反汇编工具（反解程序）与PC系列汉字CC-DOS的反汇编

北京科海培训中心
一九八九年九月

寄　　语

这套资料的宗旨：使从事系统软件设计，实用软件设计，中文信息系统设计及中西文信息处理工程技术人员和科研人员达到更高水平，不仅可以掌握CCDOS的设计之精华和设计反汇编工具的方法，而且还有一套完整的，正确的反汇编出来的CCDOS源程序清单及一套反汇编工具----反解程序及程序清单．它们对进一步开发新系统，中文信息处理系统，实用软件，以及研究反汇编工具等等将得到有益的启示．尤其是反汇编工具．它在探索程序奥秘方面将是你的得力助手．

另外备有源程序盘4片（CCDOS2．10源程序，反解程序及程序清单）．

目　　录

第一部分　PC－BIOS（基本输入输出例行程序）……1
1.1　IBM－PC的软件结构……1
1.2　BIOS基础……2
1.2.1　IBM－PC　XT机的中断系统……2
1.2.2　BIOS……4
1.2.3　功能调用……6
1.2.4　系统加电启动过程……8
1.3　BIOS环境……9
1.3.1　BIOS中断表……9
1.3.2　有关中断的一些说明……10
1.3.3　中断控制器8259A……11
1.3.4　扬声器的控制……13
1.3.5　键盘……14
1.3.6　软盘……15
1.3.7　打印机接口……16
1.3.8　RS232　IO……18
1.4　硬盘管理……18
1.4.1　硬盘参数……18
1.4.2　硬盘结构……20
1.5　BIOS数据区……22
1.5.1　设备配置数据区……22
1.5.2　键盘数据区……23
1.5.3　软盘数据区……24
1.5.4　显示数据区……24
1.5.5　定时数据区……25
1.5.6　系统数据区……25
1.5.7　硬盘数据区……25
1.5.8　打印机和RS232数据区……26
1.5.9　键盘附加数据区……26
1.5.10　附加数据区……26
1.6　BIOS的使用……26
第二部分　IBM－PC系列的汉字系统的总体结构……34
2.1　系统设计思想和整体结构……34
2.2　键盘管理模块……37
2.3　打印机管理模块……40
2.4　显示器管理模块……43
2.5　字库管理及其它……48
第三部分　反汇编工具反解程序……50
3.1　反解程序的设计思想……50
3.2　反解程序的源程序……50
3.3　反解程序的使用方法……51
3.4　冲突及其处理方法……57
第四部分　汉字CCDOS　2.10的反汇编和反解程序的源程序……59
4.1　源程序各模块说明及系统生成方法……60
4.2　源程序UN_FILE1.ASM（FILE1.EXE的反汇编）…72

4.3 源程序UN_CCCC.ASM（CCCC.EXE的反汇编）..... 74
4.3.1 IOPARM
4.3.2 源程序UN_INT10.ASM（INT10.EXE的反汇编）
4.3.3 源程序UN_VID_1.ASM（VID_1.EXE的反汇编）
4.3.4 源程序UN_KEY.ASM（KEY.EXE的反汇编）
4.3.5 源程序UN_INIT.ASM（DOSINIT.EXE的反汇编）
4.4 各种打印输出模块的源程序..... 208
4.4.1 M2024打印机的反汇编源程序
(1) UNM2024.ASM（16×16点阵打印驱动程序）
(2) UND2024.ASM（24×24点阵打印驱动程序）
4.4.2 KC_3100打印机的反汇编源程序
(1) UNK3100.ASM（16×16点阵打印驱动程序）
(2) UND3100.ASM（24×24点阵打印驱动程序）
4.4.3 TOSHIBA P351打印机的反汇编源程序
(1) UNP351.ASM（16×16点阵打印驱动程序）
(2) UND351.ASM（24×24点阵打印驱动程序
4.5 词组系统的反汇编源程序.....341
4.5.1 UN_CZ.ASM（CZ.EXE的反汇编）
4.5.2 UNFILECZ.ASM（FILECZ.EXE的反汇编）
4.5.3 UNLOADCZ.ASM（LOADCZ.EXE的反汇编）
4.6 反解程序的源程序.....368

