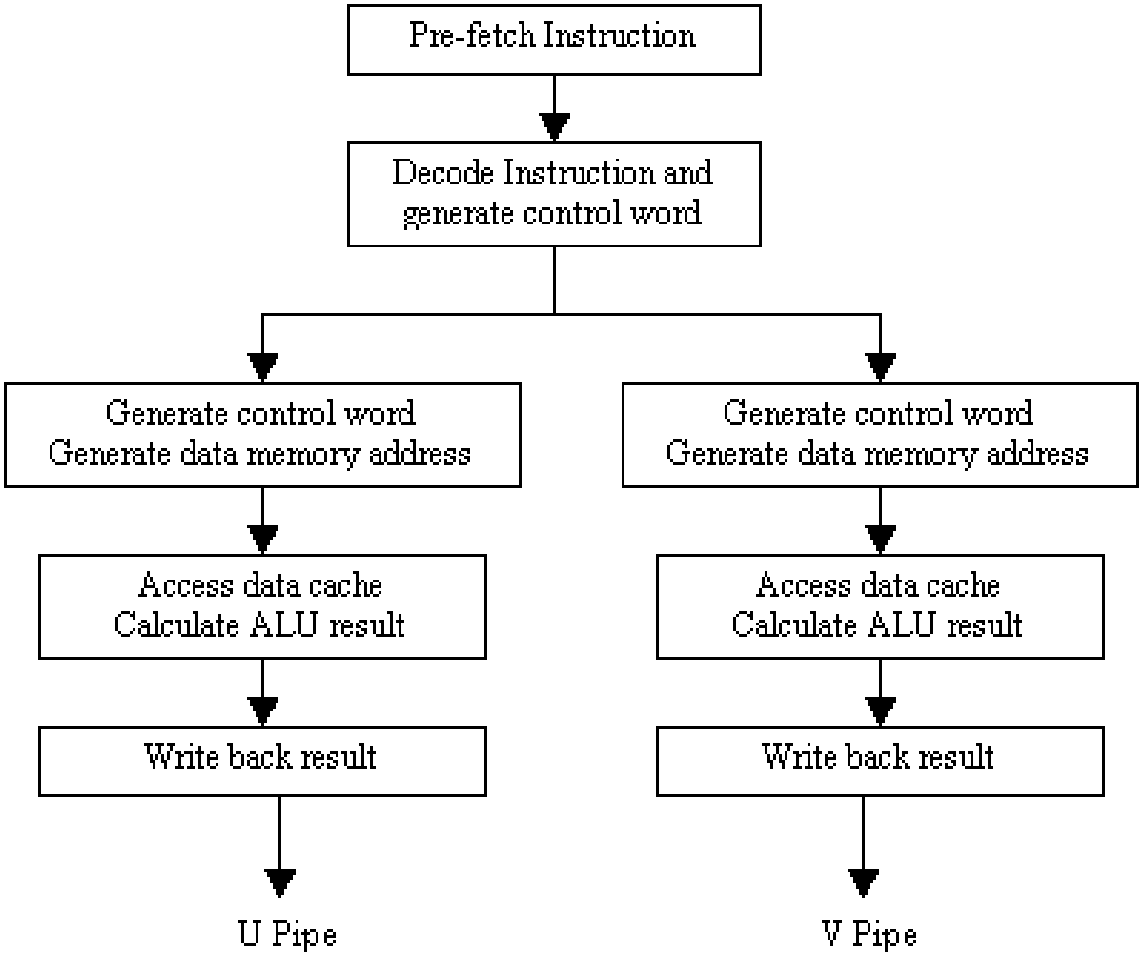
8086 High-Level Architecture



Later x86 (Pentium)

