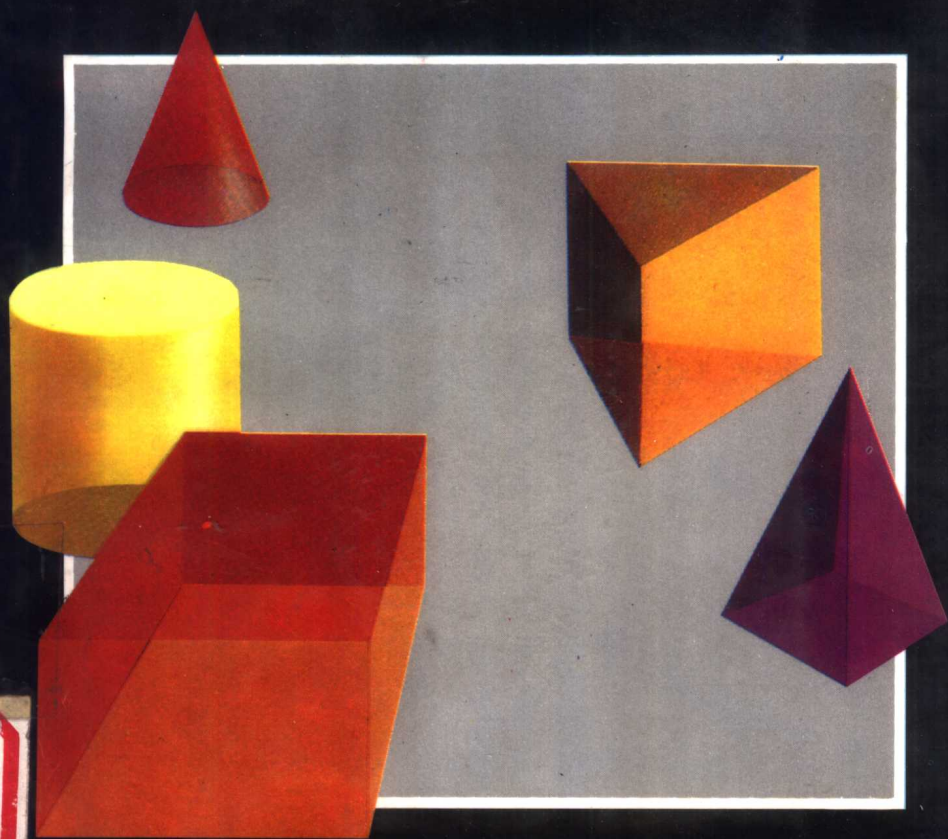


微机开发 维护技术

中国冶金建设协会 编著



冶金工业出版社

微机开发维护技术

中国冶金建设协会 编著

冶金工业出版社

(京) 新登字 036号

内 容 简 介

本书从微机系统开发维护的角度, 系统地、深入浅出地阐述了微型计算机的结构、工作原理和工作过程, 以及研究、剖析微机系统的思路、方法和技巧。书中许多内容是作者开发维护微机的经验总结。书中还附有大量的编程实例并介绍了十多个开发工具(软件), 这有益于开发维护人员的进一步提高。本书内容新颖、文字通俗易懂, 实用性强。适合从事计算机专业人员阅读, 也可供大专院校师生参考。

微机开发维护技术

中国冶金建设协会 编著

*

冶金工业出版社出版发行

(北京北河沿大街嵩靛院北巷39号)

新华书店总店科技发行所经销

冶金工业出版社印刷厂印刷

*

850×1168 1/32 印张 9.625 字数 246 千字

1993年5月第一版 1993年5月第一次印刷

印数 00,001~2,500 册

ISBN 7-5024-1181-X

TP·43 定价 8.50 元

前 言

随着计算机在我国的广泛应用，开发维护计算机的重要性，已经被越来越多的人所认识，广大用户迫切要求进行微机开发工作，以适应目前工作的需要。特别是近几年来，386机、486机的迅速发展，Auto CAD、Microstation等大型软件不断推出，计算机病毒的不断出现，把开发维护工作推向了新阶段。现实要求开发维护人员不但要对计算机系统有深刻的了解，充分发挥现有的功能，解决用户的各种难题，而且要求不断改进、增加计算机的功能，满足用户不断增长的要求。实践经验表明，在计算机上开发一个好的应用软件，不是一件容易的事。充分发挥计算机的现有功能、或者改进、增加计算机的某种功能，提高计算机的处理能力，也不是一件容易的事。前者属于使用计算机的范畴，后者属于开发维护计算机的范畴。虽然有的科技人员能够开发、研制出一些应用软件包或大型管理系统，但是，让他为自己的软件加密或者消除计算机中的病毒，却无能为力。即使编写一个小小的汉字打印驱动程序也显得力不从心，因为这已超出了使用计算机的范畴。