第一部分　PC-ROMBIOS（基本输入输出程序）

1.1　IBM-PC的软件结构

IBM-PC的硬件是以系统为基础，用各种功能板来扩充系统。其显示控制板和磁盘控制板以及打印输出接口都是选择项。IBM-PC的软件也是以系统板为核心的。在系统板上装配了一个8K的 ROM，我们习惯的称之为ROM-BIOS。由 ROMBIOS控制着系统所需的主要外部设备。这包括显示器输出和键盘输入，磁盘控制等等。其它软件在使用外部设备时，总是调用ROMBIOS。也就是说， ROMBIOS是 IBM-PC的软件的核心或最底层，其它软件都是建立在 ROMBIOS之上，在IBM-PC运行的各种操作系统和应用软件都建立在ROM-BIOS之上，使得 ROMBIOS是由各个独立的设备驱动模块组成。例如有磁盘驱动模块，键盘管理模块等等。每个模块又都是由各个功能子块组成。每个模块都有一个公共的入口；调用这些模块时，总是从同一入口进入，通过寄存器的参数，表明使用何种功能。

高层软件使用中断指令进入 ROMBIOS的各个模块。模块如何处理，怎样驱动设备与外部设备如何动作与高层软件无关，但是，由于 ROMBIOS对外部设备的管理深度很高，所以 ROMBIOS提供高层软件调用的功能行为很细，以致于在 ROMBIOS很难判断高层软件要完成一个什么样的宏功能，比如 ROMBIOS允许高层软件直接控制光标的定位，光标图形的大小，允许高层软件直接在光标位置上写出控制字符，使这控制字符的图形得以显示等等。这就是说， ROMBIOS不是简单模仿一个 CRT或一个盘系统，而是准备一批软件功能等待高层软件去组织，调用和形成各自的管理特色。

IBM-PC的 ROMBIOS不仅仅对操作系统敞开它的大门，其它各种应用软件，高级语言，数据库都可以直接使用 ROMBIOS提供的各种功能模块，这是IBM-PC软件的另一特色。

这种软件结构给我们搞汉字化工作带来了巨大的方便。只要我们认真地研究了ROMBIOS的各个功能模块，然后编出仿真的汉字模块，就可以很快实现汉字化的目标。但是众多的应用软件和语言对 ROMBIOS的直接使用又要求我们必需把握各个模块的宏功能，必须小心翼翼，尽可能做好研究工作，以适应各方面的要求。

IBM-PC的各部分软件在内存中都占据一定的固定位置。

我们知道，8088的内存空间的绝对地址可以用 5位16进制数表示。在8088中总是把这 5位16进制数的前四位做为段号。用段号来表示地址空间的方法可以简单明了地说明问题。通常的表示方法是：

××××：××××

段号　　偏移量

在PC-DOS启动时总是先从 ROMBIOS获得可用内存的大小，然后按这个信息去安排 DOS的各个部分所占据的内存区。下图是PC-DOS工作时的内存分配状况：

0000：	0000	ROMBIOS中断向量表
0040：	0000	ROMBIOS数据区
0050：	0000	DOS和 ROMBIOS通信区
0060：	0000	DOSBIOS程序区
00BF：	0000	DOS程序区
XXXX：	0000	用户区
XXXX：	0000	DOS命令解释程序复盖区
XXXX：	0000	无内存区
0B000：	0000	单色显示器VRAM区
0B800：	0000	彩色显示器VRAM区

0C000：0000　无内存区
0P600：0000　ROMBASIC区
0FE00：0000　ROMBIOS区

由上可知，DOS工作时，用户区是夹在系统程序区和DOS命令解释程序复盖区之间的。而且，用户区是浮动的，既可以向下浮动，也可以向上浮动。

1.2 BIOS基础

1.2.1 IBM-PC/XT 机的中断系统

一. 中断种类：

分不可屏蔽中断，硬中断和软中断三类。

1. 不可屏蔽中断(NMI)

不可屏蔽中断信号当存贮器奇偶错（或8087中断）时产生。不可屏蔽中断不能通过设置标志寄存器的IF位来设置的，设置或清除MI的方法是：

由A0H口送80H　允许产生NMI。

由A0H口送00H　不允许产生NMI。

2. 硬中断

（1）由中断控制器 8259A芯片为硬中断服务，其分配如下。8个中断各自独立，优先权IRQ0最高。IRQ7最低。

8025A输入	中断类型	设备（中断源）
IRQ0	INT 8	定时器（通道0）
IRQ1	INT 9	键　盘
IRQ2	INT A	保　留
IRQ3	INT B	留给RS232（第二个）
IRQ4	INT C	留给RS232（第一个）
IRQ5	INT D	硬　盘
IRQ6	INT E	软　盘
IRQ7	INT F	留给打印机

