

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

The screenshot shows the lc3_simulator.exe window with the following content:

Registers: PC: x3000, IR: x0000, PSR: x8002, CC: z, R0: x3011, R1: x6fff, R2: x0000, R3: x0000, R4: x0000, R5: x0000, R6: x0000, R7: x0000.

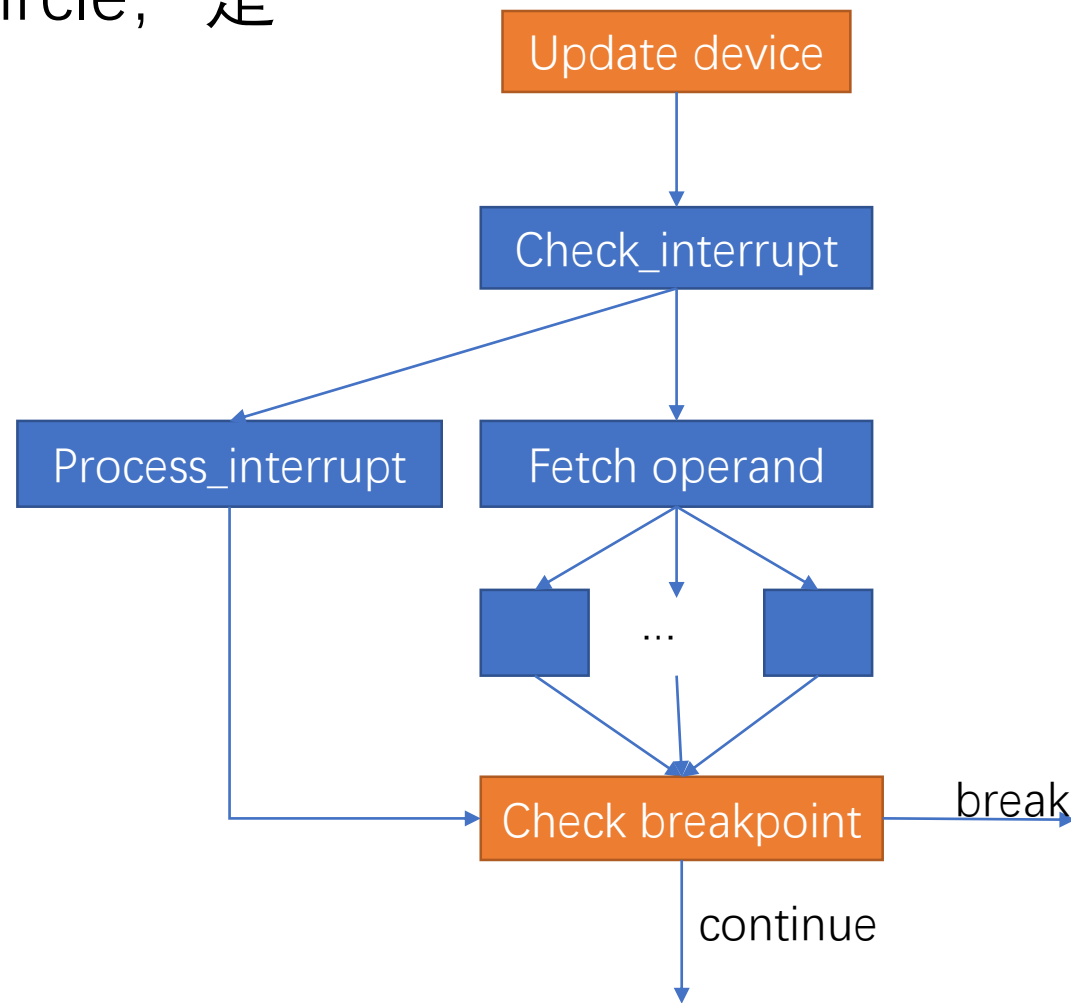
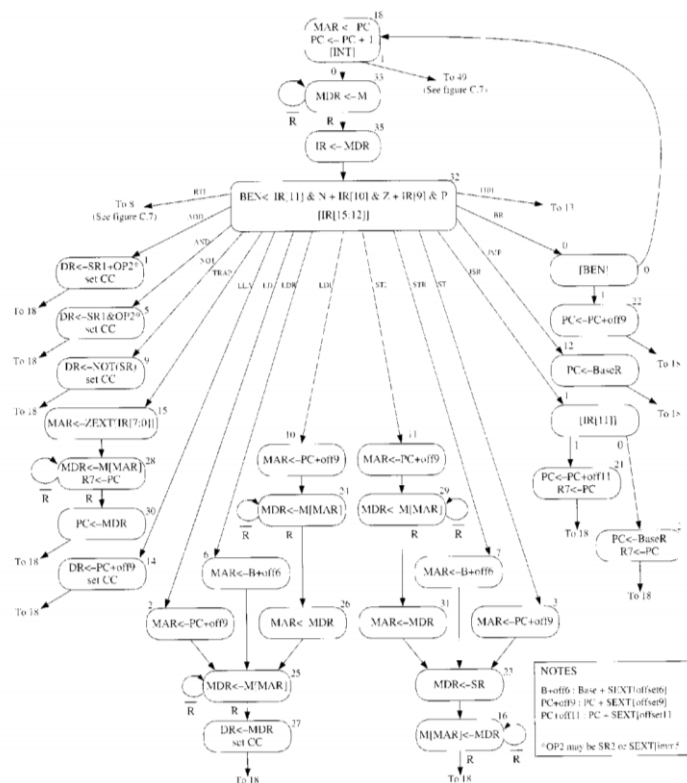
Loc	Bin	Hex	Instruction
x2ffb	0000000000000000	x0000	NOP
x2ffc	0000000000000000	x0000	NOP
x2ffd	0000000000000000	x0000	NOP
x2ffe	0000000000000000	x0000	NOP
x2fff	0000000000000000	x0000	NOP
>>>x3000	1001010001111111	x947f	NOT R2 R1
x3001	0001010010100001	x14a1	ADD R2 R2 #1
x3002	0001011000000010	x1602	ADD R3 R0 R2
x3003	0000011000000110	x0606	BRzp #6
x3004	0001101000100000	x1a20	ADD R5 R0 #0
x3005	0001000001100000	x1060	ADD R0 R1 #0
x3006	0001001101100000	x1360	ADD R1 R5 #0
x3007	1001010001111111	x947f	NOT R2 R1
x3008	0001010010100001	x14a1	ADD R2 R2 #1
x3009	0001011000000010	x1602	ADD R3 R0 R2
x300a	0000010000000110	x0406	BRz #6
x300b	0001000011100000	x10e0	ADD R0 R3 #0
x300c	0001010010000010	x1482	ADD R2 R2 R2
x300d	0000001111110110	x03f6	BRp #-10
x300e	0001011000000010	x1602	ADD R3 R0 R2
x300f	0000011111110101	x07fa	BRzp #-6
x3010	0000100111101111	x09ef	BRn #-17
x3011	0001000001100000	x1060	ADD R0 R1 #0
x3012	1111000000100101	xf025	TRAP #37
x3013	0000000000000000	x0000	NOP

