

## 实验一实验报告

### 【实验题目】接管裸机的控制权

【实验目的】学习如何搭建和应用实验环境,编写一个简单的汇编程序,让它接管裸机的控制权

【实验要求】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。

### 【实验方案】

#### 1、虚拟机配置方法

虚拟机采用 VMWare Workstation 15 Player(免费版),用它构建一个虚拟机平台.该虚拟机平台的配置为: 单核单线程 CPU,4MB 内存,32MB 硬盘。

#### 2、NASM 汇编工具

NASM 是一个汇编工具,能将汇编代码编译成对应二进制代码。使用 `nasm xx.asm -o xx.bin`,可将汇编代码转换为二进制代码。

#### 3、WinImage 磁盘映像文件浏览编辑工具

创建磁盘映像文件 `xx.img`。

#### 4、WinHex 二进制文件编辑工具

可以修改二进制文件。

#### 5、FloppyWrite

FloppyWriter 能将二进制文件一键写入到软盘映像

#### 6、编写汇编代码。

6.1 显存段地址 0B800h,文本显示的范围为 25 行(0—19) 80(0—79) 列。为了实现在某个位置显示自己的学号和姓名,使用 BIOS 的 10H 调用显示字符串。在此基础上,增加了我的个性扩展,炫酷动态变色,个性画面,代码如下:

```
xor ax, ax  
  
mov ax, Message ; Message 内容为 "wangyaning17341152"  
  
mov bp, ax; ES:BP = 串地址  
  
mov cx, 18; CX = 串长度  
  
mov ax, 01301h; AH = 13 (功能号), AL = 01h (1 表示光标放在串尾)  
  
mov bx, 0082h; 页号为 0(BH = 0) 闪烁绿字
```

```

mov dl, 10 ; 列位置
mov dh, 10 ; 行位置
int 10h; 10h 号中断

```

6.2 参考老师给的 stoneM.asm 文件，可以实现用字符‘#’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。在老师的代码基础上，增加了字符‘#’可以改变颜色的功能这里只列出 show 段的代码：

```

xor ax, ax ; 计算显存地址
mov ax, word[x]
mov bx, 80
mul bx
add ax, word[y]
mov bx, 2
mul bx
mov bp, ax
mov ah, 02h ; 0000: 黑底、1111: 亮白字（默认值为 07h）
mov al, byte[char] ; AL = 显示字符值（默认值为 20h=空格符）
mov bx, 0003h
mov word[gs:bp], ax ; 显示字符的 ASCII 码值
jmp loop1

```

6.3 为了能够直接使用[内存变量]访问内存，在汇编代码的开头写 org 7c00h, 因为主引导扇区数据为 512 字节，处理器会将主引导扇区的数据 加载到逻辑地址 0x0000:0x7c00 中，然后检测最后两字节是否为 0x55 和 0xaa，若存在则主引导扇区有效，以一个段间转移指令 jmp 0x0000:0x7c00 跳到那里继续执行，数据段的位置也要作相应修改。

