



普通高等教育“十一五”国家级规划教材



微机原理与接口技术

基于IA-32处理器和32位汇编语言
第4版

钱晓捷 主编
王义琴 范喆 张行进 马耀锋 参编

本书配有丰富的教学资源



机械工业出版社
China Machine Press

TP36/483

2008



普通高等教育“十一五”国家级规划教材

微机原理与接口技术

基于IA-32处理器和32位汇编语言

第4版

钱晓捷 主编

王义琴 范喆 张行进 马耀锋 参编



机械工业出版社
China Machine Press

本书以 32 位处理器、32 位汇编语言和 32 位个人微机系统为起点,从应用角度,采用循序渐进、深入浅出、突出实践的方法,展开论述了 IA-32 处理器的发展和微机组成、处理器编程结构、常用指令及其汇编语言程序设计(32 位 Windows 控制台环境和 16 位 DOS 环境)、存储系统、微机总线、输入输出接口及其应用技术,还特别介绍了高速缓冲存储器、指令流水线、多媒体指令、超标量、动态执行、多核等先进技术。

本书可以作为高等院校“微机原理及接口技术(微机原理及应用)”、“汇编语言程序设计”或“计算机组成原理”等课程的教材或参考书,适合计算机及电子、通信和自控等电类专业的本科学生、专科学生、高职学生及成教学生阅读,同时也适合作为计算机应用开发人员和希望深入学习微机应用技术的读者的极佳参考书。

版权所有,侵权必究。

本书法律顾问 北京市展达律师事务所

图书在版编目(CIP)数据

微机原理与接口技术:基于 IA-32 处理器和 32 位汇编语言 第 4 版/钱晓捷主编. —北京:机械工业出版社,2008.1

(普通高等教育“十一五”国家级规划教材)

ISBN 978-7-111-22926-1

I. 微… II. 钱… III. ①微型计算机—理论—高等学校—教材 ②微型计算机—接口—高等学校—教材 IV. TP36

中国版本图书馆 CIP 数据核字(2007)第 184138 号

机械工业出版社(北京市西城区百万庄大街 22 号 邮政编码 100037)

责任编辑:迟振春

北京京北制版厂印刷·新华书店北京发行所发行

2008 年 1 月第 1 版第 1 次印刷

184mm×260mm·23 印张

标准书号:ISBN 978-7-111-22926-1

定价:33.00 元

凡购本书,如有倒页、脱页、缺页,由本社发行部调换
本社购书热线:(010)68326294

前 言

本书编写完成后，掩卷而思，禁不住回忆其出版历程。

20 世纪 80 年代和 90 年代，国内“微机原理及应用”（或“微机原理及接口技术”）课程的教学内容以 8 位 Z80 微处理器和 TP801 单板机为主体。我们总结多年 16 位微机原理教学经验，整理教案，编写了以 16 位 Intel 8086/8088 微处理器和 IBM PC 系列机为主体的教材《微型计算机原理及接口技术》，并于 1999 年初出版。2001 年，加入汇编语言和 32 位微处理器内容的《16/32 位微机原理、汇编语言及接口技术》教材出版；2005 年，对其进行修订形成第 2 版。随着微型计算机技术的飞速发展，迫切需要将教学内容再次提升至以 32 位为主体。以《32 位微机原理、汇编语言及接口技术》为暂定书名，我们申报了普通高等教育“十一五”国家级规划教材，并获得批准。按照国家规划教材书目，本版教材定名为《微机原理与接口技术》。但作为我们编写的微机原理教材来说，这已经是第 4 个版本了。另外，为了体现以 32 位为主体的教学内容，我们使用了“基于 IA-32 处理器和 32 位汇编语言”的副书名。

本书以 IA-32 处理器和 32 位 PC 机为主体介绍 32 位微机原理、32 位汇编语言和接口应用技术。全书共分 10 章。

- 第 1 章“微型计算机系统概述”。本章通过微处理器的发展尤其是 Intel 80x86 系列处理器的发展引出各种基本概念，从冯·诺伊曼计算机结构引出微型计算机硬件组成，以 16 位和 32 位 PC 机为例全面理解微机层次结构，通过熟悉 Windows 控制台环境了解微机软件系统。
- 第 2 章“处理器结构”。本章以 8 位 CPU、16 位 8086、32 位 80386 和 Pentium 为例展开讲述处理器功能结构，重点学习 IA-32 处理器通用指令执行环境中的通用整数寄存器、存储器组织和数据寻址方式，并熟悉汇编语言的语句格式、程序框架和开发方法。
- 第 3 章“数据处理”。本章以数据在计算机中的表示介绍数制、数值编码和字符编码，以数据在汇编语言中的表达熟悉常量定义、变量应用以及常用伪指令，以数据在处理器中的处理展开论述 IA-32 处理器数据传送和算术逻辑运算等基本指令，并通过示例程序掌握指令功能和编程应用。
- 第 4 章“汇编语言程序设计”。本章以程序结构为主线，先介绍基本的控制转移指令，然后引出分支程序结构、循环程序结构和子程序结构，同时结合数码转换、字符串处理、键盘输入和显示输出等大量示例程序，掌握汇编语言程序设计方法。最后，介绍汇编语言在编写 32 位 Windows 程序以及 C++ 混合编程方面的应用。
- 第 5 章“微机总线”。本章展开微机总线结构，介绍总线类型、数据传输、信号时序等总线基本技术，以 16 位 8086 和 32 位 Pentium 为例学习处理器引脚信号和操作时序，以 16 位 ISA、32 位 PCI 和 USB 总线为例学习系统总线和外设总线。
- 第 6 章“存储系统”。本章以存储层次结构中的主存储器、高速缓冲存储器为主体，学习各种半导体存储器的类型、特点、地址译码，介绍 Cache 的工作原理和组成结构。最后，说明 IA-32 处理器支持操作系统进行存储管理的分段和分页机制。