Message: Instructions Executed: 0 Status: Normal

Command:

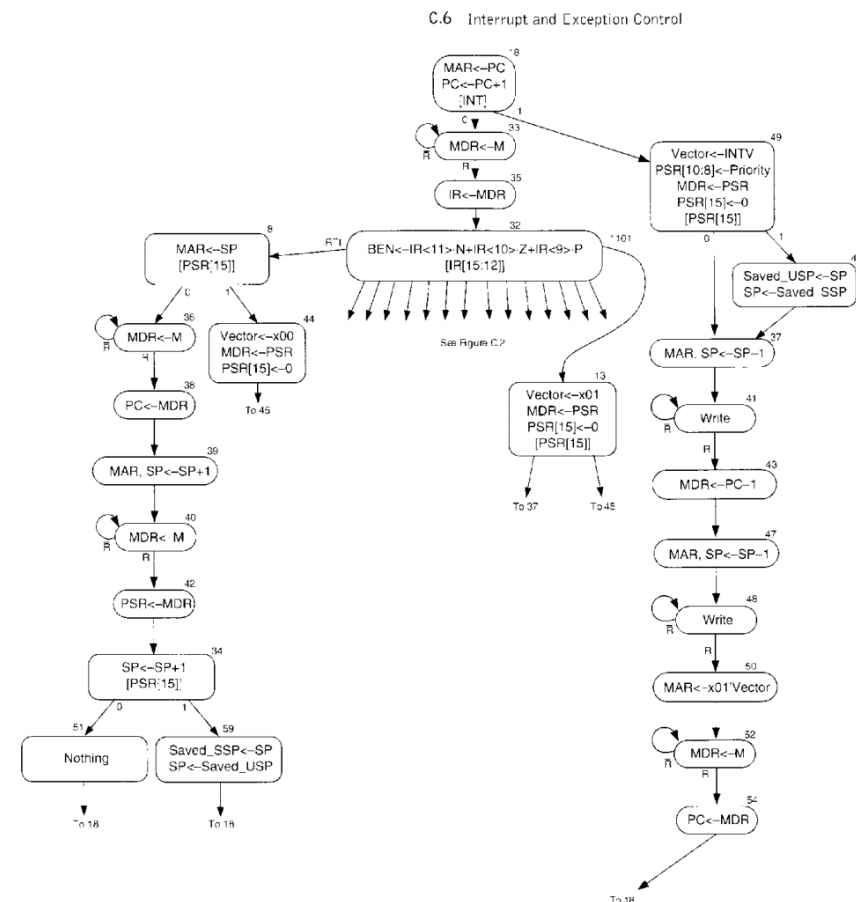
指令循环

- `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 privilege 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。

```

                e                h                i                o
Program was interrupted by pressing ESC. Press Enter to back to CMD mode.ui
```

反汇编

- 反汇编能够使得程序更清晰。

PC: x3000	IR: x0000	PSR: x8002	CC: z	
R0: x0000	0 R1: x0000	0 R2: x0000	0 R3: x0000	0
R4: x0000	0 R5: x0000	0 R6: x0000	0 R7: x0000	0
Loc	Bin	Hex	Instruction	
x2ffe	0000000000000000	x0000	NOP	
x2fff	0000000000000000	x0000	NOP	
>>>x3000	1110010000100011	xe423	LEA R2 #35	
x3001	1001100001111111	x987f	NOT R4 R1	
x3002	0001100100100001	x1921	ADD R4 R4 #1	
x3003	0001101000000100	x1a04	ADD R5 R0 R4	
x3004	0000100000011001	x0819	BRn #25	
x3005	0000010000011100	x041c	BRz #28	
x3006	0001000101100000	x1160	ADD R0 R5 #0	
x3007	0001011100100000	x1720	ADD R3 R4 #0	
x3008	0001011011000011	x16c3	ADD R3 R3 R3	
x3009	0000001000010100	x0214	BRp #20	
x300a	0001101000000011	x1a03	ADD R5 R0 R3	
x300b	0000110000000100	x0c04	BRnz #4	
x300c	0001000101100000	x1160	ADD R0 R5 #0	
x300d	0001010010100001	x14a1	ADD R2 R2 #1	
x300e	0111011010000000	x7680	STR R3 R2 #0	
x300f	0000111111111000	x0ff8	BRnzp #-8	
x3010	0000010000010001	x0411	BRz #17	
x3011	0110011010000000	x6680	LDR R3 R2 #0	
x3012	0000010000000101	x0405	BRz #5	
x3013	0001010010111111	x14bf	ADD R2 R2 #-1	
x3014	0001101000000011	x1a03	ADD R5 R0 R3	
x3015	0000110111111010	x0dfa	BRnz #-6	
x3016	0001000101100000	x1160	ADD R0 R5 #0	
Message				
Instructions Executed: 0			Status: Select	

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。

PC: x3000	IR: x0000	PSR: x8002	CC: z	
R0: x0000	0 R1: x0000	0 R2: x0000	0 R3: x0000	0
R4: x0000	0 R5: x0000	0 R6: x0000	0 R7: x0000	0
Loc	Bin	Hex	Instruction	
x2ffe	0000000000000000	x0000	NOP	
x2fff	0000000000000000	x0000	NOP	
>>>x3000	1110010000100011	xe423	LEA	R2 #35
x3001	1001100001111111	x987f	NOT	R4 R1
x3002	0001100100100001	x1921	ADD	R4 R4 #1
x3003	0001101000000100	x1a04	ADD	R5 R0 R4
x3004	0000100000011001	x0819	BRn	#25
x3005	0000010000011100	x041c	BRz	#28
x3006	0001000101100000	x1160	ADD	R0 R5 #0
x3007	0001011100100000	x1720	ADD	R3 R4 #0
x3008	0001011011000011	x16c3	ADD	R3 R3 R3
x3009	0000001000010100	x0214	BRp	#20
x300a	0001101000000011	x1a03	ADD	R5 R0 R3
x300b	0000110000000100	x0c04	BRnz	#4
x300c	0001000101100000	x1160	ADD	R0 R5 #0
x300d	0001010010100001	x14a1	ADD	R2 R2 #1
x300e	0111011010000000	x7680	STR	R3 R2 #0
x300f	0000111111111000	x0ff8	BRnzp	#-8
x3010	0000010000010001	x0411	BRz	#17
x3011	0110011010000000	x6680	LDR	R3 R2 #0
x3012	0000010000000101	x0405	BRz	#5
x3013	0001010010111111	x14bf	ADD	R2 R2 #-1
x3014	0001101000000011	x1a03	ADD	R5 R0 R3
x3015	0000110111111010	x0dfa	BRnz	#-6
x3016	0001000101100000	x1160	ADD	R0 R5 #0
Message				
Instructions Executed: 0			Status: Select	