6.4 主引导区有效标记 55aa，所以要在在汇编代码末尾加入: times 510-(\$-\$\$) db 0 dw 0xaa55

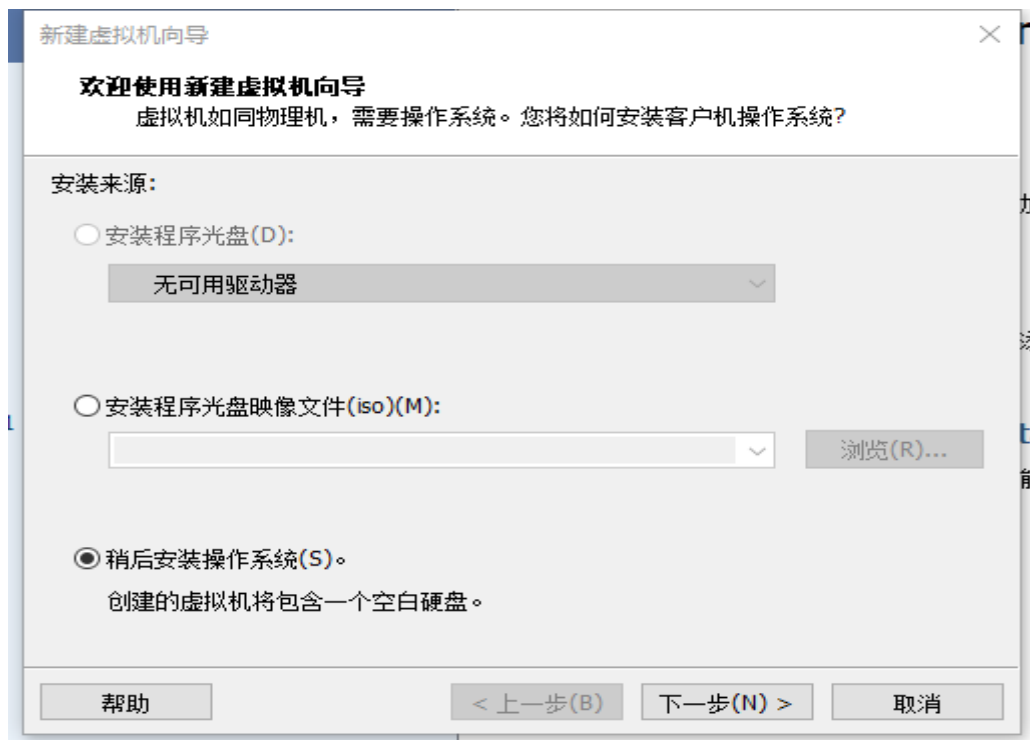
## 【实验过程】

### 1、搭建和应用实验环境

双击打开 VMware Workstation 15 Player，进入如下界面：



