实验一

数据科学与计算机学院 计算机类 18 级 18340064 黄思蓉

一、 实验题目

编写一个引导扇区程序

二、 实验要求

接管裸机的控制权：

- 搭建和应用实验环境

虚拟机安装，生成一个基本配置的虚拟机 XXXPC 和多个 1.44MB 容量的虚拟软盘，将其中一个虚拟软盘用 DOS 格式化为 DOS 引导盘，用 WinHex 工具将其中一个虚拟软盘的首扇区填满你的个人信息。

- 接管裸机的控制权

设计 IBM_PC 的一个引导扇区程序，程序功能是：用字符‘A'从屏幕左边某行位置 45 度角下斜射出，保持一个可观察的适当速度直线运动，碰到屏幕的边后产生反射，改变方向运动，如此类推，不断运动；在此基础上，增加你的个性扩展，如同时控制两个运动的轨迹，或炫酷动态变色，个性画面，如此等等，自由不限。还要在屏幕某个区域特别的方式显示你的学号姓名等个人信息。将这个程序的机器码放进放进第三张虚拟软盘的首扇区，并用此软盘引导你的 XXXPC，直到成功。

三、 实验方案

1 安装 VMware，在 VMware 中创建一个新的虚拟机，软盘的映像文件配置为用 asm 文件生成的 img 文件

2 安装 nasm 编译器，编译 asm 文件

3 学习汇编语言，编写引导程序代码

四、 实验过程

1 编写引导程序

老师提供的代码其实已经实现了以字符‘A’作运动轨迹，改变一下 ds 和 es 的指向就可以编译成功：

```
start:
    mov ax,0x7c00
    mov ds,ax                   ; DS = CS,指向数据段
    mov ax,0B800h
    mov es,ax                   ; ES = B800h, 指向显示器
```

所以在老师的代码的基础上稍作修改：char 是要显示的字符串“learnos”，number 是学号“18340064”，name 是要显示的名字“wongsiyoung”，字符后面是控制字符显示的形态和颜色

```
char db 'l',42h,'e',21h,'a',14h,'r',42h,'n',21h,'O',14h,'S',42h,'0',0       ;要显示的字符
number  db  '1',89h,'8',89h,'3',89h,'4',89h,'0',89h,'0',89h,'6',89h,'4',89h
name    db 'w',89h,'o',89h,'n',89h,'g',89h,'s',89h,'i',89h,'y',89h,'o',89h,'u',89h,'n',89h,'g',89h
```