计算机开发维护工作是一件技术性很强的工作。多年来，我们一直从事这一方面的研究工作，取得了一定的成绩。现将我们的维护经验、编程技巧、开发实例总结出来，作为引玉之砖奉献给读者。

本书从微机开发和维护的角度，介绍了一些分析、解决问题的思路和方法。如商品软件加密、文件恢复、消除病毒技术，恢复硬盘操作系统方法，从故障盘中挽救文件，修改EXE文件，不同显示卡软件的移植，编写设备驱动程序，了解内存现场等。并介绍了大量的编程实例和自编的一些软件开发工具。

本书由王洪才、李培信主编，参加编写的有金英实、胡远

· 1 ·
07571/05

玢、赖远彬、吴玉成、洪浩、石秀馨、张民久等。在编写过程中得到了一些同志的关心和支持，并提出宝贵意见，在此表示由衷地感谢。

由于编写人员水平有限，不妥之处敬请读者批评指正。

目 录

1 微机开发维护技术概论	1
1.1 微机开发技术及意义	1
1.2 硬件开发	2
1.3 软件开发	2
1.4 微机系统的三级结构	3
1.4.1 适配器级	3
1.4.2 BIOS 级	4
1.4.3 操作系统级	5
1.5 开发微机的条件	5
2 操作系统	7
2.1 DOS 操作系统的组成和建立	7
2.1.1 DOS 的组成	8
2.1.2 DOS 模块磁盘位置要求	9
2.1.2.1 引导模块	9
2.1.2.2 IBMBIO.COM 及 IBMDOS.COM 模块	9
2.1.2.3 COMMAND.COM 模块	10
2.1.3 操作系统的建立	10
2.1.3.1 使用格式化命令 FORMAT 建立	10
2.1.3.2 使用传输命令 SYS.COM 建立	11
2.2 DOS 功能调用	12
2.3 内存管理	16
2.3.1 内存分配	16
2.3.2 ROM 工作单元和 DOS 工作单元	20
2.3.3 内存管理	22
2.3.3.1 内存管理块(MCB)	23
2.3.3.2 内存管理的功能调用	24
2.4 可执行命令文件的加载	25

2.4.1	程序段前缀 PSP	25
2.4.1.1	PSP 的格式与内容	26
2.4.1.2	PSP 分析	28
2.4.2	COM 文件和 EXE 文件的加载	29
2.4.2.1	DOS 对 COM 文件的加载和运行	29
2.4.2.2	DOS 对 EXE 文件的加载和运行	30
2.4.2.3	DOS 运行现场分析	30
2.5	恢复硬盘操作系统的方法	34
2.5.1	处理无效 C 盘故障	35
2.5.2	检查操作系统的几个模块	35
2.5.2.1	检查 COMMAND.COM 文件	35
2.5.2.2	检查两个隐含文件	36
2.5.2.3	检查引导块	37
3	软盘	39
3.1	软盘的磁道结构	39
3.1.1	磁道结构	39
3.1.2	如何观察磁道结构	40
3.1.2.1	利用 INT 13 观察磁道结构	41
3.1.2.2	用 FDC 的命令观察软盘磁道结构	42
3.2	如何读写软盘	43
3.3	软盘的数据结构	44
3.4	软盘适配器编程原理	45
3.4.1	数据控制端口	46
3.4.2	FDC 端口	47
3.4.2.1	FDC 数据寄存器	47
3.4.2.2	FDC 主状态寄存器	47
3.4.3	工作单元	48
3.4.4	FDC 的时间控制	49
3.5	软盘控制器(FDC)命令	50
3.5.1	读数据命令	50

