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	Opreand size prefix	Segment Override
1 או 0	1 או 0	1 או 0	1 או 0
מספר הבתים			

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

SIB (Scale Index Base) byte				
SS	Index	Base	Displacement	Immediate
1 או 0			4 או 0,1,2	4 או 0,1,2
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 מחרוזת בלבד)
F3h = 1111 0011b   REPE / REPZ prefix
                              (פקודות מחרוזת בלבד )
F2h = 1111 0010b   REPNE / REPNZ prefix
                              (פקודות מחרוזת 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 שה<u>היסט</u> בחישוב הכתובת הוא 32 ביט (אוגר EAX+4*EBX וכו').

<u>קידוד אוגרים</u>

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

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

<u>בית ה-SIB</u>

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.

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

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

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	EQ	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 26-3. 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]	00	000	00	08	10	18	20	28	30	38
[ECX]		001	01	09	11	19	21	29	31	39
[EDX]		010	02	0A	12	1A	22	2A	32	3A
[EBX]		011	03	0B	13	1B	23	2B	33	3B
[--][--][1]		100	04	0C	14	1C	24	2C	34	3C
disp32		101	05	0D	15	1D	25	2D	35	3D
[ESI]		110	06	0E	16	1E	26	2E	36	3E
[EDI]		111	07	0F	17	1F	27	2F	37	3F
disp8[EAX]	01	000	40	48	50	58	60	68	70	78
disp8[ECX]		001	41	49	51	59	61	69	71	79
disp8[EDX]		010	42	4A	52	5A	62	6A	72	7A
disp8[EBX];		011	43	4B	53	5B	63	6B	73	7B
disp8[--][--]		100	44	4C	54	5C	64	6C	74	7C
disp8[EBP]		101	45	4D	55	5D	65	6D	75	7D
disp8[ESI]		110	46	4E	56	5E	66	6E	76	7E
disp8[EDI]		111	47	4F	57	5F	67	6F	77	7F
disp32[EAX]	10	000	80	88	90	98	A0	A8	B0	B8
disp32[ECX]		001	81	89	91	99	A1	A9	B1	B9
disp32[EDX]		010	82	8A	92	9A	A2	AA	B2	BA
disp32[EBX]		011	83	8B	93	9B	A3	AB	B3	BB
disp32[--][--]		100	84	8C	94	9C	A4	AC	B4	BC
disp32[EBP]		101	85	8D	95	9D	A5	AD	B5	BD
disp32[ESI]		110	86	8E	96	9E	A6	AE	B6	BE
disp32[EDI]		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: [1]**[--][--]** means a SIB follows the ModR/M byte.
[2]**disp8** 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.

/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

gn-extended and added to
, to be added to the index.

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

r32 Base = Base =			EAX 0 000	ECX 1 001	EDX 2 010	EBX 3 011	ESP 4 100	[*] 5 101	ESI 6 110	EDI 7 111
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)