NASM, архитектура i386: основные команды (стр.2)

Побитовые операции

and op1,op2; op1:=op1 & op2, уст. флаги
test op1,op2 ; op1 & op2, уст. флаги,
; рез-т не записывается
or op1,op2; op1:=op1 | op2, уст. флаги
xor op1,op2; op1:= op1 <> op2, устанавл. флаги

- op1 и op2 должны быть одного размера (байт, слово или двойное слово)
- команда, где оба операнда op1 и op2 – ячейки памяти, запрещены
- op1 не может быть константой
- ячейка памяти – в [ ] скобках
- если первый операнд – ячейка памяти, а второй – непосредственный (константа) необходимо явно указать размер

op1	op2
r8 r16 r32	r8, m8, i8 r16, m16, i16 r32, m32, i32
m8 m16 m32	r8,*i8 (указать размер)* r16,*i16(указать размер)* r32, *i32(указать размер)*

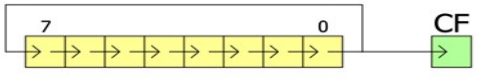
Команды сдвига

shr op1,op2 ; shift right логический сдвиг вправо,
; на «освободившиеся» позиции пишутся нули
;CF = значение последнего сдвинутого вправо
; (за пределы ячейки) бита
sar op1,op2 ; shift arithmetic right
; арифметический сдвиг вправо, на «освободившиеся»
; позиции пишется знаковый разряд
;CF = значение последнего сдвинутого вправо
; (за пределы ячейки) бита
shl OP1,OP2 ; SHL, SAR работают одинаково
sar OP1,OP2 ; на «освободившиеся» позиции
; пишутся нули CF = значение последнего сдвинутого
; влево (за пределы ячейки) бита

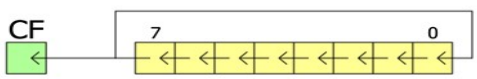
Циклический сдвиг

ror op1,op2 ; rotate right циклический сдвиг вправо
rol op1,op2 ; rotate left циклический сдвиг влево

Циклический сдвиг вправо (ROR)

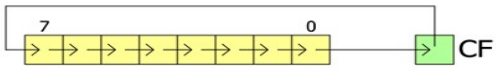


Циклический сдвиг влево (ROL)

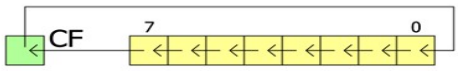


rcr op1,op2 ; **r**otate through **c**arry **r**ight циклический
; сдвиг вправо, после сдвига устанавливается новый CF
rcl op1,op2 ; **r**otate through **c**arry **l**eft циклический
; сдвиг влево после сдвига устанавливается новый CF

RCR



RCL



op1	op2 (берется по модулю 32)
r8, m8	CL, i8
r16, m16	CL, i8
r32, m32	CL, i8

Для операндов m16, m32 команды сдвига учитывают порядок байтов (little endian, big endian)
пример: `mov word[x],0x8000`
`shl word[x],1;` по адресу x будет 0

Строковые команды

cld – установка флага DF = 0 (движение слева направо)
cld – установка флага DF = 1 (движение справа налево)
movsb
movsw пересылка [edi] := [esi], изменение esi, edi
movsd

lodsb al
lodsw загрузка ax := [esi], изменение esi,
lodsd eax

stosb **al**
stosw запись **[edi] :=** **ax** , изменение edi,
stosd **eax**

scasb сканирование al
scasw (сравнение) ax c [edi],
scasd изменение edi, eax
установка флагов

cmpsb, cmpsw, cmpsd сравнение [esi] и [edi], изменение esi и edi, установка флагов

Префиксы повторения

(перед строковыми командами)

rep – повторять строковую команду ecx раз (для слов – CX раз)

repe (repz) повторять строковую команду пока ZF=1, но не более ecx (для слов – CX) раз

repne (repnz) повторять строковую команду пока ZF=0, но не более ecx (для слов – CX) раз