IBM AT286维修丛书之二

ROM BIOS 分 析

郑筑鸣 编

IBM PC/AT 微型计算机ROM BIOS分析

一、ROM BIOS简介

§1.1 概述：

在IBM PC/AT微型机中，BIOS（基本输入输出系统）对硬件系统进行初始化，并提供基本外部设备的管理驱动程序，它是操作系统和应用软件同硬设备之间的接口。IBM PC/AT的所有系统软件和应用程序，都是在BIOS的基础上工作的。

在IBM PC/AT的系统板上，驻留着固化的基本输入输出系统——ROM BIOS。它和ROM BASIC语言固化在一起，共同占用64KB存贮空间。在实地址方式下，地址为0F0000～0FFFFF；在保护方式下，地址为FF0000～FFFFFF。

ROM BIOS主要包括下述内容：

- 加电或热启动时进行系统检测，分析系统配置情况，进行系统初始化，然后引导操作系统。
- 基本外部设备的输入输出驱动程序：软盘、硬盘、键盘、显示器、打印机、异步通讯口等。
- 基本外部设备的工作参数。
- 实地址方式下基本的硬设备中断管理程序。
- 保护方式初始化程序

由于IBM PC/AT使用80286 CPU，具有两种不同的工作方式：实地址方式和保护方式（请参阅80286技术资料）。在实地址方式下工作，程序可以直接调用ROM BIOS中的功能。在保护方式下工作时，程序要求调用ROM BIOS中的功能，必须通过操作系统控制。

64KB容量的ROM中，可以分成三部：0～4751H为BIOS程序区，6000H～DFFFH为ROM BASIC程序，E000H～FFFFH系统数据区。中间还有部分空白单元。ROM BIOS使用BIOS程序区和系统数据区两部分。

BIOS中的所有程序，都在程序区中。它们既可在实地址方式下调用，也可在保护方式下调用。系统数据区内，包括系统初始化和基本外部设备初始化所用的参数，以及与PC/XT机兼容的中断处理程序入口。对于这些兼容的中断处理程序，其中断向量指向ROM中系统数据区。在系统数据中的入口处安排一条跳转指令，转移到BIOS程序区中，执行相应的中断处理程序。

BIOS工作过程中使用的数据，存放在地址0040:0000～00FF的区域内。它们的具体内容，在各个使用这些数据的程序中加以说明。

§1.2 程序入口和中断向量

1.2.1 程序入口地址：

BIOS程序区的长度较长，为此把备程序按模块分段编写，在汇编时连接装配成完整的程序。为了与源程序清单对照，在分析程序时，每个块模块都从相对地址0开始。下面给出

各个程序模块入口在BIOS段内的偏移地址。程序内的偏移地址，等于模块入口偏移地址加上模块内相对地址。

程序模块	入口偏移地址	功 能
POST1（TEST1）	002C	加电自诊断1
POST2（TEST2）	0C3F	加电自诊断2
POST3（TEST3）	16AD	加电自诊断3
POST4（TEST4）	1753	加电自诊断4
POST5（TEST5）	1853	加电自诊断5
POST6（TEST6）	199C	加电自诊断6
BOOT	1B66	DOS引导程序（INT19）
POST7（TEST7）	1C2D	加电自诊断7
SYSINIT1	1F1A	保护方式初始化
GDT—BLD	1F68	建立全局描述符表
SIDT—BLD	1FF9	建立中断描述符表
DISKETTE—IO—1	20A5	软盘输入输出驱动程序
DISK—SETUP	28DA	硬盘初始化和输入输出驱动程序
KEYBOARD—IO—1	2FC8	键盘输入输出驱动程序
PRINTER—IO—1	346F	打印机输入输出驱动程序
RS232—IO—1	34F5	异步通讯输入输出驱动程序
VIDEO—IO—1	3605	显示输入输出驱动程序
MEMORY—SIZE—DETERMINE—1	3E62	存贮器容量检测程序
EQUIPMENT—1	3E6C	设备配置检测程序
NMI—INT—1	3E76	非屏蔽中断处理程序(实地址方式)
SET—TOD	3F2F	设置时间程序
CASSETTE—IO—1	3FE2	专用程序
TIME—OF—DAY—1	445C	时间和日期管理程序
RTC—INT	462A	实时钟中断处理程序
TIMER—INT—1	4684	8254定时中断处理程序
PRINT—SCREEN—1	46CC	打印屏幕程序
ORCS	E000	系统数据区

2.1.2 实地址方式下的中断向量

BIOS中的程序，除了与加电自诊断有关的部分外，都用中断方式加以调用。在保护方式下，使用中断门描述符调用中断服务程序，在实地址方式下通过中断向量进入中断服务程序。

在实地址方式下，存贮器的最低端1K字节是中断向量表。表内按照中断类型号的顺序，依次排列各中断服务程序的入口地址——中断向量，每个中断向量占四个单元。前二个单元为中断服务程序入口的偏移地址，后二个单元为段地址。BIOS中使用的中断向量如下表所示：

实地址方式下BIOS使用的中断向量表

地　址	中断类型	中　断　名　称	标　　号	BIOS中入口地址
00—03	0	除法出错		
04—07	1	单步中断		
08—0B	2	非屏蔽中断	NMI—INT	F000：E2C3
0C—0F	3	断点中断		
10—13	4	溢出中断		
14—17	5	屏幕打印中断	PRINT—SCREEN	E000：FF54
18—1B	6	备用		
1C—1F	7	备用		
20—23	8	日时钟中断（IRQ0）	TIMER—INT	F000：FEA5
24—27	9	键盘中断（IRQ1）	KB—INT	F000：E987
28—2B	A	保留（IRQ2）		
2C—2F	B	保留（IRQ3）		
30—33	C	保留（IRQ4）		
34—37	D	保留（IRQ5）		
38—3B	E	软盘中断（IRQ6）	DISK—INT	F000：EF57
3C—3F	F	为打印机中断保留(IRQ7)		
40—43	10	显示I/O驱动程序	VIDEO—IO	FF000：F065
44—47	11	设备配置检测顺序	EQUIPMENT	F000：F84D
48—4B	12	存贮器容量检测顺序	MEMORY-S-DET	F000：F841
4C—4F	13	硬盘I/O驱动程序	DISK—IO	F000：2A71
50—53	14	通讯RS-232I/O驱动程序	RS232—IO	F000：E739
54—57	15	专用程序	CASSETTE—IO	F000：F859
58—5B	16	键盘I/O驱动程序	KEYBOARD—IO	F000：E82E
5C—5F	17	打印机I/O驱动程序	PRINTER—IO	F000：EFD2
60—63	18	ROM BASIC入口		F6000：0000
64—67	19	磁盘引导程序	BOOT—STRAP	F000：E6F2

