软件调试第二版-卷一读书笔记

作者：Delort

2.CPU基础

2.1指令和指令集

RISC：精简指令集

CISC：复杂指令集

2.1.1基本特征

第一：大多数RISC处理器指令是等长的。而CISC处理器指令长度不固定。

第二：RISC寻址方式比CISC少很多。

第三：与RISC相比，CISC处理器的通用寄存器数量较少。

第四：RISC的指令数量也比较少。

第五：从函数（或子程序）调用过程或者函数RISC有足够的寄存器，但是CISC不行。

2.1.2寻址方式

1. 立即寻址
2. 寄存器寻址
3. 直接寻址
4. 寄存器间接寻址

2.1.3指令的执行过程

高速缓存-》取址/解码单元-》指令池-》分发/执行单元-》指令池-》回收单元

2.2英特尔架构处理器

32位架构称为IA-32，也有 Intel 64.

IA-64指代安腾架构。

2.2.1 80386处理器

1. 32位地址总线，最多支持4GB内存。
2. 平坦内存模型。
3. 分页机制。
4. 调试寄存器。
5. 虚拟8086模式。

2.2.2 80486处理器

1. cpu内部集成高速缓存。
2. FPU集成到CPU内。
3. 内存对齐检查异常。
4. 系统管理模式。

2.2.3奔腾处理器

1. 数据总线宽度从32位增加到64位。
2. 加入第二条执行流水线。称为超标量架构。
3. 内部一级高速缓存增加为16KB，其中8KB用于数据，8KB用于代码。
4. 支持4MB大页面内存。
5. 引入性能监视机制。
6. 引入内部错误探测功能。
7. 引入JTAG调试。
8. 多处理器支持。
9. 支持MMX技术，及以SIMD方式提高并行运算能力。
10. 再次将一级高速缓存加倍，数据和代码各16KB。
11. 优化了，分支预测单元和指令解码器。
12. 引入了MSR寄存器和RDMSR和WRMSR俩条指令。

2.2.4 p6系列处理器

1. 内部集成二级高速缓存。
2. 地址总线宽度从32位增加到36位，最多寻址64gb内存。称为PAE-36模式。
3. 3路超标量微架构。
4. 投机取指/投机执行。
5. 去除MMX支持，后重新恢复。
6. 引入了内存类型范围寄存器。MTRR。
7. 数据和指令高速缓存提高到32KB。
8. 增加快速系统调用和返回指令。
9. 单指令多数据扩展，SSE。
10. 引入了70多条新指令和8个128位数据寄存器。
11. 增加FXSAVE和FXRSOR指令。

2.2.5 奔腾4处理器

1. 流水线的级数由10到20.
2. 超线程，一个CPU内俩个逻辑处理器，俩个线程可以同时执行。
3. 加入了分支踪迹存储。
4. 加入了SSE2指令，又加入了SSE3指令。
5. 性能计数器从2增加到18个。
6. 温度监控功能。
7. 引入EM64T技术，通过IA-32e模式支持64位计算，正式名称叫 Intel 64位架构。

2.2.6-2.2.13

略，待补充。

2.3CPU工作模式

1. 保护模式　　IA-32处理器本位模式，native模式。
2. 实地址模式　　模拟8086处理器的工作模式。
3. 虚拟8086模式 保护模式下用来执行8086任务的准模式。
4. 系统管理模式SMM 供固件执行电源管理，安全检查或与平台相关的特殊任务。
5. IA-32e模式　　支持 Intel 64 的64位模式曾经为EM64T，俩个子模式一个是64位模式，64位线性寻址，并能访问超过64GB内存的物理内存。另一个是兼容模式，执行32位程序。特注意：IA-32e模式下，系统内核和内核态的驱动程序一定是64位代码。

上电复位（实模式），CR0控制寄存器PE标志控制处于实地址模式还是保护模式。EFLAGS的VM标志用来控制处理器是在虚拟8086还是普通保护模式下运行。EFER寄存器的LME用来启用IA-32e模式。

2.4寄存器

2.4.1通用数据寄存器

略。

2.4.2标志位寄存器。

标志	位	含义
CF	0	进位或错位
PF	2	当计算结果最低字节偶数个1时，置为1
AF	4	辅助进位标志位，当位3（半个字节）处有进位或者借位置为1
ZF	6	计算结果为0置为1
SF	7	符号标志位，结果为负置为1
TF	8	陷阱标志位
IF	9	中断标志位，为0禁止响应可屏蔽中断
OF	11	溢出标志位，超过机器表达范围置为1
DF	10	方向标志，为1时使字符串指令每次操作后递减变址寄存器（ESI和EDI），为0递增
IOPL	12和13	用于表达当前任务IO的权限级别
NT	14	任务套嵌标志，为1表示当前任务是链接到了前面的执行的任务，通常用于中断或者触发了IDT表中的任务门
RF	16	控制处理器对调试异常的响应，为1暂时 禁止由于指令断点（调试寄存器设置的指令断点）导致的异常
VM	17	为1启用虚拟8086模式，0返回普通的保护模式
AC	18	设置此标志和CR0的AM标志可以启用内存对齐检查
VIF	19	与VIP标志一起用于实现奔腾处理器引入的虚拟中断机制
VIP	20	与VIF标志一起用于实现奔腾处理器引入的虚拟中断机制
ID	21	用于检测是否支持CPUID指令，如果能成功设置和清除该标志，则支持CPUID指令