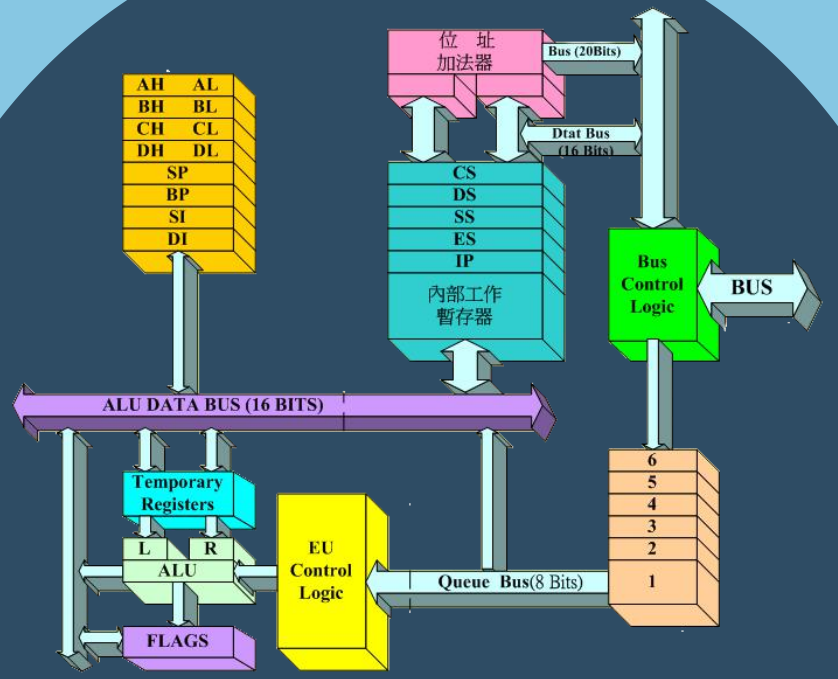
汇编过程

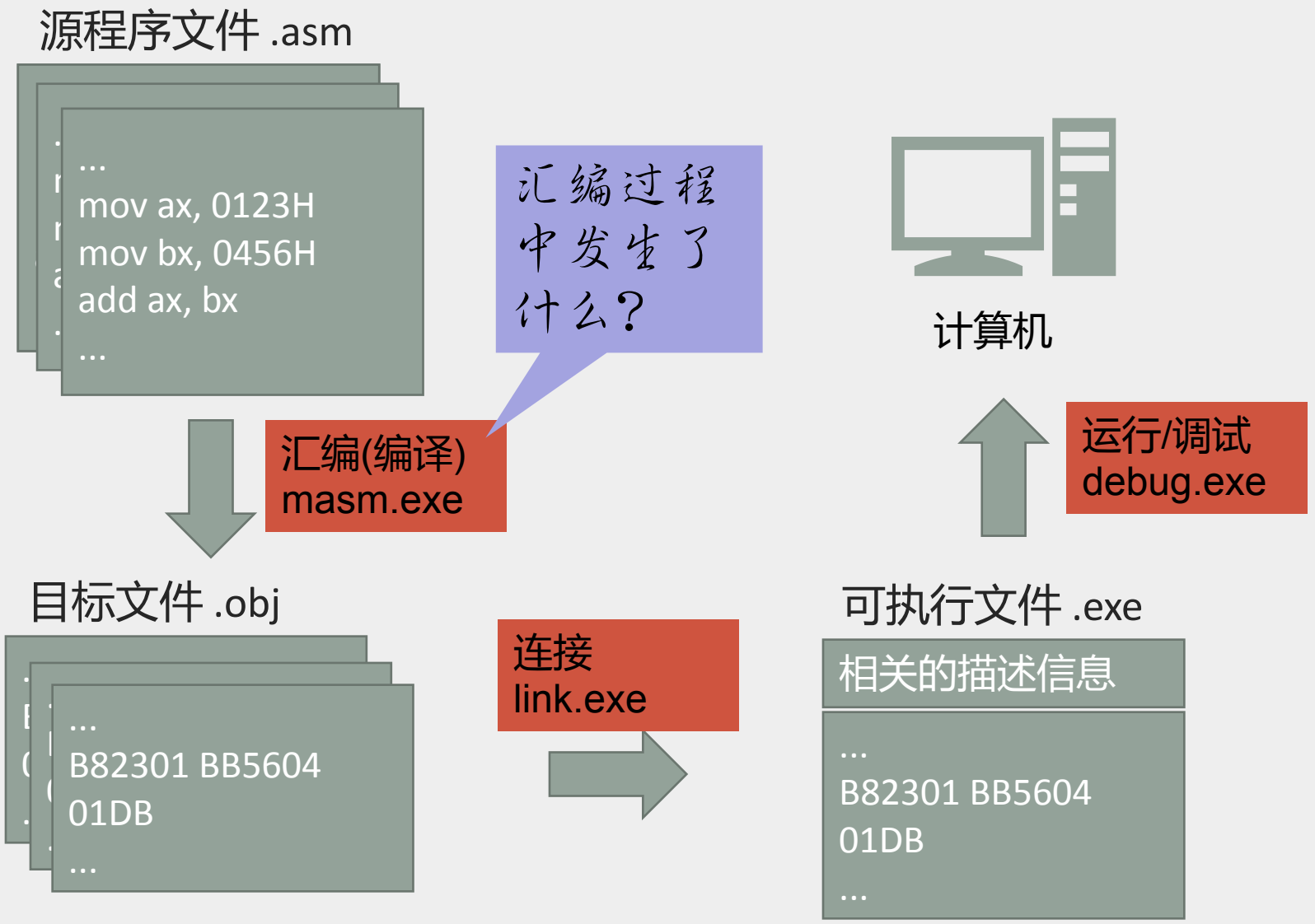
贺利坚　主讲



汇编语言程序设计

Assembly Language

.exe的诞生

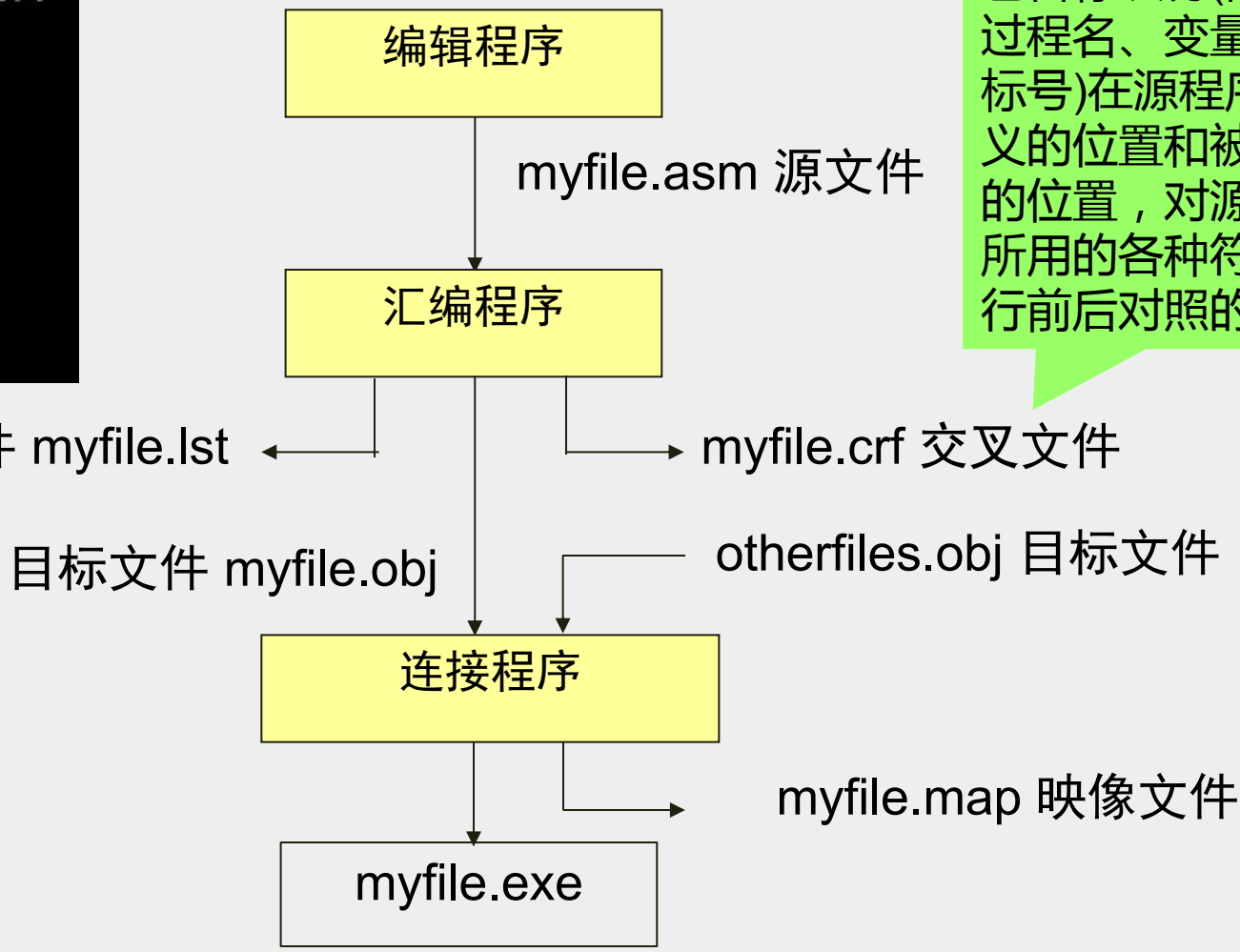

源程序文件 .asm
...
mov ax, 0123H
mov bx, 0456H
add ax, bx
...
汇编过程中发生了什么？
汇编(编译)
masm.exe
目标文件 .obj
...
B82301 BB5604
01DB
...
连接
link.exe
可执行文件 .exe
相关的描述信息
...
B82301 BB5604
01DB
...
计算机
运行/调试
debug.exe

程序运行步骤及生成的文件

```
C:\>masm ptest
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987.

Object filename [ptest.OBJ]:
Source listing  [NUL.LST]: ptest
Cross-reference [NUL.CRF]: ptest

  50596 + 465948 Bytes symbol space free

       0 Warning Errors
       0 Severe  Errors
```

列表文件LST：将源程序、目标程序、错误信息列表，以供检查程序用。

```
C:\>cref ptest.crf
Microsoft (R) Cross-Reference Utility  V
Copyright (C) Microsoft Corp 1981-1985,

Listing [ptest.REF]:

5 Symbols
```



交叉引用文件CRF：包含标识符(段名、过程名、变量名、标号)在源程序中定义的位置和被引用的位置，对源程序所用的各种符号进行前后对照的文件。

观察列表文件

```
assume cs:code
data segment
  n1 db 1
data ends
code segment
start:mov ax,data
