Команди асемблеру процесорів «IA-32»

Інкремент, декремент,
Логічні
Перекодування
Зсув
Цикл
Умовний перехід
Порівняння
Опрацювання окремих бітів

Архітектура IA-32

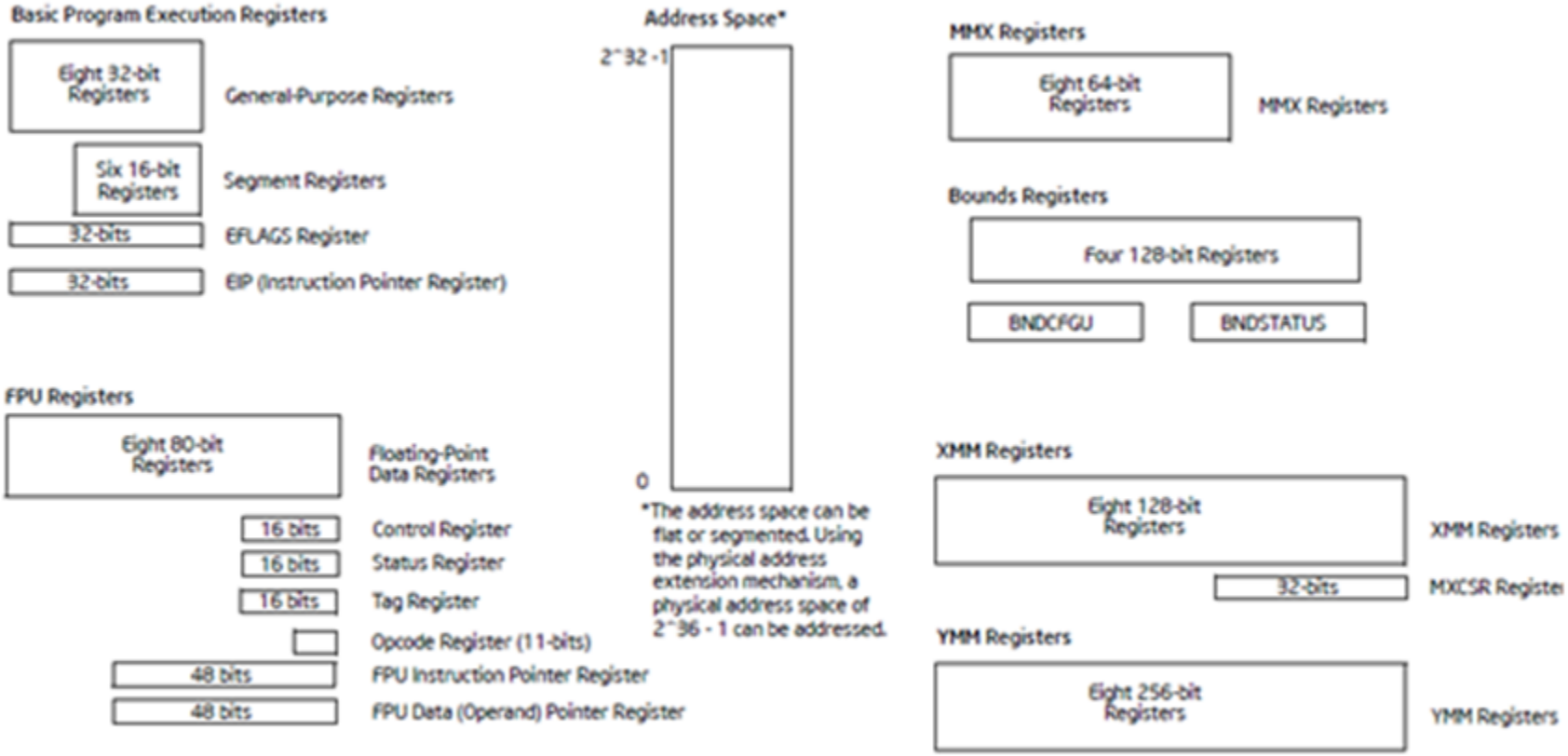


Figure 3-1. IA-32 Basic Execution Environment for Non-64-bit Modes

Зміна значення операнда на одиницю

INC (Increment) - Збільшення на одиницю

Додавання 1 до операнду.