- 第7章“输入输出接口”。本章在熟悉 I/O 接口的特点、编址和指令的基础上，结合 I/O 接口电路展开论述微机与外设进行无条件传送、查询传送、中断传送和 DMA 传送的原理，并详细介绍处理器的中断机制和编程方法。本章还引出了使用汇编语言编写 16 位 DOS 应用程序的方法。
- 第8章“常用接口技术”。本章综合已学知识，以应用为目的，熟悉定时控制、并行接口、串行通信和模拟系统的基本原理，掌握扬声器控制、打印机连接、键盘输入、数码管显示、异步串行通信和模拟系统的常用接口技术。
- 第9章“处理器性能提高技术”。本章以 IA-32 处理器为例介绍高性能处理器运用的各种先进技术，涉及精简指令集计算机思想、指令流水线技术、浮点数据的编码格式及处理指令、多媒体指令及其特点。
- 第10章“并行处理技术”。本章展开论述利用并行性进一步提高处理器性能的各种处理技术，重点说明了 IA-32 和 Intel 64 处理器所运用的超标量技术、动态执行技术、多线程技术、多核技术的含义和特点。

本书遵循我国“计算机科学与技术本科专业规范”等指导性文件，结合广大师生的反馈和我们的教学实践，删除了陈旧内容，精练了许多知识，实现了以 32 位为主体的教学思想，同时也在编排体例等多方面进行了改进。与同类教材相比，本书具有以下特色。

1. 更新教学内容，体现 32 位主体

本书不是将 32 位内容作为 16 位内容的补充，安排在各个章节最后或全书最后；而是直接以 32 位教学内容为起点，硬件上以 IA-32 处理器和 32 位 PC 机为主体介绍工作原理，软件上以 32 位指令系统展开讲述 Windows 控制台环境的汇编语言编程。教材内容不仅摒弃了陈旧的 8 位和 16 位技术，而且还引出最新的 32 位和 64 位技术。例如，汇编语言的 32 位 Windows 编程、与 Visual C++ 的混合编程，存储系统的 Cache、存储管理，指令集结构的精简指令集计算机思想、浮点指令和多媒体指令，以及系统结构的指令流水线、超标量、动态执行、多线程、多核等技术。

2. 强调工作原理，淡化技术细节

微型计算机技术的突出特点是教学内容虽不深奥但较琐碎，既有共性的工作原理又有具体应用的技术方法。本书在编著过程中，强调基本概念和工作原理，不过多表述实现细节。例如，本教材以 IA-32 处理器为例融合 8 位、16 位和 32 位微机工作原理，而不是仅引出某个处理器的所有技术；选择 32 位基本指令进行重点学习而不是所有指令泛泛而谈；抓住处理器和总线的关键信号，没有详细展开所有引脚功能；重点说明存储器地址译码原理，不分析存储器芯片的连接细节；从应用角度解释系统结构特点，不以设计者观点论述技术实现。

3. 化解汇编难点，突出应用价值

汇编语言编程是本课程的一个难点，因为其指令繁多、规则凌乱，又涉及底层硬件原理。传统的教学顺序是：先数据编码、后指令系统、接着伪指令、最后展开程序设计，即在积累了大量指令和规则后才引出程序，往往又没有输入输出交互，编出的程序不知对错。本教材从第 1 章就引出汇编语言的软件开发环境。第 2 章介绍汇编语言的语句格式、源程序框架和开发方法，并利用简单易用的输入输出子程序编写具有显示结果的程序。第 3 章结合数据编码、常量定义和变量应用，自然地引出常用伪指令；然后通过阅读源程序、掌握常用处理器指令，逐渐编写特定要求的程序片段。第 4 章以程序结构为主线，从简单到复杂逐步编

写具有实用价值的应用程序,最后展开讲述 Windows 编程和混合编程。后续章节结合 I/O 接口技术,介绍 I/O 指令和 I/O 程序、中断服务程序以及扬声器控制、键盘扫描码读取、异步串行通信程序,将上机实践贯穿始终,通过汇编语言程序更好地理解硬件工作原理。

4. 面向普通学生,降低入门要求

本书充分考虑到普通院校本、专科学生以及自学人员的实际知识水平,以清晰的逻辑结构由浅入深展开教学内容;尽量使用浅显生动的语言,不惜笔墨详尽讲解重点和难点知识。本书只要求读者具有计算机(文化)基础和高级语言的入门知识,掌握微机操作,不要求读者熟悉数字电路、计算机组成原理等先修内容。例如,本教材介绍了基本逻辑运算、门电路、锁存器、三态缓冲器和译码器等涉及硬件的知识,还补充有 Windows 控制台(及模拟 MS-DOS)环境的操作、MASM 6.15 命令行开发方法等软件方面的内容。再如,本教材详细介绍了开发软件包的构成,精选了大量示例程序,并提供了作者编写的键盘输入和显示输出 I/O 子程序库,读者完全可以依据教材所述自主完成各个程序。另外,课程虽然涉及硬件接口,但本教材设计有在 PC 机上实现的实践环节,所以可以不用配置硬件实验平台而开设本课程(当然,如果能够结合硬件实验平台,效果会更加理想)。还有,每章最后都有总结,帮助读者领悟重点知识,并配合大量习题巩固所学。

5. 开办教学网站,提供辅助资源

本书努力从结构组织、内容编排和上机实践等多方面避免同类教材的不足,努力做到结构新颖、内容充实、知识先进,让广大读者有所收获,掌握一些实实在在的东西。为了更好地服务于广大师生和读者,编者开辟了“大学微机技术系列课程教学辅助网站”(http://www2.zzu.edu.cn/qfw)。该网站面向“微机原理及接口技术”和“汇编语言程序设计”课程,提供相关教学课件(电子教案)、教学大纲、教材勘误、疑难解答、输入输出子程序库、示例源程序文件等辅助资源,是本教材的动态延伸,欢迎大家访问。有关教材的疏漏和不当以及对相关教学问题的探讨,敬请广大师生和读者通过电子邮件(qianxiaojie@zzu.edu.cn)与编者交流。你们的支持是提高教材质量、催生新版教材的最大动力,也是对编者的最大鼓励。

钱晓捷主持本版教材的编写工作,并编写了第 1、3、4、7~10 章和附录,王义琴编写了第 5 章,范喆编写了第 6 章,张行进编写了第 2 章,马耀锋参与了前 3 章部分章节的编写。全书最后由钱晓捷统稿、配置编程开发环境、编写输入输出子程序库和验证示例程序。本书的编写还得到了陈涛、穆玲玲、关国利、张青、姚俊婷等人的帮助,衷心感谢他们,同时也感谢机械工业出版社华章公司的大力支持。