3.5.2	写数据命令	51
3.5.3	读删除数据命令	51
3.5.4	写删除数据命令	51
3.5.5	读磁道命令	51
3.5.6	扫描相等命令	51
3.5.7	扫描小于或等于命令	52
3.5.8	扫描大于或等于命令	52
3.5.9	格式化一道命令	52
3.5.10	读 ID 数据命令	53
3.5.11	磁头归 0 道命令	53
3.5.12	寻找磁道命令	53
3.5.13	检查驱动器命令	53
3.5.14	送参数命令	54
3.5.15	取命令结果命令	54
3.6	格式化命令及扇区读写	55
3.7	软盘基数表	55
3.8	磁盘 BIOS 参数块(BPB)	57
3.9	BIOS 编程举例	59
3.10	规格段问题	61
3.11	软盘故障处理	62
4	COM 文件和 EXE 文件	64
4.1	COM 文件	64
4.2	EXE 文件	66
4.2.1	EXE 文件的特点	66
4.2.2	EXE 文件标题格式	67
4.2.3	EXE 文件标准格式	69
4.2.4	如何阅读 EXE 文件	70
4.2.5	伪 EXE 文件	71
4.3	如何修改 EXE 文件	71
4.3.1	怎样修改 EXE 文件长度	72

4.3.2	编制、修改指令	76
4.3.3	修改、增加的指令如何写入 EXE 文件	78
4.3.4	检查工作	78
5	视频显示系统	80
5.1	视频显示系统概述	80
5.2	CGA 显示卡	82
5.2.1	显示缓冲区	82
5.2.1.1	字符方式的缓冲区	84
5.2.1.2	图形方式的缓冲区	85
5.2.1.3	隔行扫描对缓冲区的影响	86
5.2.2	μ C6845 控制芯片	86
5.2.3	CGA 卡工作原理	88
5.2.3.1	字符显示格式	88
5.2.3.2	图形显示格式	89
5.2.4	彩色控制原理	89
5.2.4.1	字符方式的颜色	89
5.2.4.2	图形方式的颜色	90
5.2.5	BIOS 功能	91
5.2.5.1	驱动程序结构	91
5.2.5.2	CGA 卡的工作单元	92
5.2.5.3	驱动程序模块功能	92
5.3	EGA/VGA 显示卡	93
5.3.1	寄存器种类和功能	93
5.3.1.1	外部寄存器	94
5.3.1.2	定序寄存器	94
5.3.1.3	CRT 控制寄存器	94
5.3.1.4	图形控制寄存器	95
5.3.1.5	属性控制寄存器	97
5.3.1.6	数据转换(DAC)寄存器(只 VGA 用)	98
5.3.2	驱动程序模块功能调用	99

5.3.2.1	EGA、VGA 增强功能重点介绍	100
5.3.2.2	VGA 增强的三个功能调用	103
5.3.3	显示字符串功能	105
5.3.4	EGA/VGA 数据区	105
5.3.4.1	INFO 数据意义	105
5.3.4.2	INFO-3 数据意义	105
5.3.4.3	FLAGS 数据意义	105
5.3.4.4	BIOS 保留区	106
5.4	屏幕开发	108
5.4.1	用户级屏幕开发	108
5.4.2	DOS 级屏幕开发	117
5.4.2.1	定义光标键	118
5.4.2.2	屏幕设计	118
5.4.2.3	编程设计	118
5.4.2.4	有关程序(汇编语言)	119
5.4.3	BIOS 级屏幕开发	121
5.4.3.1	高级语言方法	121
5.4.3.2	汇编语言方法	121
5.4.4	适配器级屏幕开发	123
6	键盘功能开发与应用	131
6.1	83 键键盘	131
6.1.1	83 键键盘组成	131
6.1.2	扫描码工作方式	132
6.1.2.1	扫描码	132
6.1.2.2	键盘码	133
6.1.2.3	扩展码	137
6.1.3	两次硬件中断方式	137
6.1.4	键盘输入中断处理程序 INT 9	138
6.1.4.1	INT 9 功能	138
6.1.4.2	INT 9 中断处理程序	138