Adds 1 to a register or memory operand.

Формат:
```
INC  reg
INC  mem
```

Формування ознак (ознака CF не формується)

O	D	I	S	Z	A	P	C
*			*	*	*	*	

DEC (Decrement) - Зменшення на одиницю

Віднімання 1 із операнду.

Subtracts 1 from an operand. Does not affect the Carry flag.

Формат:
```
DEC  reg
DEC  mem
```

Формування ознак (ознака CF не формується)

O	D	I	S	Z	A	P	C
*			*	*	*	*	

Операції комп’ютерної логіки

AND — Logical AND

O	D	I	S	Z	A	P	C
*			*	*	?	*	0

Each bit in the destination operand is ANDed with the corresponding bit in the source operand.
Instruction formats:

```
AND   reg,reg
AND   mem,reg
AND   reg,mem
AND   reg,imm
AND   mem,imm
AND   accum,imm
```

OR — Inclusive OR

O	D	I	S	Z	A	P	C
0			*	*	?	*	0

Performs a boolean (bitwise) OR operation between each matching bit in the destination operand and each bit in the source operand.
Instruction formats:

```
OR   reg,reg
OR   mem,reg
OR   reg,mem
OR   reg,imm
OR   mem,imm
OR   accum,imm
```

XOR — Exclusive OR

O	D	I	S	Z	A	P	C
0			*	*	?	*	0

Each bit in the source operand is exclusive ORed with its corresponding bit in the destination. The destination bit is a 1 only when the original source and destination bits are different.
Instruction formats:

```
XOR   reg,reg      XOR   reg,imm
XOR   mem,reg      XOR   mem,imm
XOR   reg,mem      XOR   accum,imm
```

Перетворення кодів

NEG — Negate

O	D	I	S	Z	A	P	C
*			*	*	*	*	*

Calculates the twos complement of the destination operand and stores the result in the destination.
Instruction formats:

`NEG` *reg* `NEG` *mem*

NOT — Not

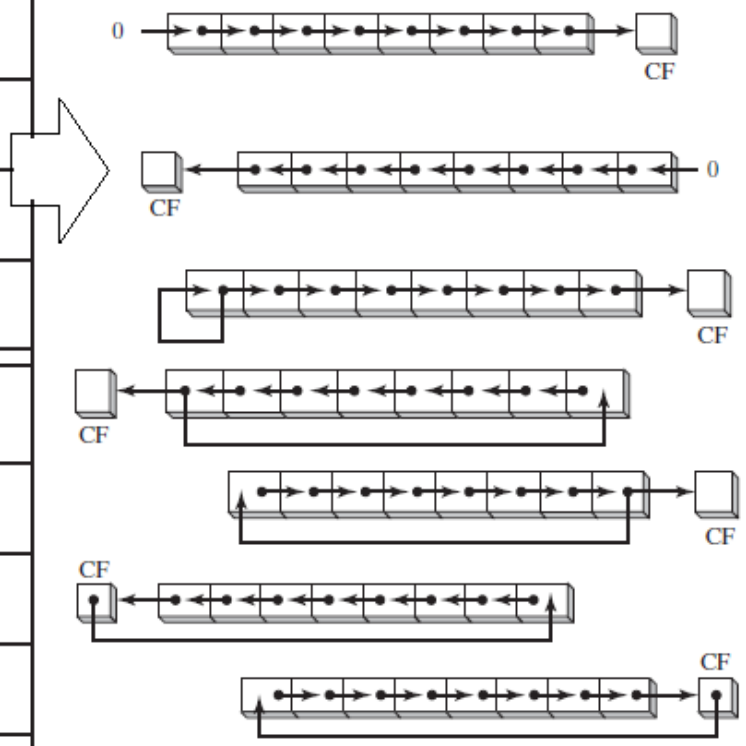
O	D	I	S	Z	A	P	C

Performs a logical NOT operation on an operand by reversing each of its bits.
Instruction formats:

