南京大学
NANJING UNIVERSITY

nasm基本语法

--161250071 刘瑗玮

- 本PPT旨在介绍一个基本的语法，一些不是必须要用到的语法可能不在讲解之列。课后自行阅读nasm.pdf和nasmdoc.pdf

```
;Section to store uninitialized variables
section .data
string: db 'Hello World', 0Ah
length: equ 13

section .bss
var: resb 1

section .text
global _start:
_start:
mov eax, 4
mov ebx, 1
mov ecx, string
mov edx, length
int 80h

;System Call to exit
mov eax, 1
mov ebx, 0
int 80h
```

Sections in NASM

- *Section .text:* This is the part of a NASM Program which contains the executable code. It is the place from where the execution starts in NASM program, analogous to the main( ) function in CProgramming.

- *section .bss :* This is the part of program used to declare variables without initialization

- *section .data* : This is the part of program used to declare and initialize the variables in the program.

example

```
section .data
     var1: db 10
     str1: db “Hello World!..”
section .bss
     var3: resb 1
     var4: resq 1
```

- **RESx** directive is used to reserve just space in memory for a variable without giving any initial values.
- **Dx** directive is used for declaring space in the memory for any variable and also providing the initial values at that moment

x	Meaning	No: of Bytes
b	BYTE	1
w	WORD	2
d	DOUBLE WORD	4
q	QUAD WORD	8
t	TEN WORD	20

声明变量

- 可能会想每次Dx或者RESx命令只能声明一个变量吗？那不是很麻烦？如果要声明一个字符串呢？每次一个字符？
- 可以这样：
- `var: db 10,5,8,9`
- `string: db “Hello”`
  `string2: db “H”, “e”, “l”, “l”, “o”`
- 上面两种是等价的

访问变量-解引用

- MOV dword[ebx], 1
  INC BYTE[label]
  ADD eax, dword[label]

- []之前可以有的：
- **BYTE, WORD, DWORD, QWORD, TWORD**

基本指令集之传送指令、算术指令

- MOV
- MOVZX
- ADD
- SUB
- MUL
- DIV

寄存器长度问题

- eax d
- ax w
- al b
- ah b
- 0000 0000 0000 0000 0000 0000 0000 0000
- 0000 0000 0000 0000 0000 0000 0000 0000
- 0000 0000 0000 0000 0000 0000 0000 0000
- 0000 0000 0000 0000 0000 0000 0000 0000

MOV

- mov eax, ebx
- mov ecx, 109
- mov al, bl
- mov byte[var1], al
- mov word[var2], 200
- mov eax, dword[var3]

MOVZX(无符号扩展)

- ```
  movzx eax, ah
  movzx cx, al
  ```


  ```

ADD

- ```
  add eax, ecx ; eax = eax + ecx
  add al, ah ; al = al + ah
  add ax, 5
  add edx, 31h
  ```
  ```