编 者

2007 年 10 月

目 录

前言

第 1 章 微型计算机系统概述	1	2.5 数据寻址方式	53
1.1 微型计算机的发展	1	2.5.1 立即数寻址方式	53
1.1.1 通用微处理器	1	2.5.2 寄存器寻址方式	54
1.1.2 专用微处理器	2	2.5.3 存储器寻址方式	54
1.1.3 摩尔定律	3	2.5.4 各种数据寻址方式总结	57
1.2 Intel 80x86 系列处理器	4	第 2 章总结	59
1.2.1 16 位 80x86 处理器	4	第 2 章习题	60
1.2.2 IA-32 处理器	5	第 3 章 数据处理	62
1.2.3 Intel 64 处理器	8	3.1 数据表示	62
1.3 微型计算机的系统组成	10	3.1.1 数制	62
1.3.1 冯·诺伊曼计算机结构	10	3.1.2 数值的编码	65
1.3.2 微型计算机的硬件系统	12	3.1.3 字符的编码	67
1.3.3 PC 微机结构	14	3.2 常量表达	69
1.3.4 计算机系统的层次结构	17	3.3 变量应用	71
1.3.5 微型计算机的软件系统	21	3.3.1 变量定义	71
第 1 章总结	24	3.3.2 变量属性	75
第 1 章习题	24	3.4 数据传送类指令	77
第 2 章 处理器结构	26	3.4.1 通用数据传送指令	77
2.1 处理器的功能结构	26	3.4.2 堆栈操作指令	79
2.1.1 处理器的基本结构	26	3.4.3 其他传送指令	82
2.1.2 8086 的功能结构	27	3.5 算术运算类指令	84
2.1.3 80386 的功能结构	29	3.5.1 加法指令	84
2.1.4 Pentium 的功能结构	30	3.5.2 减法指令	85
2.2 寄存器	31	3.5.3 乘除法指令	87
2.2.1 通用寄存器	32	3.6 位操作类指令	89
2.2.2 标志寄存器	33	3.6.1 逻辑运算指令	89
2.2.3 专用寄存器	36	3.6.2 移位指令	93
2.3 存储器组织	37	3.7 串操作类指令	96
2.3.1 存储模型	38	3.7.1 串传送指令	96
2.3.2 工作方式	38	3.7.2 串检测指令	98
2.3.3 逻辑地址	39	3.8 IA-32 指令系统	99
2.4 汇编语言基础	42	第 3 章总结	100
2.4.1 指令代码格式	42	第 3 章习题	101
2.4.2 语句格式	43	第 4 章 汇编语言程序设计	107
2.4.3 源程序框架	45	4.1 分支程序结构	107
2.4.4 开发过程	49	4.1.1 无条件转移指令	107
		4.1.2 条件转移指令	110
		4.1.3 单分支程序结构	114

4.1.4 双分支程序结构	115	第6章 存储系统	183
4.2 循环程序结构	117	6.1 存储系统的层次结构	183
4.2.1 循环指令	118	6.1.1 技术指标	183
4.2.2 计数控制循环	119	6.1.2 层次结构	183
4.2.3 条件控制循环	120	6.1.3 局部性原理	185
4.3 子程序结构	122	6.2 主存储器	186
4.3.1 子程序指令	122	6.2.1 读写存储器	186
4.3.2 子程序设计	124	6.2.2 只读存储器	190
4.3.3 参数传递	126	6.2.3 存储器地址译码	193
4.3.4 程序模块	133	6.2.4 主存空间分配	198
4.4 Windows 应用程序编程	137	6.3 高速缓冲存储器	201
4.4.1 操作系统函数调用	137	6.3.1 工作原理	201
4.4.2 控制台应用程序	140	6.3.2 地址映射	204
4.4.3 图形窗口应用程序	145	6.3.3 替换算法	207
4.5 与 C++ 语言混合编程	146	6.3.4 写入策略	208
4.5.1 嵌入汇编	146	6.3.5 80486 的 L1 Cache	210
4.5.2 模块连接	147	6.3.6 Pentium 的 L1 Cache	211
第4章总结	150	6.4 存储管理	212
第4章习题	151	6.4.1 段式存储管理	212
第5章 微机总线	154	6.4.2 页式存储管理	214
5.1 总线技术	154	第6章总结	217
5.1.1 总线类型	154	第6章习题	218
5.1.2 总线的数据传输	155	第7章 输入输出接口	221
5.1.3 总线信号和总线时序	158	7.1 I/O 接口概述	221
5.2 8086 的引脚信号	160	7.1.1 I/O 接口的典型结构	221
5.2.1 地址/数据信号	160	7.1.2 I/O 端口的编址	223
5.2.2 读写控制信号	161	7.1.3 输入输出指令	225
5.2.3 其他控制信号	162	7.1.4 16 位 DOS 应用程序	226
5.3 8086 的总线时序	163	7.2 无条件传送和查询传送	230
5.3.1 写总线周期	163	7.2.1 无条件传送	230
5.3.2 读总线周期	165	7.2.2 查询传送	233
5.4 Pentium 处理器的引脚和时序	166	7.3 中断控制系统	235
5.4.1 引脚定义	166	7.3.1 中断传送	235
5.4.2 总线周期	168	7.3.2 IA-32 中断系统	238
5.5 微机系统总线	169	7.3.3 内部中断服务程序	241
5.5.1 PC 机总线的发展	169	7.3.4 中断控制器	243
5.5.2 ISA 总线	170	7.3.5 外部中断服务程序	246
5.5.3 PCI 总线	173	7.3.6 驻留中断服务程序	249
5.5.4 USB 总线	177	7.4 DMA 传送	250
第5章总结	179	7.4.1 DMA 传送过程	250
第5章习题	180	7.4.2 DMA 控制器	252
		第7章总结	252
		第7章习题	253

