# 计算机系统基础

# 实验报告

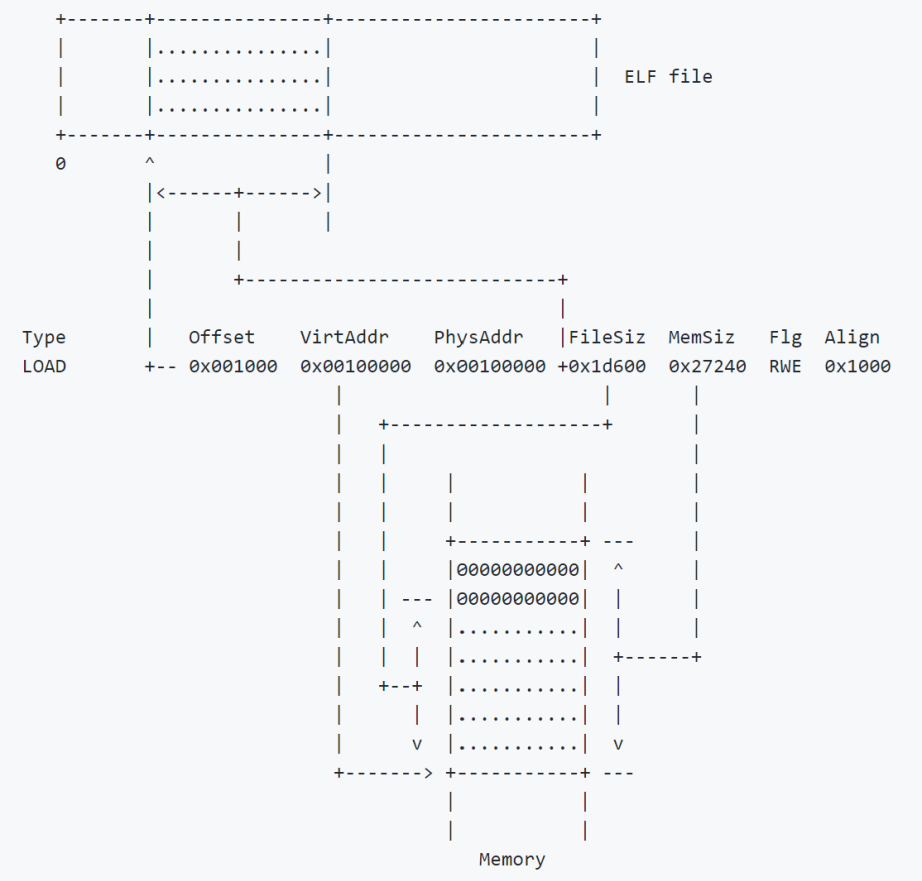
# PA 2

计算机科学与技术系
191220008 陈南曈

## 2-2：

### 1、为什么在装载时要把内存中剩余的 p_memsz - p_filesz 字节的内容清零?

如下图所示，该图为 ELF 文件的装载过程:



装载的过程可以简单描述为：

对于 p_type == PT_LOAD 的表项，将 ELF 文件中起始于 p_offset，大小为 p_filesz 字节的数据拷贝到内存中起始于 p_vaddr 的位置，并将内存中剩余的 p_memsz - p_filesz 字节的内容清零。

然而，在剩余的 p_memsz - p_filesz 字节中，由于未进行赋值，导致此前存放的数据会对该进程产生影响，故需要在装载时将这一部分置为零，防止原来的数据产生影响。