SUB

- ```
  sub eax, ecx ; eax = eax - ecx
  sub al, ah ; al = al - ah
  sub ax, 5
  sub edx, 31h
  ```
  ```

MUL

- *mul src*
- 要知道相同位数的两个数字相乘之后位数翻倍

- If src is 1 byte then AX = AL * src
- If src is 1 word (2 bytes) then DX:AX = AX * src (ie. Upper 16 bits of the result will go to DX and the lower 16 bits will go to AX)
- If src is 2 words long(32 bit) then EDX:EAX = EAX * src (ie. Upper 32 bits of the result will go to EDX and the lower 32 bits will go to EAX)

DIV

- div src
- 跟乘法有一点反过来的意思
- If src is 1 byte then AX will be divide by src, remainder will go to AH and quotient will go to AL
- If src is 1 word (2 bytes) then DX:AX will be divide by src, remainder will go to DX and quotient will go to AX
- If src is 2 words long(32 bit) then EDX:EAX will be divide by src, remainder will go to EDX and quotient will go to EAX

条件分支指令

- JMP
- CMP
- …

JMP

- label:

  JMP label

  JMP exit

  ----

  exit:

CMP

- *CMP op1, op2*
- it will affect the CPU FLAGS

Instruction	Working
JZ	Jump If Zero Flag is Set
JNZ	Jump If Zero Flag is Unset
JC	Jump If Carry Flag is Set
JNC	Jump If Carry Flag is Unset
JP	Jump If Parity Flag is Set
JNP	Jump If Parity Flag is Unset
JO	Jump If Overflow Flag is Set
JNO	Jump If Overflow Flag is Unset

i) For Unsigned numbers:

Instruction	**Working**
JE	Jump if op1 == op2
JNE	Jump if op1 ≠ op2
JA (Jump if above)	Jump if op1 > op2
JNA	Jump if op1 <= op2
JB (Jump if below)	Jump if op1 < op2
JNB	Jump if op1 >= op2

ii) For Signed numbers:

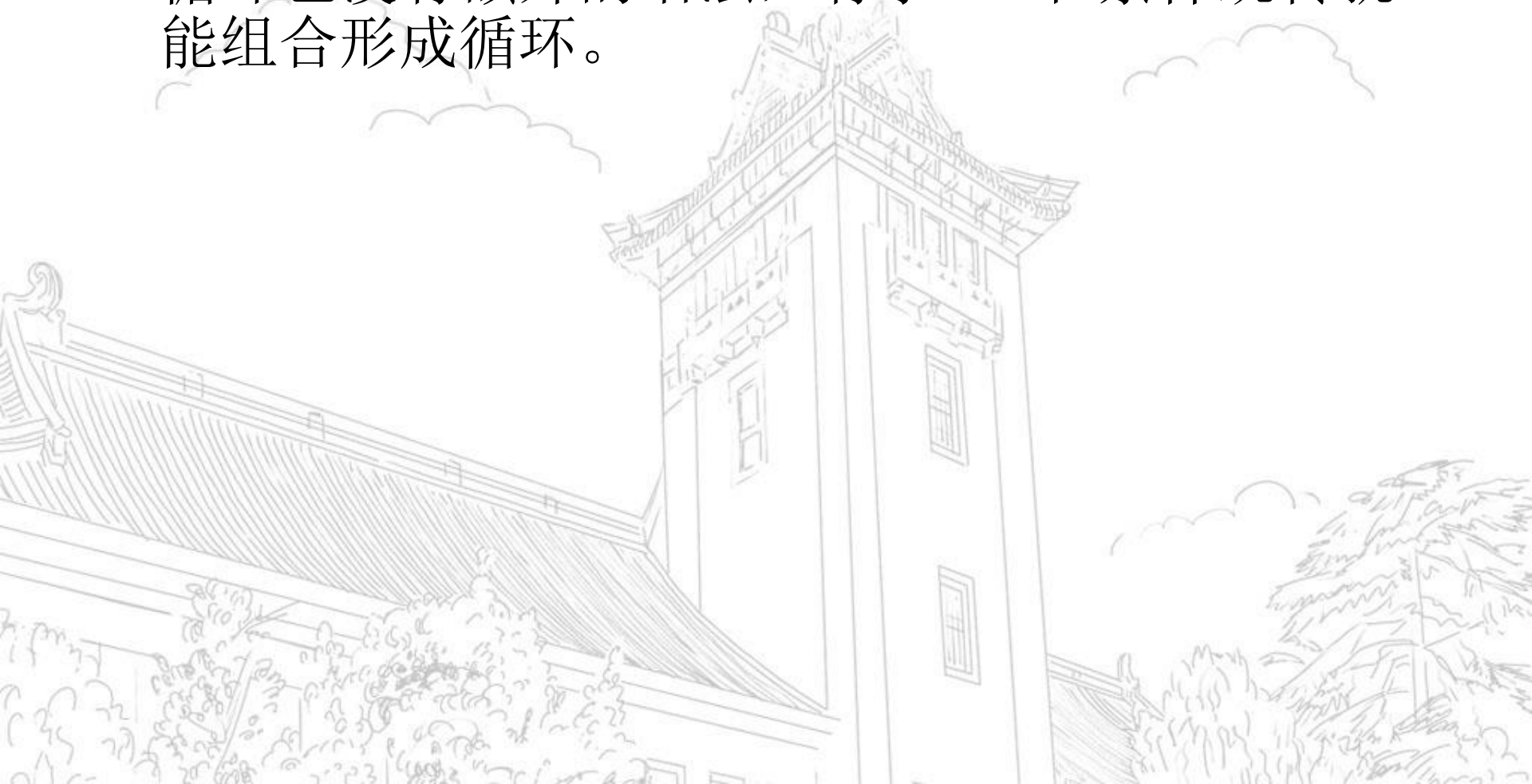
Instruction	Working
JE	Jump if op1 == op2
JNE	Jump if op1 ≠ op2
JG (Jump if greater)	Jump if op1 > op2
JNG	Jump if op1 <= op2
JL (Jump if lesser)	Jump if op1 < op2
JNL	Jump if op1 >= op2

条件分支实例

