

נספח

פורמט פקודות מכונה 8086/8

ב-8086 גודל יצוג של פקודה היה מבית אחד עד ששה בתים.

פקודות מכונה בגודל בית

בדרך כלל פקודות על אופרנד אוגר 16 ביט אחד או ללא אופרנדים.

יצוג פקודות ללא אופרנדים הם פשוט מספר פקודה. הפקודות הללו הן:

XLAT, LAHF, SAHF, PUSHF, POPF, AAA, DAA, CLC, CMC, STC, CLD, STD, CLI,
STI, HLT, IRET, WAIT, RET (ללא אופרנד), INTO, INT3

חלק מהפקודות הפועלות על אופרנד אוגר 16 ביט כללי כמו INC, POP, PUSH
ממומשות בפורמט

7	6	5	4	3	2	1	0
O P C O D E				R E G			

כאשר REG הוא קידוד של האוגרים הכלליים מוגדר ע"י

REG	
000	AX
001	CX
010	DX
011	BX
100	SP
101	BP
110	SI
111	DI

הפקודות PUSH sr ו-POP sr כאשר sr הוא אחד מאוגרי הסגמנטים הם מהצורה

7	6	5	4	3	2	1	0
0	0	0	S	R	1	1	1

כאשר SR הוא קידוד של אוגרי הסגמנט, שימש אותנו גם בהמשך,

ES	0	0
CS	0	1
SS	1	0
DS	1	1

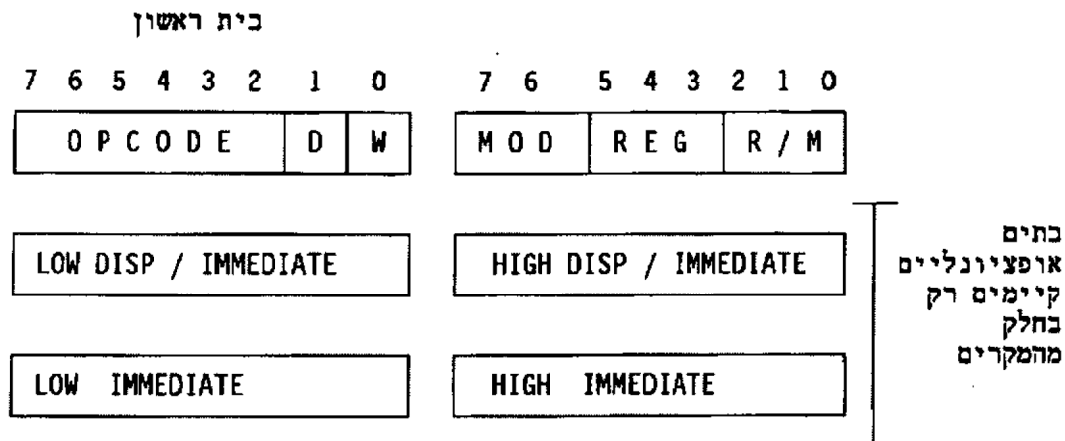
הפקודות IN AL,DX, IN AX,DX, OUT DX,AL, OUT DX,AX מממשות בפורמט:

7	6	5	4	3	2	1	0
Opcode7							W

כאשר $W == 0$ כאשר מדובר בפעולת ביט (AL)
 כאשר $W == 1$ כאשר מדובר בפעולת מילה (AX)

פקודות ארוכות יותר מבית אחד.

הפורמט הבא מתאר את מרבית פקודות המכונה של ה-8086/8:



המפתח לפענוח פקודות הארוכות יותר הם שני הבתים הראשונים:

6 הביטים הראשונים מאפינים את סוג הפקודה (ADD, MOV, ...)

ביט 0 (פקודות מכונה 2 אופרנדים בלבד):

אם D=1 שדה ה-REG בבית השני מצין את אופרנד היעד

אם D=0 שדה ה-REG בבית השני מצין את אופרנד מקור

במקרה של פעולות אוגר כללי - אוגר כללי D=1

ביט W: W=0 מדובר הפעולת בית

W=1 מדובר הפעולת מילה

הערות:

- בפקודות אריתמטיות עם קבועים (למשל CMP AX,-6, ADD CX,121) ביט ה-D נקרא S והוא מצין אם להרחיב קבוע 8 ביט ל-16 ביט תוך התחשבות בסימן. S=0 אין התחשבות בסימן. S=1 הרחבה תוך התחשבות בסימן אם W=1.

- בפקודות הזזה הביטיות ביט ה-D נקרא V והוא משמש להכדיל בין גירסאות ההזזה הבודדת של הפקודות הללו לבין הגירסאות המצינות את ההזזה ב-CL, למשל להבחין בין הפקודה SHL AX,1 לבין SHL AX,CL. V==0 הזזה בודדת. V==1 הזזה לפי CL.

- בפקודות LOOPE, LOOPNE ופקידומות REPE, REPNE ביט ה-W נקרא Z והוא משמש לאבחנה של התנאי הנוסף מעבר ל- $CX > 0$ להסתעפות:
 $Z == 0 <==> LOOPNE$ או $REPNE$
 $Z == 1 <==> LOOPE$ או $REPE$

בית 2 בפקודה

MOD - 2 ביטים המבדילים בין מיעון זיכרון ואוגרים ובמקרה של זיכרון מצינים כמה בתים של הזזה (Displacement) באים לאחר בית זה.

REG (פקודות 2 אופרנדים בלבד) - 3 ביטים המצינים שדה אוגר.

R/M - 3 ביטים שיחד עם ה-MOD קובעים את שיטת המיעון

זיכרון	[	00 אין Displacement == MOD
		01 Displacement של בית אחד
		10 Displacement של שני בתים

11 פעולת אוגר- אוגר

REG - יחד עם ביט ה-W בוחר את האוגר:

REG	W==0	W==1
000	AL	AX
001	CL	CX
010	DL	DX
011	BL	BX
100	AH	SP
101	CH	BP
110	DH	SI
111	BH	DI

בפקודות MOV שמעורבות בהם אוגרי הסגמנטים, השימוש ב-REG יהיה לפי הסדרמט:

7	6	5	4	3	2	1	0
MOD		0	SR		R / M		

כאשר SR הוא הקידוד של אוגרי הסגמנטים שתואר קודם.

