

HZ BOOKS
华章教育

计算机
基础教育课程体系

规划教材

计算机硬件技术基础

钱晓捷◎主编



机械工业出版社
China Machine Press

TP303/206

2010

计算
基础教育课程体系
规划教材

计算机硬件技术基础

钱晓捷◎主编



机械工业出版社
China Machine Press

本书以 IA-32 处理器和 32 位个人计算机系统为实例,从软件开发、计算机系统应用的角度,论述了计算机硬件技术,包括 IA-32 处理器的发展和微机组成、数据表示、数字逻辑基础、处理器结构和指令系统、总线系统、存储系统、输入输出接口,还特别介绍了精简指令集计算机、高速缓冲存储器、存储管理、指令流水线、多媒体指令、超标量、动态执行、多线程、多核等提高处理器性能的先进技术。

本书适合作为普通高等院校面向软件开发、系统应用的计算机专业的“计算机组成原理”或“计算机组织与结构”课程的教材或参考书,同时也适合作为非计算机专业的“计算机硬件技术”课程的教材或参考书。此外,本书面向一般学生和普通读者写作,起点低、内容精练、叙述深入浅出,适合软件工程、信息技术及电子、通信和自控等电类专业的本科学生使用,也适合计算机等专业的职高高专、成教学生以及计算机应用开发人员、希望深入学习计算机硬件技术的普通读者和培训班学员使用。

封底无防伪标均为盗版

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

计算机硬件技术基础/钱晓捷主编. —北京:机械工业出版社,2010.1
(计算机基础教育课程体系规划教材)

ISBN 978-7-111-29105-3

I. 计… II. 钱… III. 硬件 - 高等学校 - 教材 IV. TP303

中国版本图书馆 CIP 数据核字 (2009) 第 213215 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

北京诚信伟业印刷有限公司印刷

2010 年 1 月第 1 版第 1 次印刷

184mm × 260mm · 17 印张

标准书号:ISBN 978-7-111-29105-3

定价:29.80 元

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

客服热线:(010) 88378991; 88361066

购书热线:(010) 68326294; 88379649; 68995259

投稿热线:(010) 88379604

读者信箱:hzjsj@hzbook.com

计算机系统由硬件和软件组成，硬件是软件的物理基础，掌握计算机硬件技术，对软件开发和计算机系统应用具有重大支持作用。

在我国高等学校“计算机科学与技术本科专业规范”中，硬件技术属于“计算机体系结构和组织”知识领域。在目前我国高校计算机专业的本科教学计划中，硬件技术系列课程有：数字逻辑、计算机组成原理、汇编语言程序设计、微机原理及接口技术、计算机系统结构等。但是，对于以软件开发为主的软件工程方向和以系统应用为主的信息技术（网络工程）方向来说，既没有如此多的学时，也没有必要这样进行硬件技术教学。所以，“计算机科学与技术本科专业规范”对软件工程和信息技术方向推荐的教学计划中只有一门硬件技术核心课程，可以称之为“计算机组织与结构”，希望通过本课程让学生全面了解计算机硬件系统，熟悉计算机工作原理。非计算机本科专业，尤其是电子、机电等与计算机应用相关的专业也有类似的要求，一般将该课程称之为“计算机硬件技术基础”。专科、高职的计算机及相关专业也属于同样情况，往往开设一门“计算机组成原理”课程。

为此，遵循我国“计算机科学与技术本科专业规范”等指导性文件，参考非计算机专业本科“计算机硬件技术基础”教学要求，考虑计算机等专科专业的教学情况，结合实践教学，我们编写了本书。与同类教材相比，本书具有以下特点。

1. 综合计算机硬件技术核心内容

本书综合了目前计算机专业所有硬件技术课程的核心内容。各章结构以“计算机组成”为主体，结合“微机原理”实例，包括系统组成、数据表示、指令系统、总线、存储系统、输入输出接口等教学内容，使学生通过实例理解原理。

