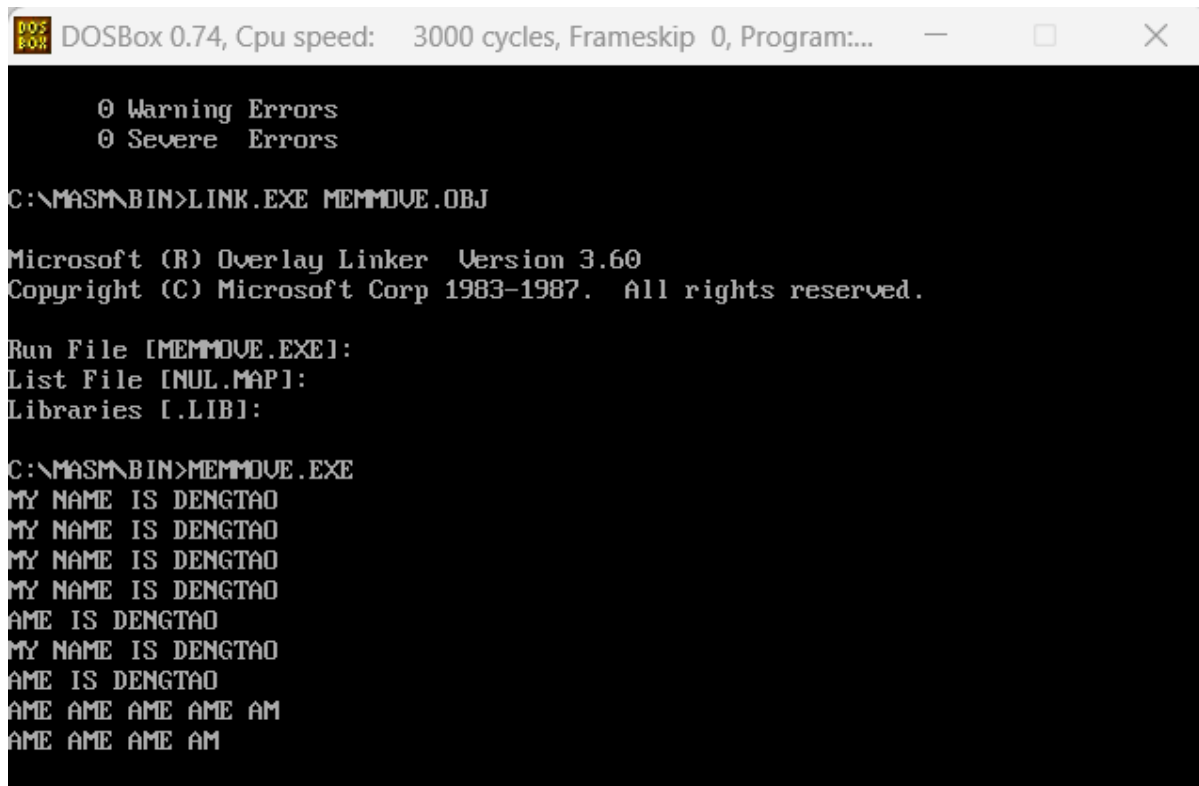


1. strcpy



```
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program:...

0 Warning Errors
0 Severe Errors

C:\MASM\BIN>LINK.EXE MEMMOVE.OBJ

Microsoft (R) Overlay Linker Version 3.60
Copyright (C) Microsoft Corp 1983-1987. All rights reserved.

Run File [MEMMOVE.EXE]:
List File [NUL.MAP]:
Libraries [.LIB]:

C:\MASM\BIN>MEMMOVE.EXE
MY NAME IS DENGTAO
MY NAME IS DENGTAO
MY NAME IS DENGTAO
MY NAME IS DENGTAO
AME IS DENGTAO
MY NAME IS DENGTAO
AME IS DENGTAO
AME AME AME AME AM
AME AME AME AM
```

memmove 处理子程序逻辑为，先计算原串的长度（以\$结尾），再将原串中每个字节依次复制到目标串的位置。

第一次调用时，string1和string2无重叠，正确复制；第二次调用时，string2地址为string1减去4，调用memmove后，string1变为了AME IS DENGTAO\$GTAO\$，因为输出默认以\$结尾，故输出变为了AME IS DENGTAO；第三次调用，string2地址为string1加上4，因为复制过程为逐个复制，所以一边修改string1的内容一边复制，导致string1变为AME AME AME AME AM\$，string2变为AME AME AME AM

2. strcmp

```
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program:...
```

```
Libraries [.LIB]:

C:\MASM\BIN>MASM.EXE STRCMP.ASM
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

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

51590 + 464954 Bytes symbol space free

0 Warning Errors
0 Severe Errors

C:\MASM\BIN>STRCMP.EXE
234
123456<234
C:\MASM\BIN>STRCMP.EXE
123456
123456=123456
C:\MASM\BIN>STRCMP.EXE
123
123456>123
C:\MASM\BIN>_
```