הוראות שבהם יש אופרנד אחד (למשל INC AL, INC BL, NOT AX, INC WORD PTR [BX]) או אופרנד מתפרש אחד (MUL, DIV) או פקודות 2 אופרנדים שאחד מהם קבוע (למעט כאשר AX או AL הם האופרנד השני) משתמשים בביטים בשדה ה-REG כהשלמה ל-opcode. כלומר יש לו משמעויות אחרות.

R/M - מצין את המיעון יחד עם ה-MOD כמתואר להלן :

R/M	MOD 11				
	MOD==00	MOD==01	MOD==10	W==0	W==1
000	BX+SI	BX+SI+DISP8	BX+SI+DISP16	AL	AX
001	BX+DI	BX+DI+DISP8	BX+DI+DISP16	CL	CX
010	BP+SI	BP+SI+DISP8	BP+SI+DISP16	DL	DX
011	BP+DI	BP+DI+DISP8	BP+DI+DISP16	BL	BX
100	SI	SI+DISP8	SI+DISP16	AH	SP
101	DI	DI+DISP8	DI+DISP16	CH	BP
110	Direct Address	BP+DISP8	BP+DISP16	DH	SI
111	BX	BX+DISP8	BX+DISP16	BH	DI

Direct Address - הכתובת נלקחת ישיר משני הבתים אחרי בית שיטת המיון .

התיחסות טהורה ל-BP (למשל MOV [BP],AX) ממומשת כהתיחסות דרך [BP+0] כלומר displacement 0 בגודל בית. ממילא השימוש שהאוגר BP נועד לו מכתוב שזמנתי ואין צורך בגרסה הזו.

בתים מקדימים Prefix bytes

לחלק מהפקודות (מכל הפורמטים) ישנם אופציות של בתים מקדימים prefix bytes משני סוגים: Instruction Prefix ו- Segment Override. הדבר יכול להגדיל יצוג של פקודת מכונה בעד 2 בתים. לפיכך הגודל המירבי של פקודת מכונה ב-8086 הוא 8 בתים.

האפשרויות של Instruction Prefix הן

F3h = 1111 0011b REP prefix (פקודות מחזוריות בלבד)
F3h = 1111 0011b REPE / REPZ prefix
(פקודות מחזוריות בלבד)
F2h = 1111 0010b REPNE / REPZ prefix
(פקודות מחזוריות בלבד)
F0h = 1111 0010b LOCK prefix

האפשרויות של Segment Override הן

26h - 0010 0110b - ES segment override prefix
2Eh - 0010 1110b - CS segment override prefix
36h - 0011 0110b - SS segment override prefix
3Eh - 0011 1110b - DS segment override prefix

מיעון בשיטת Segment Override

כאשר בפקודת היתחסות לזיכרון יש Segment Override (למעט DS) מופיע לפני הפקודה בית מיוחד המצין ל-CPU לבחור אוגר סגמנט אחר מכרירת המחדל (DS למעט כאשר BP מופיע אז נבחר SS). לאחר מכן תופיע הפקודה כמו קודם.

הערכים של ה-Segment Override נבדלים ב-2 הביטים האמצעיים:

	SR	
ES: 26h = 0 0 1 0 0 1 1 0	(0 0)	
CS: 2Eh = 0 0 1 0 1 1 1 0	(0 1)	
SS: 36h = 0 0 1 1 0 1 1 0	(1 0)	
DS: 3Eh = 0 0 1 1 1 1 1 0	(1 1)	

פקודות נוספת שאינן לפי הפורמט הנ"ל

פקודות 2 אופרנדים בין קבוע כאפרנד מקור והאוגר AX או AL כאפרנד יעד
(למשל ADD AX,7 MOV AL,9 אבל גם פקודות קלט/פלט עם קבוע למשל OUT 60h,AL)
הם מהפורמט

7 6 5 4 3 2 1 0

Opcode7	W	Const
---------	---	-------

כאשר W משמש להבדיל בין פעולת בית למילה, כמו קודם.
Const יכול להיות בית או מילה, למעט פקודות קלט/פלט (בית כלבוד).

פקודות ההסתעפות (עם אופרנד RET, INT, JE, CALL, JMP), למעט הסתעפויות עקיפות, הם לפי הפורמט:

Opcode8 Const

כאשר Const הוא קבוע בגודל בית אחד לארבעה.

בפקודות ההסתעפות מותנה Const תמיד בית אחד.

פקודה בעלת מבנה מיוחד

ESC -	11011 XXX	MOD YYY R/M	Disp-Low	Disp-High
-------	-----------	-------------	----------	-----------

דוגמאות

הפקודה ADD AX,BX מקודדת בהקסה: 03 C3

כבינארי

Opcode	D W	MOD	R	E	G	R/M
0 0 0 0	0 0 1 1	1 1	0 0	0 0	1 1	

הפקודה MOV BX,AX מקודדת בהקסה: 8B D8

בבינארי

Opcode	D W	MOD	R E G	R/M
1 0 0 0	1 0 1 1	1 1 0 1	1 0 0 0	

הפקודה MOV AL,CH מקודדת בהקסה: 8A C5

בבינארי

Opcode	D W	MOD	R E G	R/M
1 0 0 0	1 0 1 0	1 1 0 0	0 1 0 1	

הפקודה MOV AX,[BX] מקודדת בהקסה: 8B 07

בבינארי

Opcode	D W	MOD	R E G	R/M
1 0 0 0	1 0 1 1	0 0 0 0	0 1 1 1	

הפקודה MOV CX,SS:[BX+DI] מקודדת בהקסה: 36 8B 09

בבינארי

Prefix	Opcod	D W	MOD	R E G	R/M
0 0 1 1 0 1 1 0	1 0 0 0	1 0 1 1	0 0 0 0	1 0 0 1	

יצירת דוגמאות נוספות

כתוב תוכנית חוקית מבחינת השפה באסמבלי (היא לא חייבת לרוץ) והרץ עליה את tasm עם האופציה /la. תקבל קובץ lst. עם פירוט הקידוד בהקסה.

