```
1           ;代码清单12-1
2           ;文件名：c12_mbr.asm
3           ;文件说明：硬盘主引导扇区代码
4           ;创建日期：2011-10-27 22:52
5
6           ;设置堆栈段和栈指针
7           mov eax,cs
8           mov ss,eax
9           mov sp,0x7c00
10
11          ;计算GDT所在的逻辑段地址
12          mov eax,[cs:pgdt+0x7c00+0x02]       ;GDT的32位线性基地址
13          xor edx,edx
14          mov ebx,16
15          div ebx                             ;分解成16位逻辑地址
16
17          mov ds,eax                          ;令DS指向该段以进行操作
18          mov ebx,edx                         ;段内起始偏移地址
19
20          ;创建0#描述符，它是空描述符，这是处理器的要求
21          mov dword [ebx+0x00],0x00000000
22          mov dword [ebx+0x04],0x00000000
23
24          ;创建1#描述符，这是一个数据段，对应0~4GB的线性地址空间
25          mov dword [ebx+0x08],0x0000ffff     ;基地址为0，段界限为0xfffff
26          mov dword [ebx+0x0c],0x00cf9200     ;粒度为4KB，存储器段描述符
27
28          ;创建保护模式下初始代码段描述符
29          mov dword [ebx+0x10],0x7c0001ff     ;基地址为0x00007c00，512字节
30          mov dword [ebx+0x14],0x00409800     ;粒度为1个字节，代码段描述符
31
32          ;创建以上代码段的别名描述符
33          mov dword [ebx+0x18],0x7c0001ff     ;基地址为0x00007c00，512字节
34          mov dword [ebx+0x1c],0x00409200     ;粒度为1个字节，数据段描述符
35
36          mov dword [ebx+0x20],0x7c00fffe
37          mov dword [ebx+0x24],0x00cf9600
38
39          ;初始化描述符表寄存器GDTR
40          mov word [cs: pgdt+0x7c00],39       ;描述符表的界限
41
42          lgdt [cs: pgdt+0x7c00]
43
44          in al,0x92                          ;南桥芯片内的端口
45          or al,0000_0010B
46          out 0x92,al                         ;打开A20
47
48          cli                                 ;中断机制尚未工作
49
50          mov eax,cr0
51          or eax,1
52          mov cr0,eax                         ;设置PE位
53
```

```
54          ;以下进入保护模式... ...
55          jmp dword 0x0010:flush              ;16位的描述符选择子：32位偏移
56
57          [bits 32]
58    flush:
59          mov eax,0x0018
60          mov ds,eax
61
62          mov eax,0x0008                      ;加载数据段(0..4GB)选择子
63          mov es,eax
64          mov fs,eax
65          mov gs,eax
66
67          mov eax,0x0020                      ;0000 0000 0010 0000
68          mov ss,eax
69          xor esp,esp                         ;ESP <- 0
70
71          mov dword [es:0x0b8000],0x072e0750 ;字符'P'、'.'及其显示属性
72          mov dword [es:0x0b8004],0x072e074d ;字符'M'、'.'及其显示属性
73          mov dword [es:0x0b8008],0x07200720 ;两个空白字符及其显示属性
74          mov dword [es:0x0b800c],0x076b076f ;字符'o'、'k'及其显示属性
75
76          ;开始冒泡排序
77          mov ecx,pgdt-string-1               ;遍历次数=串长度-1
78    @@1:
79          push ecx                            ;32位模式下的loop使用ecx
80          xor bx,bx                           ;32位模式下，偏移量可以是16位，也可以
81    @@2:                                      ;是后面的32位
82          mov ax,[string+bx]
83          cmp ah,al                           ;ah中存放的是源字的高字节
84          jge @@3
85          xchg al,ah
86          mov [string+bx],ax
87    @@3:
88          inc bx
89          loop @@2
90          pop ecx
91          loop @@1
92
93          mov ecx,pgdt-string
94          xor ebx,ebx                         ;偏移地址是32位的情况
95    @@4:                                      ;32位的偏移具有更大的灵活性
96          mov ah,0x07
97          mov al,[string+ebx]
98          mov [es:0xb80a0+ebx*2],ax           ;演示0~4GB寻址。
99          inc ebx
100         loop @@4
101
102         hlt
103
104 ;-------------------------------------------------------------------------------
105     string          db 's0ke4or92xap3fv8giuzjcy5l1m7hd6bnqtw.'
106 ;-------------------------------------------------------------------------------
```

```
107      pgdt             dw 0
108                       dd 0x00007e00      ;GDT的物理地址
109 ;-------------------------------------------------------------------------------
110      times 510-($-$$) db 0
111                       db 0x55,0xaa
```