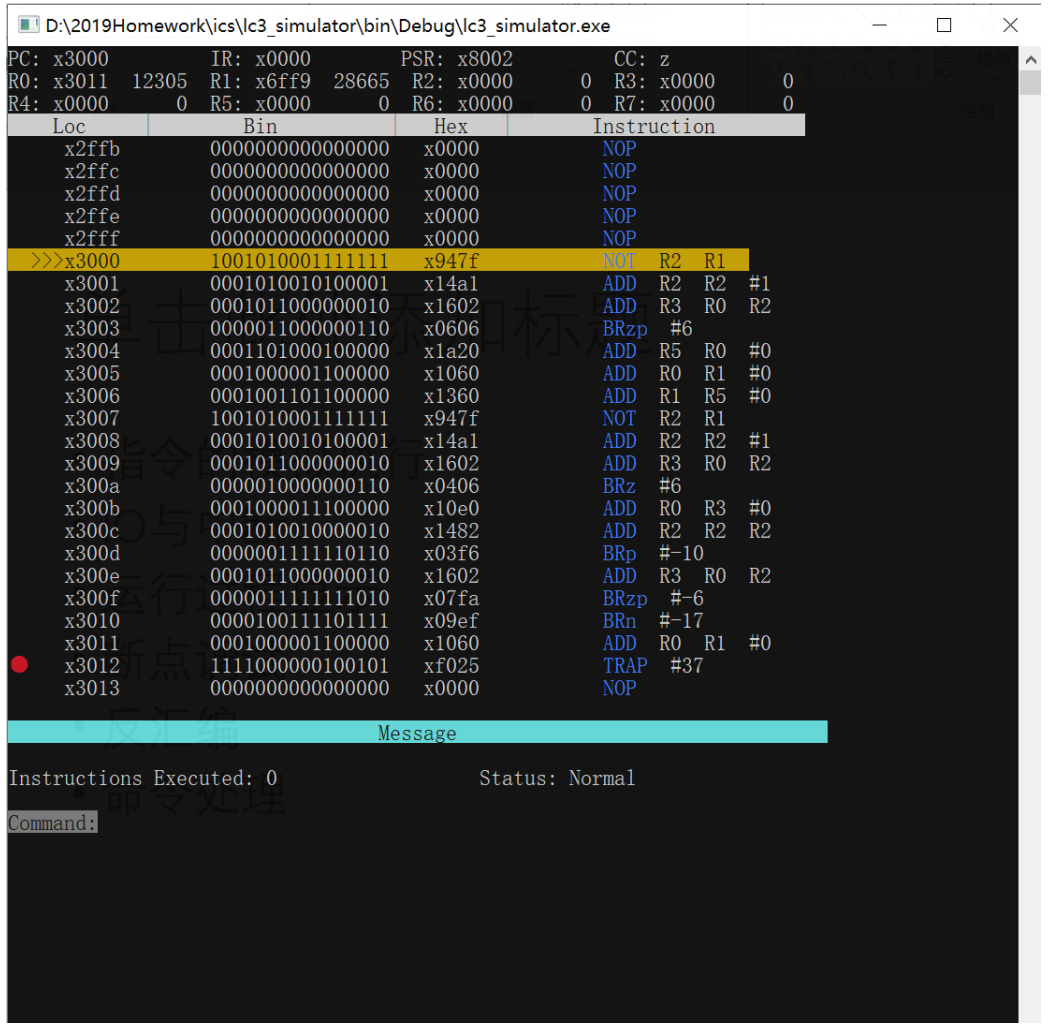
LC-3 Simulator

王瑞程 PB18111723

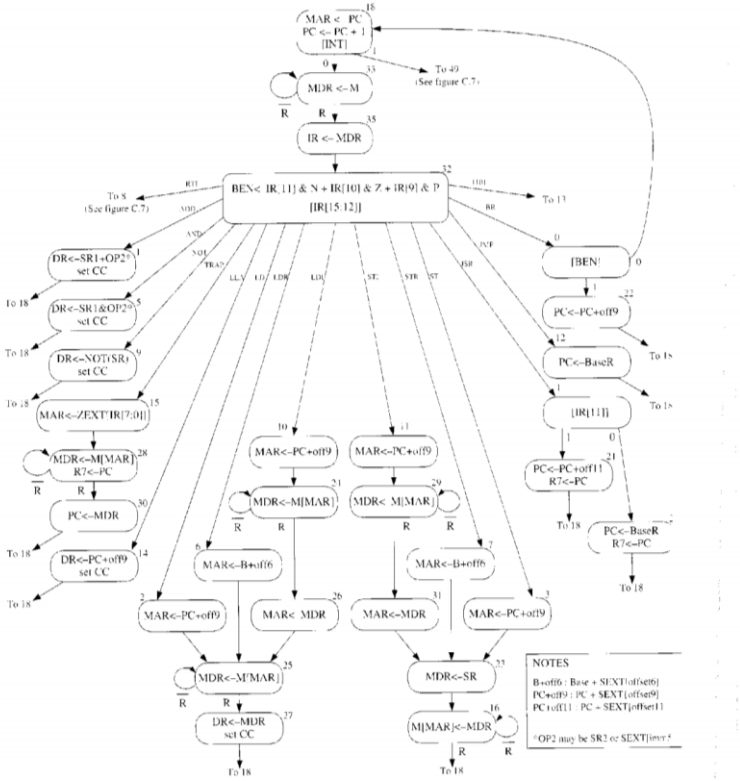