לדוגמא הפקודה:

tasm /la myprog1.asm

תיצור קובץ בשם myprog1.lst שאותו תוכל לקרוא בתוכנית editor. ליד הפקודות תראה את פירוט הקידוד הבינארי: היסטרי הפקודות ותוכנם.

מספר שורה	היסט	קידוד	הפקודה באסמבלי
		בהקסה	
32	0028	03 C3	ADD AX, BX
33	002A	2B C3	SUB AX, BX
34	002C	8B 90 0080	MOV DX, [BX+SI+80h]
35	0030	8B 90 4000	MOV DX, [BX+SI+4000h]
36	0034	8B 07	MOV AX, [BX]
37	0036	B8 0040	MOV AX, 64
38	0039	B9 0080	MOV CX, 128
39	003C	8B 46 06	MOV AX, [BP+6]
40	003F	2E: 8B 5D 06	MOV BX, CS:[DI+6]
41	0043	2E: 8B 07	MOV AX, ES:[BX]
42	0046	3E: 8B 07	MOV AX, SS:[BX]
43	0049	2E: 8B 07	MOV AX, CS:[BX]
44	004C	2E: 8B 07	MOV AX, ES:[BX]
45	004F	42	INC DX
46	0050	FE 00	INC BYTE PTR [BX+SI]
47	0052	FF 00	INC WORD PTR [BX+SI]
48	0054	03 14	ADD DX, [SI]
49	0056	03 14	ADD DX, DS:[SI]

פורמט פקודות מכונה 386 ואילך

שפת המכונה של ה-386 הוא באופן כללי הרחבה של שפת המכונה של ה-8086/8. ה-386 מכיר את פקודות המכונה בפורמט הישן ובנוסף יש לו פקודות מכונב נוספות בפורמט דומה עבור האוגרים 32 ביט. הפורמט של רוב הפקודות (כולל בעצם פקודות 8086) הוא

Instruction prefix	Address size prefix	Opereand size prefix	Segment Override
0 או 1	0 או 1	0 או 1	0 או 1
מספר הבתים			

MODR/M byte			
MOD	REG\Opcode	R/M	Opcode
0 או 1			1 או 2
מספר בתים			

SIB (Scale Index Base) byte				
SS	Index	Base	Displacement	Immediate
0 או 1			0,1,2 או 4	0,1,2 או 4
מספר בתים				

לפיכך אפשר להסיק שהאורך המירבי של פקודת מכונה ב-386 ואילך היא 16 בתים.

ערכים אפשריים ל-Instruction Prefix

F3h = 1111 0011b	REP prefix (פקודות מחזורות בלבד)
F3h = 1111 0011b	REPE / REPZ prefix (פקודות מחזורות בלבד)
F2h = 1111 0010b	REPNE / REPNZ prefix (פקודות מחזורות בלבד)
F0h = 1111 0010b	LOCK prefix

ערכים אפשריים ל- Size prefix

66h = 0110 0110b Operand size prefix

67h = 0110 0110b Address size prefix

ערכים אפשריים ל- Segment override

2Eh - 0010 1110b - CS segment override prefix

36h - 0011 0110b - SS segment override prefix

3Eh - 0011 1110b - DS segment override prefix

26h - 0010 0110b - ES segment override prefix

64h - 0110 0100b - FS segment override prefix

65h - 0110 0101b - GS segment override prefix

אם הפקודה מכילה את ה-Operand size prefix פירושו שהפעולה היא בגודל 32 ביט (אוגר EAX, EBX ... או זכרון 32 ביט).
אם הפקודה מכילה את ה-Operand address prefix פירושו שההיסט בחישוב הכתובת הוא 32 ביט (אוגר $EAX+4*EBX$ וכו').

קידוד אוגרים

השדות REG, INDEX ו-BASE הינם קודים של אוגרים, וגם R/M הוא כזה בתנאים מסוימים. בפקודות שמתקבלים בירושה מה-8086 הם קודים של אוגרים 8 ו-16 ביט. במידה ובפקודה מופיעה ה-Operand size prefix או ה-Address size prefix, השדות הללו יקודדו את האוגרים 32 ביט. זה קצת משתנה לפי אם מדובר ביצוג יעד או אפשרות של היסט, אבל באופן עקרוני הקידוד של האוגרים 32 ביט הינו

קוד	אוגר
000	EAX
001	ECX
010	EDX
011	EBX
100	ESP
101	EBP
110	ESI
111	EDI

בית ה-SIB

הבית הזה מופיע כאשר בחישוב היסט 32 ביט יש scale (2,4,8) factor ליד אוגר האינדקס ו/או כאשר בחישוב ההיסט הזה יש 2 אוגרים 32 ביט.

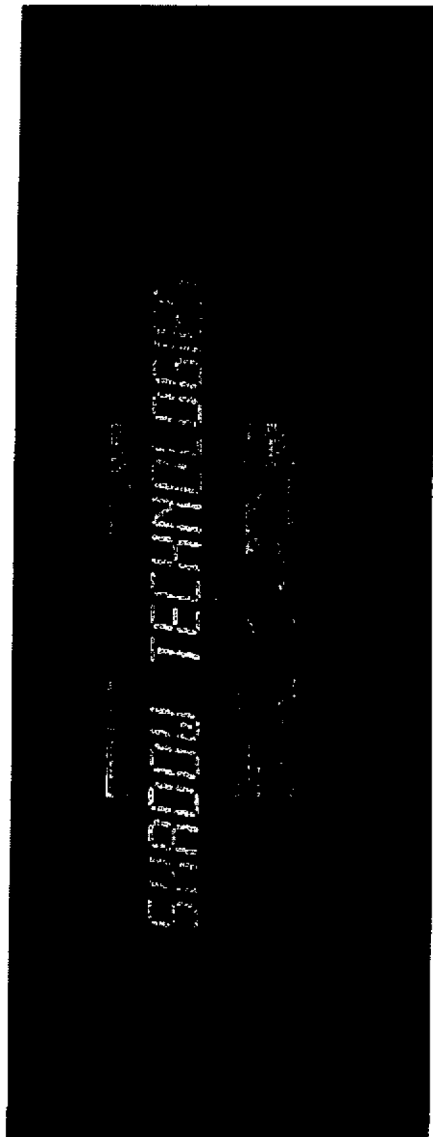
שרה ה-Base הוא קידוד של אוגר האינדקס לפי הטבלה שלעיל למעט 101 שיש לו שלושה פירושים שונים (שניים מהם כוללים את ה-EBP)

בתלות ב-MOD.