```
cmp eax, ebx
JE  if
    ------
    JMP L1
if:
    INC eax
L1:
    -----------
```

循环

- 循环也没有额外的语法，有了JMP和条件跳转就能组合形成循环。



位运算

- AND
- OR
- XOR
- NOT
- TEST
- SHL
- SHR
- ROL
- ROR
- RCL
- RCR

AND

- *AND op1, op1*
  op1=op1 and op2

- or, xor, 类似

NOT

- *NOT op1*
- *op1=~op1*

TEST

- *TEST op1, op2*

- It performs the bitwise logical AND of op1 and op2 but it won't save the result to any registers. Instead the result of the operation will affect CPU FLAGs.

SHL与SHR

- SHL – Shift Left

- *sy: SHL op1, op2*
  op1 = op1 << op2
- example

  shl eax, 5

op1 should be a reg / memory variable but op2 must be an immediate(constant) value

SHR类似，左边用0补充

ROL与ROR

- 循环左移与循环右移
- *ROL op1, op2*

栈操作

- PUSH
- POP
- PUSHA
- POPA

- PUSHA和POPA用于将所有通用寄存器压栈出栈，当你在函数调用时需要保存现场的时候用会比较方便

PUSH

- PUSH decreases the value of ESP and copies the value of a reg / constant into the system stack

- PUSH ax ;ESP减2
  PUSH eax ;ESP减4
  PUSH ebx
  PUSH dword 5
  PUSH word 258

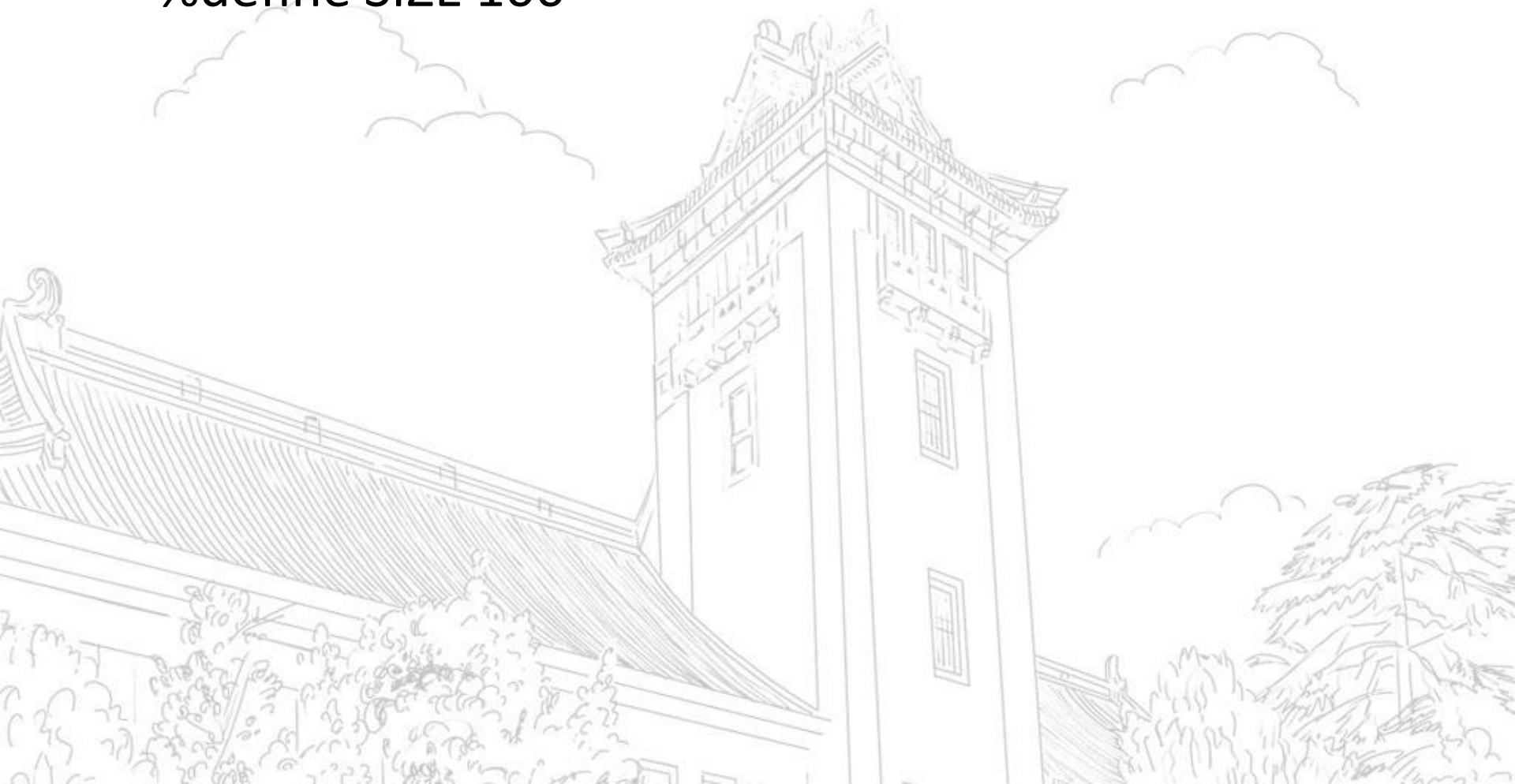
POP

- POP bx ; ESP= ESP + 2
  POP ebx ; ESP= ESP + 4

- increases the value of ESP

预处理指令

- %define SIZE 100



系统调用

- EXIT SYSTEM CALL
