6.823 Computer System Architecture
CISC ISA – x86jr

http://csg.csail.mit.edu/6.823/

x86 has a CISC-style instruction set with variable-length instructions. In the x86 architecture, each instruction is capable of performing one or more simpler instructions called micro-operations (μops). It also supports several complex addressing modes.

We introduce a (very small) subset of the x86 instruction set in the following table. (Interested readers are referred to the Intel's website for full details.)

Instruction	Operation	OF	SF	Length
`add` R_{DEST}, R_{SRC}	$R_{SRC} \leftarrow R_{SRC}$ + R_{DEST}	M	M	2 bytes
`cmp imm32,` R_{SRC2}	Temp ← R_{SRC2} - MEM[imm32]	M	M	6 bytes
`inc` R_{DEST}	$R_{DEST} \leftarrow R_{DEST}$ + 1	M	M	1 byte
`jmp label`	jump to the address specified by `label`			2 bytes
`jl label`	if (SF≠OF) jump to the address specified by `label`	T	T	2 bytes
`xor` R_{DEST}, R_{SRC}	$R_{DEST} \leftarrow R_{DEST}$ xor R_{SRC}	O	M	2 bytes

Table H2-1: Simple x86 instruction set (x86jr)

Notice that the jump instruction `jl` (jump if less than) depends on SF and OF, which are status flags. Each instruction affects them in different ways based on the result of its computation: "M" indicates the instruction modifying (writing) the status flag, "T" the instruction testing (reading but not writing) it, and "O" the instruction resetting it. A blank (as in `jmp` instruction) means that the instruction does not affect the status flag. Some instructions, like the `cmp` instruction, perform a computation and set status flags, but do not return any result.

The meanings of the status flags are given in the following table:

Name	Purpose	Condition Reported
OF	Overflow	Result exceeds positive or negative limit of number range
SF	Sign	Result is negative (less than zero)

Table H2-2: Status flags