שדה ה-Index הוא קידוד של אוגר האינדקס לפי הטבלה שלעיל למעט
100 שאינו נחשב לקידוד של ESP (שאיננו יכול להיות אוגר אינדקס,
רק בסיס).

שדה ה-SS הוא מגויר למעשה ה-scale factor, הוא החזקה של 2 של
המקדם של המכפלה של אוגר האינדקס

SS
00 - 1*,
01 - 2*,
10 - 4*,
11 - 8*.



274

8086/8088 Assembly Language Programming

Assembly/Machine Language Coding

Data Transfer

Arithmetic

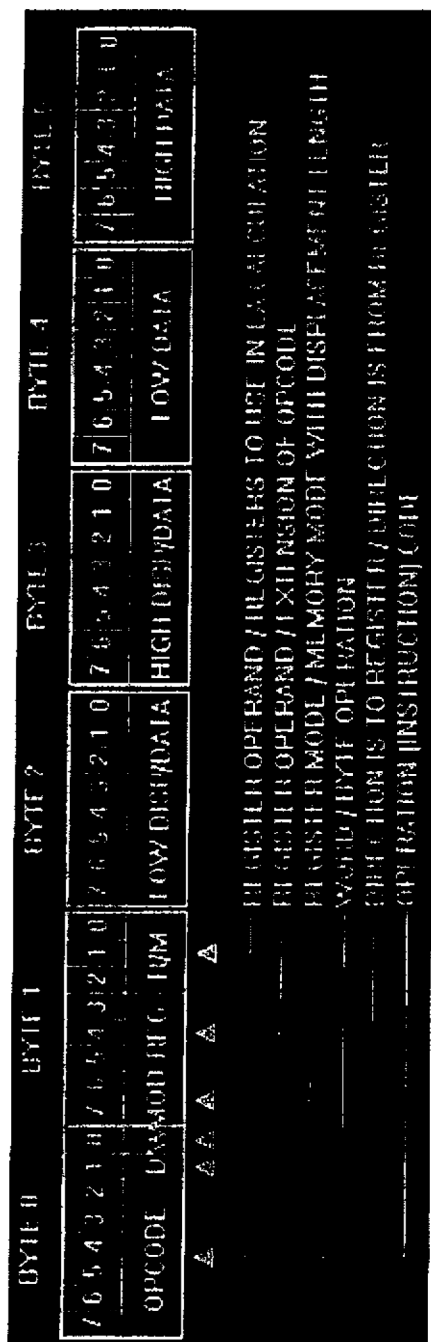
Logic

String Manipulation

Control Transfer

Processor Control

Machine Language Encoding Derivatives



MODE 11		R11 + R11 ADDRESS CALCULATION			
R/M	VAL	VAL	MOD-ES	MOD-ES	MODE 11
000	R1	000	0000 + 000	0000 + 000 + 00	0000 + 000 + 000
001	R1	000	0000 + 000	0000 + 000 + 00	0000 + 000 + 000
010	R1	000	0000 + 000	0000 + 000 + 00	0000 + 000 + 000
011	R1	000	0000 + 000	0000 + 000 + 00	0000 + 000 + 000
100	R1	000	0000 + 000	0000 + 000 + 00	0000 + 000 + 000
101	R1	000	0000 + 000	0000 + 000 + 00	0000 + 000 + 000
110	R1	000	0000 + 000	0000 + 000 + 00	0000 + 000 + 000
111	R1	000	0000 + 000	0000 + 000 + 00	0000 + 000 + 000

R/M	VAL	VAL
000	R1	000
001	R1	000
010	R1	000
011	R1	000
100	R1	000
101	R1	000
110	R1	000
111	R1	000

MOD-ES	MOD-ES
000	0000 + 000 + 00
001	0000 + 000 + 00
010	0000 + 000 + 00
011	0000 + 000 + 00
100	0000 + 000 + 00
101	0000 + 000 + 00
110	0000 + 000 + 00
111	0000 + 000 + 00

MOD-ES	MOD-ES
000	0000 + 000 + 00
001	0000 + 000 + 00
010	0000 + 000 + 00
011	0000 + 000 + 00
100	0000 + 000 + 00
101	0000 + 000 + 00
110	0000 + 000 + 00
111	0000 + 000 + 00