实现

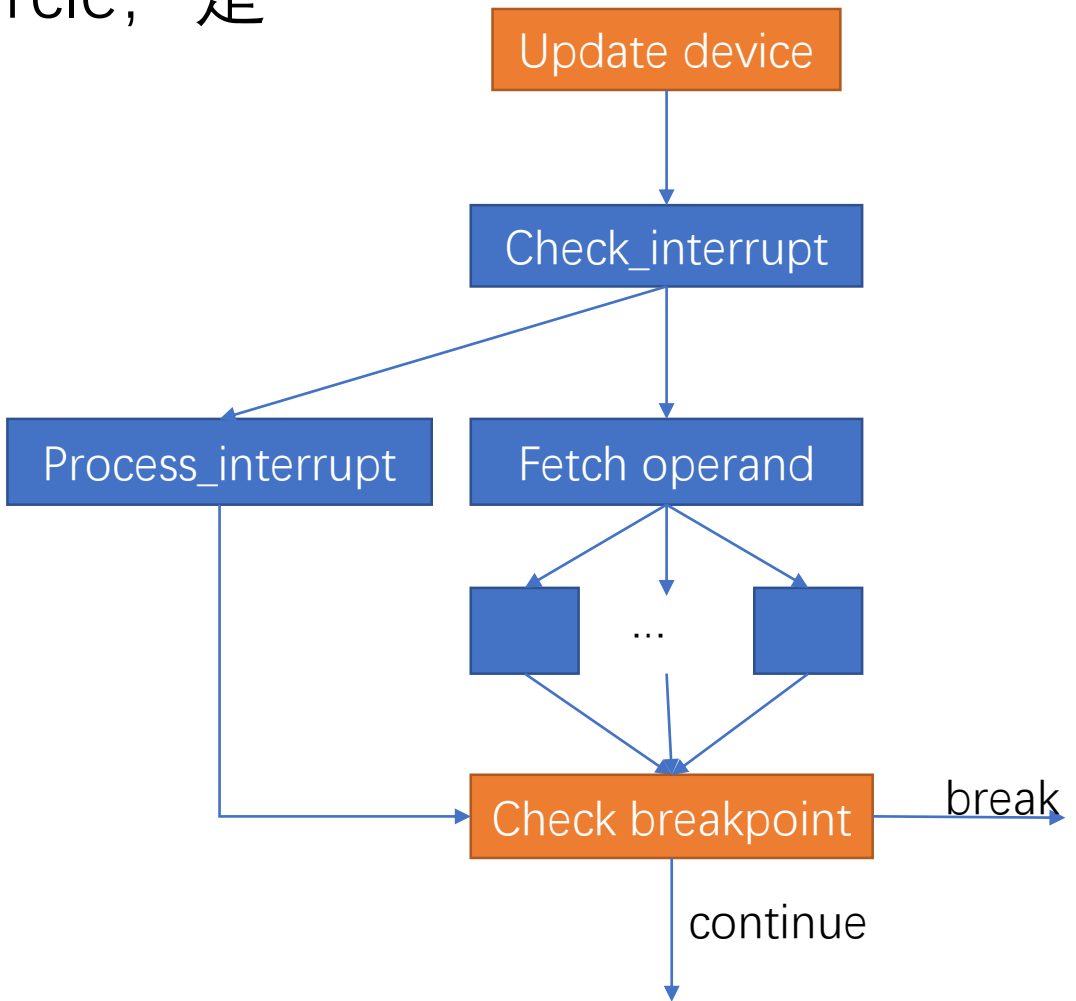
- 指令的模拟执行
- IO与中断
- 运行过程显示
- 断点与调试
- 反汇编
- 命令处理
- 统计指令数、时钟周期