第 8 章 常用接口技术	256	9.4.1 MMX 技术	326
8.1 定时控制接口	256	9.4.2 SSE 技术	328
8.1.1 8253/8254 定时器	256	9.4.3 SSE2 技术	330
8.1.2 定时器的应用	262	9.4.4 SSE3 技术	331
8.2 并行接口	264	第 9 章总结	332
8.2.1 并行接口电路 8255	264	第 9 章习题	333
8.2.2 并行接口的应用	270	第 10 章 并行处理技术	335
8.2.3 键盘及其接口	273	10.1 超标量技术	335
8.2.4 数码管及其接口	280	10.1.1 并行性概念	335
8.3 异步串行通信接口	283	10.1.2 Pentium 的超标量指令 流水线	336
8.3.1 异步串行通信格式	284	10.1.3 Pentium 的动态分支预测	337
8.3.2 异步串行接口标准	285	10.2 动态执行技术	338
8.3.3 异步串行通信程序	287	10.2.1 指令级并行	339
8.4 模拟接口	294	10.2.2 P6 微结构	341
8.4.1 模拟输入输出系统	294	10.3 同时多线程技术	343
8.4.2 D/A 转换器	295	10.3.1 Pentium 4 的 NetBurst 微结构	343
8.4.3 A/D 转换器	299	10.3.2 Pentium 4 的超线程技术	344
第 8 章总结	304	10.4 Intel 64 技术	345
第 8 章习题	304	10.4.1 64 位方式的运行环境	346
第 9 章 处理器性能提高技术	309	10.4.2 64 位方式的指令	347
9.1 精简指令集计算机技术	309	10.5 多核技术	348
9.1.1 复杂指令集和精简指令集	309	10.5.1 并行计算机结构分类	349
9.1.2 RISC 技术的主要特点	310	10.5.2 Intel Core 微结构	349
9.2 指令流水线技术	311	10.5.3 Intel 多核技术	349
9.2.1 指令流水线概述	311	第 10 章总结	351
9.2.2 80486 的指令流水线	314	第 10 章习题	351
9.3 浮点数据处理单元	315	附录 输入输出子程序库	354
9.3.1 实数编码	316	参考文献	357
9.3.2 浮点寄存器	319		
9.3.3 浮点指令及其编程	322		
9.4 多媒体指令	325		

第1章 微型计算机系统概述

数字电子计算机经历了电子管、晶体管、集成电路为主要部件的时代。随着大规模集成电路的应用,计算机的功能越来越强大,体积却越来越小,微型计算机(简称微型机或微机)应运而生,并得到广泛应用。本章以 Intel 80x86 处理器和个人微机为例,介绍微型计算机系统的发展和组成,为后续章节介绍微型计算机系统的各个组成部分奠定基础。

1.1 微型计算机的发展

在巨型机、大型机、小型机和微型机等各类计算机中,微型机(Microcomputer)是性能适中、价格低廉、体积较小的一类。在科学计算、信息管理、自动控制、人工智能等应用领域中,微型机也是最常见的一类。工作、学习和娱乐中使用的桌面个人微机是我们最熟悉也是最典型的微型机系统;支撑网络的文件服务器、WWW 服务器等各类服务器属于高档微型机系统;生产、生活中运用的各种智能化电子设备从计算机系统的角度看同样也是微型机系统,只不过作为其控制核心的处理器常被封装在电子设备内部,不易被人觉察,因此常称它们为嵌入式计算机系统。桌面系统、服务器和嵌入式计算构成现代计算机的三大主要应用形式,而微型机都是其中的主角。

计算机的运算和控制核心称为处理器(Processor),即中央处理单元(Central Processing Unit, CPU)。微型机中的处理器常采用一块大规模集成电路芯片,称之为微处理器(Microprocessor),它代表着整个微型机系统的性能。通常将采用微处理器为核心构造的计算机称为微型计算机。

处理器的性能用字长、时钟频率、集成度等基本的技术参数来衡量。字长(Word Length)表明处理器每个时间单位可以处理的二进制数据位数,如一次运算、传输的位数。时钟频率表明处理器的处理速度,反映了处理器的基本时间单位。集成度表明处理器的生产工艺水平,通常用芯片上集成的晶体管数量来表达。晶体管只是一个由电子信号控制的电子开关,集成电路在一个芯片上组合了成千上万个晶体管完成特定功能。

1.1.1 通用微处理器

1971 年,美国 Intel(英特尔)公司为日本制造商设计可编程计算器时,将采用多个专用芯片的方案修改成一个通用处理器,于是诞生了世界上第一个微处理器 Intel 4004。Intel 4004 微处理器字长为 4 位,集成了约 2300 个晶体管,时钟频率为 108kHz(赫兹)。以它为核心组成的 MCS-4 计算机也就是世界上第一台微型计算机。随后,Intel 4004 被改进为 Intel 4040。

1972 年,Intel 公司研制出 8 位字长的微处理器芯片 8008,其时钟频率为 500kHz,集成了约 3500 个晶体管。这之后的几年当中,微处理器开始走向成熟,出现了以 Motorola 公司 M6800、Zilog 公司 Z80 和 Intel 公司 8080/8085 为代表的中、高档 8 位微处理器。Apple 公司

的苹果机就是这一时期著名的个人微型机。

1978 年开始, 各公司相继推出一批 16 位字长的微处理器, 如 Intel 公司的 8086 和 8088、Motorola 公司的 M68000、Zilog 公司的 Z8000 等。例如, Intel 8086 的时钟频率为 5MHz, 集成度达到 2.9 万个晶体管。这一时期的著名微机产品是 IBM 公司采用 Intel 公司的微处理器和 Microsoft(微软)公司的操作系统开发的 16 位个人计算机(Personal Computer, PC)。

1985 年, Intel 公司借助 IBM PC 的巨大成功, 进一步推出了 32 位微处理器 80386, 其集成度达到 27.5 万个晶体管, 时钟频率达 16MHz。从这时起, 微处理器步入快速发展阶段。就 Intel 公司来说, 就陆续研制生产了 80486、Pentium(奔腾)、Pentium Pro(高能奔腾)、MMX Pentium(多能奔腾)、Pentium II、Pentium III 和 Pentium 4 等微处理器。例如, 2003 年 Intel 公司生产的新一代 Pentium 4 处理器具有 1.25 亿个晶体管, 时钟频率达到 3.4GHz。兼容 IBM PC 机的 32 位 PC 机, 还有 Apple 公司的 Macintosh 机等, 在这个时期得到飞速发展, 伴随着多媒体技术和互联网络, 成为我们工作和生活不可缺少的一部分。