Field	Value	Unit	Group
1	200	cm	200
2	100	cm	100
3	50	cm	50
4	25	cm	25
5	12.5	cm	12.5
6	6.25	cm	6.25
7	3.125	cm	3.125
8	1.5625	cm	1.5625
9	0.78125	cm	0.78125
10	0.390625	cm	0.390625
11	0.1953125	cm	0.1953125
12	0.09765625	cm	0.09765625
13	0.048828125	cm	0.048828125
14	0.0244140625	cm	0.0244140625
15	0.01220703125	cm	0.01220703125
16	0.006103515625	cm	0.006103515625
17	0.0030517578125	cm	0.0030517578125
18	0.00152587890625	cm	0.00152587890625
19	0.000762939453125	cm	0.000762939453125
20	0.0003814697265625	cm	0.0003814697265625
21	0.00019073486328125	cm	0.00019073486328125
22	9.5367431640625e-05	cm	9.5367431640625e-05
23	4.76837158203125e-05	cm	4.76837158203125e-05
24	2.384185791015625e-05	cm	2.384185791015625e-05
25	1.1920928955078125e-05	cm	1.1920928955078125e-05
26	5.9604644775390625e-06	cm	5.9604644775390625e-06
27	2.980232238769531e-06	cm	2.980232238769531e-06
28	1.4901161193847656e-06	cm	1.4901161193847656e-06
29	7.450580596923828e-07	cm	7.450580596923828e-07
30	3.725290298461914e-07	cm	3.725290298461914e-07
31	1.862645149230957e-07	cm	1.862645149230957e-07
32	9.313225746154785e-08	cm	9.313225746154785e-08
33	4.656612873077392e-08	cm	4.656612873077392e-08
34	2.328306436538696e-08	cm	2.328306436538696e-08
35	1.164153218269348e-08	cm	1.164153218269348e-08
36	5.82076609134674e-09	cm	5.82076609134674e-09
37	2.91038304567337e-09	cm	2.91038304567337e-09
38	1.455191522836685e-09	cm	1.455191522836685e-09
39	7.275957614183425e-10	cm	7.275957614183425e-10
40	3.637978807091712e-10	cm	3.637978807091712e-10
41	1.818989403545856e-10	cm	1.818989403545856e-10
42	9.09494701772928e-11	cm	9.09494701772928e-11
43	4.54747350886464e-11	cm	4.54747350886464e-11
44	2.27373675443232e-11	cm	2.27373675443232e-11
45	1.13686837721616e-11	cm	1.13686837721616e-11
46	5.6843418860808e-12	cm	5.6843418860808e-12
47	2.8421709430404e-12	cm	2.8421709430404e-12
48	1.4210854715202e-12	cm	1.4210854715202e-12
49	7.105427357601e-13	cm	7.105427357601e-13
50	3.5527136788005e-13	cm	3.5527136788005e-13
51	1.77635683940025e-13	cm	1.77635683940025e-13
52	8.88178419700125e-14	cm	8.88178419700125e-14
53	4.440892098500625e-14	cm	4.440892098500625e-14
54	2.2204460492503125e-14	cm	2.2204460492503125e-14
55	1.1102230246251562e-14	cm	1.1102230246251562e-14
56	5.551115123125781e-15	cm	5.551115123125781e-15
57	2.7755575615628905e-15	cm	2.7755575615628905e-15
58	1.3877787807814452e-15	cm	1.3877787807814452e-15
59	6.938893903907226e-16	cm	6.938893903907226e-16
60	3.469446951953613e-16	cm	3.469446951953613e-16
61	1.7347234759768065e-16	cm	1.7347234759768065e-16
62	8.673617379884032e-17	cm	8.673617379884032e-17
63	4.336808689942016e-17	cm	4.336808689942016e-17
64	2.168404344971008e-17	cm	2.168404344971008e-17
65	1.084202172485504e-17	cm	1.084202172485504e-17
66	5.42101086242752e-18	cm	5.42101086242752e-18
67	2.71050543121376e-18	cm	2.71050543121376e-18
68	1.35525271560688e-18	cm	1.35525271560688e-18
69	6.7762635780344e-19	cm	6.7762635780344e-19
70	3.3881317890172e-19	cm	3.3881317890172e-19
71	1.6940658945086e-19	cm	1.6940658945086e-19
72	8.470329472543e-20	cm	8.470329472543e-20
73	4.2351647362715e-20	cm	4.2351647362715e-20
74	2.11758236813575e-20	cm	2.11758236813575e-20
75	1.058791184067875e-20	cm	1.058791184067875e-20
76	5.293955920339375e-21	cm	5.293955920339375e-21
77	2.6469779601696875e-21	cm	2.6469779601696875e-21
78	1.3234889800848437e-21	cm	1.3234889800848437e-21
79	6.617444900424219e-22	cm	6.617444900424219e-22
80	3.3087224502121095e-22	cm	3.3087224502121095e-22
81	1.6543612251060547e-22	cm	1.6543612251060547e-22
82	8.271806125530274e-23	cm	8.271806125530274e-23
83	4.135903062765137e-23	cm	4.135903062765137e-23
84	2.0679515313825685e-23	cm	2.0679515313825685e-23
85	1.0339757656912842e-23	cm	1.0339757656912842e-23
86	5.169878828456421e-24	cm	5.169878828456421e-24
87	2.5849394142282105e-24	cm	2.5849394142282105e-24
88	1.2924697071141052e-24	cm	1.2924697071141052e-24
89	6.462348535570526e-25	cm	6.462348535570526e-25
90	3.231174267785263e-25	cm	3.231174267785263e-25
91	1.6155871338926315e-25	cm	1.6155871338926315e-25
92	8.077935669463157e-26	cm	8.077935669463157e-26
93	4.0389678347315785e-26	cm	4.0389678347315785e-26
94	2.0194839173657892e-26	cm	2.0194839173657892e-26
95	1.0097419586828946e-26	cm	1.0097419586828946e-26
96	5.048709793414473e-27	cm	5.048709793414473e-27
97	2.5243548967072365e-27	cm	2.5243548967072365e-27
98	1.2621774483536182e-27	cm	1.2621774483536182e-27
99	6.310887241768091e-28	cm	6.310887241768091e-28
100	3.1554436208840455e-28	cm	3.1554436208840455e-28

DATA TRANSFER

MOV = Move

Register/Memory to/from register

Immediate to register/meory

Immediate to register

Memory to accumulator

Accumulator to memory

Register/Memory to segment register
Segment Register to register/Memory

PUSH = PUSH

Register/Memory

Register

Segment register

$$\overline{POP} = POP$$

Register/Memory

Register

Segment register

XCHG = Exchange

Register/memory with register

Register with accumulator

100010d	w	mod reg	r/m	Disp-Lo	Disp-Hi
11000011	w	mod 000	r/m	Disp-Lo	Disp-Hi
1011w	reg	Data	Data if w=1		
10100000	w	Addr-Lo	Addr-Hi		
10100001	w	Addr-Lo	Addr-Hi		
10000111	0	mod 0	SR r/m	Disp-Lo	Disp-Hi
10000110	0	mod 0	SR r/m	Disp-Lo	Disp-Hi

```
11111111|mod 110 r/m|Disp-Lo|Disp-Hi
01010reg
000SR110
```

```
111111111|mod 110 r/m|Disp-Lo|Disp-Hi
01011reg
000SR111
```

```
1000011w|mod reg r/m|Disp-Lo|Disp-Hi
10010reg
```

