PA_2-2 实验报告

计算机科学与技术系 张桓 191220156

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？

答：程序头表表项中的 p_filesz 字段对应于 ELF 文件中该段的大小（以字节为单位），而 p_memsz 是该段在内存中所占的大小。p_memsz 应该大于等于 p_filesz，这是因为可装入段可能包含.bss 节，其中包含未初始化的全局变量。而.bss 节在 ELF 文件中是不占用空间的，仅在 ELF 文件加载到内存后才占用内存中的空间，所以出现了 p_memsz 大于 p_filesz 的情况。

因此如果出现 p_memsz 字段大于 p_filese 字段，说明 p_memsz - p_filesz 这一字节部分应该对应.bss 节。根据 i386 System V ABI 规范规定，.bss 节所在存储区域在运行时被初始化为 0。因此在装载时要把内存中剩余的 p_memsz - p_filesz 字节的内容清零。