Hand Assembly Instruction Handout

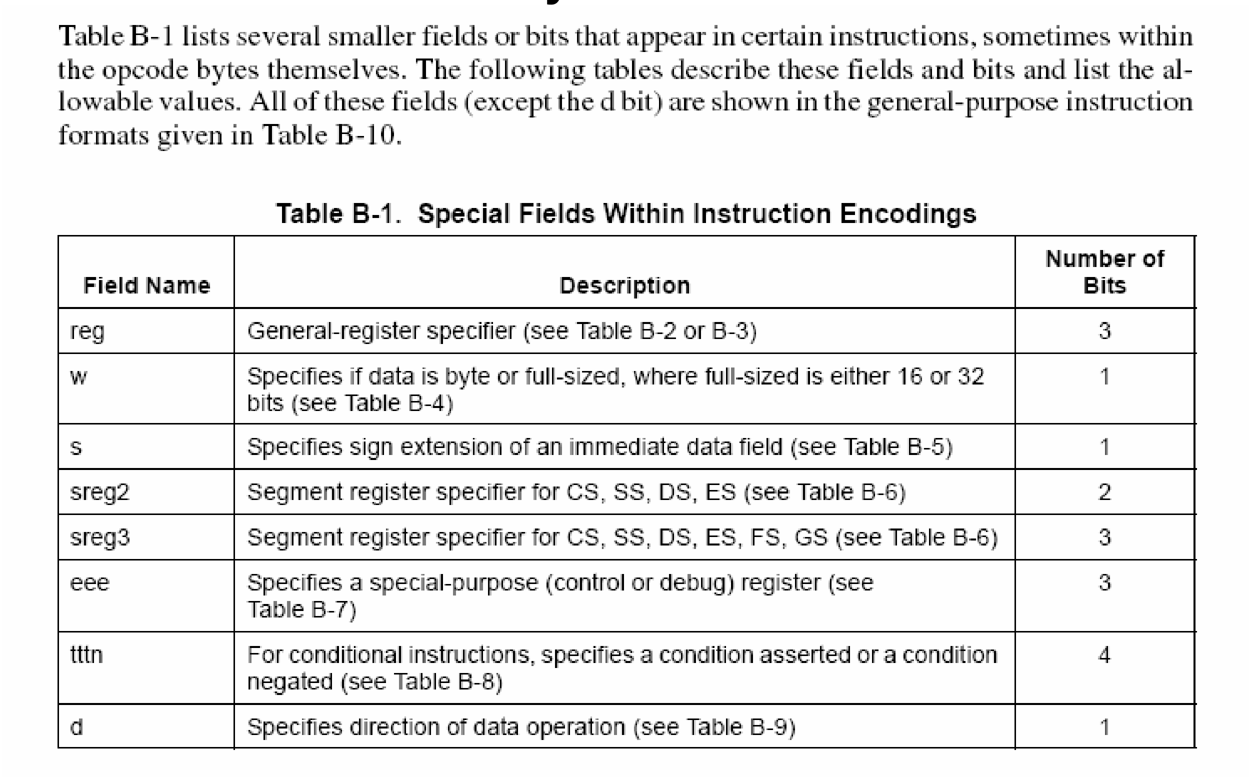


Table B-1 lists several smaller fields or bits that appear in certain instructions, sometimes within the opcode bytes themselves. The following tables describe these fields and bits and list the allowable values. All of these fields (except the d bit) are shown in the general-purpose instruction formats given in Table B-10.