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

```
D:\2019Homework\ics\lc3_simulator\bin\Debug\lc3_simulator.exe
PC: x3000  IR: x0000  PSR: x8002  CC: z
R0: x3011 12305 R1: x6ff9 28665 R2: x0000 0 R3: x0000 0
R4: x0000 0 R5: x0000 0 R6: x0000 0 R7: x0000 0
```

Loc	Bin	Hex	Instruction
x2ffb	0000000000000000	x0000	NOP
x2ffc	0000000000000000	x0000	NOP
x2ffd	0000000000000000	x0000	NOP
x2ffe	0000000000000000	x0000	NOP
x2fff	0000000000000000	x0000	NOP
>>>x3000	1001010001111111	x947f	NOT R2 R1
x3001	0001010010100001	x14a1	ADD R2 R2 #1
x3002	0001011000000010	x1602	ADD R3 R0 R2
x3003	0000011000000110	x0606	BRzp #6
x3004	0001101000100000	x1a20	ADD R5 R0 #0
x3005	0001000001100000	x1060	ADD R0 R1 #0
x3006	0001001101100000	x1360	ADD R1 R5 #0
x3007	1001010001111111	x947f	NOT R2 R1
x3008	0001010010100001	x14a1	ADD R2 R2 #1
x3009	0001011000000010	x1602	ADD R3 R0 R2
x300a	0000010000000110	x0406	BRz #6
x300b	0001000011100000	x10e0	ADD R0 R3 #0
x300c	0001010010000010	x1482	ADD R2 R2 R2
x300d	0000001111110110	x03f6	BRp #-10
x300e	0001011000000010	x1602	ADD R3 R0 R2
x300f	000001111111010	x07fa	BRzp #-6
x3010	0000100111101111	x09ef	BRn #-17
x3011	0001000001100000	x1060	ADD R0 R1 #0
x3012	1111000000100101	xf025	TRAP #37
x3013	0000000000000000	x0000	NOP

```
Message
Add breakpoint at 12306
Instructions Executed: 0
Status: Normal
Command:
```

```
D:\2019Homework\ics\lc3_simulator\bin\Debug\lc3_simulator.exe
PC: x3012  IR: x1060  PSR: x8001  CC: p
R0: x0005 5 R1: x0005 5 R2: xffff -5 R3: x0000 0
R4: x0000 0 R5: x0005 5 R6: x0000 0 R7: x0000 0
```

Loc	Bin	Hex	Instruction
x2ffe	0000000000000000	x0000	NOP
x2fff	0000000000000000	x0000	NOP
x3000	1001010001111111	x947f	NOT R2 R1
x3001	0001010010100001	x14a1	ADD R2 R2 #1
x3002	0001011000000010	x1602	ADD R3 R0 R2
x3003	0000011000000110	x0606	BRzp #6
x3004	0001101000100000	x1a20	ADD R5 R0 #0
x3005	0001000001100000	x1060	ADD R0 R1 #0
x3006	0001001101100000	x1360	ADD R1 R5 #0
x3007	1001010001111111	x947f	NOT R2 R1
x3008	0001010010100001	x14a1	ADD R2 R2 #1
x3009	0001011000000010	x1602	ADD R3 R0 R2
x300a	0000010000000110	x0406	BRz #6
x300b	0001000011100000	x10e0	ADD R0 R3 #0
x300c	0001010010000010	x1482	ADD R2 R2 R2
x300d	0000001111110110	x03f6	BRp #-10
x300e	0001011000000010	x1602	ADD R3 R0 R2
x300f	000001111111010	x07fa	BRzp #-6
x3010	0000100111101111	x09ef	BRn #-17
x3011	0001000001100000	x1060	ADD R0 R1 #0
>>>x3012	1111000000100101	xf025	TRAP #37
x3013	0000000000000000	x0000	NOP
x3014	0000000000000000	x0000	NOP
x3015	0000000000000000	x0000	NOP
x3016	0000000000000000	x0000	NOP

```
Message
Instructions Executed: 252
Status: Normal
Command:
```

- 中断测试

[illegible]

- 谢谢