指令循环

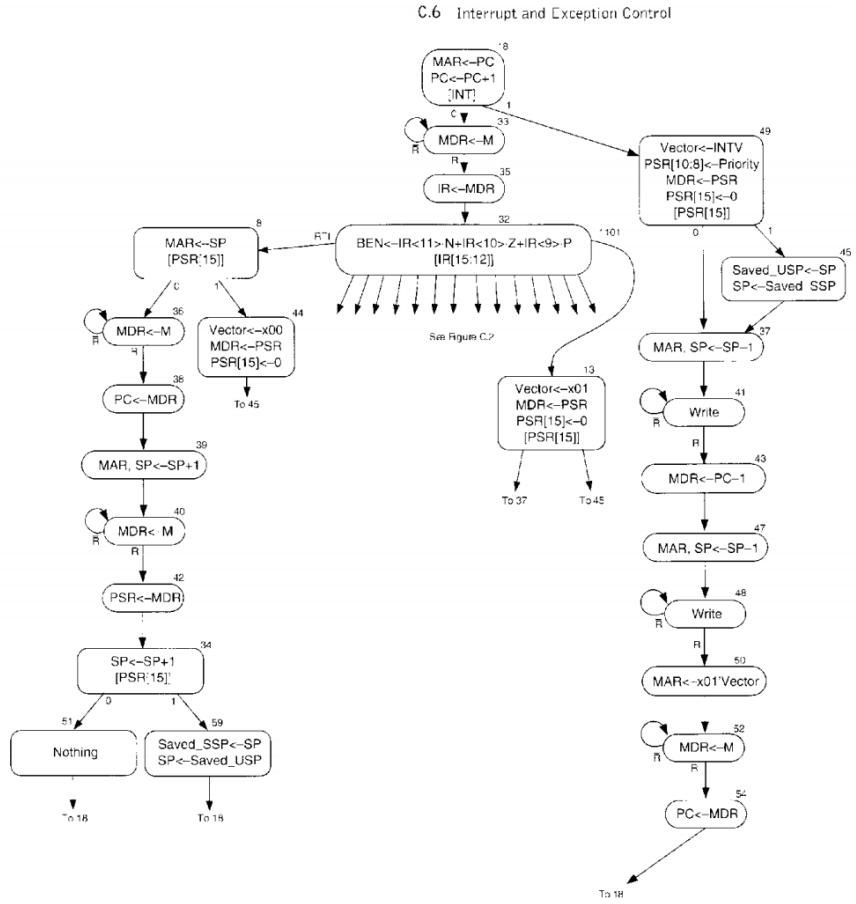
- step_over()执行一个instruction circle，是最基本的执行单元
  - 内部基于状态机的步骤实现





IO与中断

- device()是处理IO设备的函数，它独立于step_over()中，与instruction circle无关。
  - 实现模拟器输入输出的交互
  - 可以多线程实现，也可以每step_over()一次，自动执行一次
- 分为check_interrupt()和process_interrupt()两个函数实现
  - 可参考Fig. c.6