续 表

地 址	中断类型	中 断 名 称	标 号	BIOS 中入口地址
68—6B	1A	置日期和时间程序	TIME—OF—DAY	F000：FE6E
6C—6F	1B	保留		
70—73	1C	保留		
74—77	1D	视频参数指针(初始化)	VIDEO—PARMS	F000：F0A4
78—7B	1E	软盘参数指针(初始化)	DISK—BASE	F000：EFC7
7C—7F	1F	指向ASCII码128-256的指针		
100—103	40	软盘I/O驱动程序	DISKETTE—IO	F000：EC59
104—107	41	硬盘参数指针(0*驱动器)	HD—BASE—O	
118-11B	46	硬盘参数指针(1*驱动器)	HD—BASE—1	
140—143	50	实时钟中断(IRQ8)	RTC—INT	F000：462A
1D8—1DB	76	硬盘中断(IRQ4)	HD—INT	F000：2FA4

二、系统检测和磁盘引导程序

§2.1 功能

IBM PG/AT在加电或系统热启动后，对硬件基本系统进行自诊断测试。诊断正确通过后，进行系统初始化，接着引导磁盘上的操作系统，进入正常运行。如果自诊断过程中发现错误，则根据错误性质作出反应：停机、音响报警、显示出错信息等等，以便操作人员进一步处理。

系统加电时，80286 CPU处于实地址方式下工作，自动进入0FFFF：0000单元执行。此处存放一条跳转指令，控制转移到自诊断程序入口。系统在接受到热启动命令时（同时按下CPRL+ALT+DEL键），控制也转移到自诊断程序入口。加电启动或热启动的流程如图1所示。

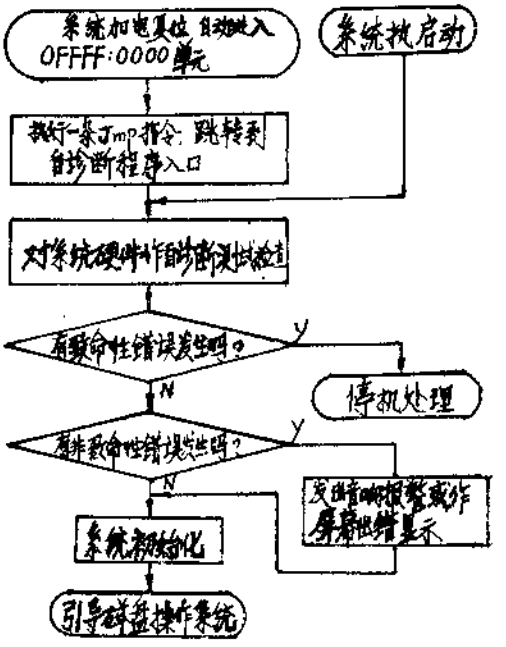


图1 系统启动流程图

系统自诊断程序占用BIOS段内000_0～20A4H存贮区。其中0～2BH是BIOS版本号，其余部分是自诊断程序。它有下列部分组成：POST1～POST7（加电测试1～7），其中包括自诊断主程序及其调

用的予程序；以及保护方式初始化程序。

在自诊断过程中，为了检测系统硬件的功能，80286有时需要进入保护方式运行。这时用SYSINIT程序启动保护方式，用GDT—BLD程序建立全局描述符表，用SIDT—BLD程序建立中断描述符表。

在保护方式检测结束后，80286就要退出保护方式，返回到实地址方式下继续运行。80286退出保护方式时，使用CMOS中的保护方式停止字节，决定停止保护方式后将控制转移到何处去。其功能如下：

停止字节内容	转移地址	功　　能
0	16E	系统加电或热启动，不存在停止。
1	9B0	测内存容量后停止。
2	1197	在内存测试后停止。
3	114A	内存测试有错时停止。
4	169B	有引导操作系统请求时停止。
5	171	停止后转移到选件的ROM初始化程序入口（有中断）。
6	11BC	通过保护方式测试POST7后停止。
7	119A	保护方式测试POST7失败后停止。
8	7F7	POST1中保护方式测试失败后停止。
9	4252	数据块传送结束后停止。
A	17D	停止后转移到选件的ROM初始化程序入口(无中断)。

在分析自诊断程序时，为了方便阅读，把POST1(TEST1)～POST7(TEST7)七个模块组合在一起。模块内部相对地址=偏移地址—模块入口地址，(模块入口地址见§1.2程序入口地址)。

§2.2 数据单元和出错信息：

2.2.1 BIOS自诊断程序建立的数据：

BIOS自诊断程序建立的数据，存放在地址为0040：0000开始的区域内，各数据单元的内容如下：

0～7	异步通讯适配器基地址
8～F	並行打印机适配器基地址
10	设备配置字节
11	打印机数和RS—232数
12	设备跳线器（开关）状态
13,14	安装的RAM容量（以KB为单位）
15,16	部件诊断故障标志
17,18	通过诊断的RAM总容量（以KB为单位）暂存单元
6B	中断标志
72	键盘标志（加电时）或热启动标志（热启动时）

