1. 插桩工具的代码框架和执行过程

PIN 插桩执行过程如图 1 所示。

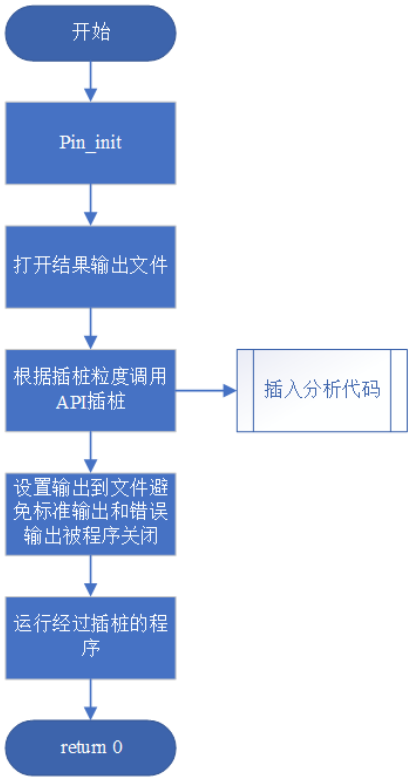

图 1 PIN 插桩流程图

2. Pi 程序插桩结果如图 2 所示，memtester 插桩结果如图 3 所示。

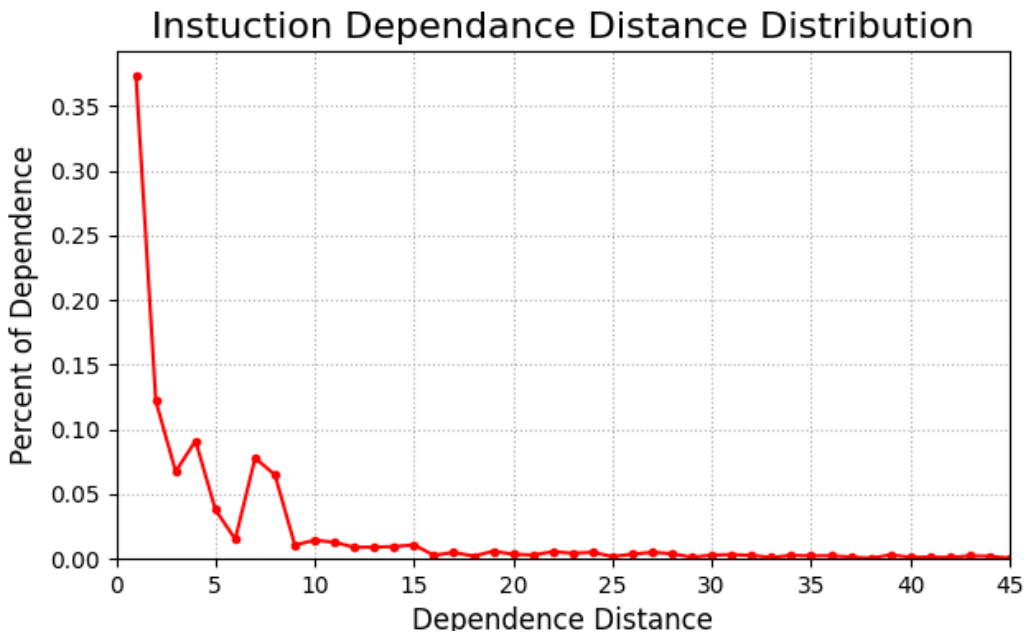

图 2 Pi 程序插桩结果

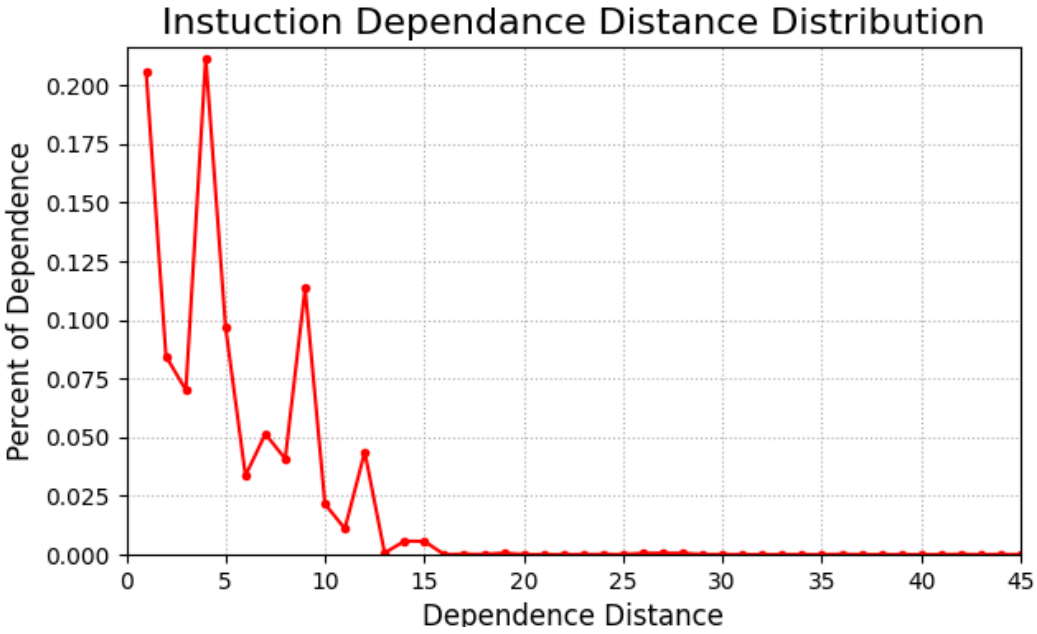

图 3 memtester 插桩结果

3. (a) 可能是栈基址寄存器、段基址寄存器，因为其设置之后可能需要经过一系列指令执行之后才进行访存操作；
(b) B 拥有更多的寄存器，从而使得它可以不用频繁地挪用一个寄存器用于存储数据，所以在依赖距离短的部分占比更小。
(c)相同。无论是使用停顿还是转发处理流水线停顿，都不会影响两条存在依赖关系的指令之间的 PC 差值。