关于LC-3中断的建议

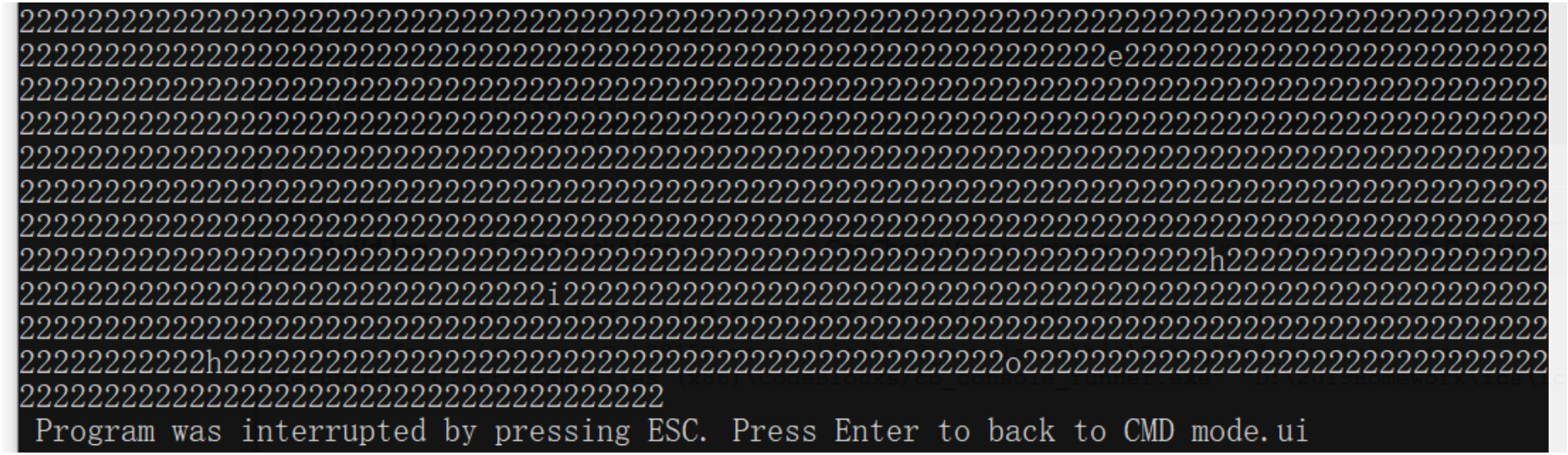
- 使用Saved_USP和Save_SSP来在User栈指针和Supervised栈指针之间切换。如果增加一个SP寄存器，则可以省去两个Saved_USP和Save_SSP，减少一个时钟周期。

- 中断 routine 中应当禁止使用 TRAP。TRAP是非栈的调用，如果出现某个TRAP routine正在执行时中断，而这个中断又调用TRAP指令，R7被覆盖，TRAP指令将无法返回

  - E.G. TRAP routine x21->INT routine->TRAP routine x21,
    A priviledge exception occurs!