IN = Input from

Fixed Port

Variable Port

1110010w|Data-8
1110110w

Out = Output to

Fixed port

Variable port

1110011w|Data-8
1110111w

XLAT = Table lookup to al

LEA = Load EA to register

LDS = Load Pointer to DS

LES = Load Pointer to ES

LAHF = Load AH with Flags

SAHF = Store AH into Flags

PUSHF = Push flags

POPF = Pop flags

11010111
10001101|mod reg r/m|Disp-Lo|Disp-Hi
11000101|mod reg r/m|Disp-Lo|Disp-Hi
11000100|mod reg r/m|Disp-Lo|Disp-Hi
10011111
10011110
10011100
10011101

ARITHMETIC

Add = add

Reg/memory with register to either

Immediate to register/memory

Immediate to accumulator

000000dw|mod reg r/m|Disp-Lo|Disp-Hi
100000sw|mod 000 r/m|Disp-Lo|Disp-Hi|Data if s:w=01
0001010w|Data|Data if w=1

ADC = Add with carry

Reg/Memory with register to either

Immediate to register/memory

Immediate to accumulator

000100dw|mod reg r/m|Disp-Lo|Disp-Hi
100000sw|mod 010 r/m|Disp-Lo|Disp-Hi|Data if s:w=01
0001010w|Data|Data if w=1

INC = Increment

Register/Memory

Register

1111111w|mod 000 r/m|Disp-Lo|Disp-Hi
01000reg

AAA = Ascii adjust for add

DAA = Decimal adjust for add

00110111
00100111

SUB = Subtract

Reg/memory and register to either
Immediate from register/memory
Immediate from accumulator

001010dw|mod reg r/m|Disp-Lo|Disp-Hi
100000sw|mod 101 r/m|Disp-Lo|Disp-Hi|Data if s:w=01
0010110w|Data|Data if w=1

SBB = Subtract with borrow

Reg/memory and register to either
Immediate from register/memory
Immediate from accumulator

000110dw|mod reg r/m|Disp-Lo|Disp-Hi
100000sw|mod 011 r/m|Disp-Lo|Disp-Hi
0001110w|Data|Data if w=1

DEC = Decrement

Register/memory
Register

1111111w|mod 001 r/m|Disp-Lo|Disp-Hi
01001reg

NEG = Change signCMP = Compare

Register/memory and register
Immediate with register/memory
Immediate with accumulator

001110dw|mod reg r/m|Disp-Lo|Disp-Hi
100000sw|mod 111 r/m|Disp-Lo|Disp-Hi|Data if s:w=1
0011110w|Data

AAS = Ascii adjust for subtract
DAS = Decimal adjust for subtract
MUL = Multiply(unsigned)
IMUL = Integer multiply(signed)
AAM = Ascii adjust for multiply
DIV = Divide(unsigned)
IDIV = Integer Divide(Signed)
AAD = Ascii Adjust for divide
CWD = Convert byte to word
CQD = Convert word to doubleword

00111111
00101111
1111011w|mod 100 r/m|Disp-Lo|Disp-Hi
1111011w|mod 101 r/m|Disp-Lo|Disp-Hi
11010100|00001010|Disp-Lo|Disp-Hi
1111011w|mod 110 r/m|Disp-Lo|Disp-Hi
1111011w|mod 111 r/m|Disp-Lo|Disp-Hi
11010101|00001010|Disp-Lo|Disp-Hi
10011000
10011001

LOGIC

NOT = Invert
SHL/SAL = Shift logical/arithmetic left
SHR = Shift logical right
SAR = Shift arithmetic right

1111011w|mod 010 r/m|Disp-Lo|Disp-Hi
110100vw|mod 100 r/m|Disp-Lo|Disp-Hi
110100vw|mod 101 r/m|Disp-Lo|Disp-Hi
110100vw|mod 111 r/m|Disp-Lo|Disp-Hi

278

<u>ROL</u>	= Rotate left	110100vw mod 000 r/m Disp-Lo Disp-Hi
<u>ROR</u>	= Rotate right	110100vw mod 001 r/m Disp-Lo Disp-Hi
<u>RCL</u>	= Rotate through carryf left	110100vw mod 010 r/m Disp-Lo Disp-Hi
<u>RCR</u>	= Rotate through carryf right	110100vw mod 011 r/m Disp-Lo Disp-Hi
<u>AND</u>	= Boolean AND	
Reg/memory with register to either		
Immediate to register/memory		
Immediate to accumulator		
<u>TEST</u>	= And function to flags no result	
Register/memory and register		
Immediate data and register memory		
Immediate and accumulator		
<u>OR</u>	= Boolean OR	
Reg/Memory and register to either		
Immediate to register memory		
Immediate to accumulator		
<u>XOR</u>	= Exclusive Boolean OR	
Reg/memory and register to either		
Immediate to register/memory		
Immediate to accumulator		

STRING MANIPULATION

<u>REP</u>	= Repeat	1111001z
<u>MOVS</u>	= Move byte/word	1010010w
<u>CMPS</u>	= Compare byte/word	1010011w
<u>SCAS</u>	= Scan byte/word	1010111w
<u>LODS</u>	= Load byte/word to AL/AX	1010110w
<u>STDS</u>	= Store byte/word from AL/AX	1010101w