Table B-1. Special Fields Within Instruction Encodings

Field Name	Description	Number of Bits
reg	General-register specifier (see Table B-2 or B-3)	3
w	Specifies if data is byte or full-sized, where full-sized is either 16 or 32 bits (see Table B-4)	1
s	Specifies sign extension of an immediate data field (see Table B-5)	1
sreg2	Segment register specifier for CS, SS, DS, ES (see Table B-6)	2
sreg3	Segment register specifier for CS, SS, DS, ES, FS, GS (see Table B-6)	3
eee	Specifies a special-purpose (control or debug) register (see Table B-7)	3
tttn	For conditional instructions, specifies a condition asserted or a condition negated (see Table B-8)	4
d	Specifies direction of data operation (see Table B-9)	1

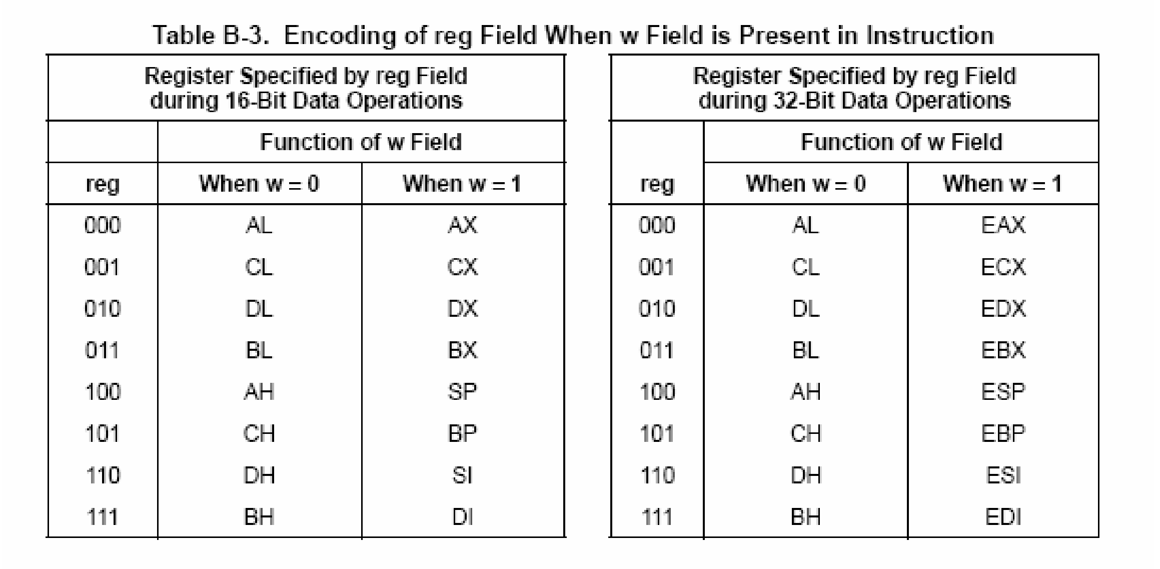


Table B-3. Encoding of reg Field When w Field is Present in Instruction

Register Specified by reg Field during 16-Bit Data Operations		
	Function of w Field	
reg	When w = 0	When 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

Register Specified by reg Field during 32-Bit Data Operations		
	Function of w Field	
reg	When w = 0	When w = 1
000	AL	EAX
001	CL	ECX
010	DL	EDX
011	BL	EBX
100	AH	ESP
101	CH	EBP
110	DH	ESI
111	BH	EDI

Mode (mod) field encoding

Mod	**Explanation**
00	Memory Mode, no displacement follows except when r/m = 110, then 16-bit displacement follows.
01	Memory mode, 8-bit displacement follows
10	Memory mode, 16-bit displacement follows
11	Register Mode (no displacement)