（2）中断屏蔽方法

a. 屏蔽所有硬中断

通过标志寄存器的IF标志位可进行屏蔽处理。

IF=0　禁止所有中断（用 CLT指令）

IF=1　允许中断（用 STI指令）

b. 分别屏蔽各中断源

中断控制器有一中断屏蔽寄存器，其每一位对应于一个中断源，用以控制是否允许相应的中断源申请中断。

7	6	5	4	3	2	1	0
↑	↑	↑	↑	↑	↑	↑	↑

```
|      |      |      |      |      |      |      |  IRQ0
|      |      |      |      |      |      |  IRQ1
|      |      |      |      |      |  IRQ2
|      |      |      |      |  IRQ3
|      |      |      |  IRQ4          相应位=0，允许中断请求
|      |      |  IRQ5                 相应位=1，禁止中断请求
|      |  IRQ6
|  IRQ7
```

例：只允许键盘请求中断

```
MOV     AL, 0FDH
OUT     21H, AL
STI
```

（3）中断结束

根据对中断控制器的编程情况，中断服务程序结束时要送中断结束信号（EOI）（经20H口送出），中断结束信号为 20H，用指令：

```
MOV     AL, 20H
OUT     20H, AL
```

3. 软中断

这是指存放在 ROMBIOS中的常用的基本输入输出例行程序。通过中断调用（ INT指令）来引用，不但操作系统予以使用，应用程序也可加以利用。

二. 中断向量表

系统对不同用途的例行程序分别指定了相应的中断号，而各相应中断程序的入口地址顺序放在内存最前面的中断向量表中（地址 0～3FFH）。其长度为1K字节。

中断程序的入口地址在向量表中存放方式是：按中断号（也称类型码）顺序排列，共 256个中断，每个中断占 4个字节， 4字节中 2个低字节是偏移地址， 2个高字节是段地址（如图 1.1所示），而偏移地址和段地址均是低位在前，高位在后。

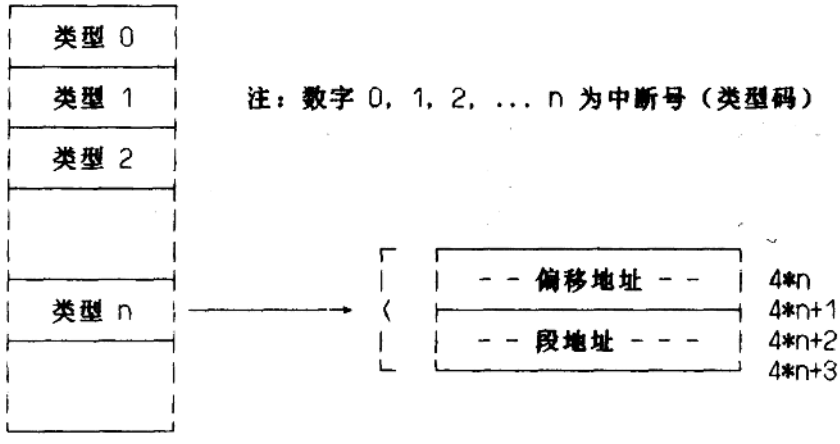


图 1.1 中断向量表

三. 中断调用

进行中断调用时，发出指令（ n为中断号）：

```
INT     n
```

即可调用相应的中断服务程序，中断响应时首先将当前有关信息保存在堆栈中，然后将中断入口地址放入CS，IP寄存器，这样就可转入运行相应例行程序。

中断响应过程是：

1.保留信息人栈

(1) 保留标志寄存器

```
(SP)=(SP)-2
((SP)+1:(SP))=FLAGS
```

(2)
```
(IF)=0
(TF)=0
```

(3)
```
(SP)=(SP)-2
((SP)+1:(SP))=(CS)        ←保存CS
(CS)=(n*4+2)(n*4+3)
```

(4)
```
(SP)=(SP)-2
((SP)+1:(SP))=(IP)        ←保存IP
(IP)=(n*4)(4*4+1)
```

2. 转入中断服务程序

从中断向量表中取得相应例行程序中断入口地址分别放入IP和CS寄存器：

```
(IP) - - - (4*n)(4*n+1)
(CS) - - - (4*n+2)(4*n+3)
```