本书的第3章是数字逻辑基础，用来弥补未单独开设“数字逻辑”课程的问题，为读者理解基本电路提供方便，使其适合软件工程、非电类专业学生和普通软件开发人员。

“计算机系统结构”核心内容在本书的最后一章“处理器性能提高技术”中体现，其中包括性能评测、指令流水线、向量处理机等内容，还跟踪了计算机技术的最新发展，特别介绍了超标量、动态执行、多媒体指令、多线程、多核等先进技术。

2. 面向软件开发和系统应用取舍内容

本书不同于国内现有的“计算机组成原理”或“计算机组织与结构”教材，因为这些教材从计算机设计的角度展开，深入到电路实现技术，要求学生具有较强的数字逻辑知识。本书则从应用的角度解释系统结构特点，不以设计者观点论述技术实现。

例如，本书舍弃了运算方法和运算器电路、微程序控制器和硬布线控制器，只是简单介绍运算原理和微程序、硬布线技术的特点。另一方面，通过举例说明C语言的整数、字符、浮点数类型，有助于读者更好地理解数据表示、数据存储，也使得学生深刻体会硬件对软件的支持。使用高级语言程序实例的教学内容还有存储器地址、局部性原理等。

本书的许多教学内容都以应用为例，不仅仅是为了理解工作原理。例如，对于实数的浮点数编码，直接使用国际标准格式；对于精简指令集计算机，简单介绍MIPS处理器；超长指令字技术引出安腾处理器。

3. 以 IA-32 处理器和个人计算机为实例

有别于宽泛的举例，本书以具有典型意义的 IA-32 处理器和桌面个人计算机为实例，使得学生在理解计算机工作原理的同时，熟悉广泛使用的计算机系统。例如，寄存器结构、指令编码、寻址方式、常用指令等都以 IA-32 处理器举例，由此自然引出汇编语言。

本书不同于目前国内的“计算机硬件技术基础”教材，因为它们实际上与“微机原理及接口技术”教材内容几乎完全相同，其中汇编语言和接口技术内容过深，但缺少计算机组成和结构方面的内容。为此，本书强调基本概念和工作原理，淡化技术实现细节。例如，重点学习 32 位基本指令而不是所有指令泛泛而谈；抓住处理器和总线的关键信号，而不详细展开所有引脚功能；重点说明存储器地址译码原理，而不分析存储器芯片的连接细节。

总之，本书从全新的视角，融合计算机组成原理、通用处理器实例和个人计算机应用，全面而系统地介绍了计算机硬件技术基础知识。全书共分 9 章。

- 第 1 章“计算机系统概述”。本章通过计算机的发展尤其是 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计算机硬件组成，以个人计算机为例理解计算机层次结构和基本工作原理。
- 第 2 章“数据表示”。本章介绍计算机内部如何表达整数、字符、实数，即定点整数编码、字符 ASCII 码和浮点实数编码，并通过 C 语言基本数据类型的程序理解编码及其存储。
- 第 3 章“数字逻辑基础”。本章展开计算机的硬件实现技术，通过对数字电路和逻辑代数的认识说明常用门电路的原理和功能，通过编码器、译码器、触发器、寄存器等常用器件说明数字电路的设计、分析过程，最后通过可编程逻辑器件引出硬件描述语言和电子设计自动化。
- 第 4 章“处理器”。本章首先介绍处理器内部的控制器和运算器的基本组成，然后介绍 8 位处理器、16 位 8086、32 位 80386 和 Pentium 的功能结构，接着展开 IA-32 处理器寄存器、工作方式和存储模型用以体会处理器编程结构。
- 第 5 章“指令系统”。本章以 IA-32 处理器指令系统为例，学习指令编码、各种寻址方式、常用指令功能，自然引出并熟悉汇编语言的语句格式、程序框架和开发方法，最后说明精简指令集技术的特点。
- 第 6 章“总线系统”。本章论述总线结构，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 7 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，介绍高速缓冲存储器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 8 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，并简单介绍常用的定时控制接口、并行接口、异步串行通信接口和模拟接口。
- 第 9 章“处理器性能提高技术”。本章以并行处理技术为逻辑主线、以 IA-32 处理器为例介绍高性能处理器所运用的各种先进技术，包括指令级并行的指令流水线、超标量、动态执行，数据级并行的向量处理机和多媒体指令，线程级并行的多线程和多核技术。

