unixwiz.net

Intel x86 JUMP quick reference

4 minutes

Getting the sense for jumps and flags has long been a troublesome area for me, especially since the Intel assembler book shows 32 of these, all with similar-sounding names. Looking more closely I found that many of the instructions were synonyms for each other, and in practice the whole gamut is not needed, and in the process found that my copy of Intel's *80386 Programmer's Reference Manual* gave an incorrect description for one of the instructions.

So I have grouped these functionally, with all instruction synonyms in the same row.

Instruction	Description	signed-ness	Flags	short jump opcodes	near jump opcodes
JO	Jump if overflow		OF = 1	70	0F 80
JNO	Jump if not overflow		OF = 0	71	0F 81
JS	Jump if sign		SF = 1	78	0F 88
JNS	Jump if not sign		SF = 0	79	0F 89
JE JZ	Jump if equal Jump if zero		ZF = 1	74	0F 84
JNE JNZ	Jump if not equal Jump if not zero		ZF = 0	75	0F 85
JB JNAE JC	Jump if below Jump if not above or equal Jump if carry	unsigned	CF = 1	72	0F 82
JNB JAE JNC	Jump if not below Jump if above or equal Jump if not carry	unsigned	CF = 0	73	0F 83
JBE JNA	Jump if below or equal Jump if not above	unsigned	CF = 1 or ZF = 1	76	0F 86
JA JNBE	Jump if above Jump if not below or equal	unsigned	CF = 0 and ZF = 0	77	0F 87

Instruction	Description	signed-ness	Flags	short jump opcodes	near jump opcodes
JL JNGE	Jump if less Jump if not greater or equal	signed	SF <> OF	7C	0F 8C
JGE JNL	Jump if greater or equal Jump if not less	signed	SF = OF	7D	0F 8D
JLE JNG	Jump if less or equal Jump if not greater	signed	ZF = 1 or SF <> OF	7E	0F 8E
JG JNLE	Jump if greater Jump if not less or equal	signed	ZF = 0 and SF = OF	7F	0F 8F
JP JPE	Jump if parity Jump if parity even		PF = 1	7A	0F 8A
JNP JPO	Jump if not parity Jump if parity odd		PF = 0	7B	0F 8B
JCXZ JECXZ	Jump if %CX register is 0 Jump if %ECX register is 0		%CX = 0 %ECX = 0	E3	

The x86 processors have a large set of flags that represent the state of the processor, and the conditional jump instructions can key off of them in combination.

CF - carry flag
: Set on high-order bit carry or borrow; cleared otherwise

PF - parity flag
: Set if low-order eight bits of result contain an even number of "1" bits; cleared otherwise

ZF - zero flags
: Set if result is zero; cleared otherwise

SF - sign flag
: Set equal to high-order bit of result (0 if positive 1 if negative)

OF - overflow flag
: Set if result is too large a positive number or too small a negative number (excluding sign bit) to fit in destination operand; cleared otherwise