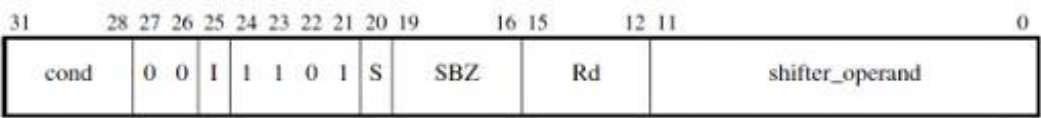


ARM 汇编指令机器码举例详解

ARM7 内核采用的是 RISC 精简指令集，所有的 ARM 指令都是 32bits 的，在这 32bits 里既包含了指令的指令码，也包含了指令需要运算的数据，以 MOV指令为例，通过 MOV 指令的 32bits 可以识别出这是一个 MOV 指令，又可以在这 32bits 里找到源寄存器和目的寄存器。我们来看一下 MOV 指令的机器

码格式：



28~31bits（cond）是条件码，就是表明这条语句里是否有大于、等于、非零等的条件判断，这 4bits 共有 16 种状态，分别为：

二进制码	指令符号	含义	二进制码	指令符号	含义
0000	EQ	相等	0001	NE	不等
0010	CS/HS	进位/无符号数大于等于	0011	CC/LO	清进位/无符号数小于
0100	MI	减/负数	0101	PL	加/正数或 0
0110	VS	溢出	0111	VC	没溢出
1000	HI	无符号数大于	1001	LS	无符号数小于等于
1010	GE	有符号数大于等于	1011	LT	有符号数小于
1100	GT	有符号数大于	1101	LE	有符号数小于等于
1110	AL	任何条件	1111	-	未定义

表 1 汇编语言条件码

指令与条件码可以有多种组合，比如 MOV 指令可以有 MOV、MOVEQ、MOVLT 等多种形式。前面我们说过状态寄存器里有 NZCV 的状态标志，

当执行一条指令时，芯片就会将这条指令的条件码与状态寄存器中的状态标志做比较，如果状态寄存器中的状态标志满足这条指令的条件码时，则执行这条语句，如果不满足 则不执行这条指令。状态寄存器中的状态标志是受某些指令影响的，因此在使用有条件码的指令进行判断前，必然会有其它指令配合使用，先修改状态寄存器中的状态标志

指令： MOV R1, #0x64		机器码： E3A01064					
指令格式							
cond	00	I	opcode	S	SBZ	Rd	shifer_operand
1110	00	1	1101	0	0000	0001	000001100100
条件码为 1110 适用任何条件		立即数方式	MOV 的指令码	指令没有 S 标志		目的寄存器为 R1	源操作数为立即数 0x64
指令： MOVS PC, R14		机器码： E1B0F00E					
指令格式							
1110	00	0	1101	1	0000	1111	000000001110
条件码为 1110 适用任何条件		寄存器方式	MOV 的指令码	指令有 S 标志		目的寄存器为 R15	源操作数为寄存器 R14
指令： MOVLt R3, #0x1		机器码： B3A03001					
指令格式							
1011	00	1	1101	0	0000	0011	000000000001
Lt 的条件码为 1011		立即数方式	MOV 的指令码	指令没有 S 标志		目的寄存器为 R3	源操作数为立即数 1
指令： MOVEQ R0, R1		机器码： 01A00001					
指令格式							
0000	00	0	1101	0	0000	0000	000000000001
EQ 的条件码为 0000		寄存器方式	MOV 的指令码	指令没有 S 标志		目的寄存器为 R0	源操作数为寄存器 R1