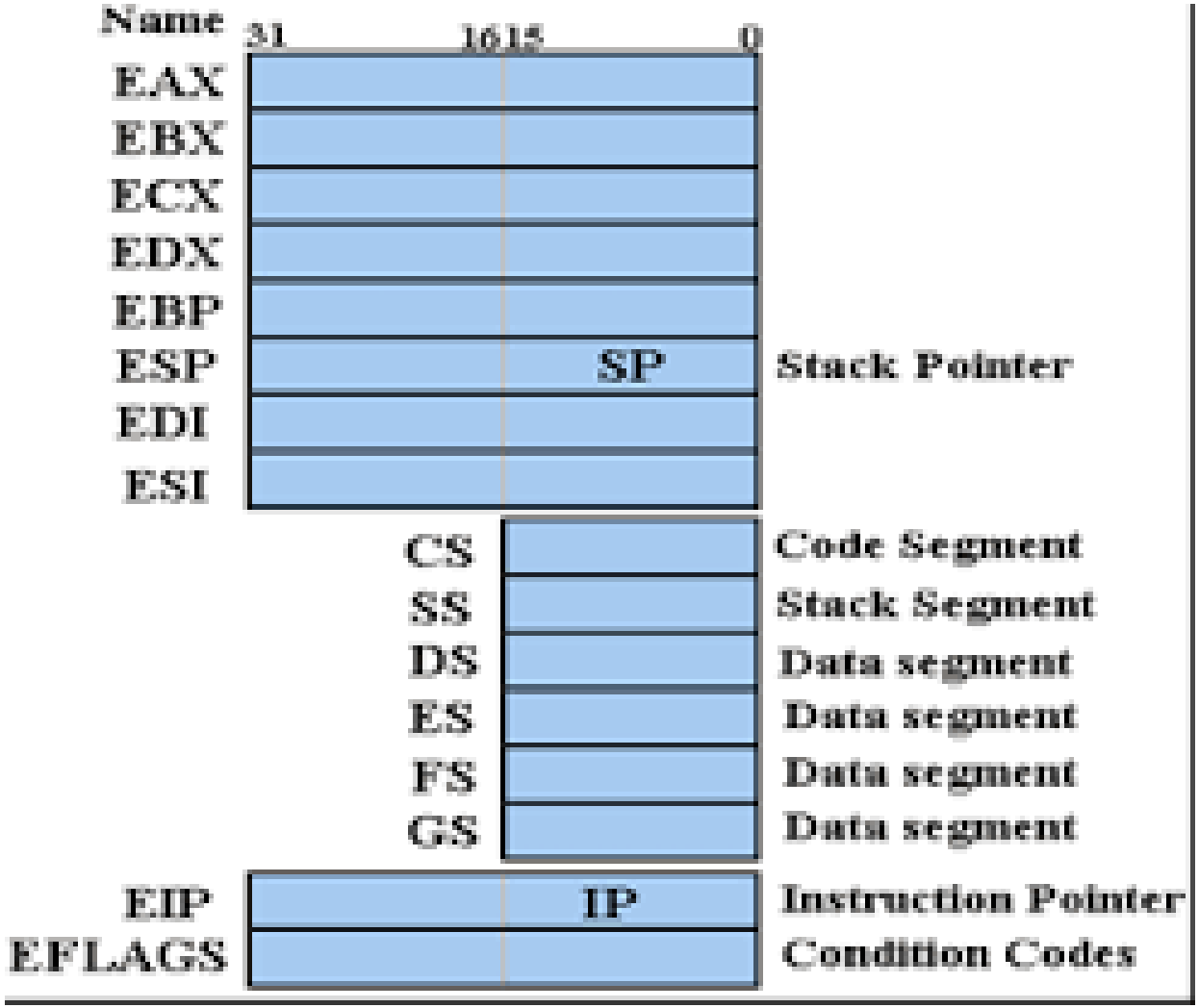


Later x86 (Pentium)



Pentium Pipeline Stages

Later x86 (Pentium)



Later x86 (Pentium)

8086 Instructions

- Loop instructions
- Factorial program
- 8086 Hello World
- Interrupts
- ASCII Codes

Further Reading

- Intel 8086 Instruction Summary
- X86 Instruction Reference
- 8086 Instruction Set Opcodes
- Comparison of 80x86 and MIPS Architectures
- A Hacker's Tour of the x86 CPU Architecture