3. 中断返回

中断返回指令：

```
IRET
```

将放在堆栈中的现场信息弹出，从而实现程序继续执行下一条指令。

1.2.2 BIOS

在PC系列机中 BIOS (Basic Input/Output System) 是基本的输入输出系统，它是一组8088程序，驻留在 ROM中，长度为8K字节，装在系统板上，一旦机器起动，就运行BIOS的系统自测和初始化程序，使机器得以正常起动，同时BIOS提供了主要的系统支持程序，也即输入输出例行程序（中断服务程序），如屏幕显示，键盘输入，磁盘管理等。BIOS与硬件的接口通过口子（端口）进行。应用程序可对BIOS中的例行程序进行调用，另外还可改写某些例行程序。也可增添ROM BIOS的内容。下面将作简要介绍。

一. 中断调用内容

1. 中断调用分类

```
INT     0H    ┐
INT     1H    ├  Intel 公司规定
  :           │
INT     4H    ┘
INT     5H
INT     6H    ┐
INT     7H    ┘  保留
INT     8H    ┐
```

```
    :          |  硬中断   ┐
INT    FH      ┘           |
INT    10H     ┐           |   BIOS
INT    11H     |           |
    :          |  软中断   ┘
INT    1FH     ┘
INT    20H     ┐
INT    21H     |  DOS
    :          |
INT    27H     ┘
```

INT 28H～3FH 保留给DOS
INT 40H～5FH 保留
INT 60H～67H 保留给用户软中断
INT 68H～7FH 不用
INT 80H～85H 保留给BASIC
INT F1H～FFH 不用

共256个

2. BIOS的中断内容

BIOS包括有INT 8～INT 1FH，其中常用的有：

INT 10H 显示输出
INT 13H 磁盘管理
INT 14H 异步通讯（RS232）
INT 16H 键盘输入
INT 17H 打印机输出
INT 5H 屏幕打印

关于中断调用功能和入口地址等内容，将放到 1.3节中讨论。

二. BIOS的调用

1. 对BIOS已有功能的调用，发出指令

INT n

即可调用，但在发 INT n 以前，须先按规定，将AH寄存器置成相应的功能号，并将有关参数放入相应寄存器，现以软盘管理 INT 13H 为例说明其要求。

ROMBIOS 中的 INT 13，提供了关于 5寸盘的IO处理程序，盘有六种可选择的处理功能，即：盘复位、读盘状态、读盘、写盘、检验和盘格式化。程序根据用户填在（AH）中的选择码来执行和完成中选的处理功能。

(AH)=0 若复位盘系统，在此处理过程中要根据系统情况填写数据输出寄存器内容(DOR)，初始化SEEK状态寄存器和DISKETTE状态寄存器，并置位盘控制器(RDC)。在开始对盘进行读写前，一般要进行此操作。

(AH)=1 读(AL)中的系统状态，在盘操作结束后，要回送状态信息，执行这个功能是将 DISKETTE-STATUS的内容送入(AL)，使用户明了命令执行情况。

(AL)可能是下列状态：

0 1 命令错
0 2 地址标记没找到
0 3 企图写一个写保护盘
0 4 要求的扇没找到
0 8 DMA 溢出

0 9 DMA 企图超越 64K界线
1 0 盘读时 CRC错误
2 0 NEC 控制器错
4 0 SEEK操作错
8 0 连接器未响应

(AH)=2 读要求扇数的内容送入存贮器
(AH)=3 将内存中数据写到要求的扇
(AH)=4 检验要求的扇
(AH)=5 格式化指定的道

在进入这四种功能操作时，(DL)＝驱动器号，(DH)＝磁头号，(CH)＝道号，(CL)＝扇号，(AL)＝扇数，(ES:BX)＝缓冲区地址。同时在格式化时，还要提供一系列由 4个信息组成的信息组，供格式化用，同时这个信息被记录在每个扇开始以供读／写存取期间用来查找需要的扇。

对于盘设备的驱动是由盘控制器执行15个命令来完成的，这15个命令和用户不发生关系，每个命令后面跟的参数是由程序根据盘操作参数表给出的，盘参数表共有11个参数，中断 1EH指向表的首址。