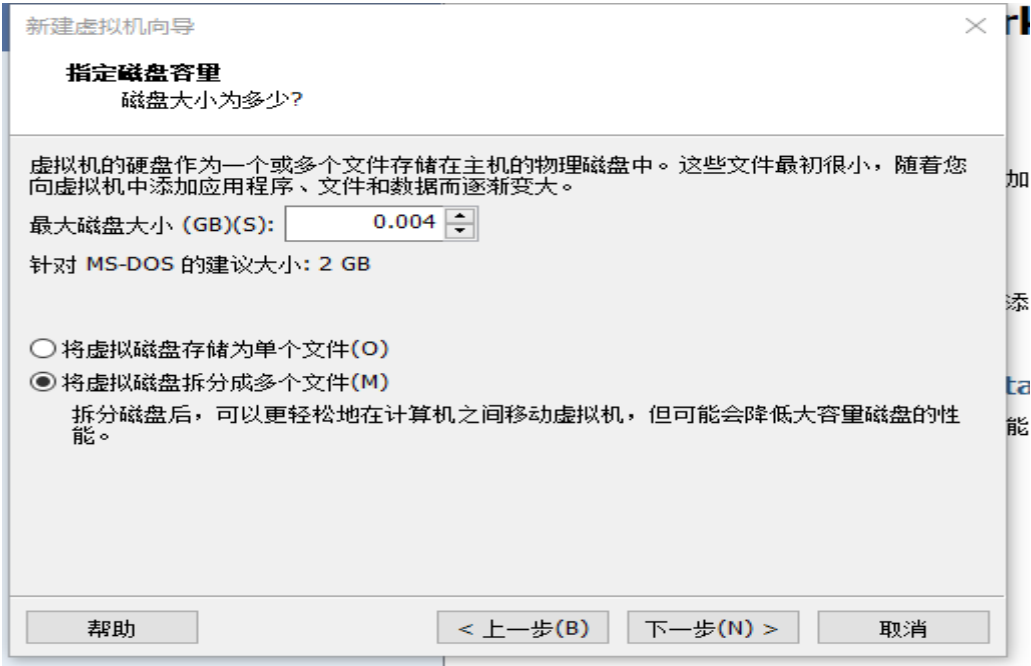
点击创建新虚拟机，进入如下界面：



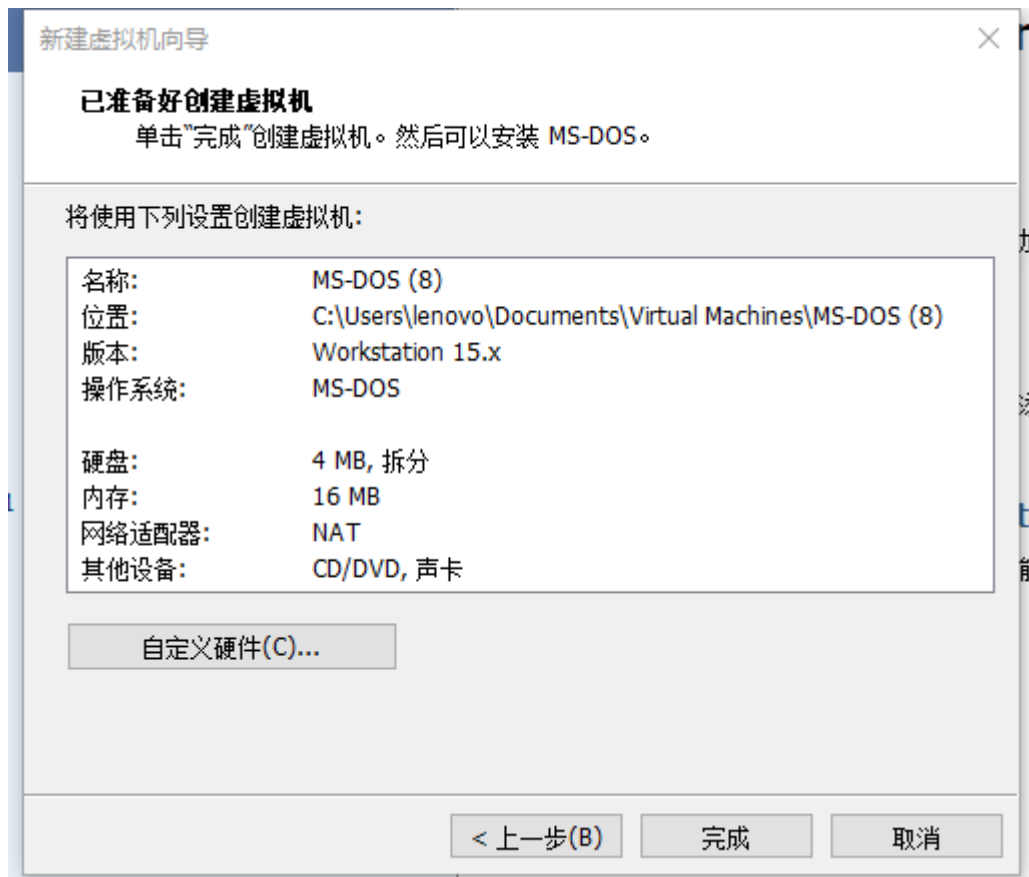
选择稍后安装操作系统，点击下一步。进入如下界面：



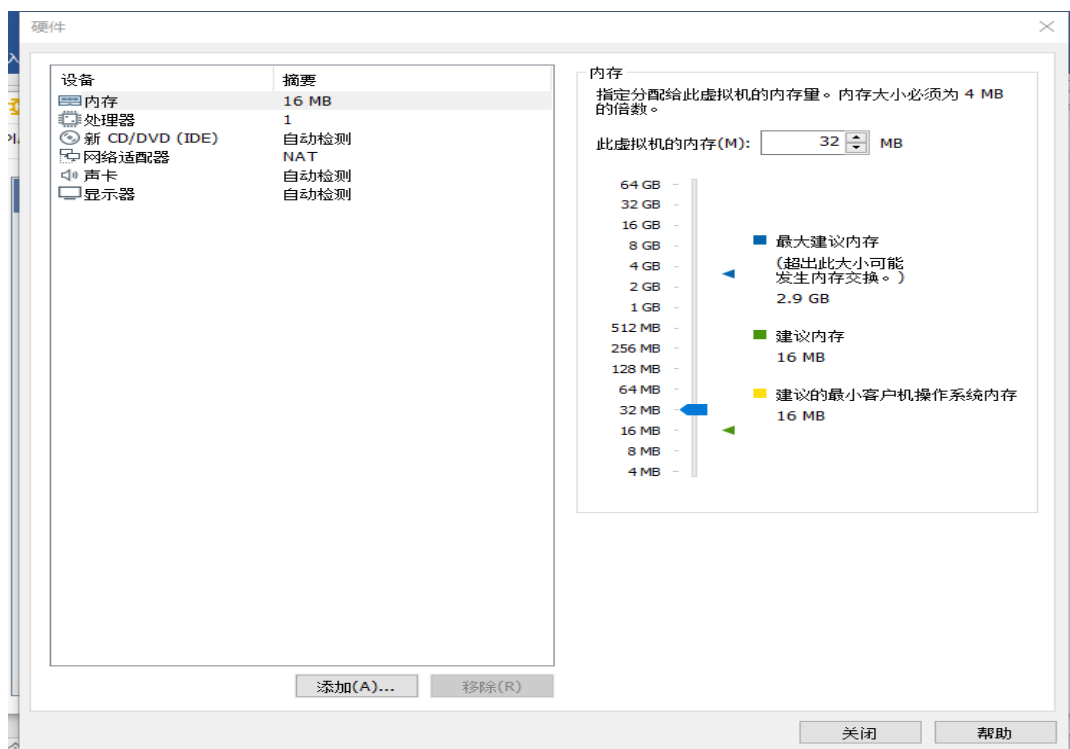
版本选择 MS-DOS，点击下一步，出现界面自己定义虚拟机名称和存放位置，点击下一步，进入如下界面：