本书在编写过程中，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，以清晰的逻辑结构循序渐进地展开教学内容；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；每章最后都进行总结，帮助读者领悟重点知识，并通过大量习题巩固所学。本书不求读者熟悉数字逻辑等内容，只要具有计算机（文化）基础和高级语言的入门知识，就可以学习本书内容。

作为普通本科生课程的教材，全面讲授本书各章内容需要 68~72 学时；如果只讲授各章主要内容，也可以安排 51~54 学时。此外，还可以配合第 2 章等安排 C/C++ 语言编程、第 5 章等安排汇编语言编程的实践环节。各章授课学时数可参考下表。对于专科生课程的教学，可以根据学生的实际水平和接受能力，适当降低要求或者增加辅导学时。而对于程度较高的学生，主讲教师也可以考虑采用精讲形式，减少课堂教学学时数。

章号	全面讲授本书各章内容建议学时（总学时 68）	讲授各章主要内容建议学时（总学时 51）
1	6	6
2	10	8
3	10	8
4	6	4
5	8	6
6	4	4
7	10	7
8	8	6
9	6	2

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>）。该网站是本书的动态延伸，提供本书的教学课件（电子教案）、例题源程序文件、配套汇编语言开发软件包等辅助资源，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，广大师生和读者可以通过电子邮件（qianxiaojie@zzu.edu.cn）或者教辅网站的论坛与编者交流。

本书由钱晓捷主编，其中杨镇江编写了第 3 章初稿，马琦参与了第 2 章的编写工作，其余各章均由钱晓捷编写。本书的编写还得到了石磊、卢红星、李正民、关国利、程楠、张青等人的支持，衷心感谢他们，同时也感谢机械工业出版社华章公司一直以来的大力支持。

编者

2009 年 10 月

目 录 Contents

前 言	
第 1 章 计算机系统概述	1
1.1 计算机的发展	1
1.1.1 计算机的发展概况	1
1.1.2 微型计算机的发展	2
1.2 Intel 80x86 系列处理器	4
1.2.1 16 位 80x86 处理器	4
1.2.2 IA-32 处理器	5
1.2.3 Intel 64 处理器	9
1.3 计算机系统组成	10
1.3.1 冯·诺伊曼计算机结构	10
1.3.2 微型计算机的硬件系统	13
1.3.3 PC 微机结构	14
1.3.4 计算机系统的层次结构	17
1.3.5 计算机的软件系统	21
第 1 章总结	22
第 1 章习题	22
第 2 章 数据表示	24
2.1 数制	24
2.1.1 二进制和十六进制	24
2.1.2 数制之间的转换	25
2.2 整数编码	27
2.2.1 定点整数格式	27
2.2.2 有符号整数编码	28
2.3 字符编码	31
2.3.1 BCD	31
2.3.2 ASCII	31
2.3.3 Unicode	34
2.4 实数编码	35
2.4.1 浮点数据格式	35
2.4.2 浮点数的舍入控制	38
2.5 校验编码	41
2.5.1 奇偶校验码	41
2.5.2 海明码	42
2.5.3 循环冗余码	43
第 2 章总结	45
第 2 章习题	45
第 3 章 数字逻辑基础	48
3.1 逻辑代数	48
3.1.1 逻辑关系	48
3.1.2 逻辑代数的运算规则	52
3.1.3 逻辑函数的形式、 转换及化简	54
3.2 逻辑门电路	56
3.2.1 门电路实现	57
3.2.2 集成电路	59
3.2.3 三态门	60
3.3 组合逻辑电路	62
3.3.1 编码器	62
3.3.2 译码器	63
3.3.3 加法器	65
3.4 时序逻辑电路	65
3.4.1 触发器	66
3.4.2 寄存器	69
3.4.3 计数器	70
3.5 可编程逻辑器件	71
3.5.1 PLD 器件	71
3.5.2 电子设计自动化	72
第 3 章总结	75
第 3 章习题	75
第 4 章 处理器	78
4.1 处理器组成	78
4.1.1 控制器	78
4.1.2 运算器	80
4.2 处理器结构	81
4.2.1 处理器的基本结构	81
4.2.2 8086 的功能结构	82
4.2.3 80386 的功能结构	83
4.2.4 Pentium 的功能结构	84
4.3 寄存器	86