2000 年, Intel 公司在微型机的高端产品服务器中使用了 64 位字长的新一代微处理器 Itanium(安腾)。事实上, 其他公司的 64 位微处理器在 20 世纪 90 年代已经出现, 但也是主要应用于服务器产品中, 不能与通用 80x86 微处理器兼容。2003 年 4 月, AMD 公司推出首款兼容 32 位 80x86 结构的 64 位微处理器, 被称为 x86-64 结构。2004 年 3 月, Intel 公司也发布了首款扩展 64 位能力的 32 位微处理器, 它采用扩展 64 位主存技术 EM64T(Extended Memory 64 Technology)。64 位微处理器主要将整数运算和主存寻址能力扩大到 64 位, 极大地提高了微型机的处理能力。2005 年以后, 采用 64 位技术的桌面微机逐渐获得用户青睐。与此同时, 生产厂商已经可以在一个半导体芯片上制作两个微处理器核心, 原来面向高端的并行处理器技术开始走向桌面系统, 微型计算机系统也进入了一个全新的多核处理器阶段。

1.1.2 专用微处理器

除了装在 PC、笔记本电脑、工作站、服务器上的通用微处理器(常简称为 MPU)外, 还有其他应用领域的专用微处理器: 单片机(微控制器)和数字信号处理器。

单片机(Single Chip Microcomputer)是指通常用于控制领域的微处理器芯片, 其内部除 CPU 外还集成了计算机的其他一些主要部件, 例如, ROM 和 RAM、定时器、并行接口、串行接口, 有的芯片还集成了 A/D、D/A 转换电路等。换句话说, 一个芯片几乎就是一个计算机, 只要配上少量的外部电路和设备, 就可以构成具体的应用系统。

单片机是国内习惯的名称, 国际上多称为微控制器(Micro Controller)或嵌入式控制器(Embedded Controller), 简称为 MCU。微控制器的初期阶段(1976~1978 年)以 Intel 公司的 8 位 MCS-48 系列为代表。1978 年以后, 微控制器进入普及阶段, 以 8 位为主, 最著名的是 Intel 公司的 8 位 MCS-51 系列, 还有 Atmel(爱特梅尔)公司的 AT89 系列(与 MCS-51 兼容)、Microchip Technology 公司的 PIC 系列。1982 年以后, 出现了高性能的 16 位、32 位微控制器, 例如, Intel 公司的 MCS-96/98 系列、Atmel 公司的 AT91 系列(基于 ARM 内核)。

数字信号处理器(Digital Signal Processor), 简称 DSP 芯片, 实际上也是一种微控制器(单片机), 但更专注于数字信号的高速处理, 其内部集成有高速乘法器, 能够进行快速乘法和加法运算。DSP 芯片自 1979 年 Intel 公司开发 2920 以后也经历了多代发展, 其中美国德州仪器(Texas Instruments, TI)公司的 TMS320 各代产品具有代表性, 例如, 1982 年的 TMS32010、

1985 年的 TMS320C20、1987 年的 TMS320C30、1991 年的 TMS320C40，还有 TMS320C2000、TMS320C5000、TMS320C6000 系列等。DSP 芯片市场主要分布在通信、消费类电子产品和计算机领域。我国推广和应用较多的是 TI 公司、AD 公司和 Motorola 公司的 DSP 芯片。

利用微控制器、数字信号处理器或通用微处理器，结合具体应用就可以构成一个控制系统，例如，当前的主要应用形式是嵌入式系统。嵌入式系统融合了计算机软硬件技术、通信技术和半导体微电子技术，把计算机直接嵌入到应用系统之中，构造信息技术 (Information Technology, IT) 的最终产品。嵌入式系统有三个级别的体系结构。

- IP (Intellectual Property, 知识产权) 级结构。也就是片上系统 (System on Chip, SoC) 形式。它把不同的 IP 单元，根据应用的要求集成在一个芯片上，各种嵌入式软件也能以 IP 方式集成在芯片中。
- 芯片级结构。这是目前最常见的嵌入式系统形式。它根据各种 IT 产品的要求，选用相应的处理器芯片 (MCU、DSP、MPU 等)、RAM 和 ROM 以及 I/O 接口芯片等组成相应的嵌入式系统，相应的系统软件和应用软件也固化在 ROM 中。
- 模块级结构。以 80x86 微处理器构成的计算机模块嵌入到应用系统中。

自从 20 世纪 70 年代微处理器产生以来，它就一直沿着通用 CPU、微控制器和 DSP 芯片三个方向发展。这三类微处理器的基本工作原理一样，但各有其特点，技术上它们不断地相互借鉴和交融，应用上却大不相同。本书以通用微处理器 Intel 80x86 和由其构成的 PC 微机为蓝本展开教学，但基本原理也适用于其他微处理器应用系统，可以认为是其他微处理器的一个基础知识。学习微控制器和 DSP 芯片构成的专用应用系统需要另外的课程和教材。

1.1.3 摩尔定律

从利用算盘实现机械式计算到电子计算机出现，这期间经历了千年历史。但从 1946 年第一台通用电子数字计算机 ENIAC (Electronics Numerical Integrator And Calculator) 开始到现在计算机广泛应用的信息时代，却只有短短的几十年时间。大规模集成电路生产技术的不断提高推动了计算机的飞速发展。摩尔定律 (Moore's Law) 很好地说明了这个现象。

1965 年，Intel 公司的创始人之一摩尔 (G. Moore) 预言：集成电路上的晶体管密度每年将翻倍。现在，这个预言通常被表达为：每隔 18 个月硅片密度 (晶体管容量) 将翻倍；也常被表达为：每 18 个月，集成电路的性能将提高一倍，而其价格将降低一半。这个预言就是所谓的摩尔定律。摩尔预计这个规律将持续 10 年，而事实上这个规律已经持续了 40 年，并将继续维持 5 年或 10 年。

伴随着摩尔定律，我们看到原来封闭在机房的庞大计算机系统已经走入普通家庭，成为日常使用的桌面微机。事实上，以微处理器为基础的计算机在整个计算机设计领域占据了统治地位。工作站和 PC 成为计算机工业的主要产品，使用微处理器的服务器取代了传统的小型机，大型机则几乎都由流行的微处理器组成的多处理器系统取代，甚至高端的巨型机也采用微处理器。更不用说无处不在的嵌入式计算机正改变着我们应用计算机的方式。也正因为如此，为了方便论述，在不会引起歧义的情况下，本书将使用术语“处理器”表示“微处理器”。