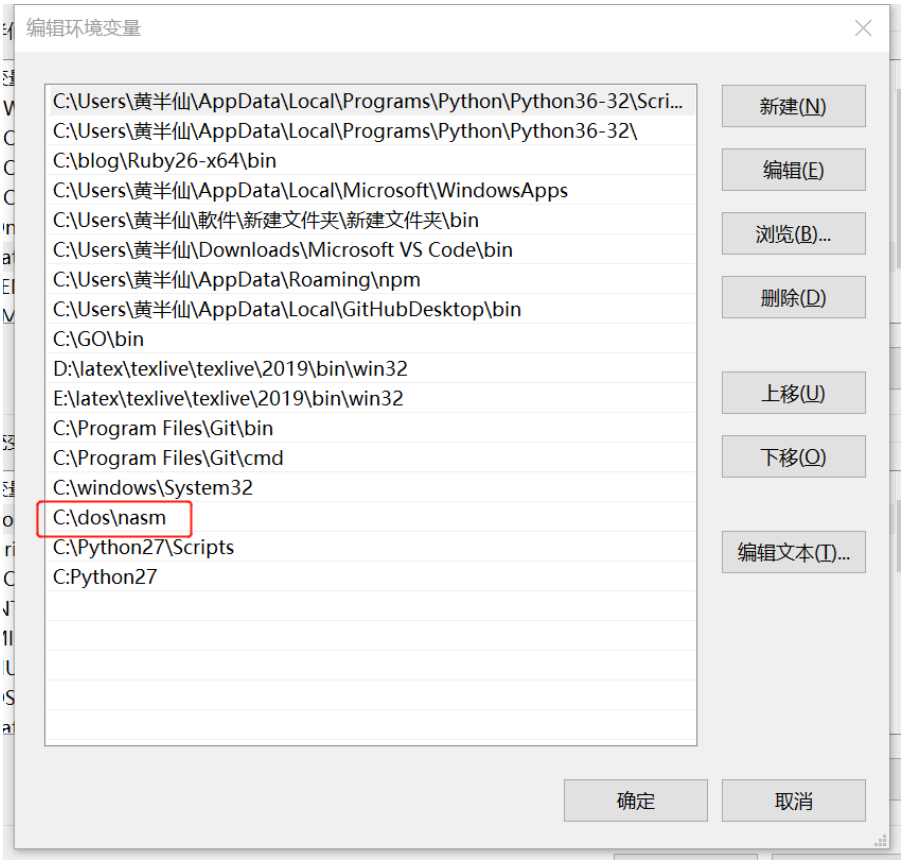
下图是稍微修改显示字符的控制代码，避免“learnos”字符串轨迹运动时吃掉了个人信息字符串的显示

```
show:
    mov ax,word[x];ax=8
    mov bx,80
    mul bx;8*80=行*列？
    add ax,word[y];640+列=641
    mov bx,2
    mul bx;ax=2*641=1282
    mov bx,ax

    mov dx,[es:bx]
    cmp dl,' '
    jnz loop1           ;避开显示的信息

    mov di,[cnt]
    mov al,byte[char+di]    ;  要显示的字符
    mov ah,byte[char+di+1]              ;  设置字符属性

    cmp al,'0'
    jz s1

    add di,2
    mov [cnt],di

con:
    mov [es:bx],ax          ;  送入显示器
    jmp loop1

s1:
    mov word[cnt],0
    mov al,byte[char]
    mov ah,byte[char+1]
    jmp con
```