4.3.1 通用寄存器	86	6.3 8086 的总线时序	143
4.3.2 标志寄存器	87	6.3.1 写总线周期	143
4.3.3 专用寄存器	92	6.3.2 读总线周期	144
4.4 存储器组织	93	6.4 Pentium 处理器的引脚和时序	145
4.4.1 存储模型	93	6.4.1 引脚定义	145
4.4.2 工作方式	94	6.4.2 总线周期	147
4.4.3 逻辑地址	95	6.5 微机系统总线	148
第4章总结	98	6.5.1 PC 机总线的发展	148
第4章习题	98	6.5.2 ISA 总线	150
第5章 指令系统	101	6.5.3 PCI 总线	152
5.1 指令格式	101	6.5.4 USB 总线	156
5.1.1 指令编码	101	第6章总结	158
5.1.2 IA-32 指令格式	103	第6章习题	159
5.2 寻址方式	105	第7章 存储系统	162
5.2.1 数据寻址	105	7.1 存储系统的层次结构	162
5.2.2 指令寻址	109	7.1.1 技术指标	162
5.2.3 堆栈及堆栈寻址	111	7.1.2 层次结构	162
5.3 通用指令及其功能	113	7.1.3 局部性原理	164
5.3.1 数据传送类指令	113	7.2 主存储器	165
5.3.2 算术运算类指令	114	7.2.1 读写存储器	165
5.3.3 位操作类指令	115	7.2.2 只读存储器	169
5.3.4 控制转移类指令	117	7.2.3 存储器地址译码	172
5.4 汇编语言基础	119	7.2.4 主存空间分配	177
5.4.1 语句格式	119	7.3 高速缓冲存储器	180
5.4.2 源程序框架	121	7.3.1 工作原理	180
5.4.3 开发过程	123	7.3.2 地址映射	183
5.5 精简指令集计算机技术	125	7.3.3 替换算法	186
5.5.1 复杂指令集和精简指令集	125	7.3.4 写入策略	187
5.5.2 RISC 技术的主要特点	126	7.3.5 80486 的 L1 Cache	189
5.5.3 MIPS 处理器	127	7.3.6 Pentium 的 L1 Cache	189
第5章总结	128	7.4 存储管理	191
第5章习题	130	7.4.1 段式存储管理	191
第6章 总线系统	133	7.4.2 页式存储管理	193
6.1 总线技术	133	第7章总结	196
6.1.1 总线类型	133	第7章习题	197
6.1.2 总线的数据传输	134	第8章 输入输出接口	199
6.1.3 总线信号和总线时序	138	8.1 I/O 接口概述	199
6.2 8086 的引脚信号	139	8.1.1 I/O 接口的典型结构	199
6.2.1 地址/数据信号	140	8.1.2 I/O 端口的编址	201
6.2.2 读写控制信号	140	8.1.3 输入输出指令	203
6.2.3 其他控制信号	142		

8.2 外设数据传送方式	204	9.1.2 并行计算机结构分类	236
8.2.1 无条件传送	204	9.1.3 计算机性能评测	237
8.2.2 查询传送	206	9.2 指令级并行	238
8.2.3 中断传送	208	9.2.1 指令流水线技术	238
8.2.4 中断控制系统	211	9.2.2 超标量技术	243
8.2.5 DMA 传送	215	9.2.3 动态执行技术	246
8.3 常用输入输出接口	217	9.2.4 超长指令字技术	248
8.3.1 定时控制接口	217	9.3 数据级并行	249
8.3.2 并行接口	224	9.3.1 向量处理机	249
8.3.3 异步串行通信接口	227	9.3.2 多媒体指令	250
8.3.4 模拟接口	230	9.4 线程级并行	255
第8章总结	232	9.4.1 同时多线程技术	255
第8章习题	233	9.4.2 单芯片多处理器技术	258
第9章 处理器性能提高技术	236	第9章总结	260
9.1 并行处理技术	236	第9章习题	261
9.1.1 并行性概念	236	参考文献	263