但是，摩尔定律不会永远持续，电子器件的物理极限在悄然逼近。20 世纪 80 年代中期以前，微处理器的性能提高主要是工艺技术驱动。此后，微处理器的性能提高更多地得益于

计算机系统结构的革新。从通用寄存器结构、精简指令集计算机 RISC、高速缓冲存储器 Cache、虚拟存储器管理,到指令级并行、线程级并行、单芯片多核心等并行技术,先进的系统结构已经成为提高微处理器性能的主要推动力。本书将以 Intel 80x86 系列微处理器为例,向读者介绍这些激动人心的技术。

1.2 Intel 80x86 系列处理器

美国 Intel 公司是目前世界上最有影响的处理器生产厂家,也是世界上第一个处理器芯片的生产厂家,其生产的 80x86 系列处理器一直是个人微机的主流处理器,该系列处理器的发展就是微型计算机发展的一个缩影。

1.2.1 16 位 80x86 处理器

1971 年,Intel 公司生产的 4 位处理器芯片 4004 宣告了微型计算机时代的到来。1972 年,Intel 公司开发了 8 位处理器 8008 芯片;1974 年,生产了 Intel 8080;1977 年,Intel 公司将 8080 及其支持电路集成在一块集成电路芯片上,形成了性能更高的 8 位处理器 8085。从 1978 年开始,Intel 公司在其 8 位处理器基础上,陆续推出了 16 位结构的 8086、8088 和 80286(也可以表示成 Intel 286,本书采用 80286 这种形式)等处理器,它们在 IBM PC 系列机中获得广泛应用,被称为 16 位 80x86 处理器。

1. 8086

1978 年,Intel 公司推出 16 位 8086 处理器,这是该公司生产的第一个 16 位芯片。8086 的数据总线为 16 位,地址总线为 20 位,主存容量为 1MB,时钟频率为 5MHz。8086 支持的所有指令,即指令系统(Instruction Set)成为整个 Intel 80x86 系列处理器的 16 位基本指令集。

为了方便与当时的 8 位外部设备连接,1979 年,Intel 公司推出准 16 位处理器 8088。8088 只是将外部数据总线设计为 8 位,内部仍保持 16 位结构,指令系统等都与 8086 相同。随后的 80186 和 80188 则分别是以 8086 和 8088 为核心并配以支持电路构成的芯片,但它们在 8086 指令系统的基础上增加了若干条实用指令,涉及堆栈、输入输出、移位、乘法、支持高级语言等操作。

处理器芯片的对外引脚(Pin)用于与其他电路进行连接,以构成微型计算机。处理器引脚也常称为处理器总线(Bus),主要由三组信号总线组成:数据总线(Data Bus, DB)、地址总线(Address Bus, AB)和控制总线(Control Bus, CB)。

数据总线是处理器与存储器或外设交换信息的通道,其个数(条数)就是一次能够传送数据的二进制位数,通常等于处理器字长。

地址总线用于指定存储器或外设的具体单元,其个数反映处理器能够访问的主存储器容量或外设范围。由于每个信号只能为高或低电平两种状态,对应 1 或 0 两种编码,所以对于 20 位地址信号线的 8086 来说,最多能够组合 2^{20} 个状态(编码)。每个编码就是一个地址,每个地址指示一个存储单元或 I/O 端口,其中包含一个字节(Byte)数据。这样,8086 的主存容量为 $2^{20} \text{B} = 1024 \times 1024 \text{B} = 1024 \text{KB} = 1 \text{MB}$,这里 $1 \text{KB} = 2^{10} \text{B} = 1024 \text{B}$ 。

控制总线用于控制处理器数据传送等操作,例如,存储器读信号(MEMR)有效说明处理器正在从存储器中读取信息,还有存储器写(MEMW)、外设读(IOR)、外设写(IOW)等信号。

2. 80286

1982年, Intel公司推出仍为16位结构的80286处理器, 但地址总线扩展为24位, 即主存储器具有16MB容量。80286设计了与8086工作方式一样的实方式(Real Mode), 还新增了保护方式(Protected Mode)。在实方式下, 80286相当于一个快速8086。在保护方式下, 80286提供了存储管理、保护机制和多任务管理的硬件支持。这些传统上由操作系统实现的功能在处理器硬件支持下, 使微机系统的性能得到极大提高。

1. 2. 2 IA-32 处理器

IBM PC系列机的广泛应用推动了处理器芯片的生产。Intel公司在推出32位结构的80386处理器后, 确定80386芯片的指令集结构(Instruction Set Architecture, ISA)为以后开发的80x86系列处理器的标准, 称为Intel 32位结构(Intel Architecture-32, IA-32)。现在, Intel公司的80386、80486以及Pentium各代处理器统称为IA-32处理器或32位80x86处理器。

1. 80386

1985年, Intel 80x86微处理器进入第三代80386。80386处理器采用32位结构, 数据总线为32位, 地址总线也是32位, 可寻址4GB($1\text{GB} = 2^{30}\text{B} = 1024\text{MB}$)主存, 时钟频率有16、25和33MHz。IA-32指令系统在兼容原16位80286指令系统的基础上, 全面升级为32位, 还新增了有关位操作、条件设置等指令。

80386除保持与80286兼容外, 又提供了虚拟8086工作方式(Virtual 8086 Mode)。虚拟8086方式是在保护方式下的一种特殊状态, 类似于8086工作方式但又接受保护方式的管理, 能够模拟多个8086处理器。32位PC的Windows操作系统采用保护方式, 其MS-DOS命令行(环境)就是虚拟8086方式, 而早期采用的DOS操作系统是以实方式为基础建立的。

为了适应便携机的要求, Intel公司在1990年生产的低功耗节能型芯片中, 增加了一种新的工作状态: 系统管理方式(System Management Mode, SMM)。它是指当处理器进入这种工作状态后, 处理器会根据当时不同的使用环境, 自动减速运行, 甚至停止运行。这时处理器还可以控制其他部件停止工作, 从而使微机的整体耗电降到最少。

2. 80486

1989年, Intel公司推出80486处理器。它的内部集成了120万个晶体管, 最初的时钟频率为25MHz, 但很快发展到33MHz和50MHz。从结构上来说, $80486 = 80386 + 80387 + 8\text{KB Cache}$, 即80486把80386处理器与80387数学协处理器和8KB高速缓冲存储器(Cache)集成在一个芯片上, 使处理器的性能大大提高。