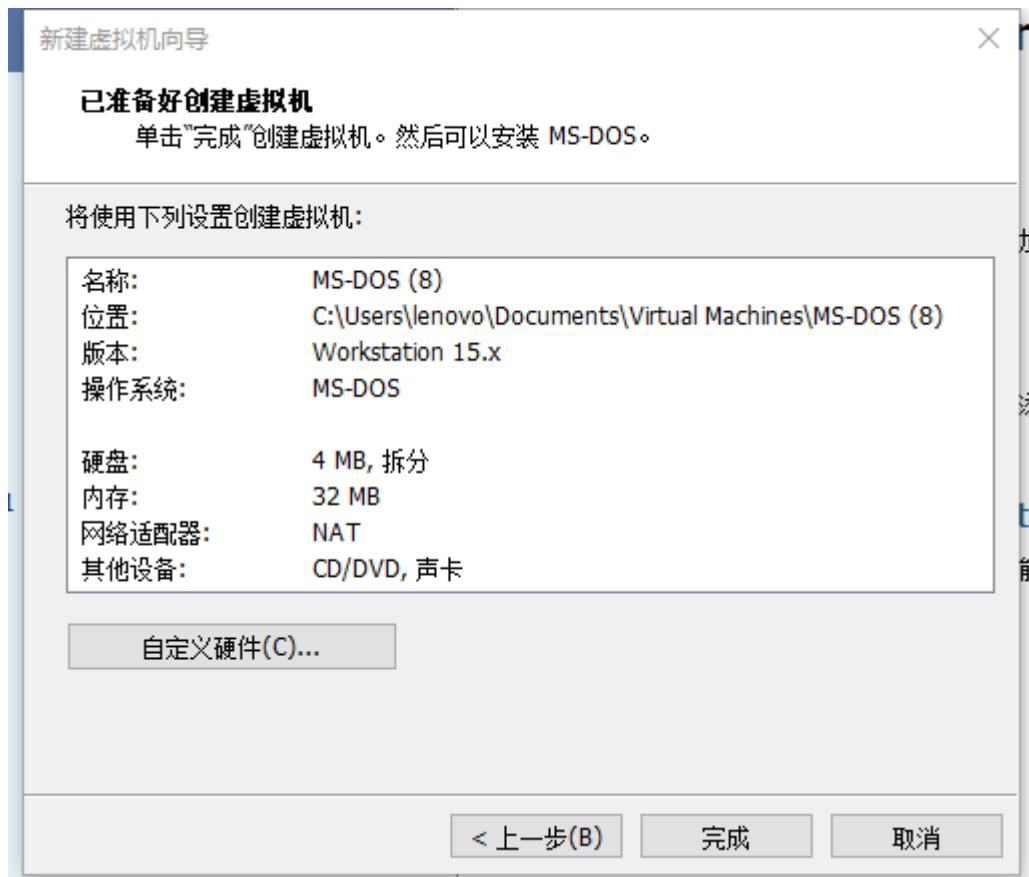


这里可自定义磁盘大小，点击下一步，进入如下界面：



这里点击自定义硬件，可以决定内存大小，这里我们定义 32MB，如下

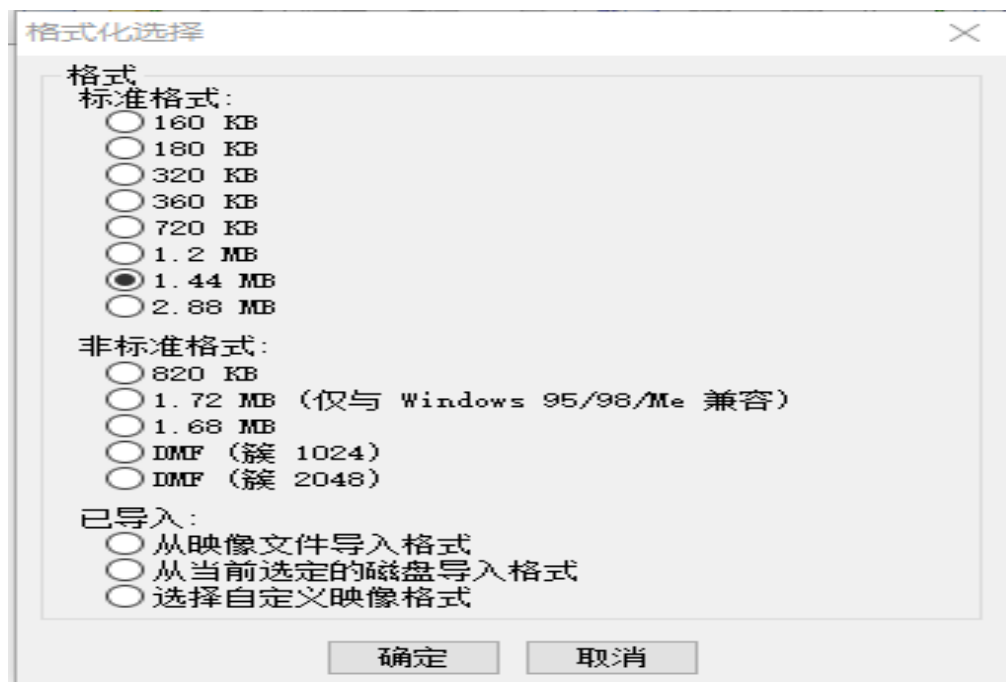




点击完成，虚拟机即创建成功。

## 2、创建 1.44MB 容量的虚拟软盘

使用 WinImage 生成 文件-> 新建, 在 标准格式中选择 1.44MB, 选择 确定。 然后 点击 保存, 此时文件类型选择 Image file(\*.ima), 文件名 为 xxx.img.














