机器指令

- 机器指令是计算机系统执行的基本命令，是中央处理器执行的基本单位
- 指令由一个或多个字节组成，包括操作码字段、一个或多个操作数地址字段、以及一些表征机器状态的状态字以及特征码
- 指令完成各种算术逻辑运算、数据传输、控制流跳转

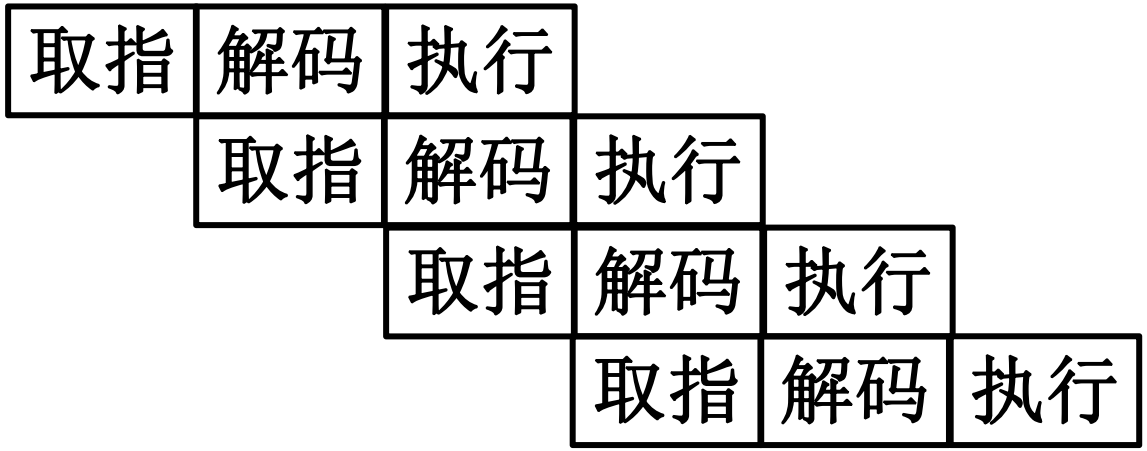
指令执行过程

- CPU根据PC取出指令，放入IR，并对指令译码，然后发出各种控制命令，执行微操作系列，从而完成一条指令的执行
- 一种指令执行步骤如下：
  - 取指：根据PC从存储器或高速缓冲存储器中取指令到IR
  - 解码：解译IR中的指令来决定其执行行为
  - 执行：连接到CPU部件，执行运算，产生结果并写回，同时在CC里设置运算结论标志；跳转指令操作PC，其他指令递增PC值

指令执行周期与指令流水线

- 指令执行周期

- 指令流水线



特权指令与非特权指令

- 用户程序并非能够使用全部机器指令，那些与计算机核心资源相关的特殊指令会被保护
  - 如：启动I/O指令、置PC指令、等等
  - 核心资源相关的指令只能被操作系统程序使用

- 特权指令：只能被操作系统内核使用的指令
- 非特权指令：能够被所有程序使用的指令

处理器模式

- 计算机通过设置处理器模式实现特权指令管理
- 计算机一般设置0、1、2、3等四种运行模式，建议分别对应：0操作系统内核、1系统调用、2共享库程序、3用户程序等保护级别
- 0模式可以执行全部指令；3模式只能执行非特权指令；其他每种运行模式可以规定执行的指令子集
- 一般来说，现代操作系统只使用0和3两种模式，对应于内核模式和用户模式

处理器模式的切换

- 简称模式切换，包括“用户模式→内核模式”和“内核模式→用户模式”的转换
- 中断、异常或系统异常等事件导致用户程序向OS内核切换，触发：用户模式→内核模式
  - 程序请求操作系统服务
  - 程序运行时发生异常
  - 程序运行时发生并响应中断
- OS内核处理完成后，调用中断返回指令（如Intel的iret）触发：内核模式→用户模式