以上四个功能操作都是在建立 DMA方式后将向各自的命令序列（即命令字—参数）传送到盘控制器，命令执行完后的结果字节再传送到处理机，并以中断做为盘操作的结束。

三．BIOS的使用途径

BIOS的使用途径有三：

1. 对BIOS中已有的输入输出例行程序进行调用，其使用方法上节中已介绍了。
2. 更换BIOS中的例行程序模块

BIOS的例行程序是固化在 ROM中，本身是不能更改的，但当为了满足某种应用要求（如汉字处理）需要改其中某些例行程序模块时，在编写并调试完成了相应新例行程序后，将其驻留在内存适当位置（可用 INT 27H），然后将中断向量表中相应的入口地址改为新程序在内存中的驻留地址（可用功能调用25——置中断向量），由此可以实现例行程序的替换。

3. ROM BIOS提供了手段，系统中可以增添 ROM模块。系统在进行加电自测过程中，同时检测是否有增添的 ROM模块，如存在，将运行新的 ROM程序模块。这新的例行程序模块可在中断向量表中为新程序设置相应入口地址，以便得到系统的控制。

ROM BIOS在加电自测过程中，对存贮区地址c800:0H～F400:0H区域内测试是否有增添的ROM BIOS模块，以2K字节为单位进行检测。

增添模块的标志如下：

字节 0: 55H
字节 1: AAH
字节 2: ROM长度（以 512字节为单位）。在加电自测时，要对这个 ROM模块进行代码和检察。 ROM模块中各字节相加， 取100H为模，代码和必须为零。

当检测存在正确的 ROM模块（新增添）标志时，BIOS的加电自测程序即转到该模块的字节 3（用CALL实现）接着运行。这时添加的 ROM模块可以进行新例行程序本身需要的初始化等工作，完成后需返回原 BIOS （用 RET指令）。

硬盘的 INT 13H例行程序模块就是用这种方法添加到系统中的。

1.2.3 DOS的功能调用

一. 功能调用

1. DOS操作系统提供了一套内容很丰富的功能调用，而新的版本还在加强其功能。功能调用的内容有字符的输入输出，文件管理，内存管理，日期功能，运行程序等。应用程序的开头编写，往往离不开对功能调用的利用。这里只能简单介绍。详见〈IBM Disk Operating System〉 2.00版。

功能调用有：

0 - E	传统的字符输入输出
F - 24	传统的文件处理
25 - 26	中断向量等
27 - 29	传统的文件处理
2A - 2E	时间和日期等
2F - 38	扩展功能
39 - 3B	文件目录
3C - 46	扩展的文件处理
47	文件目录
48 - 4B	扩展的内存处理
4C - 4F	扩展功能
54 - 57	扩展功能

2. 功能调用的使用

功能调用是 INT 21H，其使用方法与中断调用相似，将功能号放入AH，按要求将有关参数放入相应寄存器，然后发出 INT 21H。

例：从 B盘上删除一个文件(TEST.EXE)。

功能调用 41H: 从指定目录中删除一个文件。 DS:DX指向文件名的地址。
（注：文件名以 '0'终止，见程序第 5条语句）。

```
STACK SEGMENT  PARA      STACK        STACK'
      DB       256   DUP(0)
STACK ENDS
DATA  SEGMENT  PARA      'DATA'
FNAME DB       "B:TEST.EXE", 0
DATA  ENDS
CODE  SEGMENT  PARA      'CODE'
START PROC     FAR
      ASSUME   CS:CODE,DS:DATA
      PUSH     DS
      MOV      AX, 0
      PUSH     AX
      MOV      AX,DATA
      MOV      DS,AX
      MOV      DX,OFFSET  FNAME
      MOV      AH,41H
      INT      21H
      RET
START ENDP
CODE  ENDS
      END      START
```

二. DOS扩展的屏幕和键盘功能

DOS操作系统2.00以上版本对屏幕显示和键盘的控制提供了扩展功能，在程序中可用规定的字符串序列来控制屏幕上光标的位置。也可对键盘的各键重新进行定义（详见IBM Disk Operating System 说明书第 13 章 UsingExteded Screen and Keyboard Control ）。在开发应用程序时可对这些功能加以利用。例如用来定义功能键，也可对显示屏幕加以灵活的控制。

顺便提一下，为利用这些扩展功能，机器起动时用的 DOS系统盘上应有 CONFIG.SYS 和 ANSI.SYS 文件，且 CONFIG.SYS 文件中有：

DEVICE=ANSI.SYS

下面举例说明使用方法。

例：清屏

清屏的控制字符串序列是 ESC([2J)

```
MOV   AX,CS
MOV   DS,AX
MOV   DX,200
MOV   AH,09
INT   21
INT   3
DB    1B,"[2J$"
```