4、生成二进制文件

打开NASM 软件，使用命令 `nasm xxx.asm -o xxx.bin` 生成二进制文件 `xxx.bin`，次二进制文件位置和.asm 文件位置一样。

```
W 选择nasm
Microsoft Windows [版本 10.0.17134.648]
(c) 2018 Microsoft Corporation。保留所有权利。

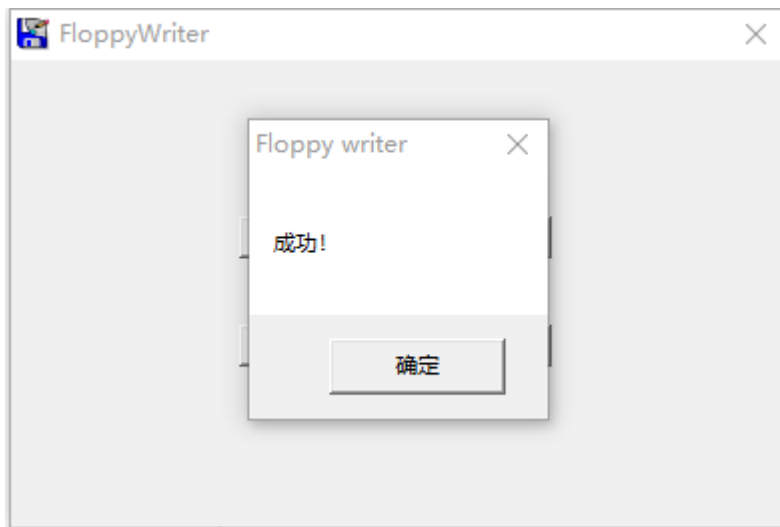
C:\Users\lenovo\AppData\Local\nasm>nasm stoneM.asm -o stoneM.bin
C:\Users\lenovo\AppData\Local\nasm>nasm stoneM.asm -o stoneM.bin
C:\Users\lenovo\AppData\Local\nasm>nasm stoneM.asm -o stoneM.bin
C:\Users\lenovo\AppData\Local\nasm>nasm stoneM.asm -o stoneM.bin
C:\Users\lenovo\AppData\Local\nasm>>nasm stoneM.asm -o stoneM.bin
C:\Users\lenovo\AppData\Local\nasm>nasm stoneM.asm -o stoneM.bin
C:\Users\lenovo\AppData\Local\nasm>nasm stoneM.asm -o stoneM.bin
C:\Users\lenovo\AppData\Local\nasm>nasm stoneM.asm -o stoneM.bin
C:\Users\lenovo\AppData\Local\nasm>nasm stoneM.asm -o stoneM.bin
C:\Users\lenovo\AppData\Local\nasm>
```

	myos1.bin	2019/3/17 23:15	BIN 文件	1 KB
	nasm	2019/3/18 21:29	文件	0 KB
	nasm	2014/2/20 8:05	应用程序	886 KB
	nasm	2014/2/20 8:04	图标	3 KB
	nasmdoc	2014/2/20 8:05	PDF 文件	755 KB
	nasmpath	2019/3/9 22:49	Windows 批处理...	1 KB
	ndisasm	2014/2/20 8:05	应用程序	490 KB
	qingping	2019/3/16 21:49	ASM 文件	2 KB
	qingping.bin	2019/3/16 21:33	BIN 文件	1 KB
	stoneM	2019/3/18 21:55	ASM 文件	4 KB
	stoneM.bin	2019/3/18 21:55	BIN 文件	1 KB

