汇编

Liam

2023 年 9 月 15 日

1 基础知识

1.1 存储器

存储器中存储了**指令**和**数据**，同时存储器又被划分为若干个存储单元。CPU 对数据进行读写需要获取：地址信息，控制信息，数据信息。通过：**地址总线，控制总线**和**数据总线**进行传输。

1.1.1 地址总线

一个 CPU 有 N 根地址线，则该 CPU 的地址总线的宽度为 N，这样 CPU 可以寻址 2^N 个内存单元。注意：每个内存单元可以容纳 8 位的数据比特。

1.2 数据总线

数据总线宽度决定了数据传输速度。

1.3 控制总线

控制总线宽度决定了 CPU 对外部器件的控制能力。

1.4 内存地址空间

各种物理器件，在 CPU 操控的时候，都是将他们看作内存来对待---所有物理存储器被看作**一个由若干存储单元组成的逻辑存储器**。每个物理存储器在这个逻辑存储器中占有一个地址段，即一段地址空间。CPU 向对应的地址读写数据，相当于向对应的物理存储器中读写数据。

2 寄存器

CPU 由原算起，控制器和寄存器等器件构成，二程序员通过改变寄存器中的内容来实现对 CPU 的控制。

2.1 通用寄存器

一个 16 位寄存器可以存储 16 位的数据，并且有些可以将 16 位寄存器拆成**高八位寄存器**和**低八位寄存器**使用。

2.2 物理地址

么一个内存单元在内存空间中都有唯一的地址，我们称为**物理地址**。

2.3 16 位结构的 CPU

- 运算器一次处理 16 位数据
- 寄存器最大宽度为 16 位
- 寄存器和运算器之间通路为 16 位

2.4 16 位 8086CPU 给出 20 位寻址能力的办法

采用公式（即段地址左移 4 位）：

$$\text{物理地址} = \text{段地址} \times 16 + \text{偏移地址} \tag{1}$$

来合成 20 位物理地址。（注意本身内存是没有被划分成一段段的，只是人们为了管理而虚指的）

2.5 段寄存器

2.5.1 CS 和 IP

CS 为段寄存器，IP 为指令指针寄存器。在 8086PC 机中，任意时刻 CS 中内容为 M，IP 中内容为 N，则 CPU 将会从 $M \times 16 + N$ 单元开始，读取一条指令并执行。
步骤：

1. CS:IP 指向的内存单元读取指令，指令进入指令缓冲区

2. IP=IP+ 所读取的指令的长度并指向下一条指令

3. 执行指令，回到步骤 1

2.6 修改 CS，IP 指令

通过指令 jmp段地址 : 偏移地址 来将修改 CS 和 IP。

通过指令 jmp ，来将修改 CS 和 IP，所以任意代码段的执行，只能依靠 CS:PC 来确定执行。