2.2.2 诊断故障显示代码：

自诊断程序发现错误时，在CRT进行工作后显示出错代码和信息，它们的意义如下：

101 系统板上8259错

102 系统板上8254定时器错

103 系统板上8254定时器太慢

104 系统板上CPU保护方式错

105 系统板上键盘接口错

106 系统板上数据转换错

107 系统板上非法NMI

108 系统板上8254数据线错

109 系统板上1M内地址选择错

161 电池失效

162 CMOS累加和错或系统配置错

163 实时钟错

164 RAM容量设置错

201 RAM数据错或奇偶校验错

202 地址线A0～A15错

203 地址线A16～A23错

301 键盘错

302 键盘锁闭锁

303 键盘接口错

304 键盘时钟信号错

401 单色显示适配器（MDA）故障

501 彩色图形显示适配器（CGA）故障

601 软盘故障

602 软盘引导扇区无内容

1780 0*硬盘驱动器初始化错

1781 1*硬盘驱动器初始化错

1782 硬盘控制器故障

1790 0*硬盘驱动器读操作错

1791 1*硬盘驱动器读操作错

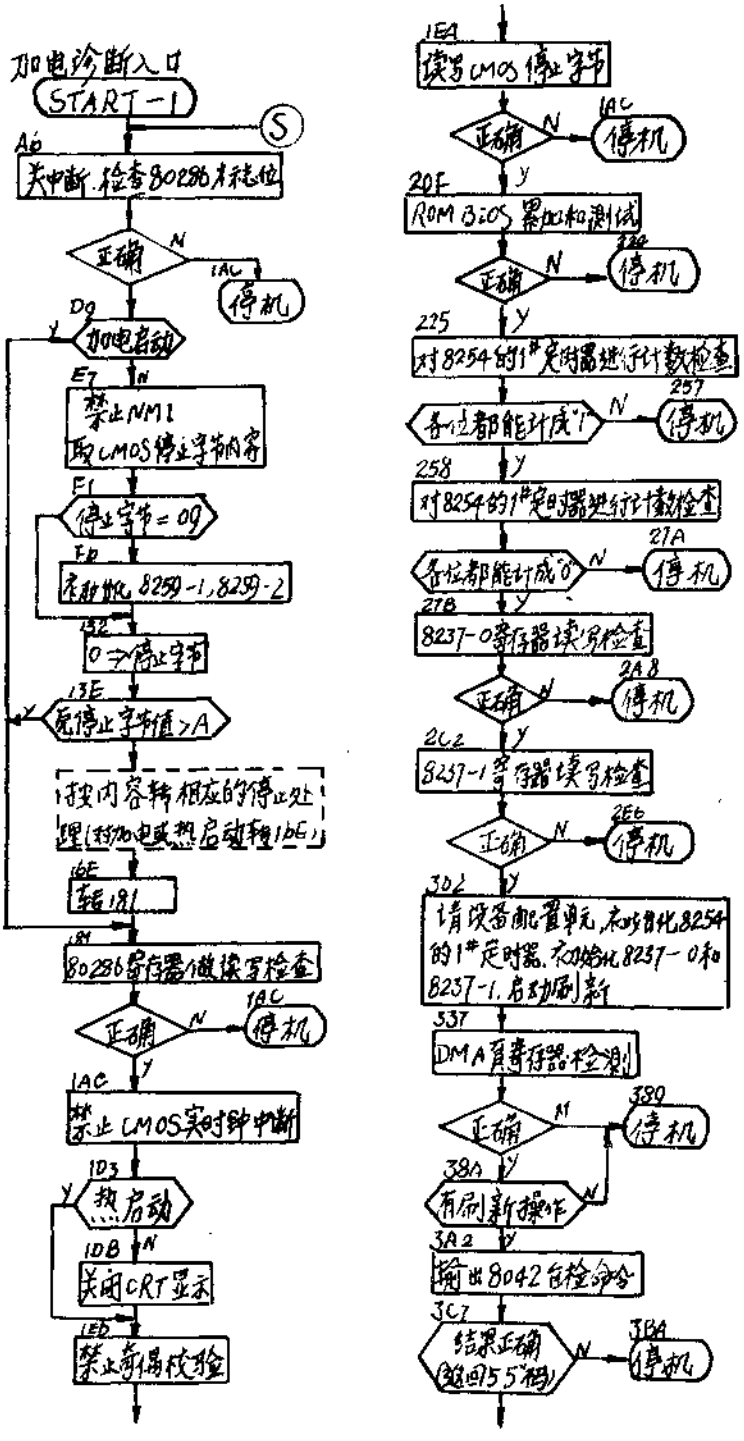
PARITY CHECK1 系统板RAM奇偶校验错