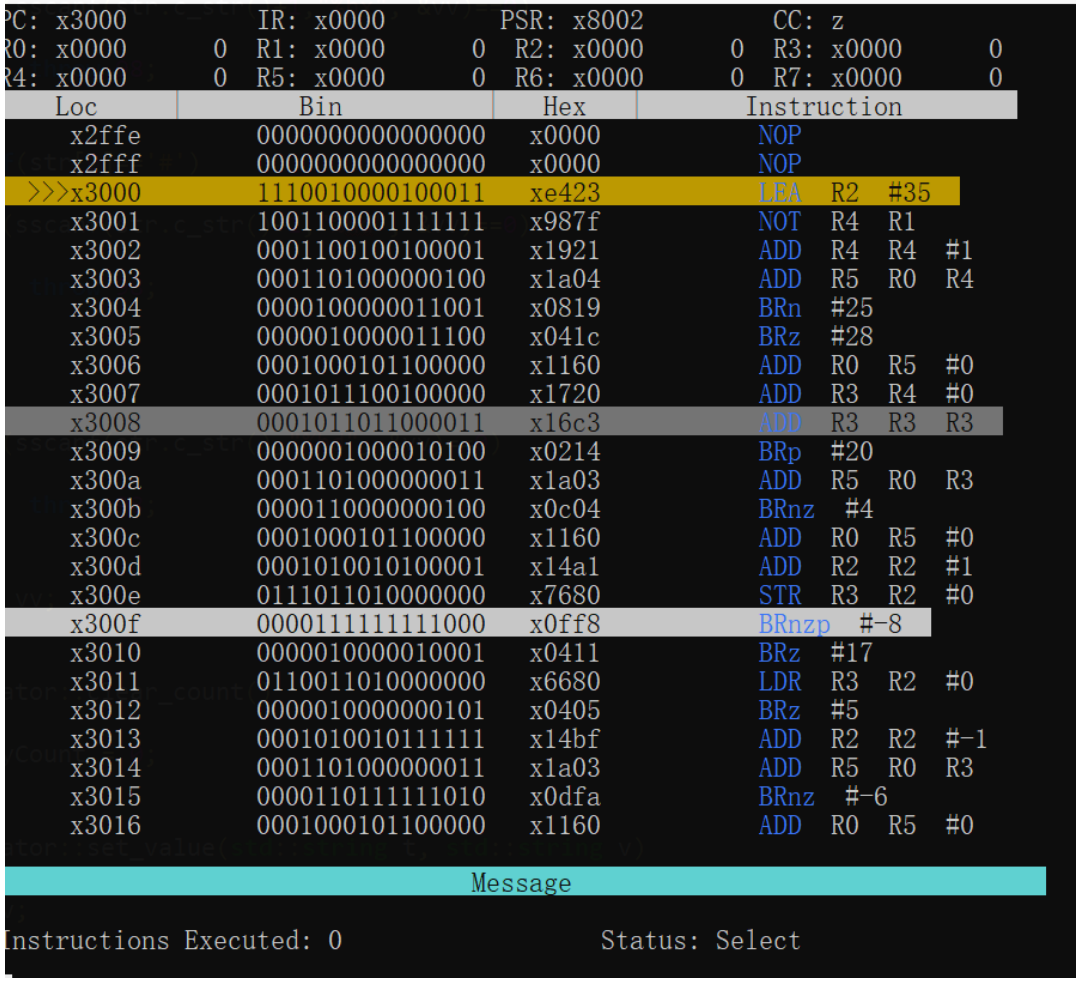
断点与调试

- 为模拟器设置多种状态{Normal, Breakpoint,…}在step_over()中加入对状态的检查，在断点处暂停执行。
- 允许用户终止程序执行，允许用户在运行过程中按ESC停止模拟，防止陷入死循环。