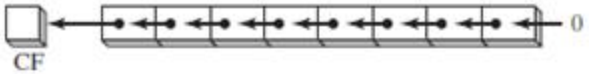
`NOT` *reg* `NOT` *mem*

Операції зсуву

SHR	Shift right
SHL	Shift left
SAL	Shift arithmetic left
SAR	Shift arithmetic right
ROL	Rotate left
ROR	Rotate right
RCL	Rotate carry left
RCR	Rotate carry right
SHLD	Double-precision shift left
SHRD	Double-precision shift right



Зсув вліво



SHL
SAL

Shift Left

Shift Arithmetic Left

`SHL reg,imm8`	`SAL reg,imm8`
`SHL reg,CL`	`SAL reg,CL`
`SHL mem,imm8`	`SAL mem,imm8`
`SHL mem,CL`	`SAL mem,CL`

Shifts each bit in the destination operand to the left, using the source operand to determine the number of shifts. The highest bit is copied into the Carry flag, and the lowest bit is filled with a zero (identical to SAL). The *imm8* operand must be a 1 when using the 8086/8088 processor.

O	D	I	S	Z	A	P	C
*			*	*	?	*	*

Можливе застосування - множення на значення, кратне степіню 2.

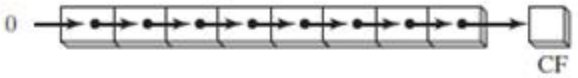
```
mov  dl,10     ; before:  00001010
shl  dl,2      ; after:   00101000
```

Зсув вправо

SHR — **Shift Right**

Shifts each bit in the destination operand to the right, using the source operand to determine the number of shifts. The highest bit is filled with a zero, and the lowest bit is copied into the Carry flag. The *imm8* operand must be a 1 when using the 8086/8088 processor.

```
SHR   reg, imm8      SHR   mem, imm8
SHR   reg,CL         SHR   mem,CL
```



O	D	I	S	Z	A	P	C
*			*	*	?	*	*

SAR — **Shift Arithmetic Right**

Shifts each bit in the destination operand to the right, using the source operand to determine the number of shifts. The lowest bit is copied into the Carry flag, and the highest bit retains its previous value. This shift is often used with signed operands because it preserves the number's sign. The *imm8* operand must be a 1 when using the 8086/8088 processor.

```
SAR   reg, imm8      SAR   mem, imm8
SAR   reg,CL         SAR   mem,CL
```

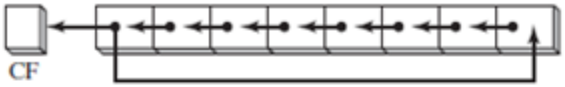
Можливе застосування - ділення на значення, кратне степіню 2.

```
a) mov  al,0F0h          ; AL = 11110000b (-16)
   sar  al,1             ; AL = 11111000b (-8), CF = 0

b) mov  al,01000000b     ; AL = 64
   shr  al,3             ; divide by 8, AL = 00001000b

c) mov  ax,-128          ; EAX = ????FF80h
   shl  eax,16           ; EAX = FF800000h
   sar  eax,16           ; EAX = FFFFFF80h
```

Приклади застосування команди ROL



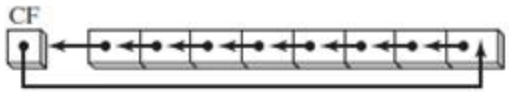
а) Зсуви на тетраду з відтворенням початкового значення:

```
mov  ax,6A4Bh
rol  ax,4          ; AX = A4B6h
rol  ax,4          ; AX = 4B6Ah
rol  ax,4          ; AX = B6A4h
rol  ax,4          ; AX = 6A4Bh
```

б) Перетворення 26h в 62h:

```
mov  al,26h
rol  al,4        ; AL = 62h
```

Приклад застосування команди RCL



Перевірка біту LSB (контроль числа на парність):

```
.data
testval BYTE  01101010b
.code
shr  testval,1          ; shift LSB into Carry flag
jc   exit               ; exit if Carry flag set
rcl  testval,1          ; else restore the number
```

Подвійний зсув вліво SHLD

Операнд-отримувач зміщується вліво на задану кількість бітів. Позиції бітів, відкриті зсувом, заповнюються найбільш значущими бітами операнда-джерела. Значення операнда-джерела не змінюється.