传统上, 中央处理单元CPU主要是整数处理器。为了协助处理器处理浮点数据(实数), Intel公司设计了数学协处理器, 后被称为浮点处理单元(Floating-point Processing Unit, FPU)。配合8086和8088整数处理器的数学协处理器是8087, 配合80286的是80287, 配合80386的是80387。而从80486开始, FPU已经被集成到处理器中。这样, IA-32处理器能够直接支持浮点数据的操作指令。

高速缓冲存储器是处理器与主存之间速度很快但容量较小的存储器, 可以有效地提高整个存储器系统的存取速度。80486不仅在芯片内部集成有8KB第一级高速缓存(L1 Cache), 而且支持外部第二级高速缓存(L2 Cache)。

Intel 80x86 系列处理器是传统的复杂指令集计算机 (Complex Instruction Set Computer, CISC), 它采用大量的、复杂的但功能强大的指令来提高性能。复杂指令一方面提高了处理器性能, 另一方面却为进一步提高性能带来了麻烦。所以, 人们又转而设计主要由简单指令组成的处理器, 以期在新的技术条件下生产更高性能的处理器, 这就是精简指令集计算机 (Reduced Instruction Set Computer, RISC)。80486 及以后的 IA-32 处理器吸取 RISC 技术特长并将其融入 CISC 中, 同时采用流水线方式的指令重叠执行方法, 使 80486 可以在一个时钟周期执行完一条简单指令。指令流水线技术是将指令的执行划分成多个步骤, 在多个部件中独立地进行, 这样使得多条指令可以在不同的执行阶段同时进行, 就像工厂中的产品流水线一样。

80486 DX4 综合了此前所使用的所有技术, 是 80486 处理器中最快的一种芯片。它采用时钟倍频 (Clock Doubling) 思想, 将外部时钟频率 25MHz 或 33MHz 提高 3 倍作为内部工作时钟频率, 形成 75MHz 或 100MHz 两款产品。以前的微机系统中, 处理器的内部时钟频率和外部时钟频率是一样的, 也是处理器与外围部件的数据传输频率。处理器的时钟频率提高了, 系统的运行速度当然也就提高了。但是, 当外部数据传输频率太高时, 会给外围部件、主板等设计带来困难。为了既能尽量提高处理器的时钟频率以增强性能, 又能迁就较慢速的外围部件, 使高频率的处理器照样能够使用, Intel 公司使用了这种时钟倍频技术。

3. Pentium

Pentium 芯片即俗称的 80586 处理器, 因为数字很难进行商标版权保护的缘故而特意取名。其实, Pentium 是源于希腊文“pente”(数字 5), 再加上后缀-ium(化学元素周期表中命名元素常用的后缀)变化而来的。同时, Intel 公司为其取了一个响亮的中文名称“奔腾”, 并进行了商标注册。

Intel 公司于 1993 年制造成功 Pentium。其内部时钟频率有 120、133、166 和 200MHz 等多款, 外部频率主要是 60MHz 和 66MHz。Pentium 虽然仍属于 32 位结构, 但其与主存连接的外部数据总线却是 64 位的, 这样大大提高了存取主存的速度。

Pentium 引入了超标量 (Superscalar) 技术, 内部具有可以并行工作的两条整数处理流水线, 可以达到每个时钟周期执行两条指令。Pentium 还将 L1 Cache 分成两个彼此独立的 8KB 代码和 8KB 数据高速缓冲存储器, 即双路高速缓冲结构, 这种结构可以减少争用 Cache 的情况。另外, Pentium 对浮点处理单元作了重大改进, 包含了专用的加法、乘法和除法单元。Pentium 还对常用的简单指令直接用硬件逻辑实现, 对指令的微代码进行了重新设计。这些都提高了 Pentium 的整体性能。

4. Pentium Pro

Pentium Pro 于 1995 年正式推出, 原来被称为 P6, 中文名称为“高能奔腾”。Pentium Pro 由两个芯片组成: 一是含 8KB 代码和 8KB 数据 L1 Cache 的 CPU, 它由 550 万个晶体管构成; 二是 CPU 上还封装了 256KB 或 512KB 的 L2 Cache, 它由 1550 万或 3100 万个晶体管构成。Pentium Pro 扩展了超标量技术, 具有 12 级指令流水线, 能同时执行 3 条指令。

Pentium Pro 在处理器结构上的最大革新是采用了动态执行技术。动态执行是 3 种技术结合的总称: 分支预测、数据流分析和推测执行。分支预测技术预测程序的正确转移方向; 数据流分析技术分析哪些指令依赖于其他指令的结果或数据, 以便创建最优的指令执行序列; 而推测执行技术利用分支预测和数据流分析, 推测着执行指令。指令的实际执行顺序是动态

的、乱序的，即不一定是指令的原始静态顺序，执行的临时结果暂存于处理器的缓冲区中，但最终的输出执行顺序仍然是指令的正确顺序。动态技术可以使处理器尽量繁忙，避免可能引起的流水线停顿。

5. Pentium II

前面所述的各代 IA-32 处理器都新增了若干实用指令，但非常有限。为了顺应微机向多媒体和通信方向发展，Intel 公司及时在其处理器中加入了多媒体扩展 (MultiMedia eXtension, MMX) 技术。MMX 技术于 1996 年正式公布，它在 IA-32 指令系统中新增了 57 条整数运算多媒体指令，可以用这些指令对图像、音频、视频和通信方面的程序进行优化，使微机对多媒体的处理能力较原来有了大幅度提升。MMX 指令应用于 Pentium 处理器就是 Pentium MMX (多能奔腾)。MMX 指令应用于 Pentium Pro 处理器就是 Pentium II，它于 1997 年推出。

在以往的结构中，L1 Cache 最快，在处理器内部与处理器同频工作；L2 Cache 次之，在主板上与主板同频 (即处理器外部频率) 工作。处理器与 L2 Cache 间的通道和处理器与系统其他部件间的通道共用一条 64 位总线，这就造成主板总线上数据传输混乱、拥挤；而且由于主板的总线工作频率远低于处理器内部主频 (多倍关系)，使得数据传输速度较慢。Pentium II 采用双重独立总线 (Dual Independent Bus) 结构，处理器与 L2 Cache 间单独使用一条 64 位的背侧总线，且其工作频率独自与处理器的主频保持 1/2 的关系。这样，便提高了 L2 Cache 的速度。Pentium II 内部 L1 Cache 增大为 32KB + 32KB，L2 Cache 为 512KB。对于 233/266/300/333MHz 内频的 Pentium II，其外频是 66MHz；后来内频为 350/400/450MHz 的 Pentium II 采用 100MHz 外部频率。