- mov eax, 1 ;System Call Number
  mov ebx, 0 ;Parameter
  int 80h ;Triggering OS Interrupt

- 注意将系统调用号放在eax寄存器里，参数放在其他通用寄存器里，然后使用int指令。

Read System Call

- ```
  mov eax, 3
  mov ebx, 0
  mov ecx, var
  mov edx, dword[size]
  int 80h
  ```
  ```

Write System Call

- mov eax, 4
  mov ebx, 1
  mov ecx, msg1
  mov edx, size1
  int 80h

Hello World

```
section .text ;Code Section
global _start:
_start:
mov eax, 4 ;Using int 80h to implement
write() sys_call
mov ebx, 1
mov ecx, string
mov edx, length
int 80h
;Exit System Call
mov eax, 1
mov ebx, 0
int 80h
```

```
section .data
string: db 'Hello World', 0Ah
length: equ 13
```

函数

- CALL与RET

```
SECTION .data
msg     db      'Hello, brave new world!', 0Ah

SECTION .text
global  _start

_start:
    mov     eax, msg
    call    strlen

    mov     edx, eax
    mov     ecx, msg
    mov     ebx, 1
    mov     eax, 4
    int     80h

    mov     ebx, 0
    mov     eax, 1
    int     80h
```

```
strlen:
    push    ebx
    mov     ebx, eax

nextchar:
    cmp     byte [eax], 0
    jz      finished
    inc     eax
    jmp     nextchar

finished:
    sub     eax, ebx
    pop     ebx
    ret
```

谢谢！