

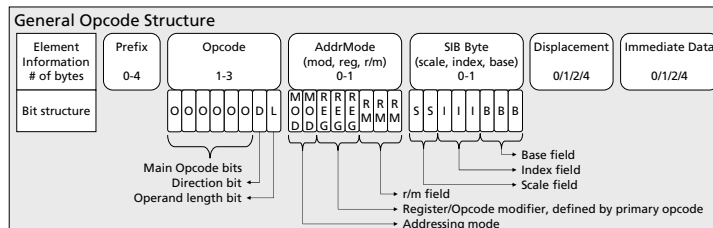


x86 Opcode Structure and Instruction Overview

1 st \ 2 nd	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
0	ADD					ES	ES	OR					CS	TWO BYTE				
1	ADC					PUSH SS	POP SS	SBB					PUSH DS	POP DS				
2	AND					ES SEGMENT OVERRIDE	DAA	SUB					CS SEGMENT OVERRIDE	DAS				
3	XOR					SS	AAA	CMP					DS	AAS				
4	INC					DEC												
5	PUSH					POP												
6	PUSHAD	POPAD	BOUND	ARPL	FS SEGMENT OVERRIDE	GS	OPERAND SIZE	ADDRESS SIZE	PUSH	IMUL	PUSH	IMUL	INS	OUTS				
7	JO	JNO	JB	JNB	JE	JNE	JBE	JA	JS	JNS	JPE	JPO	JL	JGE	JLE	JG		
8	ADD/ADC/AND/XOR OR/SBB/SUB/CMP					TEST	XCHG	MOV REG			MOV SREG	LEA	MOV SREG	POP				
9	NOP	XCHG EAX					CWD	CDQ	CALL	WAIT	PUSHFD	POPFD	SAHF	LAHF				
A	MOV EAX			MOVS		CMPS	TEST	STOS		LODS		SCAS						
B	MOV																	
C	SHIFT IMM	RETN		LES	LDS	MOV IMM	ENTER	LEAVE	RETF		INT3	INT IMM	INTO	IRETD				
D	SHIFT 1		SHIFT CL		AAM	AAD	SALC	XLAT	FPU									
E	LOOPNZ	LOOPZ	LOOP	JECXZ		IN IMM	OUT IMM	CALL	JMP	JMPF	JMP SHORT	IN DX		OUT DX				
F	LOCK EXCLUSIVE ACCESS	ICE BP	REPNE	REPE CONDITIONAL REPETITION	HLT	CMC	TEST/NOT/NEG [i]MUL/[i]DIV		CLC	STC	CLI	STI	CLD	STD	INC DEC	INC/DEC CALL/JMP PUSH		

1 st	2 nd	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0		(L,S)JLDT (L,S)JSTR VER(R,W)	(L,S)JGDT (L,S)JIDT (L,S)JMSW	LAR	LSL			CLTS		INVD	WBINVD		UD2		NOP		
1		SSE{1,2,3}								Prefetch SSE7	HINT_NOP						
2		MOV CR/DR								SSE{1,2}							
3		WRMSR	RDTSC	RDMSR	RDPMC	SYSENTER	SYSEXIT		GETSEC SMX	MOVBE / THREE BYTE		THREE BYTE SSE4					
4		CMOV															
5		SSE{1,2}															
6		MMX, SSE2															
7		MMX, SSE{1,2,3}, VMX												MMX, SSE{2,3}			
8		JO	JNO	JB	JNB	JE	JNE	JBE	JA	JS	JNS	JPE	JPO	JL	JGE	JLE	JG
		Jcc SHORT															
9		SETO	SETNO	SETB	SETNB	SETE	SETNE	SETBE	SETA	SETS	SETNS	SETPE	SETPO	SETL	SETGE	SETLE	SETG
		SETcc															
A		PUSH FS	POP FS	CPUID	BT	SHLD				PUSH GS	POP GS	RSM	BTS	SHRD		*FENCE	IMUL
B		CMPXCHG	LSS	BTR	LFS	LGS	MOVZX		POPCNT	UD	BT BTS BTR BTC	BTC	BSF	BSR	MOVSX		
C		XADD	SSE{1,2}					CMPXCHG	BSWAP								
D		MMX, SSE{1,2,3}															
E		MMX, SSE{1,2}															
F		MMX, SSE{1,2,3}															

Arithmetic & Logic	Prefix
Memory	System & I/O
Stack	No Operation (NOP) / Multiple Instructions / Extended Instruction Set
Control Flow & Conditional	



mod	00	01	10	11
r/m	16bit	32bit	16bit	32bit
000	[BX+SI] [EAX]	[BX+SI]+disp8	[EAX]+disp16	[EAX]+disp32
001	[BX+DI] [ECX]	[BX+DI]+disp8	[ECX]+disp16	[ECX]+disp32
010	[BP+SI] [EDX]	[BP+SI]+disp8	[EDX]+disp16	[EDX]+disp32
011	[BP+DI] [EBX]	[BP+DI]+disp8	[EBX]+disp16	[EBX]+disp32
100	[SI]	[SI]+disp8	[SI]+disp16	[SI]+disp32
101	[DI]	[DI]+disp8	[DI]+disp16	[DI]+disp32
110	[ESI]	[ESI]+disp8	[ESI]+disp16	[ESI]+disp32
111	[EDI]	[EDI]+disp8	[EDI]+disp16	[EDI]+disp32

encoding	scale (2bit)	Index (3bit)	Base (3bit)
000	2 ⁰ =1	[EAX]	EAX
001	2 ¹ =2	[ECX]	ECX
010	2 ² =4	[EDX]	EDX
011	2 ³ =8	[EBX]	EBX
100	--	none	ESP
101	--	[EBP]	disp32 / disp16 + [EBP] / disp32 + [EBP]
110	--	[ESI]	ESI
111	--	[EDI]	EDI

SIB value = index * scale + base