6. Pentium III

1999 年，针对因特网和三维多媒体程序的应用要求，Intel 公司在 Pentium II 的基础上又新增了 70 条 SSE (Streaming SIMD Extensions) 指令 (原称为 MMX-2 指令)，开发了 Pentium III。SSE 指令侧重于浮点单精度多媒体运算，极大地提高了浮点 3D 数据的处理能力。SSE 指令类似于 AMD 公司发布的 3D Now! 指令。由于这些多媒体指令具有显著的单指令多数据 (Single Instruction Multiple Data, SIMD) 处理能力，即一条指令可以同时进行多组数据的操作，所以现在统称为 SIMD 指令。

后来，Intel 公司又推出了代号 “Coppermine (铜矿)” 的改进型 Pentium III。它将半速于 CPU 的 L2 Cache 改成集成在 CPU 芯片中的全速 L2 Cache，集成了约 1000 万个晶体管，内频达到 1GHz，而外频是 133MHz。

7. Pentium 4

Pentium Pro、Pentium II 和 Pentium III 都基于 P6 微结构。2000 年 11 月，Intel 公司推出 Pentium 4。它采用全新的称为 NetBurst 的微结构，超级流水线达 20 级。最初的 Pentium 4 新增了 76 条 SSE2 指令集，侧重于增强浮点双精度多媒体运算能力。2003 年，新一代 Pentium 4 处理器又新增了 13 条 SSE3 指令，用于补充完善 SIMD 指令集。该处理器具有 1.25 亿个晶体管、3.4GHz 时钟频率，L2 Cache 更是达到了前所未有的 1MB 容量。

处理器性能的提高依赖于新工艺和先进体系结构。半导体工艺水平决定了芯片的集成度和可以达到的时钟频率，而体系结构则决定了在相同集成度和时钟频率下处理器的执行效率，所以说体系结构对处理器至关重要。处理器的内部结构通常称为微体系结构或微结构 (Microarchitecture)。

Pentium 4 一方面沿袭指令级并行 (Instruction-Level Parallel, ILP) 方法, 通过进一步发掘指令之间可以同时执行的能力来提高性能, 如其 NetBurst 微结构; 另一方面通过开发线程级并行 (Thread-Level Parallel, TLP) 方法从更高层次发掘程序中的并行性来提高性能, 如其超线程 (Hyper Threading, HT) 技术。进程 (Process) 是一段可以独立运行的程序, 当一个进程被多个处理器以共享代码和地址空间的形式执行时称为线程 (Thread)。在现在服务器应用程序、在线处理、Web 服务甚至桌面应用程序中都包含可以并行执行的多个线程。3.06GHz 的 Pentium 4 开始支持 HT 技术, 它使一个物理处理器对操作系统来说看似有两个逻辑处理器, 这就允许两个程序线程, 不管有关还是无关都可以同时执行。

8. Celeron 和 Xeon

为了满足不断发展的应用和市场需求, Intel 公司从 Pentium II 开始将同一代处理器产品进一步细分。面向低端 (低价位 PC), Intel 公司推出 Celeron (赛扬) 处理器; 面向高端 (服务器), Intel 公司推出 Xeon (至强) 处理器。

Celeron 处理器采用减少高速缓存容量、改用低成本封装或降低时钟频率等方法来降低芯片成本, 是同代处理器的简化版本, 当然性能也有所降低。1998 年, Intel 公司推出首款 Celeron 处理器。它从 Pentium II 衍生而来, 核心为 7500 万个晶体管, 采用 0.25 μm 制造工艺, 内含 32KB L1 Cache, 外部频率仍为 66MHz。开始推出的 266 和 300MHz 的 Celeron 处理器不含 L2 Cache, 也就没有 Pentium II 的最大技术优势——双重独立总线结构, 其性能略高于 233MHz 的 MMX Pentium。后来推出的 300A、333、366 和 533MHz 的 Celeron 内置了 128KB L2 Cache, 性能有了很大提高。2000 年 5 月, 生产了基于 Pentium III 的 Celeron II 处理器。它采用 0.18 μm 制造工艺, 内频有 533 和 566MHz, 但外频仍然保持为 66MHz。2001 年, Celeron II 将外频提升为 100MHz。基于 Pentium 4 等后续产品, 同样也有低端 Celeron 处理器。

Xeon 处理器主要用于网络服务器或图形工作站, 通过增加 Cache 容量、提高工作频率、支持多处理器、率先采用革新技术等方法提高性能, 但价格也相应较高。另外, 针对便携式 PC (笔记本电脑) 要求功耗低、发热量小等特点, Intel 公司推出了 Pentium M (Mobile) 系列处理器; 还有 Centrino (迅驰) 系列处理器产品, 可以支持无线通信。

1.2.3 Intel 64 处理器

信息时代的应用对微型计算机性能提出了越来越高的要求, 尤其随着互联网和电子商务的发展, 人们对服务器的性能提出了更高的要求, 32 位处理器已不能适应这一要求。

当前, Intel、AMD、IBM、Sun 等厂商已陆续设计并推出了多种采用 RISC 结构的 64 位处理器。但是, 这些 64 位处理器主要面向服务器和工作站等高端应用, 不能兼容通用 PC。例如, Intel 公司于 2000 年推出 64 位 Itanium (安腾) 处理器, 2002 年又推出 Itanium 2 处理器。它们采用了 Intel 和 HP 公司联合开发的显式并行指令计算 (Explicitly Parallel Instruction Computing, EPIC) 技术。Intel 公司称该处理器的指令集结构为 Intel 64 位 (IA-64) 结构, 以区别于原来的 Intel 32 位 (IA-32) 结构。虽然这两个名称似乎有继承性, 但实际上 IA-64 结构不是 IA-32 结构的 64 位扩展。Itanium 处理器利用超长指令字 (Very Long Instruction Word, VLIW) 技术, 主要依靠软件提高指令级并行性; 而 IA-32 处理器利用超标量技术, 主要借助硬件提高指令级并行性。