执行，清屏。

1.2.4 系统加电启动过程

1. 上电

系统加电启动时，8088进入复位状态，这时CS寄存器置成 FFFFH，IP寄存器置成 0000H，而FFFF:0000H处是一条转移指令如下：

FFFF:0000 JMP RESRT

故加电后 CPU执行的第一条指令是 JMP RESET，随即转入 RESET程序段的入口 (F000:E05BH) 继续运行，进行测试和设备的初始化等工作。

2. 加电自测内容大致如下：

(1) 对8088各寄存器作全 1全 0测试。

(2) 对 8K ROM BIOS作代码和检查。

(3) 对前 16K内存作AA、55、FF、01和00图案测试。

(4) 对外围接口 (8255A)， DMA(8237)，中断控制器 (8259A)，定时器(8253)，显示器接口板，键盘、软盘驱动器和盒带等进行测试和初始化。

(5) 对系统板 16K以后内存和扩充板上内存，以及显示器上的 RAM作AA、55、FF、01和00图案测试（如为热启动，则跳过这项测试）。

(6) 测定设备的配置，如内存量，扩充箱，软盘驱动器、显示器、打印机接口和 RS232通信口等，并作相应初始化。

(7) 填写中断向量表 (INT 1FH)。

(8) 检测是否有增添的 ROM模块，如有，对该模块进行代码和检查，及执行模块中有关程序。

上面 (1)-(2)项测试中如发现错误，则停机。(4)项测试有错则发一长一短音响信号，并停机。

3. 如上面测试均正常，则调用 INT 19H（引导加载），读软盘A:的0 道 1扇到内存地址 0:7000H（如有硬盘，则读硬盘），转入 0:7000H进行，如读盘失败，则调用 INT 13H进入 ROM BASIC。

1.3 BIOS环境

1.3.1 BIOS中断表

中断调用功能和入口地址

中断类型	功 能	入口地址	备 注
INT0	被 0除错误		DOS置入口
INT1	单步		DOS置入口
INT2	不可屏蔽中断(NMI)	NMI-INT (F000:F2C3)	
INT3	断点		DOS置入口
INT4	溢出		DOS置入口
INT5	屏幕打印	TRINT-SREEN (F000:FF54)	
INT6、7			保留
INT8	时钟中断	TIMER-INT (F000:FEA5)	
INT9	键盘中断	KB-INT (F000:E987)	
INTA			保留
INTB、C	留给通讯口中断		
INTD	硬盘中断	HD-INT (C8000:0766)	
INTE	软盘中断	DISK-INT (F000:EF57)	
INT10	显示器管理	VIDEO-IO (F000:F065)	
INT11	设备配置测定	EQUIPMENT (F000:F84D)	
INT12	内存容量测定	MEMORY-SIZE-DET (F000:F841)	
INT13	磁盘管理	DISKETTE-TO (F000:FF59)	只有软盘时
		DISK-IO (C800:0256)	带硬盘时
INT14	通信口管理 (RS232)	RS232-IO (F000:E739)	
INT15	盒带管理	CASSETTE-IO (F000:F859)	
INT16	键盘管理	KEYBOAD-IO	

		(F000:E82E)	
INT17	打印管理	PRINTER-IO (F000:EFD2)	
INT18	ROM BASIC	F600:0000	
INT19	引导装载	BOOT-STRAP (F000:F6F2)	只有软盘时
		BOOT-STRAP (C800:0186)	带硬盘时
INT1A	时钟管理	TIME-OF-DAY (F000:FE6E)	
INT1B	键盘CTL+Break键		DOS置入口
INT1C	时钟滴 答中断	DUMMY-RETURN (F000:FF53)	
INT1D	显示器初始化参数区	VIDEO-PARMS (F0000:F0A4)	
INT1A	软盘参数区	DISK-BASE (F000:EFC7) (0000:0522)	DOS1.1 DOS2.0 DOS置入口
INT1F	扩充图形字符		
INT40	转向软盘	DISKETTE-IO (F000:EC59)	带硬盘时
INT41	硬盘参数区	FD-TBL (C800:03E7)	带硬盘时

1.3.2 有关中断的一些说明

(1) INT 13H 磁盘管理

当系统只有软盘而不带硬盘时，INT 13H指向软盘管理的入口地址(F000:E059)。当系统带有硬盘时，INT 13H指向硬盘管理的入口地址(C800:0256)。装有硬盘时，由硬盘 INT 13H判别是使用硬盘（驱动器号)=80H) 还是软盘（驱动器号(80)，如是软盘，则再调用 INT 40H（放着软盘 INT 13H的入口地址）进入软盘管理程序。