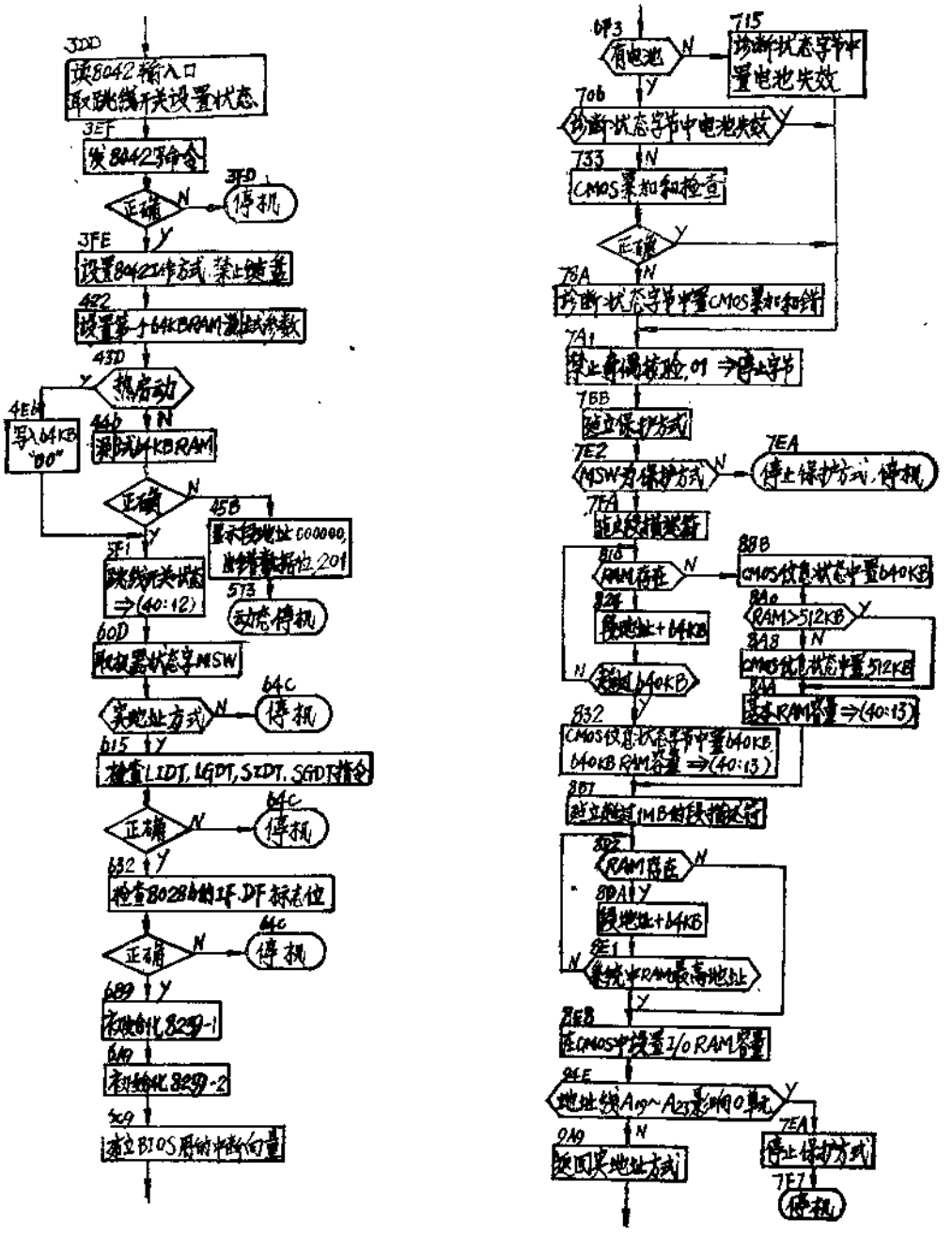
PARITY CHECK2 IO RAM奇偶校验错

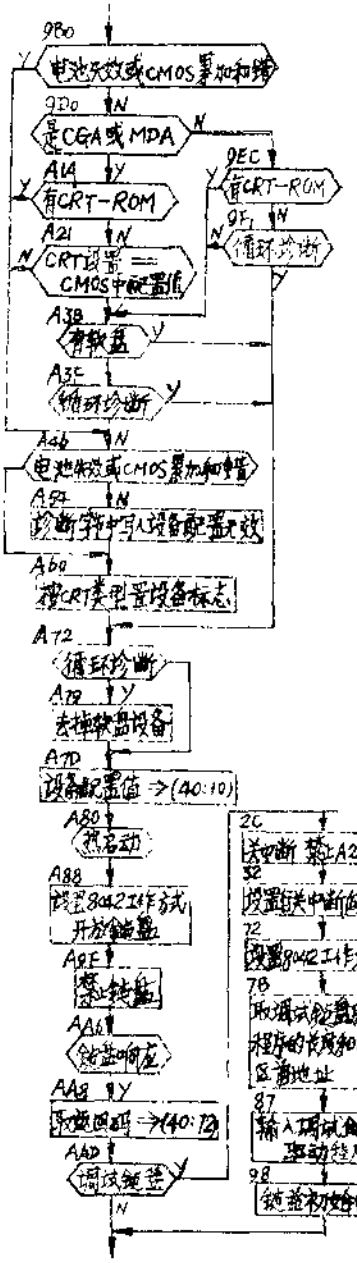
ROM ERROR ROM累加和错

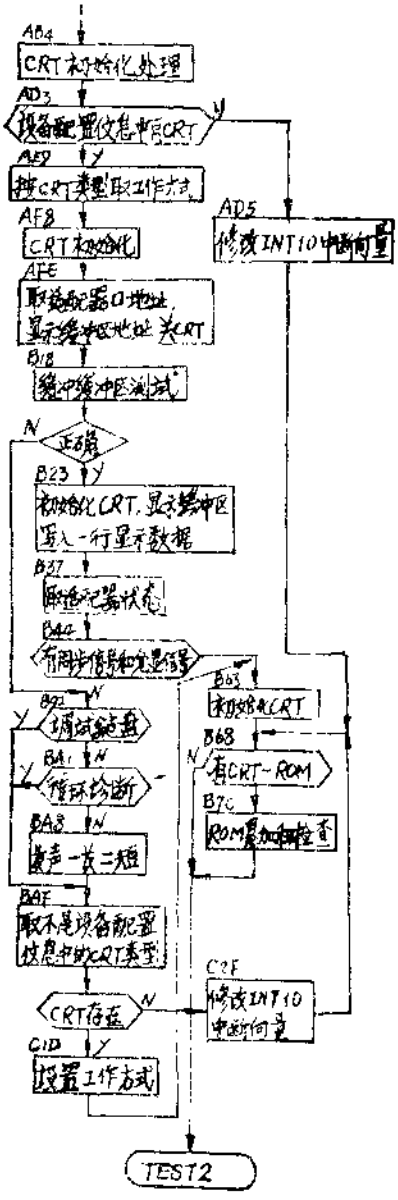
§2.3 BIOS自诊断程序分析

2.3.1 TEST（POST1）：加电诊断程序(1)

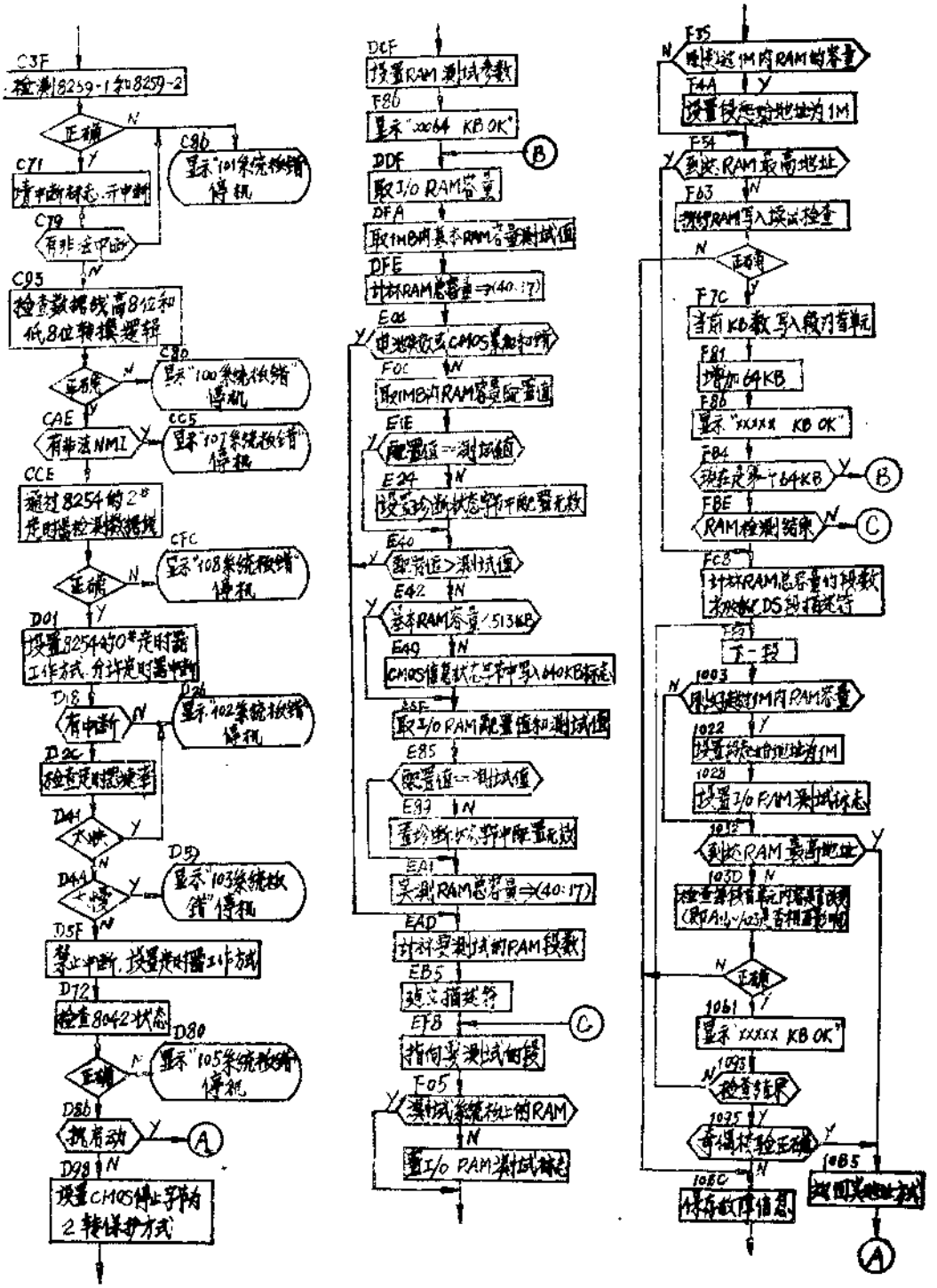


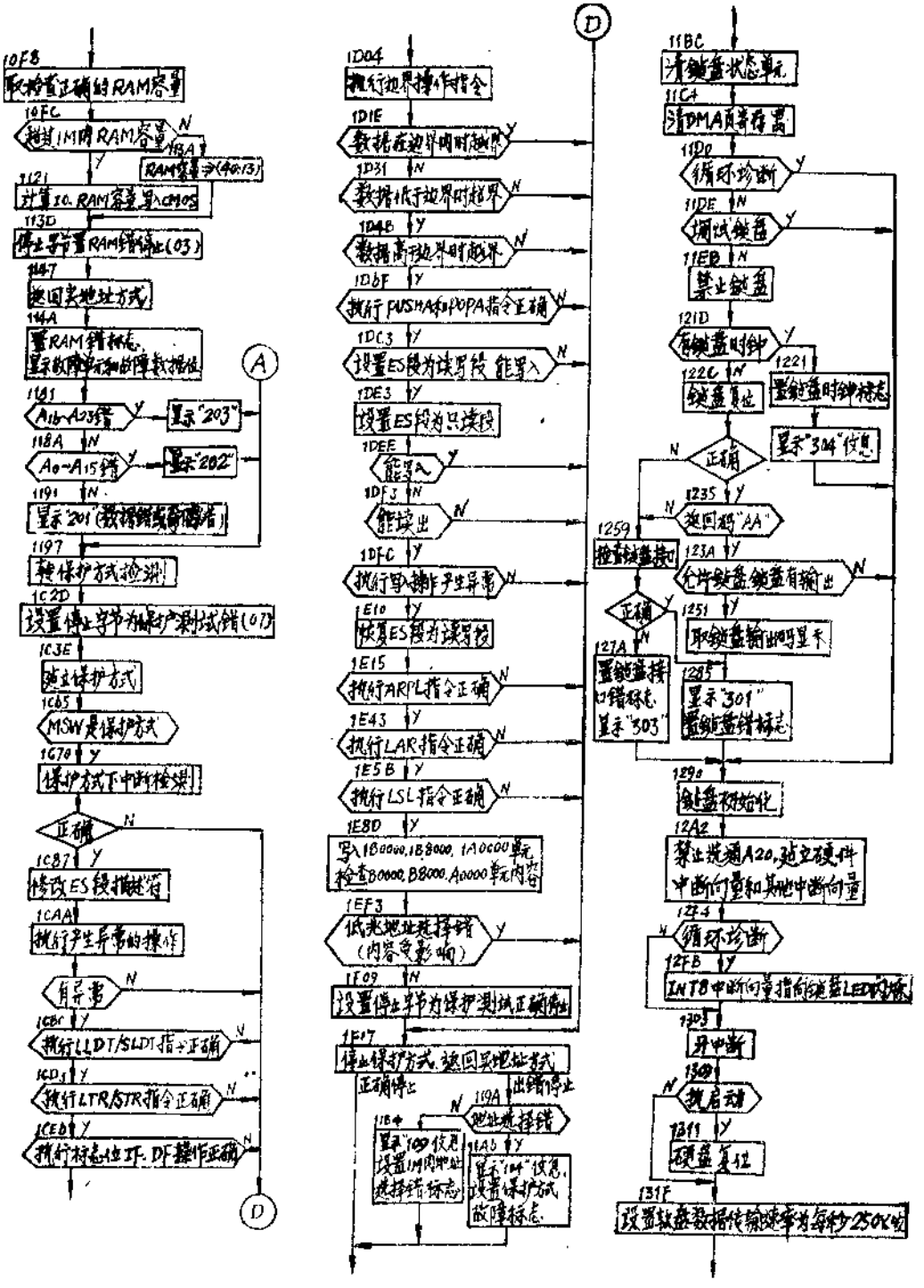

JDD
读8042输入口
取跳线开关设置状态
3EF
发8042写命令
3FD
停机
正确
N
Y
3FE
设置8042工作方式,禁止键盘
422
设置第一个64KBRAM测试参数
43D
热启动
Y
4EB
写入64KB
"00"
44b
N
测试64KBRAM
正确
N
45B
显示错地址000000,
出错参数指位201
Y
5F1
跳线开关设置
⇒(40:12)
573
动态停机
60D
取设置状态字MSW
实地址方式
N
64C
停机
Y
b15
检查LIDT,LGDT,SIDT,SGDT指令