计算机系统概述

电子数字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,介绍计算机系统的发展和组成,为后续章节奠定基础。

1.1 计算机的发展

计算机的诞生和发展是 20 世纪最重要的科技成果之一。微型计算机的应用深入到人类社会的方方面面,极大地改变了人们的工作、学习和生活方式,成为信息时代的主要标志。

1.1.1 计算机的发展概况

美国宾夕法尼亚大学摩尔学院的莫克利(J. W. Mauchly)和埃克特(J. P. Eckert)制造了世界上第一台通用电子数字计算机 ENIAC (Electronics Numerical Integrator And Calculator)。ENIAC 计算机最初用于为军队编制各种武器的弹道表,后经多次改进,成为能进行各种科学计算的通用计算机,于 1946 年得以公开。

1. 计算机发展简史

计算机的发展突飞猛进,经历了电子管、晶体管、中小规模集成电路和超大规模集成电路 4 个阶段。

- 第一代计算机是从第一台计算机 ENIAC 问世开始到 20 世纪 50 年代末。这一时期的主要特征是使用电子管作为逻辑器件,软件还处于初始阶段,使用机器语言与符号语言编制程序。

第一代计算机是计算机发展的初级阶段,其体积比较大,运算速度比较低,存储容量不大。为了解决一个问题,所编制的程序很复杂。这一代计算机主要用于科学计算。

- 第二代计算机是从 20 世纪 50 年代末到 20 世纪 60 年代初。这一时期的主要特征是使用晶体管作为电子器件,在软件方面开始使用计算机高级语言,为更多的人学习和使用计算机铺平了道路。

这一代计算机的体积大大减小,具有重量轻、寿命长、耗电少、运算速度快、存储容量较大等优点。因此,这一代计算机不仅用于科学计算,还用于数据处理和事务处理,并逐渐用于工业控制。

- 第三代计算机是从 20 世纪 60 年代中期到 20 世纪 70 年代初期。这一时期的主要特征是使用中小规模集成电路作为电子器件,操作系统的出现使计算机的功能越来越强,应用范围越来越广。

使用中小规模集成电路制成的计算机,其体积与功耗都进一步减小,可靠性和运算速度等指标都进一步提高,为计算机的小型化、微型化提供了良好的条件。在这一时期,计算机不仅用于科学计算,还用于文字处理、企业管理、自动控制等,出现了计算机技术与通信技术相结合的管理信息系统,可用于生产管理、交通管理、情报检索等领域。

- 第四代计算机是指用大规模与超大规模集成电路作为电子器件制成的计算机。这一代计算机在各种性能上都有了大幅度的提高,软件也越来越丰富,其应用涉及国民经济的各个领域,已经在办公室自动化、数据库管理、图像识别、语音识别、专家系统等众多领域中大显身手,并且进入了家庭。

1971年以来,作为第四代计算机重要产品的微型计算机得到了飞速的发展,对计算机的普及起到了决定性的作用。

计算机的应用有力地推动了国民经济的发展和科学技术的进步,同时也对计算机技术提出了更高的要求,从而促进了计算机技术的进一步发展。以超大规模集成电路为基础,未来的计算机将向巨型化、微型化、网络化与智能化的方向发展,其中“巨型化”并非指计算机的体积大,而是指计算机的运算速度更高、存储容量更大、功能更强。

2. 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机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。所以,在不会引起歧义的情况下,本书将“微处理器”简称为“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,处理器的性能提高主要是工艺技术驱动。此后,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、单芯片多核等并行技术,先进的系统结构已经成为提高处理器性能的主要推动力。

1.1.2 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(PC)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来完成特定功能。

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,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。

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。

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。

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,也是世界上第一个微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 $2^{20}B = 1024 \times 1024B = 1024KB = 1MB$ ，这里 $1KB = 2^{10}B = 1024B$ 。

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增技术。

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,一个进程可以创建多个线程 (Thread),每个线程以共享代码和地址空间形式处理一个任务。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