NASM, архитектура i386: основные команды

Пересылка, сложение, вычитание

mov op1, **op2**; op1:=op2, флаги не уст.

add op1, op2; op1:=op1+op2, уст. флаги

sub op1, op2; op1:=op1-op2, уст. флаги

стр op1, **op2**; op1-op, устанавл. флаги

adc op1, op2; op1:=op1+op2+CF, уст. флаги

sbb op1, **op2**; op1:=op1-op2 -CF, уст. флаги

 – ор1 и ор2 должны быть одного размера (байт, слово или двойное слово)

 команда, где оба операнда ор1 и ор2 – ячейки памяти, запрещены

– op1 не может быть константой

– ячейка памяти − в [] скобках

пример:

mov eax, х; запись <u>адреса</u> х в еах **mov** eax, [x]; содержимого памяти-

; двойного слова в еах

- если первый операнд - ячейка памяти, а второй – непосредственный (константа) необходимо явно указать размер, например:

mov byte [x], 0 ; запись байта mov word [x], 0 ; запись слова

mov dword [x], 0 ;запись дв.слова

- команды add, sub, cmp, adc, sbb меняют флаги ZF, SF, CF, OF;

команда mov флаги ZF. SF. CF. OF не меняет

op1	op2		
r8	r8, m8, i8		
r16	r16, m16, i16		
r32	r32, m32, i32		
m8	r8, <u>i8 (указать размер)</u>		
m16	r16, <u>i16(указать размер)</u>		
m32	r32, <u>i32(указать размер)</u>		

Команда обмена

xchg op1, op2; поменять содержимое

; ячеек ор1 и ор2

 – op1 и op2 должны быть одного размера (байт, слово или двойное слово)

– пересылки, где оба ор1 и ор2 – ячейки памяти,

запрешены

op1	op2
r8	r8, m8
r16	r16, m16
r32	r32, m32
m8	r8
m16	r16
m32	r32

Расширение

	Знаков	Беззнак.		
byte→ word	cbw	AX:=AL	Записать 0 в	
word→ dword	cwd	DX:AX:=AX	старшие разряды	
word→ dword	cwde	EAX := AX	(команда mov)	
dword→ qword	cdq	EDX:EAX := EAX		

Пересылка с расширением размера

доп. знаковым битом доп. нулями

movzx op1,op2 movsx op1,op2

op1	op2			
r16	r8, m8			
r32	r8, m8, r16, m16			

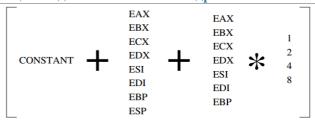
Загрузка исполнительного адреса

lea op1,op2

Примеры:

lea eax, [esp+8*ecx+5]

Общий вид исполнительного адреса



Однооперандные команды

neg op1; op1:=0-op1

inc op1; op1:= op1 + 1, не меняет CF

dec op1; op1:= op1 – 1, не меняет CF

not op1; побитовое отрицание

op1 | r8, m8, r16, m16, r32, m32

Для m8, m16, m32 нужно указать размер операнда

Умножение и деление

mul op1 ; беззнаковое умножение

imul op1 ; знаковое умножение div op1 ; беззнаковое деление

idiv op1 ; знаковое умножение

	op1	умножение		деление		
	разрядн.	неявный	результат	делимое	частное	остаток
	(бит)	множитель	умножения			
ĺ	8	AL	AX	AX	AL	AH
	16	AX	DX:AX	DX:AX	AX	DX
	32	EAX	EDX:EAX	EDX:EAX	EAX	EDX

ор1 – ячейка памяти или регистр (умножения на константу нет)