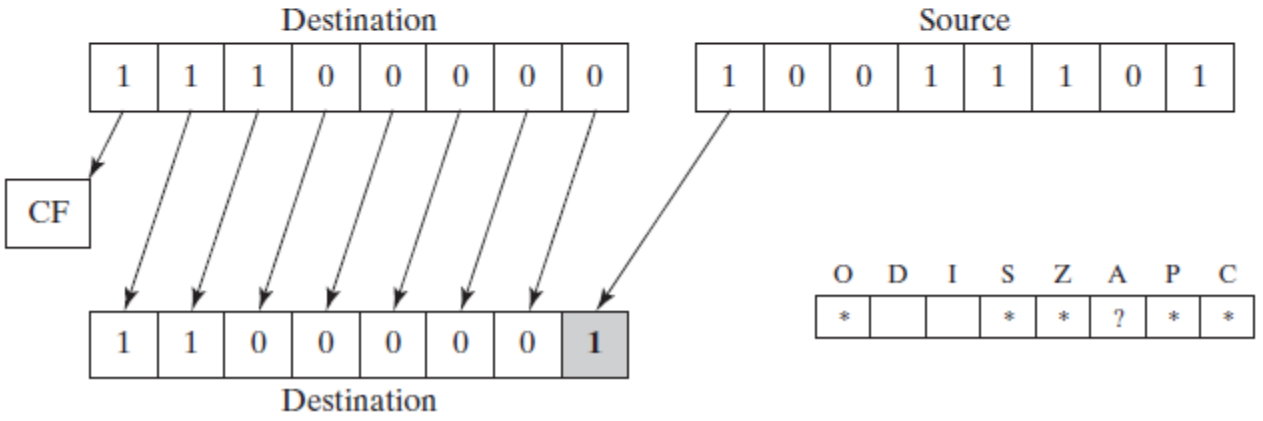
SHLD — **Double-Precision Shift Left (x86)**

Shifts the bits of the second operand into the first operand. The third operand indicates the number of bits to be shifted. The positions opened by the shift are filled by the most significant bits of the second operand. The second operand must always be a register, and the third operand may be either an immediate value or the CL register.

Instruction formats:

```
SHLD dest, source, count

SHLD reg16,reg16,imm8        SHLD mem16,reg16,imm8
SHLD reg32,reg32,imm8        SHLD mem32,reg32,imm8
SHLD reg16,reg16,CL          SHLD mem16,reg16,CL
SHLD reg32,reg32,CL          SHLD mem32,reg32,CL
```



Подвійний зсув вправо SHRD

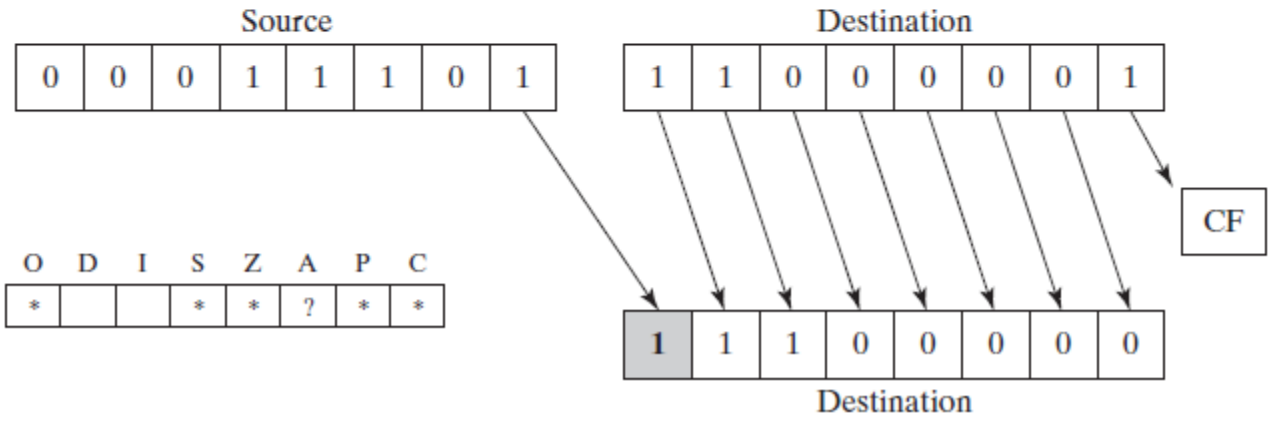
Операнд-отримувач зміщується вправо на задану кількість бітів. Позиції бітів, відкриті зсувом, заповнюються найменш значущими бітами операнда-джерела. Значення операнда-джерела не змінюється.