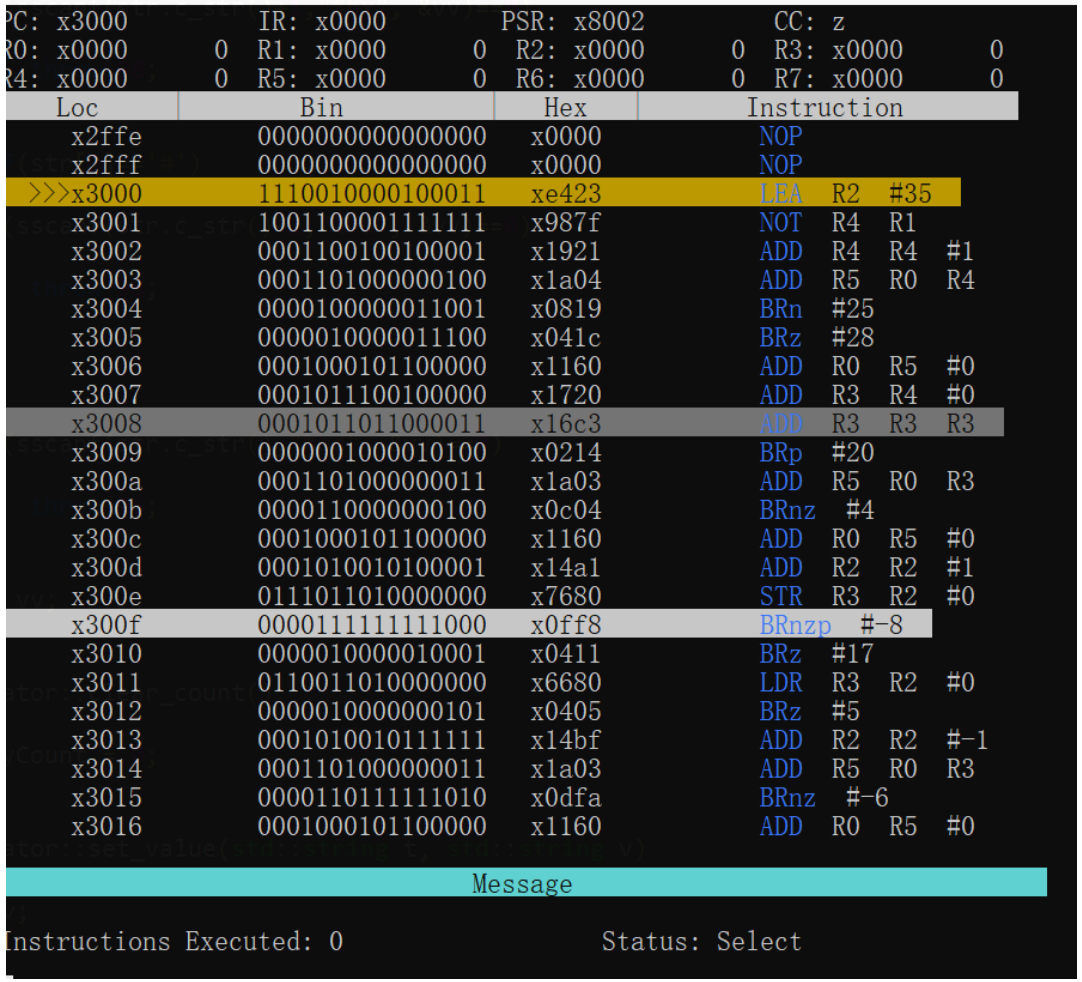
反汇编

- 反汇编能够使得程序更清晰。



滚动模式

- 允许上下选择
- 跳转提示特色功能，当选中BR指令时，会提示跳转位置。

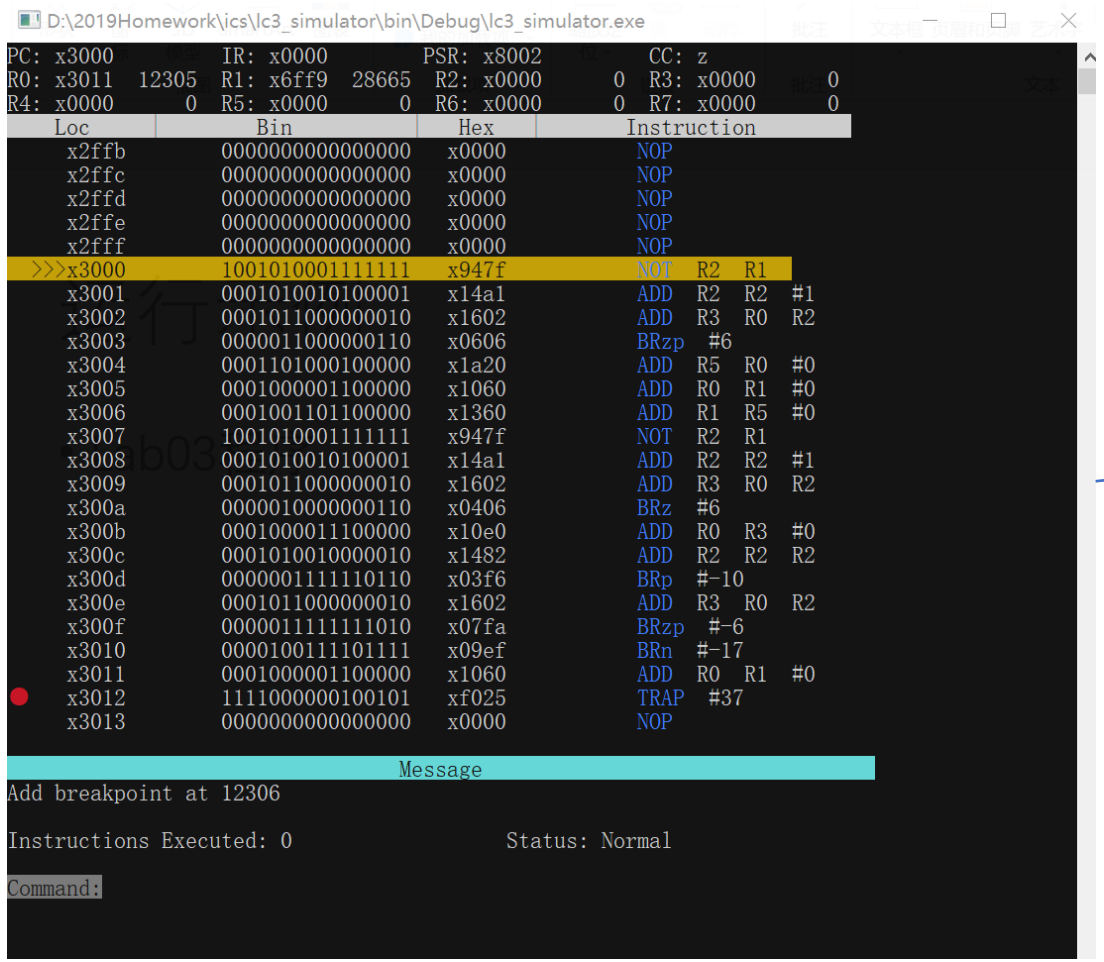


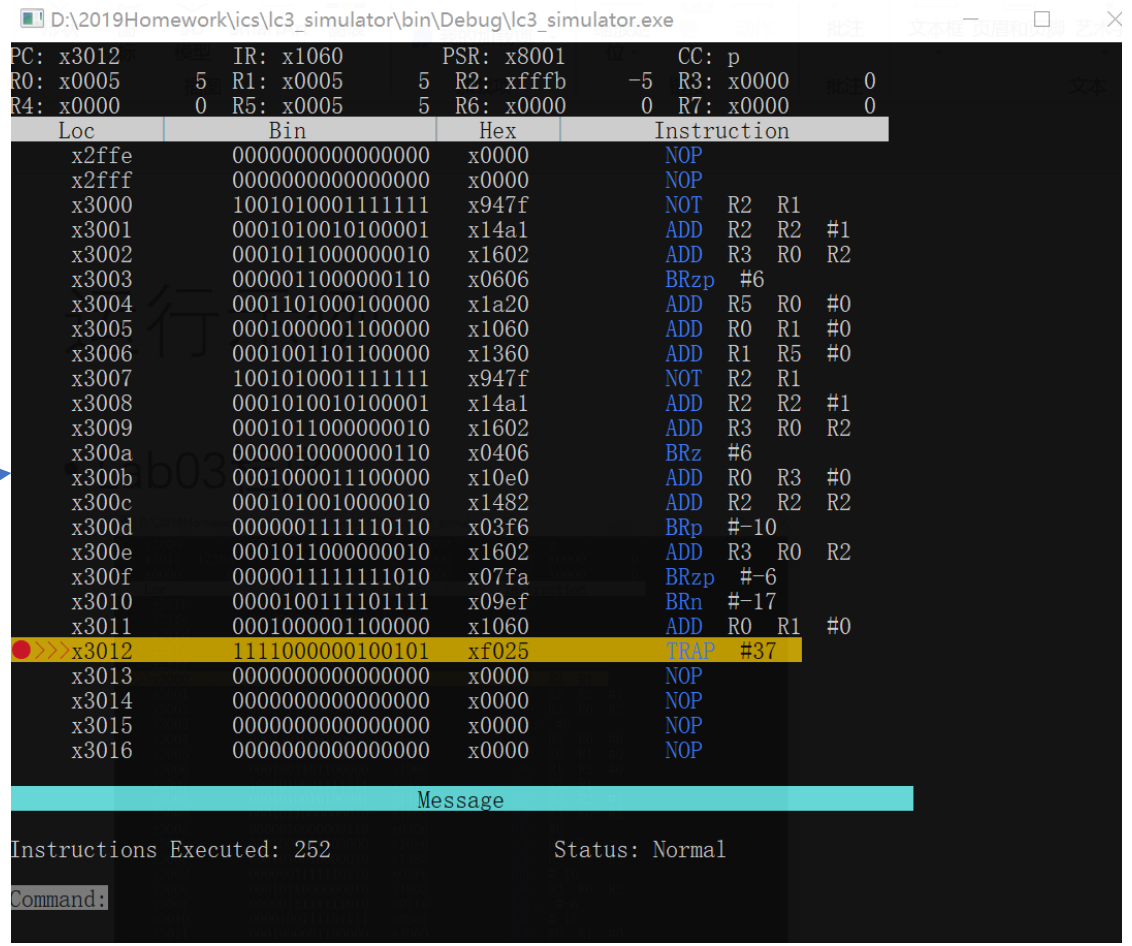
主要命令

命令	作用
showmem/smm	显示某一块内存。若为指明那一块，则自动跟踪PC显示。
setvalue/setv/sv	设置寄存器或内存的值
load	加载.bin .obj .hex文件
n/nn/nnn…	单步执行（若干次）
run	运行程序。运行时可以按下ESC终止。
view/w	进入选择模式，可以在上下滚动内存选择查看，以及提示
setbk/sbk	设置断点
cancelbk/cbk	取消断点(cabk命令取消所有断点)
clearcount/cc	清除计数
reset	重置模拟器
exit	退出模拟器