CONTROL TRANSFER

CALL = Call

Direct within segment

Indirect within segment

Direct intersegment

Indirect intersegment

RET = Return from call

Within segment

Within segment adding immediate to SP

Intersegment

Intersegment adding immediate to SP

JE/JZ = Jump equal/zero

JL/JNGE = Jump less/not greater-equal

JLE/JNG = Jump less or equal/not greater

JBE/JNAE = Jump below/not above equal

JBE/JNA = Jump below equal/not above

JP/JPE = Jump parity/parity even

JO = Jump on overflow

JS = Jump on sign

JNE/JNZ = Jump not equal/not zero

JNL/JGE = Jump not less/greater or equal

JNLE/JG = Jump not less equal/greater

JNB/JAE = Jump not below/above or equal

JNBE/JA = Jump not below or equal/above

JNP/JPO = Jump not parity/parity odd

JNO = Jump not overflow

JNS = Jump not sign

JCXZ = Jump on CX zero

JMP = Unconditional Jump

Direct within segment

Direct within segment-short

Indirect within segment

Direct intersegment

Indirect intersegment

LOOP

= Loop CX times

LOOPZ/LOOPE

= Loop while zero/equal

LOOPNZ/LOOPNE

= Loop not zero/equal

11101000|IP-INC-LO|IP-INC-HI
11111111|mod 010 r/m|Disp-Lo|Disp-Hi
10011010|IP-Lo|IP-Hi|CS-Lo|CS-HI
11111111|mod 011 r/m|Disp-Lo|Disp-Hi

11000011
11000010|Data-Lo|Data-Hi
11001011
11001010|Data-Lo|Data-Hi

01110100|IP-INC8
01111100|IP-INC8
01111110|IP-INC8
01110010|IP-INC8
01110110|IP-INC8
01111010|IP-INC8
01110000|IP-INC8
01111000|IP-INC8
01110101|IP-INC8
01111101|IP-INC8
01111111|IP-INC8
01110011|IP-INC8
01110111|IP-INC8
01111011|IP-INC8
01110001|IP-INC8
01111001|IP-INC8
11100011|IP-INC8

11101001|IP-INC-LO|IP-INC-HI
11101011|IP-INC8
11111111|mod 100 r/m|Disp-Lo|Disp-Hi
11101010|IP-Lo|IP-Hi|CS-Lo|CS-HI
11111111|mod 101 r/m|Disp-Lo|Disp-Hi

11100010|IP-INC8
11100001|IP-INC8
11100000|IP-INC8

280

INT = Interrupt

Type specified

INT3 11001101 | Data-8
INTO = Interrupt on overflow 11001100
IRET = Interrupt return 11001110
11001111

PROCESSOR CONTROL

CLC = Clear carry 11111000
CMC = Complement carry 11110101
STC = Set carry 11111001
CLD = Clear direction 11111100
STD = Set direction 11111101
CLI = Clear interrupt 11111010
STI = Set interrupt 11111011
HLT = Halt 11110100
WAIT = wait 10011011
ESC = Escape to external device 11011xxx | mod yyy r/m | Disp-Lo | Disp-Hi
LOCK = Buss lock prefix 11110000
SEGMENT = Segment override prefix 001SR110

281

Table 26-2. 16-Bit Addressing Forms with the ModR/M Byte

r8(r) r16(r) r32(r) /digit (Opcode) REG =			AL AX EAX 0 000	CL CX ECX 1 001	DL DX EDX 2 010	BL BX EBX 3 011	AH SP ESP 4 100	CH BP EBP 5 101	DH SI ESI 6 110	BH DI EDI 7 111
Effective Address	Mod R/M		ModR/M Values 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		110	06	0E	16	1E	26	2E	36	3E
[BX]		111	07	0F	17	1F	27	2F	37	3F
[BX + SI] + disp8	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	5B	63	6B	73	7B
[SI] + disp8		100	44	4C	54	5C	64	6C	74	7C
[DI] + disp8		101	45	4D	55	5D	65	6D	75	7D
[BP] + disp8		110	46	4E	56	5E	66	6E	76	7E
[BX] + disp8		111	47	4F	57	5F	67	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	11	000	C0	C8	D0	D8	E0	E8	F0	F8
ECX/CX/CL		001	C1	C9	D1	D9	E1	E9	F1	F9
EDX/DX/DL		010	C2	CA	D2	DA	E2	EA	F2	FA
EBX/BX/BL		011	C3	CB	D3	DB	E3	EB	F3	FB
ESP/SP/AH		100	C4	CC	D4	DC	E4	EC	F4	FC
EBP/BP/CH		101	C5	CD	D5	DD	E5	ED	F5	FD
ESI/SI/DH		110	C6	CE	D6	DE	E6	EE	F6	FE
EDI/DI/BH		111	C7	CF	D7	DF	E7	EF	F7	FF

NOTES: **disp8** denotes an 8-bit displacement following the ModR/M byte, to be sign-extended and added to the index. **disp16** denotes a 16-bit displacement following the ModR/M byte, to be added to the index. Default segment register is SS for the effective addresses containing a BP index, DS for other effective addresses.