正确
N
64C
停机
Y
632
检查8028bit IF,DF标志位
正确
N
64C
停机
Y
689
初始化8259-1
6A9
初始化8259-2
729
建立BIOS用的中断向量
0F3
有电池
N
715
诊断状态字节中
置电池失效
Y
70b
诊断状态字节中电池失效
Y
733
N
CMOS累加和检查
正确
Y
N
78A
诊断状态字节中置CMOS累加和错
7A1
禁止奇偶检验,01⇒停止字节
7BB
建立保护方式
7E2
MSW为保护方式
N
7EA
停止保护方式,停机
Y
7FA
建立段描述符
818
RAM存在
N
88B
CMOS仅基状态中置640KB
824
段地址+64KB
8A0
RAM>512KB
Y
8A8
N
CMOS仅扩状态中置512KB
8AA
基本RAM容量⇒(40:13)
N
到达640KB
Y
832
CMOS仅基状态字节中置640KB,
640KB RAM容量⇒(40:13)
8D7
建立描述IMB的段描述符
8DC
RAM存在
N
8DA1
Y
段地址+64KB
8E1
N
系统中RAM最高地址
Y
8EB
在CMOS中设置I/O RAM容量
9LE
地址线A19~A23影响0单元
Y
9A9
N
返回实地址方式
7EA1
停止保护方式
7F7
停机