SHRD — **Double-Precision Shift Right (x86)**

Shifts the bits of the second operand into the first operand. The third operand indicates the number of bits to be shifted. The positions opened by the shift are filled by the least significant bits of the second operand. The second operand must always be a register, and the third operand may be either an immediate value or the CL register.

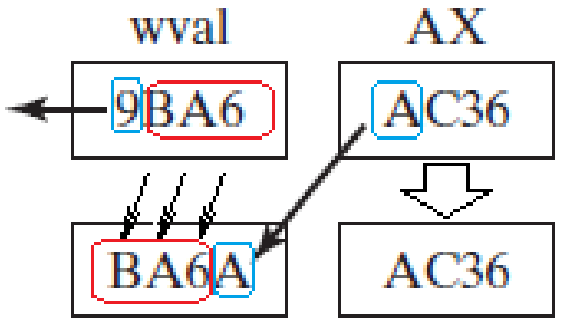
Instruction formats: `SHRD dest, source, count`

```
SHRD reg16,reg16,imm8        SHRD mem16,reg16,imm8
SHRD reg32,reg32,imm8        SHRD mem32,reg32,imm8
SHRD reg16,reg16,CL          SHRD mem16,reg16,CL
SHRD reg32,reg32,CL          SHRD mem32,reg32,CL
```



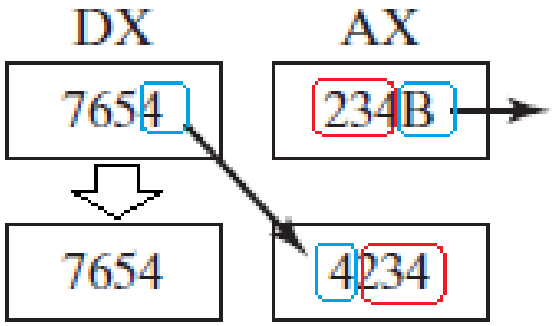
Приклади застосування SHLD та SHRD

```
.data
wval WORD 9BA6h
.code
mov   ax,0AC36h
shld  wval,ax,4
```

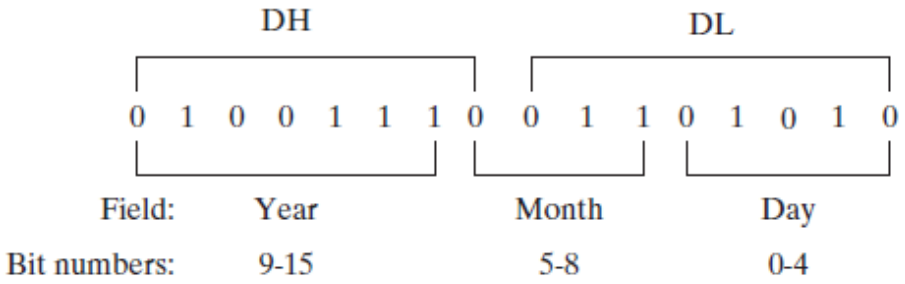



```
; wval = BA6Ah
```

```
mov   ax,234Bh
mov   dx,7654h
shrd  ax,dx,4
```



Приклад отримання частин від коду дати



а) Отримання значення "день"

```
mov  al,dl                  ; make a copy of DL
and  al,00011111b           ; clear bits 5-7
mov  day,al                 ; save in day
```

б) Отримання значення "місяць"

```
mov  ax,dx                  ; make a copy of DX
shr  ax,5                   ; shift right 5 bits
and  al,00001111b           ; clear bits 4-7
mov  month,al               ; save in month
```