Register/Memory (r/m) field encoding

mod = 00		mod = 01		mod = 10		mod = 11		
Effective Address Calculation								
r/m		**r/m**		**r/m**		**r/m**	**w=0**	**w=1**
000	(BX) + (SI)	**000**	(BX) + (SI) + D8	**000**	(BX) + (SI) + D16	**000**	AL	AX
001	(BX) + (DI)	**001**	(BX) + (DI) + D8	**001**	(BX) + (DI) + D16	**001**	CL	CX
010	(BP) + (SI)	**010**	(BP) + (SI) + D8	**010**	(BP) + (SI) + D16	**010**	DL	DX
011	(BP) + (DI)	**011**	(BP) + (DI) + D8	**011**	(BP) + (DI) + D16	**011**	BL	BX
100	(SI)	**100**	(SI) + D8	**100**	(SI) + D16	**100**	AH	SP
101	(DI)	**101**	(DI) + D8	**101**	(DI) + D16	**101**	CH	BP
110	Direct Address	**110**	(BP) + D8	**110**	(BP) + D16	**110**	DH	SI
111	(BX)	**111**	(BX) + D8	**111**	(BX) + D16	**111**	BH	DI

Jcc – Jump if Condition is met, (see conditional jump instructions table Ch4 Uffenbeck)