(2) INT 1BH 键盘 CTL+Break键

按下键盘的 CTL+Break键时的中断处理程序。

(3) INT 1CH 时钟滴答中断

此中断在时钟中断(INT 8H)程序中调用，每秒钟调用约18.2次。系统启动时，INT 1CH初始化成指向一条IRET指令，故不作任何处理。使用时可根据应用需要编制程序并修改相应入口地址。

(4) INT 1FH 扩充图形字符

显示器以图形方式工作时，ASCII码中基本字符0～127字符图形点阵在ROM BIOS中已有，而扩充字符128～255字符图形点阵未包括进去。需用扩充字符图形时需建立这部分的字符图形表（1K字节），将 INT 1FH 的入口地址指向所建立的字符图形表。

(5) INT 40H 转向软盘

当系统带有硬盘时，中断向量表中 INT 40H放着软盘管理的中断入口地址（参阅(1)）。

(6) INT 41H 硬盘参数区

此中断指向 IBM提供的硬盘的参数区。如配接其他硬盘可能需要另建参数区和修改 INT 41H的入口地址。

(7) INT 2H 不可屏蔽中断(NMI)

不可屏蔽中断是存贮器奇偶错（或8087中断）。

·设置 NMI（能产生 NMI）的方法是：由 80H口子送出 80H。

·清除 NMI（不产生 NMI）的方法是：由 80H口子送出 00H。

1.3.3 中断控制器 8259A

1. 中断概述

IBM-PC机用中断控制器 8259A芯片为 8个硬中断服务。相应设备的中断请求信号由IRQ0～IRQ7线送至 8259A芯片（见下表），这 8个中断信号各自独立，优先权IRQ0最高，IRQ7最低。

8025A 输入	中断类型	设备（中断源）
IRQ0	INT8	定时器（通道 0）
IRQ1	INT9	键盘
IRQ2	INTA	保留
IRQ3	INTB	留给 RS232（第二个）
IRQ4	INTC	留给 RS232（第一个）
IRQ5	INTD	硬盘
IRQ6	INTE	软盘
IRQ7	INTF	留给打印机