в) Отримання значення "рік"

```
mov  al,dh                  ; make a copy of DH
shr  al,1                   ; shift right one position
mov  ah,0                   ; clear AH to zeros
add  ax,1980                ; year is relative to 1980
mov  year,ax                ; save in year
```

Команди циклу

LOOP (Loop) - Цикл
LOOPD (x86)
LOOPW (16-bit Counter)

Формат:
```
LOOP shortlabel
LOOPD shortlabel
LOOPW shortlabel
```

Зменшення значення регістру ECX/CX на 1, перевірка остачі та передача керування за вказаною міткою, якщо значення остачі в регістру ECX/CX більше нуля.
Мітка повинна вказувати на адресу із зміщенням -128...+127 байт відносно адреси наступної команди.
В процесорах IA-32 за умовчанням використовується регістр ECX.

Decrements ECX and jumps to a short label if ECX is not equal to zero. The destination must be −128 to +127 bytes from the current location.

O	D	I	S	Z	A	P	C

Формування ознак немає:

LOOPE, (Loop if Equal (Zero)) - Цикл, якщо нуль
LOOPZ

Формат:
```
LOOPE shortlabel
LOOPZ shortlabel
```

Декремент значення регістру ECX/CX, перевірка остачі та передача керування за вказаною міткою, якщо значення остачі в регістрі ECX/CX більше нуля і ознака ZF дорівнює одиниці.

Decrements (E)CX and jumps to a short label if (E)CX > 0 and the Zero flag is set.

Формування ознак немає

LOOPNE, (Loop if Not Equal (Zero)) - Цикл, якщо не нуль
LOOPNZ

Формат:
```
LOOPNE shortlabel
LOOPNZ shortlabel
```

Декремент значення регістру ECX/CX, перевірка остачі та передача керування за вказаною міткою, якщо значення остачі в регістрі ECX/CX більше нуля і ознака ZF дорівнює нулю.

Decrements (E)CX and jumps to a short label if (E)CX > 0 and the Zero flag is clear.

Формування ознак немає

Умовний і безумовний перехід

Jcondition

Conditional Jump

Умовний перехід

O	D	I	S	Z	A	P	C

Перехід до мітки, якщо вказане значення ознаки є істинним. На процесорах x86 зміщення мітки може бути позитивним або негативним 32-бітовим значенням.

Jumps to a label if a specified flag condition is true. When using a processor earlier than the x86, the label must be in the range of −128 to +127 bytes from the current location. On x86 processors, the label's offset can be a positive or negative 32-bit value.

Instruction format: `Jcondition label`

JMP

Jump Unconditionally to Label

Безумовний перехід

O	D	I	S	Z	A	P	C

Jump to a code label. A short jump is within −128 to +127 bytes from the current location. A near jump is within the same code segment, and a far jump is outside the current segment.

Instruction formats:

```
JMP shortlabel      JMP reg16
JMP nearlabel       JMP mem16
JMP farlabel        JMP mem32
```

Умовний перехід за ознаками (прапорами)

Mnemonic	Comment	Mnemonic	Comment
JA	Jump if above	JE	Jump if equal
JNA	Jump if not above	JNE	Jump if not equal
JAE	Jump if above or equal	JZ	Jump if zero
JNAE	Jump if not above or equal	JNZ	Jump if not zero
JB	Jump if below	JS	Jump if sign
JNB	Jump if not below	JNS	Jump if not sign
JBE	Jump if below or equal	JC	Jump if carry
JNBE	Jump if not below or equal	JNC	Jump if no carry
JG	Jump if greater	JO	Jump if overflow
JNG	Jump if not greater	JNO	Jump if no overflow
JGE	Jump if greater or equal	JP	Jump if parity
JNGE	Jump if not greater or equal	JPE	Jump if parity equal
JL	Jump if less	JNP	Jump if no parity
JNL	Jump if not less	JPO	Jump if parity odd
JLE	Jump if less or equal	JNLE	Jump if not less than or equal

Команди зіставлення операндів

CMP

Compare

Зіставлення

O	D	I	S	Z	A	P	C
*			*	*	*	*	*

Зіставлення операндів за результатами виконання неявної операції віднімання

Compares the destination to the source by performing an implied subtraction of the source from the destination.