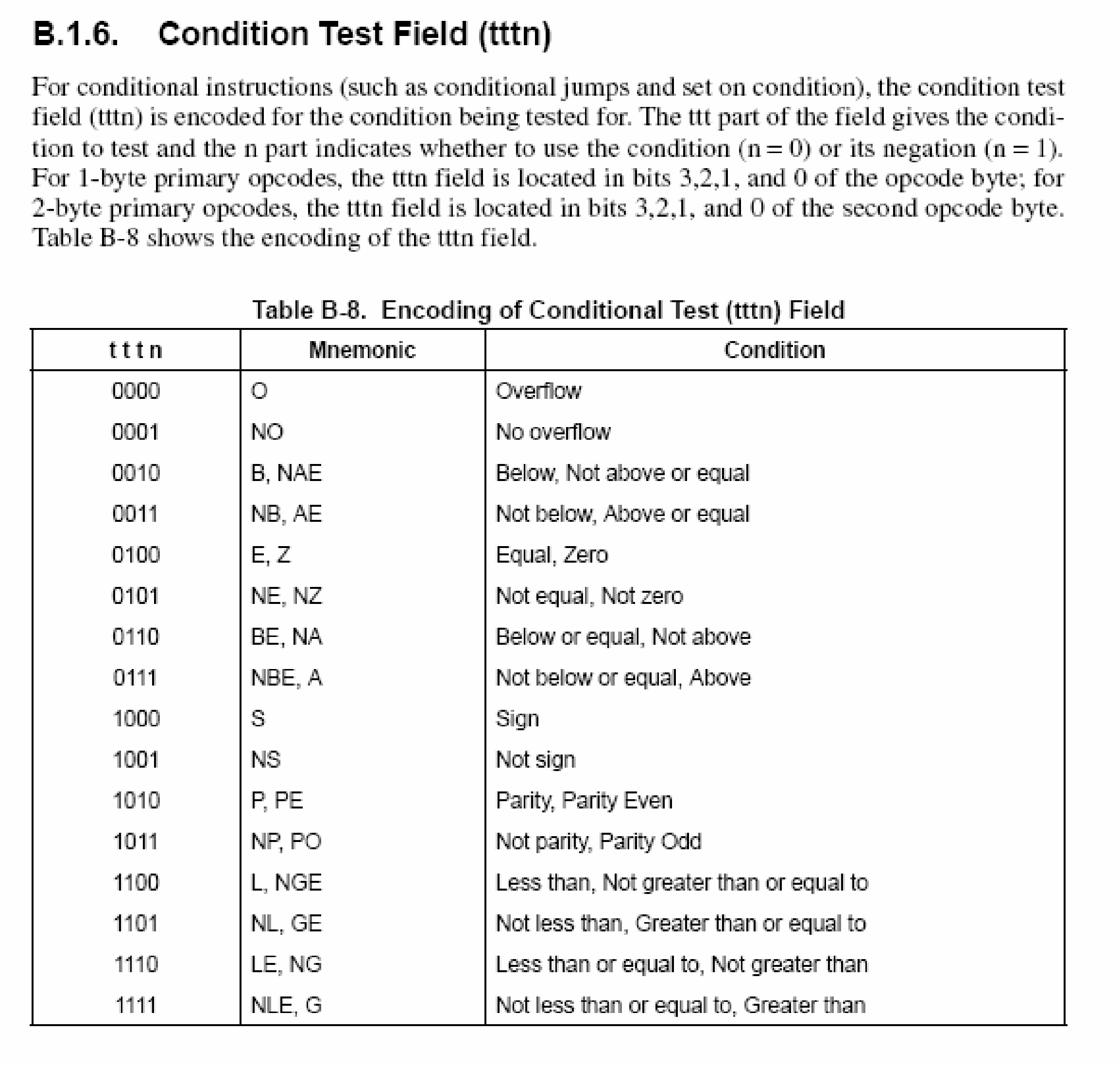
8-bit displacement

0111 t t t n	byte offset

Full displacement

0000 1111	1000 t t t n	word offset

Hex		t	t	t	n	Flag Test	unsigned	signed	Other
0		**0**	**0**	**0**	**0**	OF = 1		JO	
1		**0**	**0**	**0**	**1**	OF = 0		JNO	
2		**0**	**0**	**1**	**0**	CF = 1	JB, JNAE		
3		**0**	**0**	**1**	**1**	CF = 0	JNB, JAE		
4		**0**	**1**	**0**	**0**	ZF = 1	JE, JZ	JE, JZ	
5		**0**	**1**	**0**	**1**	ZF = 0	JNE, JNZ	JNE, JNZ	
6		**0**	**1**	**1**	**0**	CF = 1 or ZF = 1	JBE, JNA		
7		**0**	**1**	**1**	**1**	CF = 0 and ZF = 0	JNBE, JA		
8		**1**	**0**	**0**	**0**	SF = 1		JS	
9		**1**	**0**	**0**	**1**	SF = 0		JNS	
A		**1**	**0**	**1**	**0**	PF = 1			JP
B		**1**	**0**	**1**	**1**	PF = 0			JNP
C		**1**	**1**	**0**	**0**	SF $\neq$ OF		JNGE, JL	
D		**1**	**1**	**0**	**1**	SF = OF		JGE, JNL	
E		**1**	**1**	**1**	**0**	ZF = 1 or SF $\neq$ OF		JNG, JLE	
F		**1**	**1**	**1**	**1**	ZF = 0 and SF = OF		JG, JNLE	



B.1.6. Condition Test Field (tttn)

For conditional instructions (such as conditional jumps and set on condition), the condition test field (tttn) is encoded for the condition being tested for. The ttt part of the field gives the condition to test and the n part indicates whether to use the condition (n = 0) or its negation (n = 1). For 1-byte primary opcodes, the tttn field is located in bits 3,2,1, and 0 of the opcode byte; for 2-byte primary opcodes, the tttn field is located in bits 3,2,1, and 0 of the second opcode byte. Table B-8 shows the encoding of the tttn field.

Table B-8. Encoding of Conditional Test (tttn) Field

t t t n	Mnemonic	Condition
0000	O	Overflow
0001	NO	No overflow
0010	B, NAE	Below, Not above or equal
0011	NB, AE	Not below, Above or equal
0100	E, Z	Equal, Zero
0101	NE, NZ	Not equal, Not zero
0110	BE, NA	Below or equal, Not above
0111	NBE, A	Not below or equal, Above
1000	S	Sign
1001	NS	Not sign
1010	P, PE	Parity, Parity Even
1011	NP, PO	Not parity, Parity Odd
1100	L, NGE	Less than, Not greater than or equal to
1101	NL, GE	Not less than, Greater than or equal to
1110	LE, NG	Less than or equal to, Not greater than
1111	NLE, G	Not less than or equal to, Greater than

JMP – Unconditional Jump (to same segment)

Short	1110 1011: 8-bit displacement
Direct	1110 1001: full displacement
Register indirect	1111 1111: 11 100 reg
Memory indirect	1111 1111: mod 100 r/m

Examples:

JMP unconditional jump (same argument)

1110 1011: byte displacement (EB __)

8bit-> +127 forward to -128 bytes backward, expressed in Hex

1110 1001: word displacement (E9 __)

JCXZ jump if CX = 0

1110 0011: byte displacement (E3 __)

(to work with ECX use address size prefix)

LOOP

1110 0010: byte displacement (E2 __)

Include auto-decrement of the CX register.
Jump if CX is not zero after decrement.