3. charcount

```
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program:...
```

```
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

Object filename [CHARCO~1.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:

51504 + 465040 Bytes symbol space free

0 Warning Errors
0 Severe Errors

C:\MASM\BIN>LINK.EXE CHARCO~1.OBJ

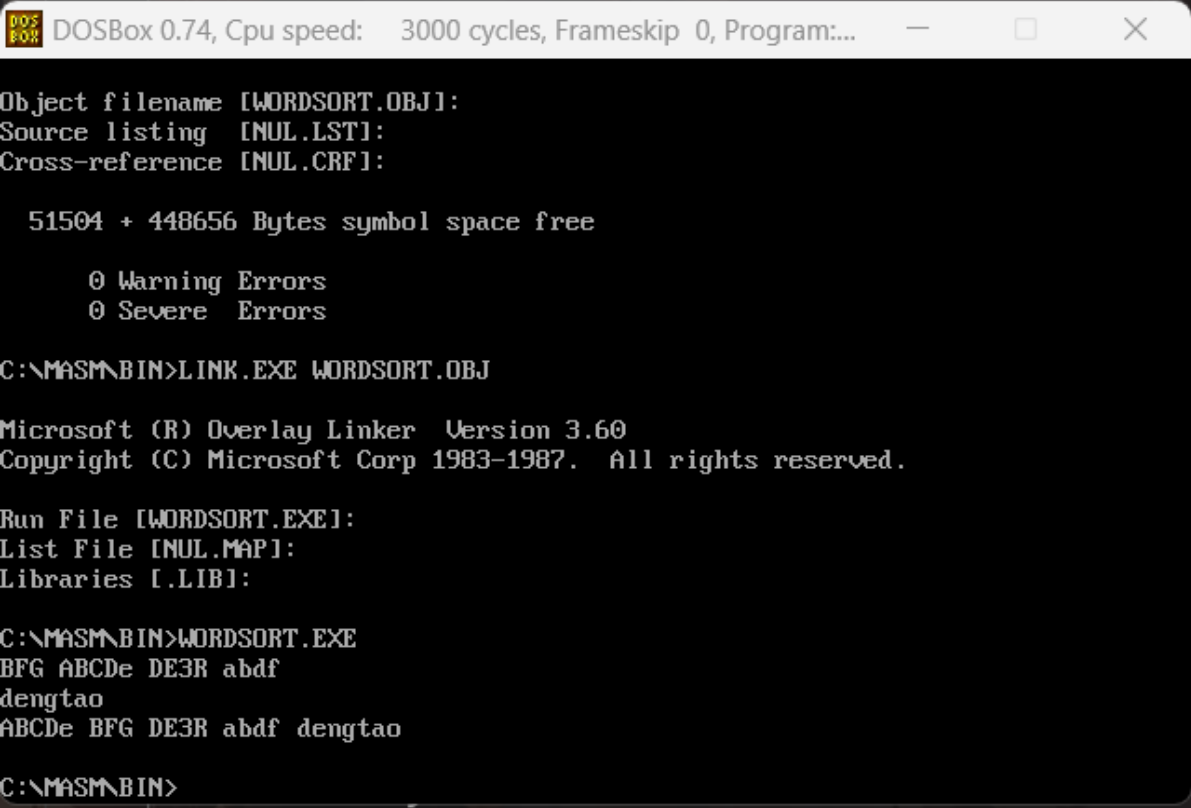
Microsoft (R) Overlay Linker Version 3.60
Copyright (C) Microsoft Corp 1983-1987. All rights reserved.

Run File [CHARCO~1.EXE]:
List File [NUL.MAP]:
Libraries [.LIB]:

C:\MASM\BIN>CHARCO~1.EXE
AbAcD
00002
C:\MASM\BIN>_
```

子程序如果想从堆栈中获取参数，没有办法直接POP出来，因为CALL指令调用时，会先将下一条指令地址压入栈中，想要获取CX和SI必须先把栈顶保存，取出CX和SI再恢复栈顶

4. wordsort



```
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program:...  
Object filename [WORDSORT.OBJ]:  
Source listing [NUL.LST]:  
Cross-reference [NUL.CRF]:  
  
51504 + 448656 Bytes symbol space free  
  
0 Warning Errors  
0 Severe Errors  
  
C:\MASM\BIN>LINK.EXE WORDSORT.OBJ  
  
Microsoft (R) Overlay Linker Version 3.60  
Copyright (C) Microsoft Corp 1983-1987. All rights reserved.  
  
Run File [WORDSORT.EXE]:  
List File [NUL.MAP]:  
Libraries [.LIB]:  
  
C:\MASM\BIN>WORDSORT.EXE  
BFG ABCDe DE3R abdf  
dengtao  
ABCDe BFG DE3R abdf dengtao  
  
C:\MASM\BIN>
```

按字典序升序排列，可以看到ABCDe与BFG交换了位置，并且输入的dengtao也插入到了单词表中