Instruction formats:

```
CMP   reg,reg      CMP   reg,imm
CMP   mem,reg      CMP   mem,imm
CMP   reg,mem      CMP   accum,imm
```

TEST

Test

Тестування

O	D	I	S	Z	A	P	C
0			*	*	?	*	0

Порозрядна неявна операція ТА

Tests individual bits in the destination operand against those in the source operand. Performs a logical AND operation that affects the flags but not the destination operand.

Instruction formats:

```
TEST  reg,reg      TEST  reg,imm
TEST  mem,reg      TEST  mem,imm
TEST  reg,mem      TEST  accum,imm
```

Типи умов у командах передачі керування

Інструкції умовної передачі курування можна розділити на чотири групи відповідно до умов:

- значень прапора;
- рівності між операндами або значення (E) CX;
- порівняння незнакових операндів;
- порівняння знакових операндів.

1. Перехід за умовами відповідно до значень прапорів Zero, Carry, Overflow, Parity, Sign

Mnemonic	Description	Flags / Registers
JZ	Jump if zero	ZF = 1
JNZ	Jump if not zero	ZF = 0
JC	Jump if carry	CF = 1
JNC	Jump if not carry	CF = 0
JO	Jump if overflow	OF = 1
JNO	Jump if not overflow	OF = 0
JS	Jump if signed	SF = 1
JNS	Jump if not signed	SF = 0
JP	Jump if parity (even)	PF = 1
JNP	Jump if not parity (odd)	PF = 0

2. Перехід за умовами відповідно до результатів перевірки на рівність

За результатами порівнянь двох операндів, наприклад командою CMP, або на основі значення CX, ECX (RCX).

```
CMP leftOp,rightOp
```

Mnemonic	Description
JE	Jump if equal (*leftOp* = *rightOp*)
JNE	Jump if not equal (*leftOp* ≠ *rightOp*)
JCXZ	Jump if CX = 0
JECXZ	Jump if ECX = 0
JRCXZ	Jump if RCX = 0 (64-bit mode)

3. Перехід за умовами відповідно до результатів порівняння незнакових операндів

```
CMP leftOp,rightOp
```

Mnemonic	Description
JA	Jump if above (if *leftOp* > *rightOp*)
JNBE	Jump if not below or equal (same as JA)
JAE	Jump if above or equal (if *leftOp* ≥ *rightOp*)
JNB	Jump if not below (same as JAE)
JB	Jump if below (if *leftOp* < *rightOp*)
JNAE	Jump if not above or equal (same as JB)
JBE	Jump if below or equal (if *leftOp* ≤ *rightOp*)
JNA	Jump if not above (same as JBE)

4.Перехід за умовами відповідно до результатів порівняння знакових операндів

```
CMP leftOp,rightOp
```

Mnemonic	Description
JG	Jump if greater (if *leftOp* > *rightOp*)
JNLE	Jump if not less than or equal (same as JG)
JGE	Jump if greater than or equal (if *leftOp* ≥ *rightOp*)
JNL	Jump if not less (same as JGE)
JL	Jump if less (if *leftOp* < *rightOp*)
JNGE	Jump if not greater than or equal (same as JL)
JLE	Jump if less than or equal (if *leftOp* ≤ *rightOp*)
JNG	Jump if not greater (same as JLE)

Приклади команд умовного переходу

```
mov  al,+127    ; hexadecimal value is 7Fh
cmp  al,-128    ; hexadecimal value is 80h
ja   IsAbove    ; jump not taken, because 7Fh < 80h
jg   IsGreater  ; jump taken, because +127 > -128
```

Example 1

```
mov   edx,-1
cmp   edx,0
jnl   L5   ; jump not taken (-1 >= 0 is false)
jnle  L5   ; jump not taken (-1 > 0 is false)
jl    L1   ; jump is taken (-1 < 0 is true)
```