6.1.4.3	常数表	140
6.1.4.4	八个控制功能键	140
6.1.4.5	编程技巧	141
6.1.5	键盘输出中断 INT 16	143
6.1.5.1	键盘输出中断意义	143
6.1.5.2	键盘输出中断 INT 16 的功能	143
6.1.5.3	键盘输出中断程序	144
6.1.5.4	INT 9 与 INT 16 的关系	144
6.1.5.5	键盘嵌入命令过程	145
6.1.6	键盘缓冲区	145
6.2	84 键键盘和 101 键键盘	146
6.2.1	101 键键盘与 83 键键盘的区别	146
6.2.2	8042 芯片功能简介	146
6.2.3	键盘控制原理	148
6.2.4	键盘控制器命令	150
6.2.5	键盘控制命令	152
6.2.6	由键盘发送的命令	153
6.2.7	编程举例	154
6.2.8	101 键键盘的中断处理程序	158
6.2.9	101 键键盘的组成及其使用方法	158
6.3	DOS 的键盘扩展功能	160
6.4	键盘功能范例一	161
6.5	键盘功能范例二	164
6.5.1	CCDOS 键盘输出中断 INT 16	164
6.5.2	键盘管理模块工作过程	165
6.5.3	键盘管理模块总框图	165
6.6	键盘开发工作概述	166
6.6.1	用户级的键盘开发	166
6.6.2	操作系统级开发键盘功能	167
6.6.3	BIOS 级开发键盘功能	168

6.6.4	非正常情况下的键盘开发	168
6.7	开发工具 JPXS.EXE	169
7	文件恢复	171
7.1	文件恢复命令	171
7.1.1	RECOVER 命令	171
7.1.2	CHKDSK 命令	173
7.2	恢复删除文件	175
7.3	恢复顺序文件	177
7.4	恢复伪顺序文件	178
7.5	介绍开发工具 REWJ.EXE	180
8	商品软件加密技术	181
8.1	商品软件加密原理	182
8.2	加密与解密的对抗发展	182
8.2.1	还原方式	183
8.2.2	消除软件保护功能	183
8.2.3	复制钥匙盘	183
8.3	商品软件加密方法	184
8.3.1	软加密方法	184
8.3.1.1	组合法	184
8.3.1.2	代替法	185
8.3.1.3	两个单词的后半部相互交换	185
8.3.1.4	压缩法	185
8.3.1.5	口令法	185
8.3.1.6	逻辑运算	186
8.3.1.7	函数法	186
8.3.1.8	DEU 8294A 芯片法	186
8.3.2	硬加密方法	187
8.3.2.1	多余磁道法	187
8.3.2.2	单独磁道法	187
8.3.2.3	多余扇区法	187

8.3.2.4	伪扇区技术	187
8.3.2.5	螺线磁道法	188
8.3.2.6	超级扇区法	188
8.3.2.7	扇区对齐法	188
8.3.2.8	宽磁道法	188
8.3.2.9	弱位技术	188
8.3.2.10	激光孔法	189
8.3.2.11	掩膜法	189
8.3.2.12	指纹法	189
8.3.2.13	特殊格式法	190
8.4	防跟踪技术	190
8.4.1	防阅读技术	190
8.4.2	多重循环技术	190
8.4.3	破坏单指令中断和断点中断	191
8.4.4	利用时钟中断	191
8.4.5	利用变形程序	191
8.4.6	重新设置屏幕特性	192
8.4.7	封锁键盘法	192
8.5	软件加密实例	192
8.5.1	BASICA 的 P 加密	192
8.5.2	PROLOK 中的一个加密算法	193
8.5.3	封锁键盘	194
8.6	一个加密软件的剖析	195
9	计算机病毒	206
9.1	计算机病毒概述	206
9.1.1	病毒类型	206
9.1.2	病毒特性	206
9.1.3	病毒的清除	208
9.1.4	病毒的预防	209
9.2	病毒举例——大麻病毒	210

9.2.1	大麻病毒结构	210
9.2.2	大麻病毒分析	213
9.3	病毒举例二——1575 病毒	216
9.3.1	1575 病毒结构	216
9.3.2	1575 病毒程序框图	217
9.3.2.1	主框图	217
9.3.2.2	激活病毒	218
9.3.2.3	表现部分	218
9.3.3	1575 病毒分析	222
9.4	如何正确使用消毒软件	224
9.5	提高自我保护能力	227
9.5.1	如何发现病毒	228
9.5.1.1	使用消毒软件查找病毒	228
9.5.1.2	开发人员检查病毒	228
9.5.2	如何不受病毒传染	229
9.6	如何编制消毒程序	230
9.6.1	分离病毒	230
9.6.2	编制消毒程序	231
10	维护开发工具	233
10.1	BTTYPE.EXE	233
10.2	BTDIR.EXE	234
10.3	BTCOMP.COM	236
10.4	BTEDLIN.COM	237
10.5	BTJCP.EXE	237
10.6	REWJ.EXE	240
10.7	BTDEBUG.COM	243
10.8	JPXS.EXE	246
10.9	PSP.EXE 和 PSP.COM	247
10.10	INT44B.EXE	248
10.11	BTDM.EXE	252