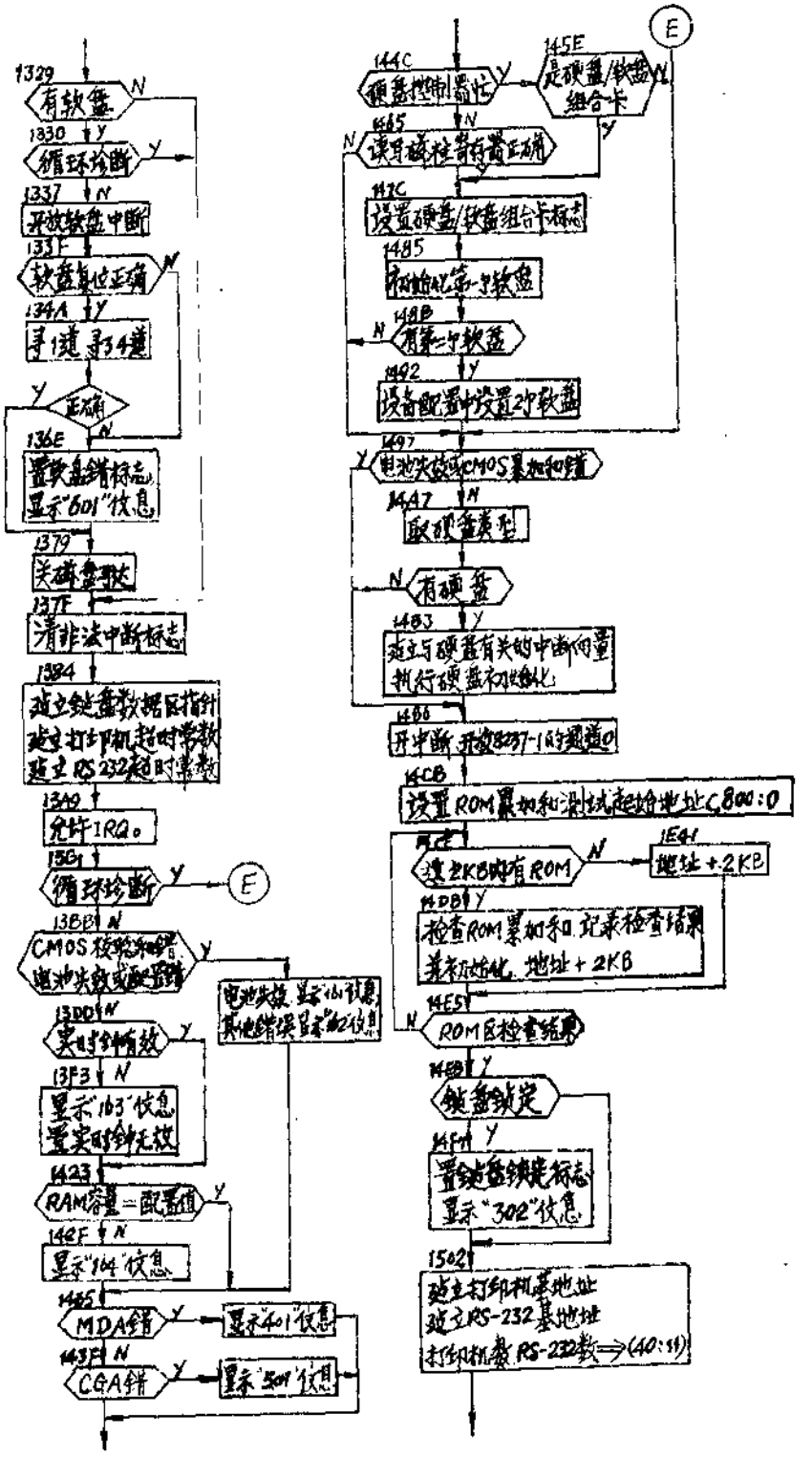

9B0
电池失效或CMOS累加和错
9D0
是CGA或MDA
9EC
有CRT-ROM
A14
有CRT-ROM
9F1
循环诊断
A21
CRT设置 == CMOS中配置值
A38
有软盘
A3F
循环诊断
A46
电池失效或CMOS累加和错
A54
诊断字节中写入设备配置无效
A60
搜CRT类型置设备标志
A72
循环诊断
A78
去掉软盘设备
A7D
设备配置值 -> (40:10)
A80
热启动
A88
设置8042工作方式
开放键盘
A9E
禁止键盘
AA6
键盘响应
AA8
读键回码 -> (40:12)
AAD
调试键盘
2C
关中断 禁止A20
32
设置向量中断向量
72
设置8042工作方式
7B
取调试键盘驱动程序的代码和缓冲区首地址
87
输入调试键盘驱动程序
98
键盘初始化

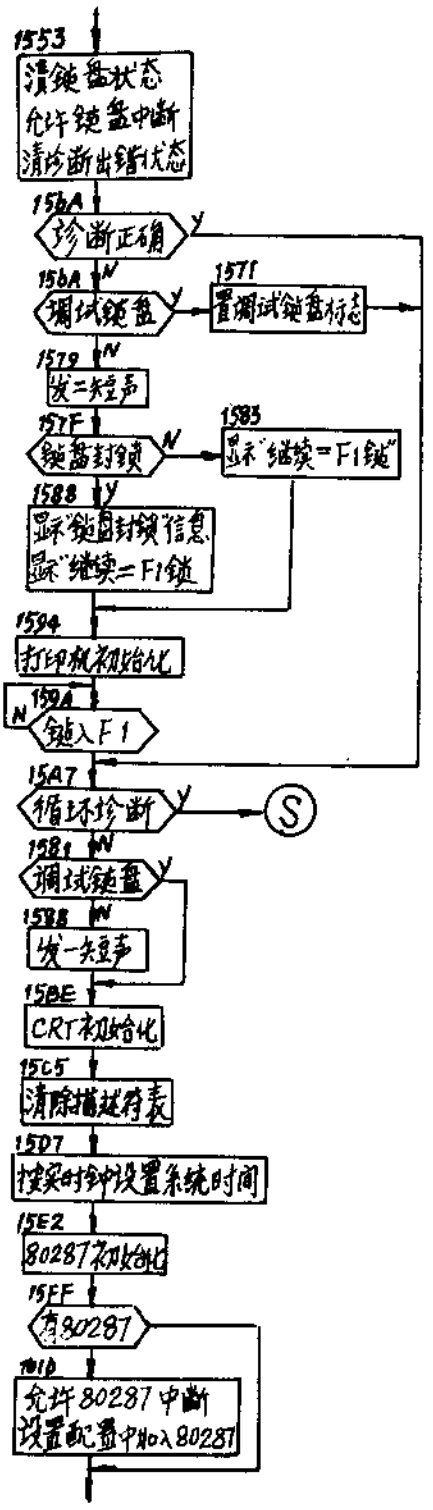

AB4
CRT初始化处理
AD3
设备配置仅指明CRT
AE9
搜CRT类型取工作方式
AF8
CRT初始化
AD5
修改INT10中断向量
AFE
取适配器口地址,
显示缓冲区地址 关CRT
B18
缓冲缓冲区测试
正确
B23
初始化CRT,显示缓冲区
写入一行显示数据
B37
置适配器状态
B44
有同步信号和显示信号
B63
初始化CRT
B92
调试键盘
B68
有CRT-ROM
BA1
循环诊断
B7C
ROM累加和检查
BA8
扬声一长二短
BAF
取不是设备配置
仪指明的CRT类型
C2F
修改INT10
中断向量
CRT存在
C1D
设置工作方式
TEST2

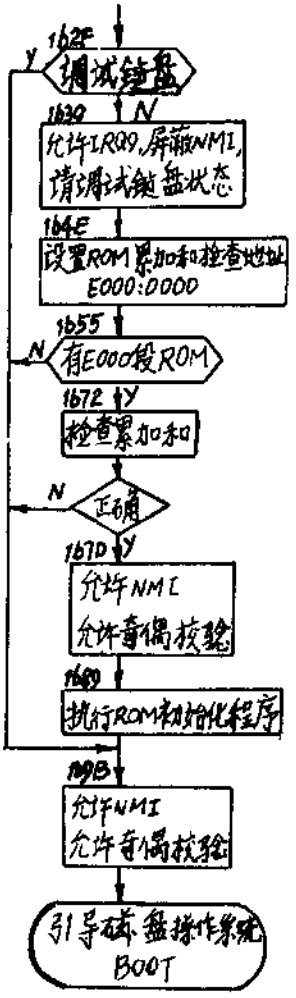
2.3.2 TEST2（POST2）：加电诊断程序(2)