Example 2

```
mov   bx,+32
cmp   bx,-35
jng   L5   ; jump not taken (+32 <= -35 is false)
jnge  L5   ; jump not taken (+32 < -35 is false)
jge   L1   ; jump is taken (+32 >= -35 is true)
```

Example 3

```
mov  ecx,0
cmp  ecx,0
jg   L5    ; jump not taken (0 > 0 is false)
jnl  L1    ; jump is taken (0 >= 0 is true)
```

Example 4

```
mov  ecx,0
cmp  ecx,0
jl   L5    ; jump not taken (0 < 0 is false)
jng  L1    ; jump is taken (0 <= 0 is true)
```

Приклади переходу відповідно до значень контрольних бітів

Example 1

```
mov   al,status
test  al,00100000b   ; test bit 5
jnz   DeviceOffline
```

Example 2

```
mov   al,status
test  al,00010011b   ; test bits 0,1,4
jnz   InputDataByte
```

Example 3

```
mov   al,status
and   al,10001100b   ; mask bits 2,3,7
cmp   al,10001100b   ; all bits set?
je    ResetMachine   ; yes: jump to label
```

Сканування бітів

Сканує операнд з метою пошуку першого встановленого біту. Якщо біт знайдено, то прапорець ZF=0, а в операнді dist вказується на номер біта (індекс) першого біту. Якщо встановлений біт не знайдено, то ZF=1.
BSF сканує від біта LSB до MSB, а BSR - від біта MSB до LSB .

BSF, BSR

Bit Scan (x86)

O	D	I	S	Z	A	P	C
?			?	?	?	?	?

Scans an operand to find the first set bit. If the bit is found, the Zero flag is cleared, and the destination operand is assigned the bit number (index) of the first set bit encountered. If no set bit is found, ZF = 1. BSF scans from bit 0 to the highest bit, and BSR starts at the highest bit and scans toward bit 0.

Instruction formats (apply to both BSF and BSR):

```
BSF reg16,r/m16
BSF reg32,r/m32
```

Тестування бітів

BT, BTC, BTR, BTS

Bit Tests (x86)

Тестування бітів

O	D	I	S	Z	A	P	C
?			?	?	?	?	*

Copies a specified bit (*n*) into the Carry flag. The destination operand contains the value in which the bit is located, and the source operand indicates the bit's position within the destination. BT copies bit *n* to the Carry flag. BTC copies bit *n* to the Carry flag and complements bit *n* in the destination operand. BTR copies bit *n* to the Carry flag and clears bit *n* in the destination. BTS copies bit *n* to the Carry flag and sets bit *n* in the destination.

BT встановлює ознаку CF (Carry) відповідно до значення біту операнда-отримувача, номер якого (n) вказаний в операнді-джерелі.
BTC, BTR, BTS також (відповідно) інвертує, скидає в 0, встановлює в 1 значення біту (n) операнда-отримувача.

Instruction formats:

```
BT r/m16,imm8
BT r/m32,imm8
BT r/m16,r16
BT r/m32,r32
```

Умовне встановлення

SET*condition*	**Set Conditionally** **Умовне встановлення** O D I S Z A P C ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
	If the given flag condition is true, the byte specified by the destination operand is assigned the value 1. If the flag condition is false, the destination is assigned a value of 0. The possible values for *condition* were listed in Table B-2. Встановлення в одиничне значення байту операнда-отримувача у разі наявності вказаної умови, інакше - в нульове значення. Умови аналогічні умовампереходу за ознаками (J) Instruction formats: `SETcond reg8` `SETcond mem8`

Завдання до самостійної роботи

1. Засвоїти формат команд на мові асемблера архітектури IA-32 і правила виконання відповідних операцій.
2. Виконати в середовищі MASM32 і налагоджувачі усі приклади, які наведено на слайдах, з вказаними даними та іншими довільними операндами.

Література

1. Intel® 64 and IA-32 Architectures Software Developer's Manual. - Order Number: 325462-067US, May 2018 (ch.5)
2. Kip R. Irvine. Assembly Language for x86 Processors. Florida International University School of Computing and Information Sciences. 7th Edition, 2014 (ch.6.1-6.4,7.1,app.A)