5、将.bin 文件写入磁盘映像文件.img 里，如图：



点击“Write File to Image”，选择 stoneM.bin, 在选择刚才创建的虚拟软盘映像文件，则写入成功。如图

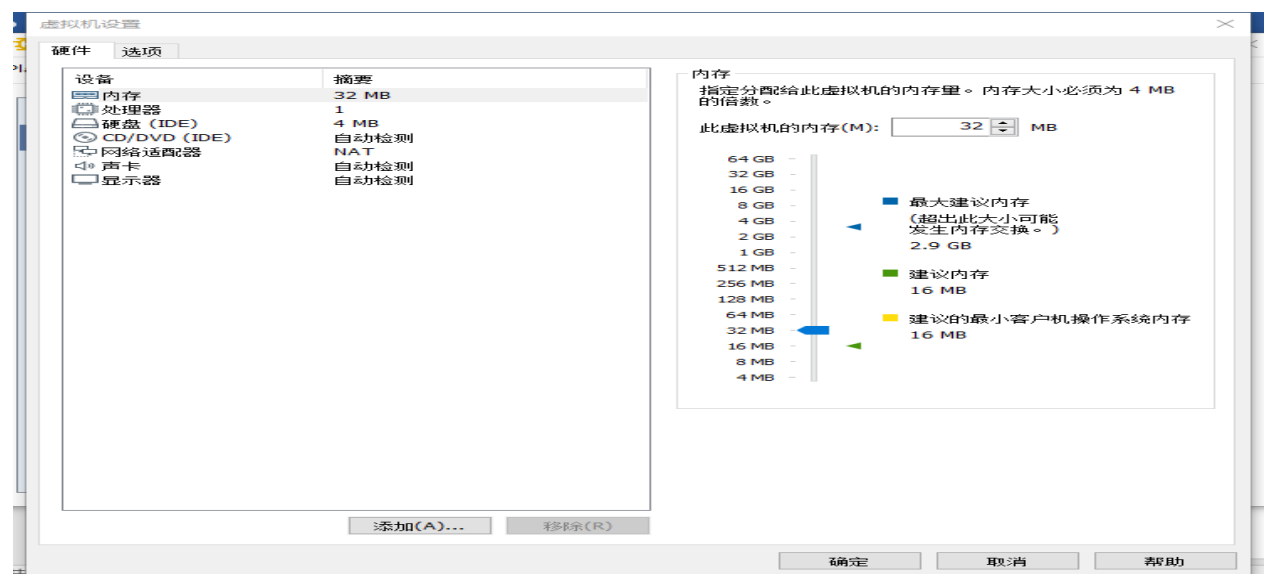


6、打开刚才创建的虚拟机如图：

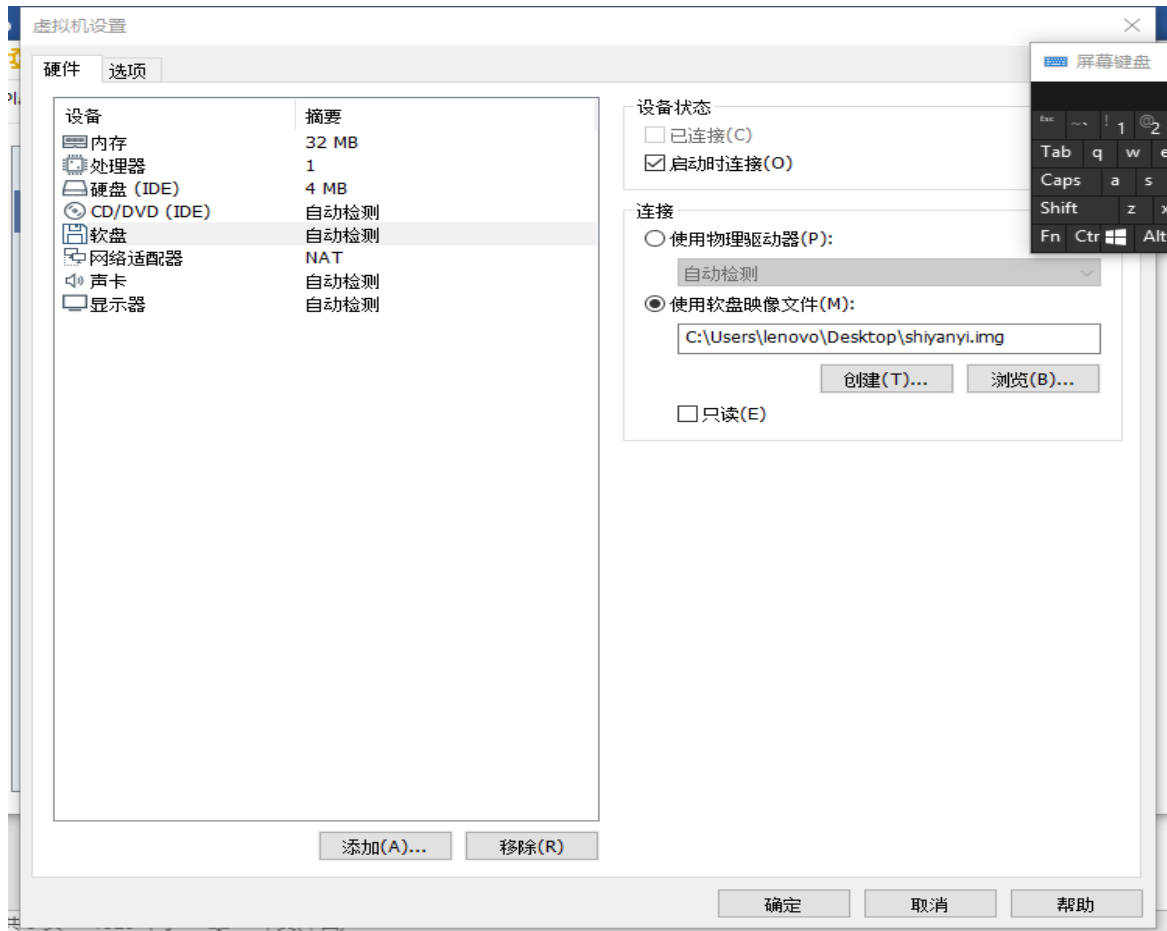




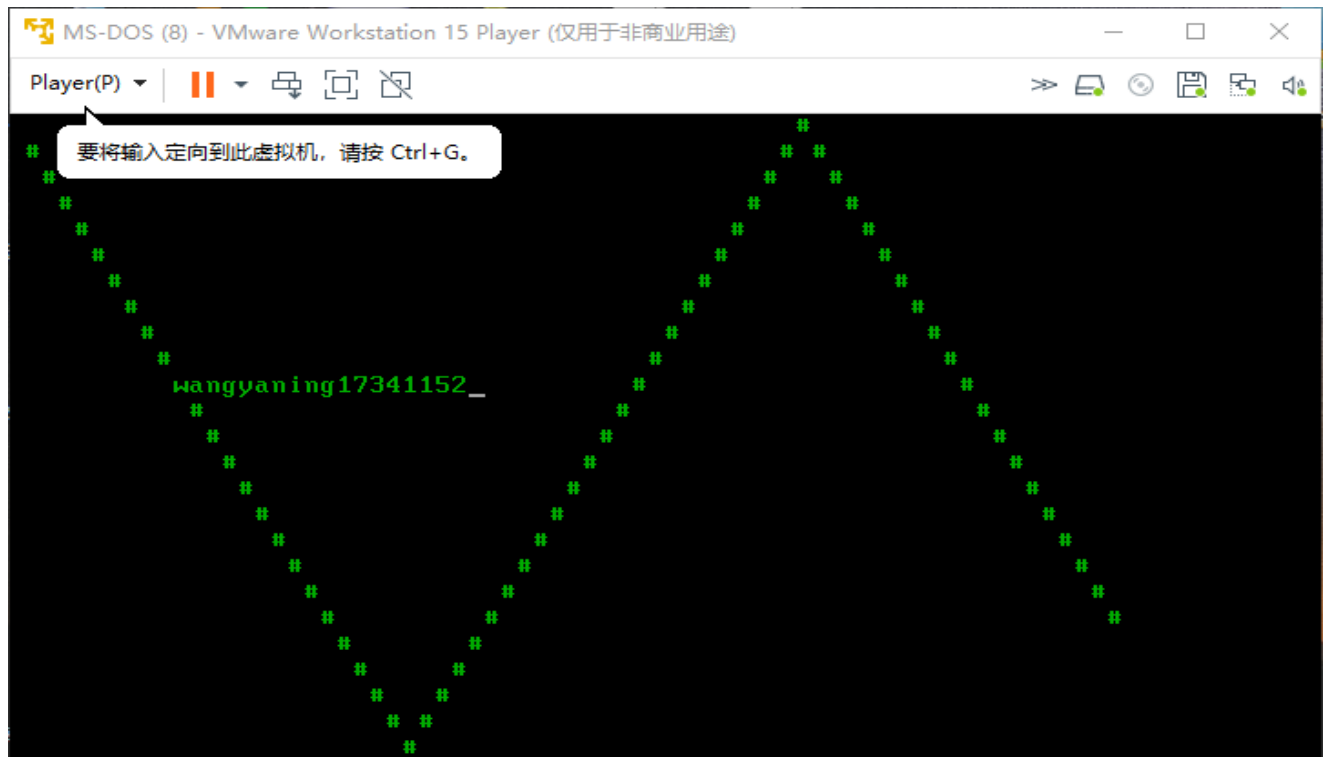
点击编辑虚拟机设置，如图：

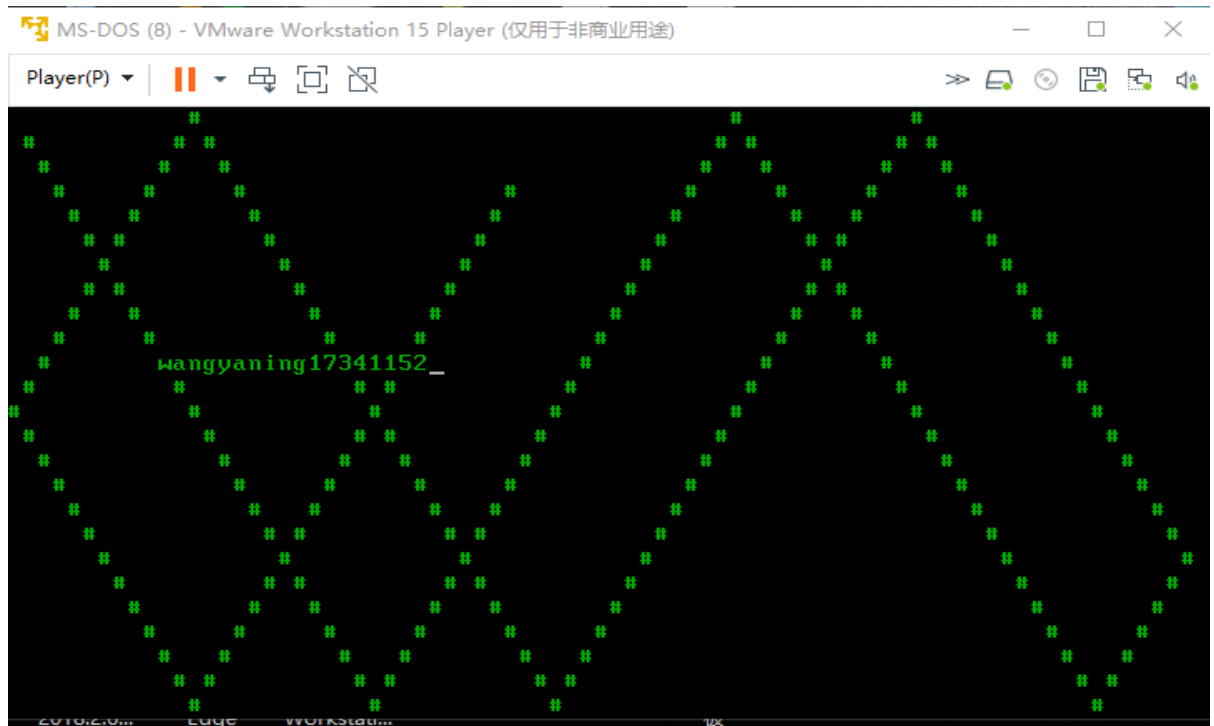


点击添加，添加刚才创建的虚拟软盘，如图：



点击确定，然后就可以点击播放虚拟机了，如图实验结果：





## 【实验总结】

一、本次实验我觉得重点是学习如何搭建和应用实验环境，因为有许多软件要下载安装并学会使用。我对这些软件起初并不了解，所以花在学习使用这些软件的时间较长，现在总结一些软件的应用：

### 1、虚拟机生成软件

虚拟机采用 VMWare Workstation 15 Player(免费版),用它构建一个虚拟机平台. VMWare Workstation 是付费版。