10F8
取检查正确的RAM容量
10FC
超过1M用RAM容量
N
Y
1BA
RAM容量⇒(40:13)
1121
计算10.RAM容量写CMOS
113D
停止写置RAM错误地址(03)
1147
返回实地址方式
114A
置RAM错标志,
显示故障单元和出错数据位
A
1161
A16-A23错
Y
显示"203"
118A
N
A0-A15错
Y
显示"202"
1191
N
显示"201"(数据错或奇偶错)
1197
转保护方式检测
1C2D
设置停止字节为保护测试错(07)
1C3E
进入保护方式
1C65
MSW置保护方式
1C70
Y
保护方式下中断检测
正确
N
Y
1C87
修改ES段描述符
1CAA
执行产生异常的操作
有异常
N
Y
1CBC
执行LLDT/SLDT指令正确
N
Y
1CD1
执行LTR/STR指令正确
N
Y
1CEB
执行标志位IF、DF操作正确
N
D
1D04
执行边界操作指令
1D1E
数据在边界时越界
Y
1D31
N
数据低于边界时越界
N
1D4B
Y
数据高于边界时越界
N
1D6F
Y
执行PUSHA和POPA指令正确
N
1DC3
Y
设置ES段为读写段 能写入
N
1DE3
Y
设置ES段为只读段
1DEE
能写入
Y
1DF3
N
能读出
N
1DFC
Y
执行写操作产生异常
N
1E10
Y
恢复ES段为读写段
1E15
执行ARPL指令正确
N
1E43
Y
执行LAR指令正确
N
1E5B
Y
执行LSL指令正确
N
1E8D
Y
写入18000,1B8000,1A0000单元
检查B0000,B8000,A0000单元内容
1EF3
低来地址选择错
(内容受影响)
Y
1F09
N
设置停止字节为保护测试正确值
1F17
停止保护方式,返回实地址方式
正确停止
出错停止
119A
地址选择错
N
Y
11B中
显示"109"信息
设置IM内出错
选择错标志
11A5
Y
显示"104"信息
设置保护方式
故障标志
11BC
清键盘状态单元
11C4
清DMA等待置
11D0
循环检测
Y
11DE
N
调试键盘
Y
11EB
N
禁止键盘
121D
有键盘时钟
Y
1221
置键盘时钟标志
122C
N
键盘复位
正确
N
Y
显示"304"信息
1235
N
Y
返回码"AA"
1259
检查键盘接口
123A
Y
允许键盘,键盘有输出
N
正确
Y
1251
取键盘输出码显示
N
127A
置键盘接口错标志,
显示"303"
1285
显示"301"
置键盘错标志
1290
键盘初始化
12A2
禁止扩展A20,独立硬件中断向量和其他中断向量
12E4
循环检测
N
Y
12FB
INT8中断向量指向键盘LED闪烁
1303
开中断
1307
N
热启动
Y
1311
硬盘复位
131F
设置软盘数据传输速率为每秒250K位


1329
有软盘
N
1830
Y
循环检测
Y
1337
N
开放软盘中断
133F
软盘复位正确
N
134A
Y
寻1道 寻34道
Y
正确
N
136E
置软盘错标志
显示"601"信息
1379
关硬盘驱动
137F
清非法中断标志
1384
建立键盘数据区指针
建立打印机超时常数
建立RS-232超时常数
13A9
允许IRQ0
15G1
循环检测
Y
E
13BB1
N
CMOS校验和错误
电池失效或配置错
Y
电池失效 显示"161"信息
其他错误显示"162"信息
13D0
N
实时钟有效
Y
13F3
N
显示"163"信息
置实时钟无效
1423
RAM容量=配置值
Y
142F
N
显示"164"信息
1485
MDA卡
Y
显示"401"信息
143F
N
CGA卡
Y
显示"501"信息
144C
硬盘控制器忙
Y
145E
是硬盘/软盘组合卡
N
1465
N
读寄存器存储正确
Y
147C
设置硬盘/软盘组合卡标志
1485
初始化第一个软盘
148B
有第二个软盘
N
Y
1492
设备配置中设置2个软盘
1497
电池失效或CMOS累加和错
Y
N
14A7
取硬盘类型
N
有硬盘
Y
14B3
建立与硬盘有关的中断向量
执行硬盘初始化
14B6
开中断 开放8237-1的通道0
14CB
设置ROM累加和测试起始地址C800:0
14CE
1E41
N
读2KB的ROM
地址+2KB
14DB
Y
检查ROM累加和 记录检查结果
置初始化 地址+2KB
14E5
N
ROM区检查结果
Y
14EB
键盘锁定
Y
14FH
置键盘锁定标志
显示"302"信息
1502
建立打印机基地址
建立RS-232基地址
打印机数 RS-232数 ⇒(40:11)


1553
清键盘状态
允许键盘中断
清诊断出错状态
156A
诊断正确
Y
N
156A
调试键盘
Y
1571
置调试键盘标志
N
1579
发一次短声
157F
键盘封锁
N
1583
显示"继续=F1键"
Y
1588
显示"键盘封锁"信息
显示"继续=F1键"
1594
打印机初始化
N
159A
键入F1
15A7
循环诊断
Y
S
N
1581
调试键盘
Y
N
1585
发一次短声
15BE
CRT初始化
15C5
清除描述符表
15D7
检查时钟中设置系统时间
15E2
80287初始化
15FF
有80287
1610
允许80287中断
设置配置中加入80287


162F
调试键盘
Y
N
1639
允许LRQ9,屏蔽NMI,
清调试键盘状态
164E
设置ROM累加和检查地址
E000:0000
1655
有E000段ROM
N
Y
1672
检查累加和
N
正确
Y
167D
允许NMI
允许奇偶校验
1689
执行ROM初始化程序
1698
允许NMI
允许奇偶校验
引导磁盘操作系统
BOOT