ADD – Add	
register1 to register2	0000 000w : 11 reg1 reg2
register2 to register1	0000 001w : 11 reg1 reg2
memory to register	0000 001w : mod reg r/m
register to memory	0000 000w : mod reg r/m
immediate to register	1000 00sw : 11 000 reg : immediate data
immediate to AL, AX, or EAX	0000 010w : immediate data
immediate to memory	1000 00sw : mod 000 r/m : immediate data
DAA – Decimal Adjust AL after Addition	0010 0111
DAS – Decimal Adjust AL after Subtraction	0010 1111
DEC – Decrement by 1	
register	1111 111w : 11 001 reg
register (alternate encoding)	0100 1 reg
memory	1111 111w : mod 001 r/m
DIV – Unsigned Divide	
AL, AX, or EAX by register	1111 011w : 11 110 reg
AL, AX, or EAX by memory	1111 011w : mod 110 r/m
IN – Input From Port	
fixed port	1110 010w : port number
variable port	1110 110w
INC – Increment by 1	
reg	1111 111w : 11 000 reg
reg (alternate encoding)	0100 0 reg
memory	1111 111w : mod 000 r/m
INS – Input from DX Port	0110 110w
INT n – Interrupt Type n	1100 1101 : type
INT – Single-Step Interrupt 3	1100 1100
J*cc* – Jump if Condition is Met	
8-bit displacement	0111 tttn : 8-bit displacement
full displacement	0000 1111 : 1000 tttn : full displacement
JCXZ/JECXZ – Jump on CX/ECX Zero Address-size prefix differentiates JCXZ and JECXZ	1110 0011 : 8-bit displacement
JMP – Unconditional Jump (to same segment)	
short	1110 1011 : 8-bit displacement
direct	1110 1001 : full displacement
register indirect	1111 1111 : 11 100 reg
memory indirect	1111 1111 : mod 100 r/m
JMP – Unconditional Jump (to other segment)	
direct intersegment	1110 1010 : unsigned full offset, selector
indirect intersegment	1111 1111 : mod 101 r/m

MOV – Move Data	
register1 to register2	1000 100w : 11 reg1 reg2
register2 to register1	1000 101w : 11 reg1 reg2
memory to reg	1000 101w : mod reg r/m
reg to memory	1000 100w : mod reg r/m
immediate to register	1100 011w : 11 000 reg : immediate data
immediate to register (alternate encoding)	1011 w reg : immediate data
immediate to memory	1100 011w : mod 000 r/m : immediate data
memory to AL, AX, or EAX	1010 000w : full displacement
AL, AX, or EAX to memory	1010 001w : full displacement
NOP – No Operation	1001 0000
NOT – One's Complement Negation	
register	1111 011w : 11 010 reg
memory	1111 011w : mod 010 r/m
OR – Logical Inclusive OR	
register1 to register2	0000 100w : 11 reg1 reg2
register2 to register1	0000 101w : 11 reg1 reg2
SUB – Integer Subtraction	
register1 to register2	0010 100w : 11 reg1 reg2
register2 to register1	0010 101w : 11 reg1 reg2
memory to register	0010 101w : mod reg r/m
register to memory	0010 100w : mod reg r/m
immediate to register	1000 00sw : 11 101 reg : immediate data
immediate to AL, AX, or EAX	0010 110w : immediate data
immediate to memory	1000 00sw : mod 101 r/m : immediate data