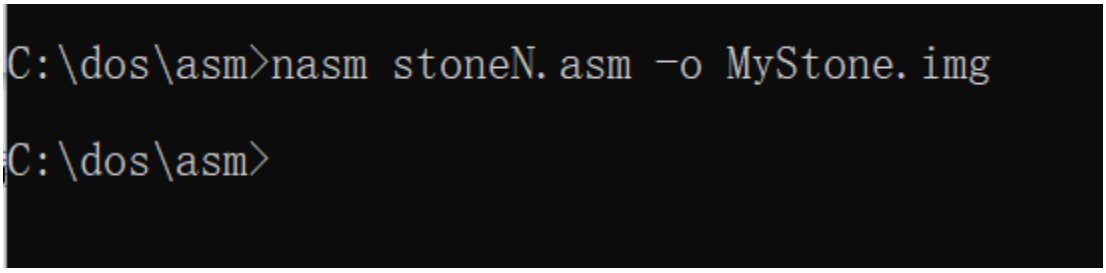
2　安装 nasm，编译 asm 程序

直接进入 nasm 官网下载安装包

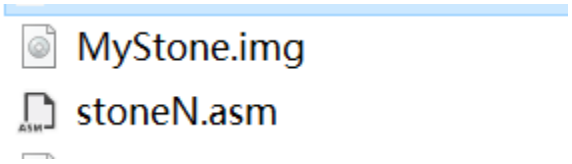
设置环境变量就可以全局使用了：



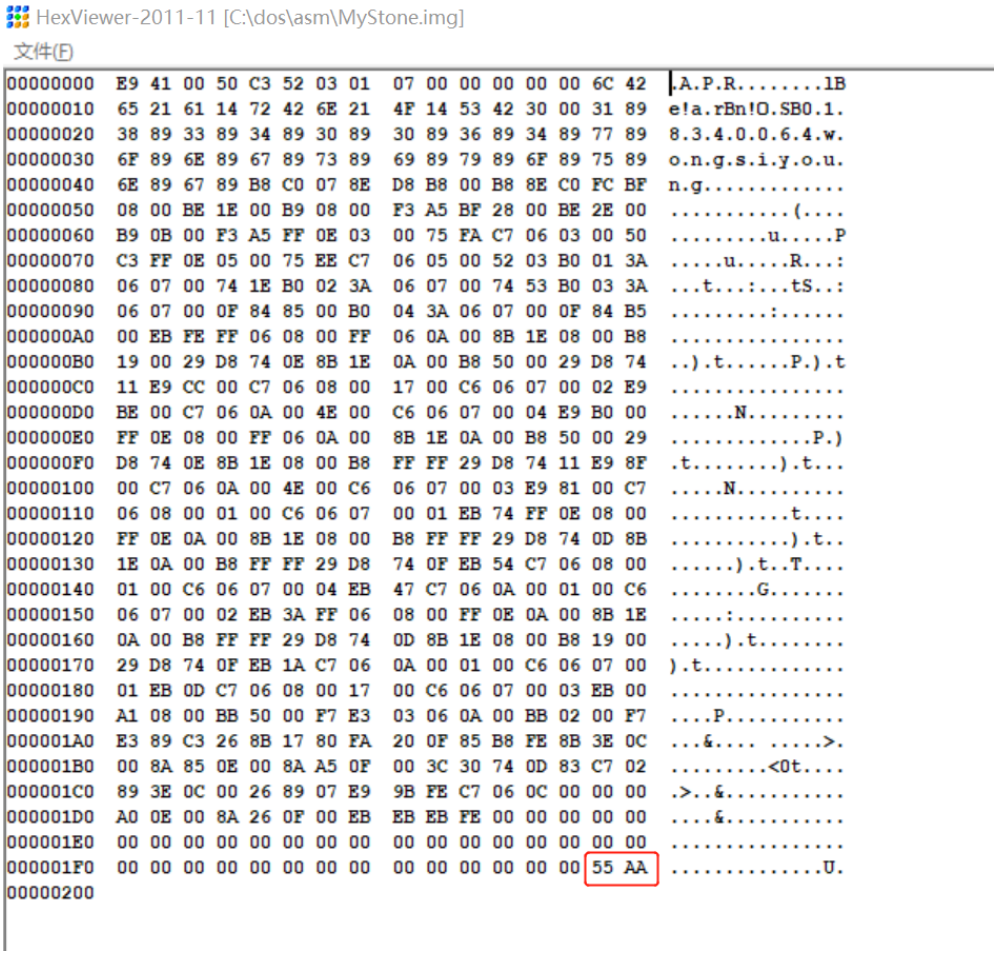
在 cmd 中使用以下命令编译刚刚编写的汇编代码：（也可以通过命令：nasm stonrN.asm -o MyStone.bin,生成二进制文件）



就可以看到在文件夹下就新增了 MyStone.img 文件：



使用资料书《 x86 汇编语言-从实模式到保护模式》中提供的软件 HexViewer 查看 MyStone.img 文件



可以看到共有 512 字节，且以 0x55aa 结尾，说明是可引导程序

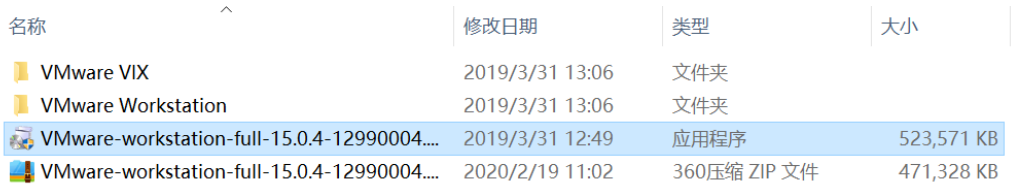
其实只要在代码最后中加

```
;code ENDS
;      END start
times 510-($-$$) db 0
 db 0x55,0xaa
```