中断控制器中断响应过程：

(1) 设备的中断请求信号经相应的IRQ0～IRQ7（中断请求线）送给中断控制器。

(2) 中断控制器判别优先权最高的中断请求。

(3) 接收中断请求，向 CPU发中断请求信号INTR（可屏蔽中断）。

(4) CPU 对中断作出响应后（ CPU在当前指令执行执行完成后响应），读取 8059A送来的中断类型码。

(5) CPU 转入相应的中断服务程序（参阅前面中断调用的响应过程）运行。

(6) 中断结束标志是向 8259A送中断结束命令 EOI (20H)。

2. 中断控制器 8259A的编程

(1) 中断屏蔽

〈1〉 屏蔽所有中断

标志寄存器的中断标志位IF用以屏蔽所有中断：

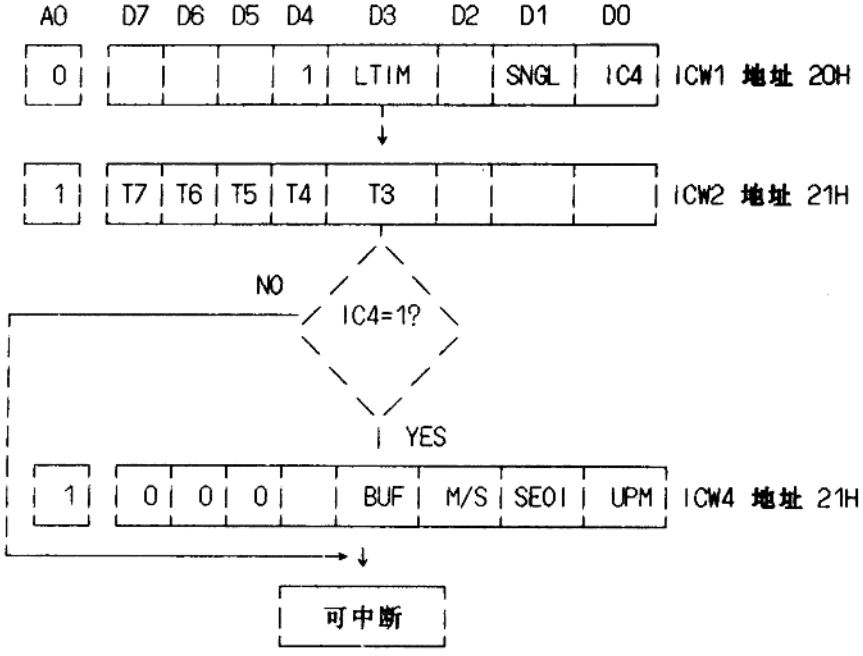
IF=0 禁止所有中断（用 CLI指令）

IF=1 允许中断 （用 STI指令）

〈2〉 8259A 里有一个中断屏蔽寄存器（IMR），其中每一位对应于一个中断源，用以控制是否允许相应的中断源申请中断，但只有当上述标志寄存器IF=1时起作用，用 OUT指令向 21H口子送相应值加以控制。

中断控制器 8259A可根据需要通过软件编程。编程内容主要是初始化和发送中断信号，以及设备屏蔽等，分别通过口子送初始化命令字（ICW)和操作命令字（OCW)等来实现。下面简述了命令中与IBM-PC机有关的部分。

〈3〉中断初始化命令字：初始化时按下述口子送出初始化命令字 ICW。



IC4:1=需要ICW4，0=无ICW4
SNGL:1 =单独使用， 0=级联使用
LTIM: 中断检测，1=电平检测， 0=边沿检测
T3～T7: 中断类型
UPM:1=8086方式，0=8085方式
AEOI: 1=自动 EOI方式，0= EOI方式
M/S: 1=主控制器，0=从控制器
BUF: 1=缓冲方式，0=不是缓冲方式
空的位：8086未用
系统启动时，BIOS给 8259A初始化指令如下：

```
    MOV  AL,13H          ;ICW1- 电平检查，单独使用，需要ICW4
    OUT  INTA00,AL       ;INTA00为 20H
    MOV  AL,8            ;ICW2- 中断类型号 8
    OUT  INTA01,AL       ;INTA01为 21H
    MOV  AL,9            ;ICW4- 缓冲，8086方式， EOI方式
    OUT  INTA01,AL
```

(2) 中断操作命令字 OCW

A0	D7	D6	D5	D4	D3	D2	D1	D0	
1	M7	M6	M5	M4	M3	M2	M1	M0	OCW1地址 21H

M0～M7：中断屏蔽（参阅前面中断屏蔽寄存器 IMR）
相应位=0 允许中断
相应位=1 禁止中断

A0	D7	D6	D5	D4	D3	D2	D1	D0	
0	R	SL	EOF						OCW2地址 20H

D7D6D5=0 0 1时表示一般 EOI（对正在服务的中断复位）

A0	D7	D6	D5	D4	D3	D2	D1	D0	
0				0	1	P	RR	RIS	OCW3地址 20H

其中，
D2D1D0=0 1 1时，表示在下一读指令时，读正在服务的中断。
(3) 中断结束
中断服务程序结束时需送中断结束信号 EOI，用以下指令：

```
MOV  AL, 20H
OUT  20H, AL        ;OCW2-送 EOI
```

1.3.4 扬声器的控制

扬声器的控制方式有两种：
(1) 通过定时器通道 2编程控制。
(2) 通过外围接口 8255 PB口 (61H)的 1位来编程序控制。
BIOS的键盘中断(INT 9H)中有一段当缓冲器满时发出音响信号的程序，它是用方式(2)方法编制的。
下面的例子是产生 600周音响信号，持续时间约 2秒的程序。
注：声音持续时的计算方法是：8088的主频是477MHZ，故一个时钟周期约为 210毫微秒。LOOP指令有转移时的时钟周期数是17。LOOP的循环计数值CX=233。所以，声音半周持续时间=17×210×233×10(-9)秒

$$\text{声音的频率} = \frac{1}{2\times17\times210\times233\times10(-9)} \approx 600\text{赫}$$

600 赫的周数 DX=1200
声音的持续时间 =1200×(1/600)=2秒
例 2：产生 600周音响信号，持续时间约为 2秒的程序

```
STACK   SEGMENT   PARA  STACK 'STACK'
        DB        256  DUP(0)          ; 256个字节空间
STACK   ENDS
DATA    SEGMENT   PARA  PUBLIC 'DATA'
FREQ    DW        233                  ;为 600周，半周所需的CX值
```