      mov ds,ax
      lea bx, n1
      call subprog
      call subprog
      mov ax,4c00h
      int 21h
subprog:
      mov ax,bx
      mov cx,[bx]
      mov dx,100h
      ret
code ends
end start
```

列表文件：

```
Microsoft (R) Macro Assembler Version 5.00                  6/19/17 15:47:06
                                                            Page     1-1


                                assume cs:code
0000                            data segment
0000  01                            n1 db 1
0001                            data ends
0000                            code segment
0000  B8 ---- R                 start:mov ax,data
0003  8E D8                           mov ds,ax
0005  8D 1E 0000 R                    lea bx, n1
0009  E8 0014 R                       call subprog
000C  E8 0014 R                       call subprog
000F  B8 4C00                         mov ax,4c00h
0012  CD 21                           int 21h
0014                            subprog:
0014  8B C3                           mov ax,bx
0016  8B 0F                           mov cx,[bx]
0018  BA 0100                         mov dx,100h
001B  C3                              ret
001C                            code ends
                                end start
Microsoft (R) Macro Assembler Version 5.00                  6/19/17 15:47:06
                                                            Symbols-1
```

体会汇编过程(两遍汇编)

- 第一次汇编：确定地址，翻译成各条机器码，字符标号原样写出；
- 第二次汇编：标号代真，将字符标号用计算出的地址值或偏移量代换。

源　程　序	第一遍汇编	第二遍汇编
assume cs:codesg		
codesg segment	0000	0000
org 1000H	1000	1000
START:	1000	1000
lea bx, BUF	1000　8D 1E BUF	1000　8D 1E 1015
mov dx,[bx]	1004　8B 17	1004　8B 17
BACK: mov cx, [bx]	1006　8B 0F	1006　8B 0F
jcxz OK	1008　E3 OK	1008　E3 04
inc bx	100A　43	100A　43
inc bx	100B　43	100B　43
jmp short BACK	100C　EB BACK	100C　EB F8
OK: mov dx, bx	100E　8B D3	100E　8B D3
mov ax, 4c00H	1010　B8 4C00	1010　B8 4C00
int 21H	1013　CD 21	1013　CD 21
BUF dw 1234H	1015　1234	1015　1234
codesg ends	1017	1017
end start		

- 伪指令不产生机器码；
- 汇编指令与机器指令一一对应。