Table 28-3. 32-Bit Addressing Forms with the ModR/M Byte

r8(/r) r16(/r) r32(/r) /digit (Opcode) REG =			AL AX EAX 0 000	CL CX ECX 1 001	DL DX EDX 2 010	BL BX EBX 3 011	AH SP ESP 4 100	CH BP EBP 5 101	DH SI ESI 6 110	BH DI EDI 7 111
Effective Address	Mod R/M		ModR/M Values in Hexadecimal							
[EAX] [ECX] [EDX] [EBX] [--][--] ¹ disp32 [ESI] [EDI]	00	000	00	08	10	18	20	28	30	38
		001	01	09	11	19	21	29	31	39
		010	02	0A	12	1A	22	2A	32	3A
		011	03	0B	13	1B	23	2B	33	3B
		100	04	0C	14	1C	24	2C	34	3C
		101	05	0D	15	1D	25	2D	35	3D
		110	06	0E	16	1E	26	2E	36	3E
		111	07	0F	17	1F	27	2F	37	3F
disp8[EAX] disp8[ECX] disp8[EDX] disp8[EBX]; disp8[--][--] disp8[EBP] disp8[ESI] disp8[EDI]	01	000	40	48	50	58	60	68	70	78
		001	41	49	51	59	61	69	71	79
		010	42	4A	52	5A	62	6A	72	7A
		011	43	4B	53	5B	63	6B	73	7B
		100	44	4C	54	5C	64	6C	74	7C
		101	45	4D	55	5D	65	6D	75	7D
		110	46	4E	56	5E	66	6E	76	7E
		111	47	4F	57	5F	67	6F	77	7F
disp32[EAX] disp32[ECX] disp32[EDX] disp32[EBX] disp32[--][--] disp32[EBP] disp32[ESI] disp32[EDI]	10	000	80	88	90	98	A0	A8	B0	B8
		001	81	89	91	99	A1	A9	B1	B9
		010	82	8A	92	9A	A2	AA	B2	BA
		011	83	8B	93	9B	A3	AB	B3	BB
		100	84	8C	94	9C	A4	AC	B4	BC
		101	85	8D	95	9D	A5	AD	B5	BD
		110	86	8E	96	9E	A6	AE	B6	BE
		111	87	8F	97	9F	A7	AF	B7	BF
EAX/AX/AL ECX/CX/CL EDX/DX/DL EBX/BX/BL ESP/SP/AH EBP/BP/CH ESI/SI/DH EDI/DI/BH	11	000	C0	C8	D0	D8	E0	E8	F0	F8
		001	C1	C9	D1	D9	E1	E9	F1	F9
		010	C2	CA	D2	DA	E2	EA	F2	FA
		011	C3	CB	D3	DB	E3	EB	F3	FB
		100	C4	CC	D4	DC	E4	EC	F4	FC
		101	C5	CD	D5	DD	E5	ED	F5	FD
		110	C6	CE	D6	DE	E6	EE	F6	FE
		111	C7	CF	D7	DF	E7	EF	F7	FF

NOTES: ¹[--][--] means a SIB follows the ModR/M byte.

²disp8 denotes an 8-bit displacement following the SIB byte, to be sign-extended and added to the index. disp32 denotes a 32-bit displacement following the SIB byte, to be added to the index.

Intel.

INSTRUCTION SET

M Byte

CH	DH	BH
BP	SI	DI
EBP	ESI	EDI
5	6	7
101	110	111

decimal

28	30	38
29	31	39
2A	32	3A
2B	33	3B
2C	34	3C
2D	35	3D
2E	36	3E
2F	37	3F
68	70	78
69	71	79
6A	72	7A
6B	73	7B
6C	74	7C
6D	75	7D
6E	76	7E
6F	77	7F
A8	B0	B8
A9	B1	B9
AA	B2	BA
AB	B3	BB
AC	B4	BC
AD	B5	BD
AE	B6	BE
AF	B7	BF
E8	F0	F8
E9	F1	F9
EA	F2	FA
EB	F3	FB
EC	F4	FC
ED	F5	FD
EE	F6	FE
EF	F7	FF

32-bit extended and added to
to be added to the index.

Table 26-4. 32-Bit Addressing Forms with the SIB Byte

32-Bit Base =			EAX	ECX	EDX	EBX	ESP	[*]	ESI	EDI
Base =			0	1	2	3	4	5	6	7
Base =			000	001	010	011	100	101	110	111
Scaled Index	SS Index		SIB Values in Hexadecimal							
[EAX]	00	000	00	01	02	03	04	05	06	07
[ECX]		001	08	09	0A	0B	0C	0D	0E	0F
[EDX]		010	10	11	12	13	14	15	16	17
[EBX]		011	18	19	1A	1B	1C	1D	1E	1F
none		100	20	21	22	23	24	25	26	27
[EBP]		101	28	29	2A	2B	2C	2D	2E	2F
[ESI]		110	30	31	32	33	34	35	36	37
[EDI]		111	38	39	3A	3B	3C	3D	3E	3F
[EAX*2]	01	000	40	41	42	43	44	45	46	47
[ECX*2]		001	48	49	4A	4B	4C	4D	4E	4F
[EDX*2]		010	50	51	52	53	54	55	56	57
[EBX*2]		011	58	59	5A	5B	5C	5D	5E	5F
none		100	60	61	62	63	64	65	66	67
[EBP*2]		101	68	69	6A	6B	6C	6D	6E	6F
[ESI*2]		110	70	71	72	73	74	75	76	77
[EDI*2]		111	78	79	7A	7B	7C	7D	7E	7F
[EAX*4]	10	000	80	81	82	83	84	85	86	87
[ECX*4]		001	88	89	8A	8B	8C	8D	8E	8F
[EDX*4]		010	90	91	92	93	94	95	96	97
[EBX*4]		011	98	99	9A	9B	9C	9D	9E	9F
none		100	A0	A1	A2	A3	A4	A5	A6	A7
[EBP*4]		101	A8	A9	AA	AB	AC	AD	AE	AF
[ESI*4]		110	B0	B1	B2	B3	B4	B5	B6	B7
[EDI*4]		111	B8	B9	BA	BB	BC	BD	BE	BF
[EAX*8]	11	000	C0	C1	C2	C3	C4	C5	C6	C7
[ECX*8]		001	C8	C9	CA	CB	CC	CD	CE	CF
[EDX*8]		010	D0	D1	D2	D3	D4	D5	D6	D7
[EBX*8]		011	D8	D9	DA	DB	DC	DD	DE	DF
none		100	E0	E1	E2	E3	E4	E5	E6	E7
[EBP*8]		101	E8	E9	EA	EB	EC	ED	EE	EF
[ESI*8]		110	F0	F1	F2	F3	F4	F5	F6	F7
[EDI*8]		111	F8	F9	FA	FB	FC	FD	FE	FF

NOTES: [*] means a disp32 with no base if MOD is 00, [EBP] otherwise. This provides the following addressing modes:
 disp32[Index] (MOD = 00)
 disp8[EBP][Index] (MOD = 01)
 disp32[EBP][Index] (MOD = 10)