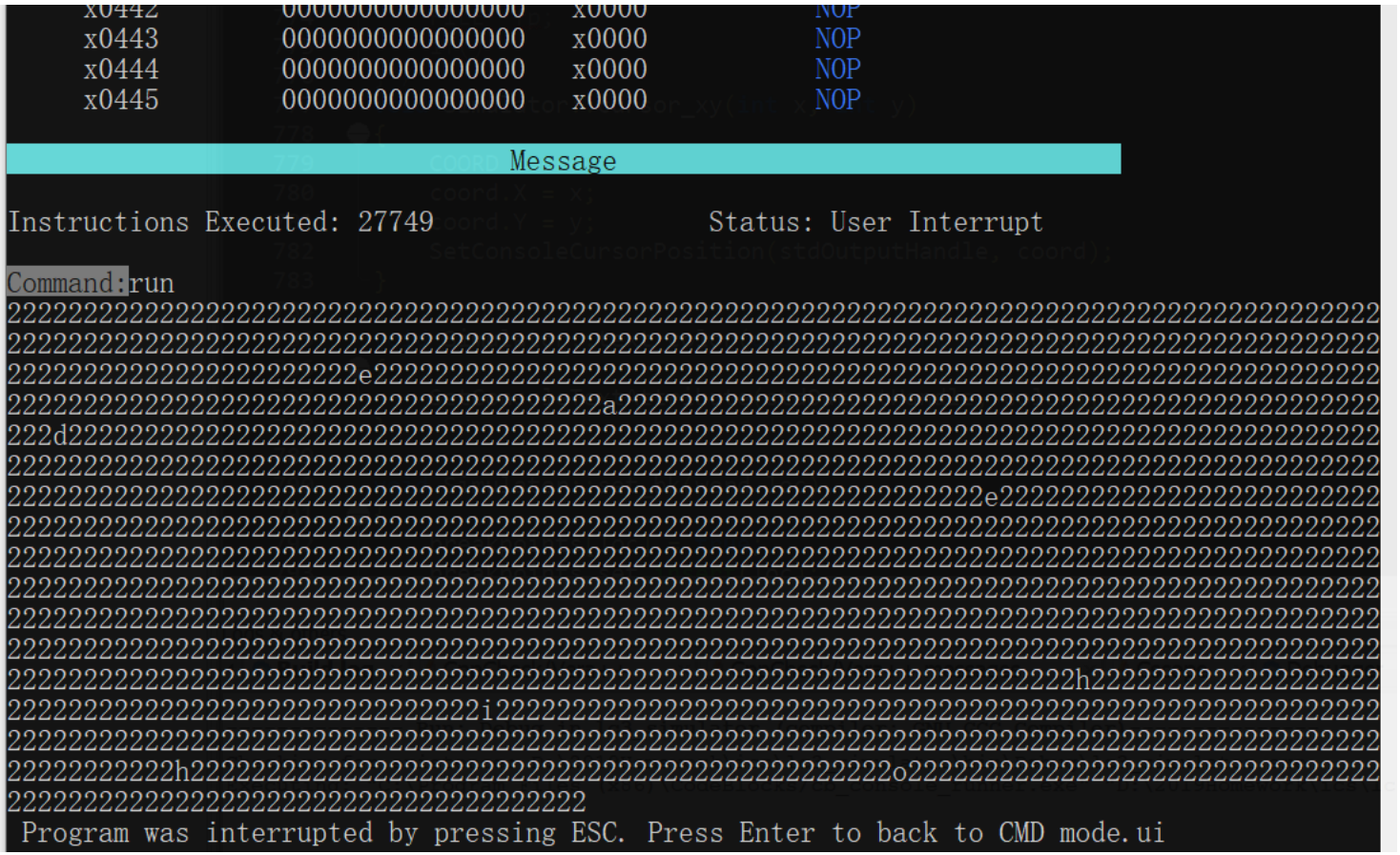
运行示例

- Lab03程序





- 中断测试


x0443 0000000000000000 x0000 NOP
x0444 0000000000000000 x0000 NOP
x0445 0000000000000000 x0000 NOP
Message
Instructions Executed: 27749 Status: User Interrupt
Command:run
Program was interrupted by pressing ESC. Press Enter to back to CMD mode.ui

- 谢谢