### 2、NASM 汇编工具

NASM 是一个汇编工具，能将汇编代码编译成对应二进制代码。使用 `nasm xx.asm -o xx.bin`,可将汇编代码转换为二进制代码，将.asm 文件放在和 `nasm` 同一个文件目录中，编译时不需要在文件名前加上路径了。

### 3、WinImage 磁盘映像文件浏览编辑工具

创建磁盘映像文件 `xx.img`，在创建虚拟软盘时，选择保存文件类型为.ima，文件名要加.img 后缀。

### 4、WinHex 二进制文件编辑工具

可以修改二进制文件。

### 5、FloppyWrite

FloppyWriter 能将二进制文件一键写入到软盘映像

## 二、对一些之前不熟悉的专业术语总结

镜像文件：通常意义上的镜像文件可以再扩展一下，在镜像文件中可以包含更多的信息。比如说系统文件、引导文件、分区表信息等，这样镜像文件就可以包含一个分区甚至是一块硬盘的所有信息。

软盘引导扇区：软盘启动时，BIOS 会检查软盘的 0 面 0 磁道 1 扇区，如果发现此扇区以 0xaa55 结束。则 BIOS 认为此扇区是一个可引导扇区（Boot Sector）。

.bin 文件：二进制文件，其用途依系统或应用而定。一种文件格式 binary 的缩写。一个后缀名为".bin"的文件，只是表明它是 binary 格式。

.asm 文件：.asm 文件是以 asm 作为扩展名的文件，是汇编语言的源程序文件。它是文本格式的文件，可以用任何文本编辑器（如：windows 下的 notepad、notepad+、editplus、ultraedit，dos 下的 edit.com、qe.exe 等）进行创建或编辑

三、起初对 x86 汇编语言并不熟悉，看不懂老师的汇编代码。后来参考一些文献学习了 x86 汇编代码，才熟悉了老师给的代码，并在此基础上进行个人个性扩展。

### 【参考文献】

- 1、于渊 著.《Orange's: 一个操作系统的实现》. 电子工业出版社, 2009 年 6 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
- 3、<https://www.cnblogs.com/jiftle/p/8453106.html>