2.3.3 TEST3（POST3）：加电诊断实用程序(1)

系统ROM累加和检查子程序：

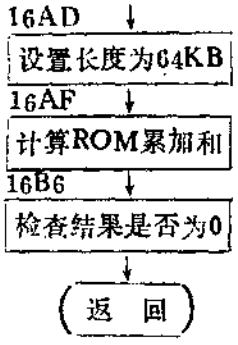
检测BIOS（F000）段和E000段ROM累加和

入口参数：DS：BX＝ROM起始地址

返回参数：ZF＝1(AL＝0)—正确

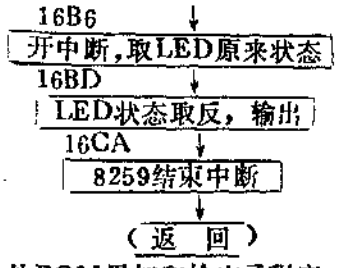
ZF＝0(AL≠0)—不正确

ROS—CHECKSUM



调试键盘初始化时LED闪烁中断处理程序：

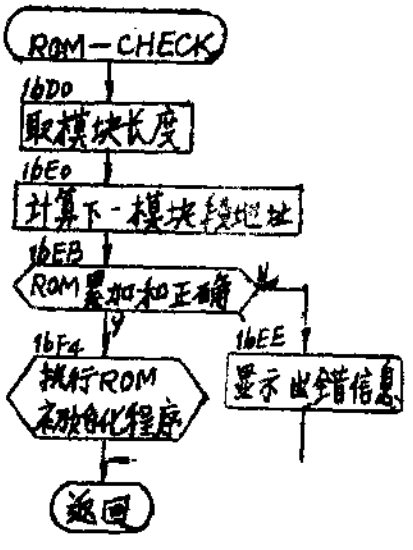
BLINK—INT



选件ROM累加和检查子程序：

入口参数：DS：BX＝ROM起始地址

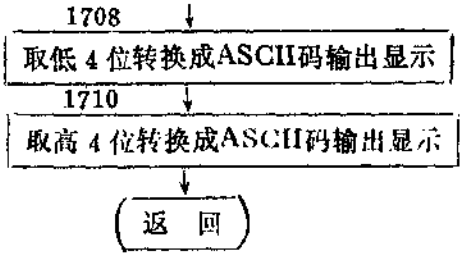
返回参数：ZF＝1(AL＝0)—正确



用十六进制方式显示AL内容子程序：

入口参数：AL—显示数据

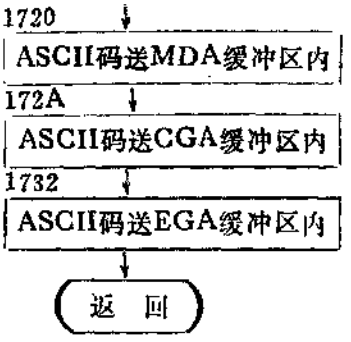
XPC—BYTE



保护方式下把AL中ASCII码送显示缓冲区：

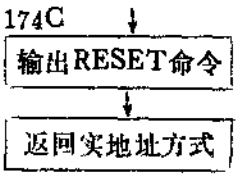
入口参数：AL＝ASCII码，DI＝缓冲区内位置

PROT—PRT—HEX



停止保护方式子程序：

PROC—SHUTDOWN

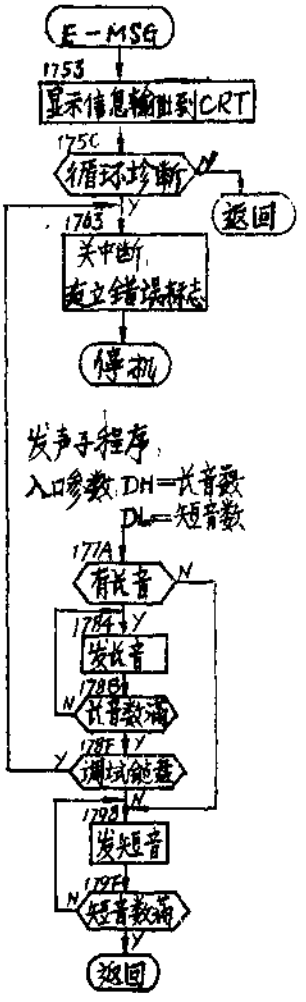


2.3. 4 TEST4（POST4）：加电诊断实用程序(2)

出错信息显示子程序：

入口参数：CS：SI＝信息存放区首地址

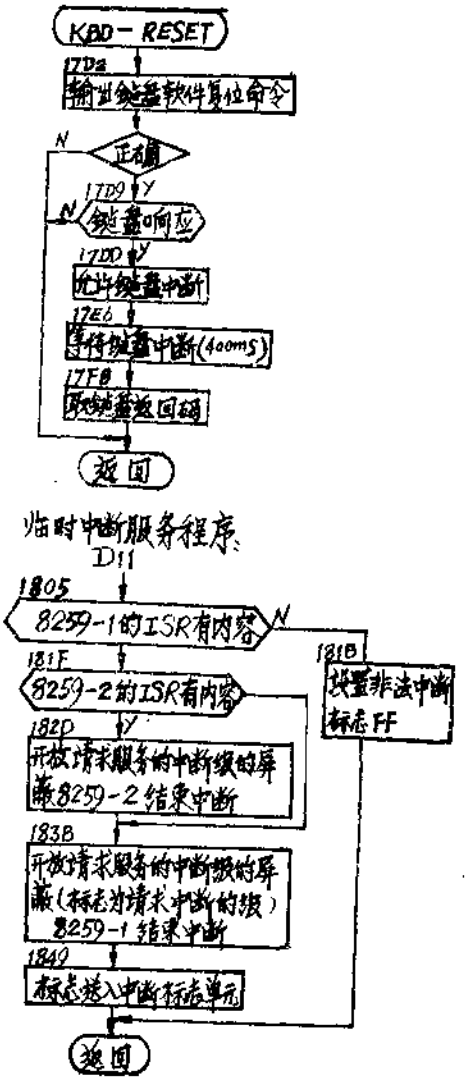
CX＝信息长度(最大36个字符)



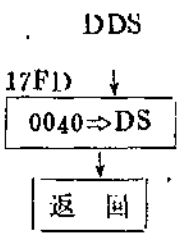
键盘软件复位子程序：

返回参数：AL＝BL＝AA—产品键盘

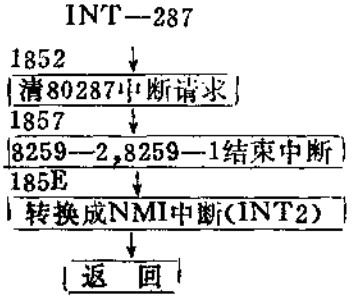
AL＝BL＝65—调试键盘



设置BIOS数据区段地址子程序：

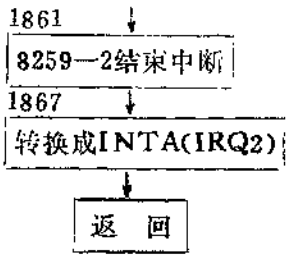


80287中断服务程序(INT 75，IRQ13)：



INT 71中断服务程序(IRQ9):

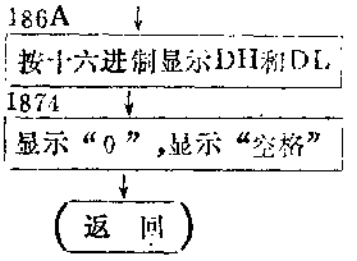
RE—DIRECT



显示段地址子程序

入口参数：DX＝段地址

PRT—SEG



2.3. 5 TEST5（POST5）保护方式下的异常和中断处理程序：