附录 A CGA 卡寄存器	256
A-1 μ C6845 芯片的内部寄存器	256
A-2 CGA 端口及有关寄存器	257
A-2-1 端口地址	257
A-2-2 方式控制寄存器	257
A-2-3 状态寄存器	258
A-2-4 彩色选择寄存器	259
附录 B EGA / VGA 卡寄存器	259
B-1 外部寄存器	259
B-1-1 混合输出寄存器	259
B-1-2 特征控制寄存器	260
B-1-3 输入状态寄存器 0	261
B-1-4 输入状态寄存器 1	261
B-1-5 视频系统使能寄存器(VGA)	261
B-2 定序寄存器	262
B-2-1 地址寄存器和数据寄存器	262
B-2-2 复位寄存器	262
B-2-3 时钟模式寄存器	263
B-2-4 映象屏蔽寄存器	263
B-2-5 字符映象选择寄存器	264
B-2-6 存储器模式寄存器	265
B-3 CRT 控制寄存器	265
B-3-1 CRT 控制寄存器功能	265
B-3-2 CRTC 寄存器的值	270
B-4 图形控制寄存器	271
B-5 属性控制寄存器	274
B-5-1 属性地址寄存器(端口 3COH)	274
B-5-2 调色板寄存器	274
B-5-3 属性模式控制寄存器(索引号为 10H)	275
B-5-4 过扫描彩色寄存器(EGA)	

调色板寄存器(VGA)(索引号为11H)	275
B-5-5 彩色平面使能寄存器(索引号为 12H)	276
B-5-6 水平像素卷动寄存器(索引号为 13H)	276
B-5-7 色彩选择寄存器(VGA)(索引号为 14H)	277
B-6 数据转换(DAC)寄存器(VGA)	277
附录 C EGA / VGA 卡功能调用	278
C-1 设置调色板寄存器子功能	278
C-2 字符发生器界面子功能	280
C-3 视频系统状态子功能	282
C-4 取 VIDEO BIOS 功能及状态信息	284
C-5 BIOS 保留区数据表	287

1 微机开发维护技术概论

1.1 微机开发技术及意义

在使用微机过程中，经常会遇到以下几方面的问题：

(1) 增加新功能。尽管微机在国民经济部门及生活领域中已得到广泛应用，它几乎可以完成人们所要求的各种工作，但对某台具体的微机来讲，常常不能满足人们的所有要求，迫切需要增加某种新功能。例如增加微机的汉字功能、计算结果分页打印功能、全屏幕编辑功能以及过程控制功能等。这些要求即使实现，今后人们还会不断提出新的要求，也需继续增加其他新的功能。

(2) 改进某种功能。在微机已有的功能中，有些还不能满足人们的要求，希望改进某种功能的事例仍然存在。例如汉字表格功能中字距与行距的可调性、汉字打印时字体的大小等，这些问题虽在微机排版系统中已初步得到解决，但其代价是字型库占用了大量的存贮资源，在用于工程计算和辅助设计的微机上还不能方便使用。

(3) 软件的修改或移值。微机的更新换代日益突出，最明显的是各种分辨率显示器的出现和使用，使许多过去的软件不能在 EGA 卡或 VGA 卡上使用，或者在这种机型上可以运行的软件不能在另一种机型上使用，因此需要对某些软件进行适当的修改和移值。

(4) 消除计算机病毒。目前我国已发现不少种类的计算机病毒，大部分微机都受到过病毒的侵蚀和危害。虽然人们已研制出不少解毒程序，但有时还不能完全消除所遇到的各种病毒，而且新的病毒仍在继续出现，所以消除计算机病毒和不断开发新的解毒软件也是经常遇到的任务之一。

(5) 处理计算机出现的各种问题。在使用计算机过程中，常会出现一些意想不到的事情，例如打印不出汉字、硬盘系统被冲