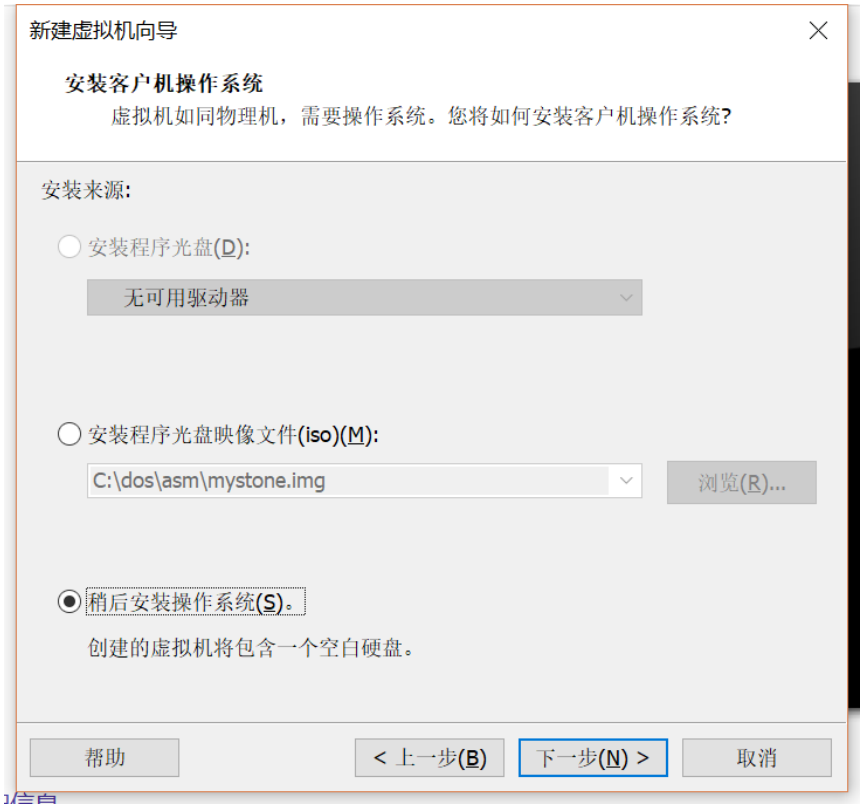
这两行代码就行了，前提是前面的代码量不超过 510 字节。

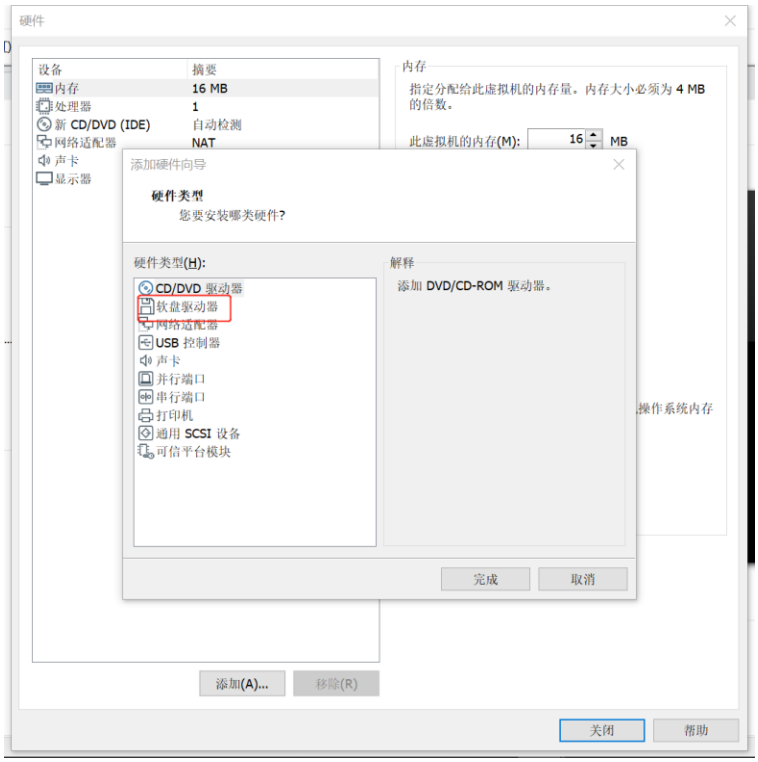
3 创建虚拟机

一样地从官网获取 VMware 安装包，然后在本机上安装就可以了

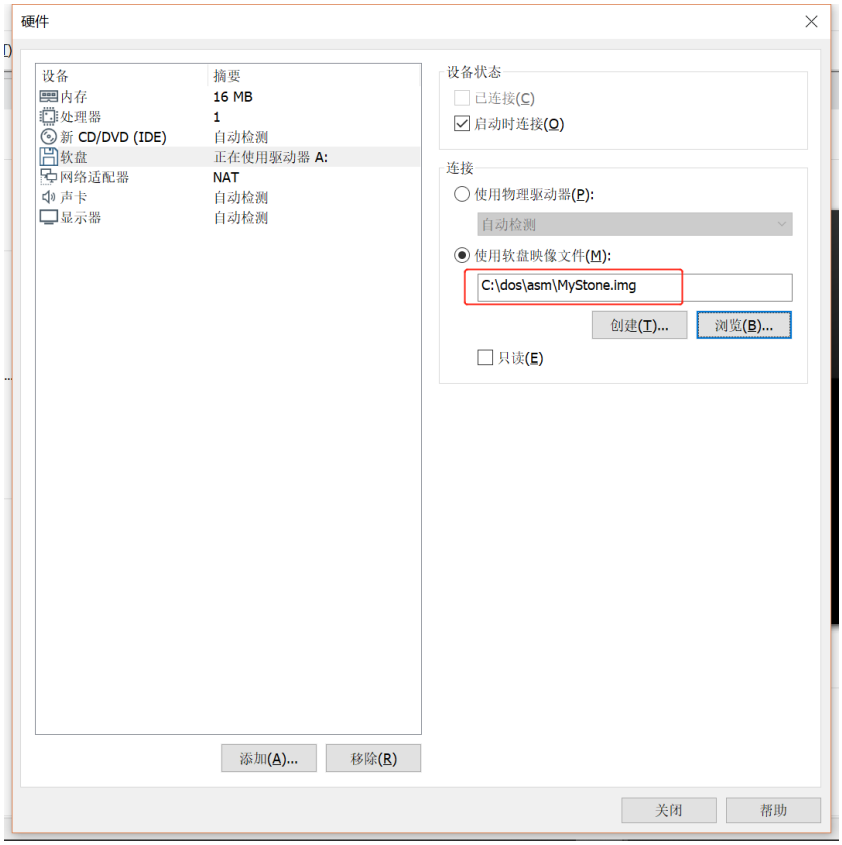


打开 VMware，新建一个虚拟机，以下是简要步骤截图：（一般只用点击下一步就可以了，不用过多设置）



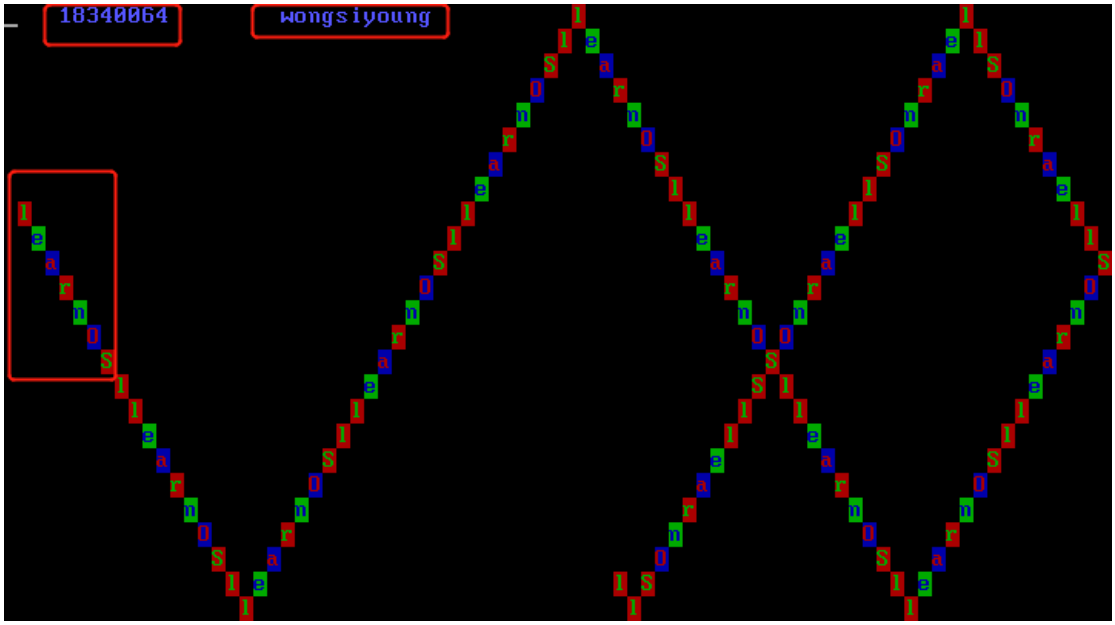


这里添加软盘，以便配置刚刚生成的 MyStone.img 文件：



创建虚拟机完毕，开机即可。

效果：



五、 实验总结

实验成功之后，把过程写程实验报告，回看实验报告的流程看似很简单，但其中有很多曲折。

一开始对于实验内容其实是很模糊的，主要也是因为缺乏汇编知识。在学习计算机组成原理的时候接触的是 mips 指令，对于 x86 是不了解的，所以一开始在看到老师的代码的时候，一来看不懂，二来直接对老师提供的代码编译会报错。

所以一开始是先看了王爽的《汇编语言（第 3 版）》才对汇编语言有所了解，接着也看了李忠的《x86 汇编语言-从实模式到保护模式》，再回看老师提供的代码就看懂了。编译不成功的，其实只用把代码中的：

```
start:
    ;xor ax,ax                  ; AX = 0    ³ÌÐò¼ÓÔØµ½0000£º100h²ÅÄÜÕýÈ·Ö´ÐÐ
    mov ax,cs
    mov es,ax                   ; ES = 0
    mov ds,ax                   ; DS = CS
    mov es,ax                   ; ES = CS
    mov ax,0B800h               ; ÎÄ±¾´°¿ÚÎÔ´æÆðÊ¼µØÖ·
    mov gs,ax                   ; GS = B800h
    mov byte[char],'A'
```

改成：

```
start:
    mov ax,0x7c00
    mov ds,ax                   ; DS = CS,指向数据段
    mov ax,0B800h
    mov es,ax                   ; ES = B800h, 指向显示器
```

就可以了！

不过因为王爽的汇编语言书是用 masm 的，而李忠的汇编语言书用的 nasm，一开始并不知道两者的区别，后来实践的时候就知道了……所以因为先看的王爽的汇编书，而用 masm 只能编译成.obj 和.exe 文件，无法直接在虚拟机中配置使用，在这里折腾了挺久的，后来使用 nasm，可以很方便的编译成 img 或 bin 文件就解决问题了。

在完成了添加个人信息和字符的一些个性变化后，尝试过写如同时控制两个运动的轨迹，写了之后感觉逻辑上是可以的，但是代码量太长了，超过了 512 字节，还在想着改进办法……

最后总的来说，当启动虚拟机后，看到画面的运动轨迹还是很有成就感的！另外也要加紧汇编语言的学习！

六、 参考资料

1. 王爽著.《汇编语言（第 3 版）》.清华大学出版社》.2003 年 9 月
2. 李忠著. 《 x86 汇编语言-从实模式到保护模式》.电子工业出版社，2013 年 1 月