ESET 349 – Microcontroller Architecture

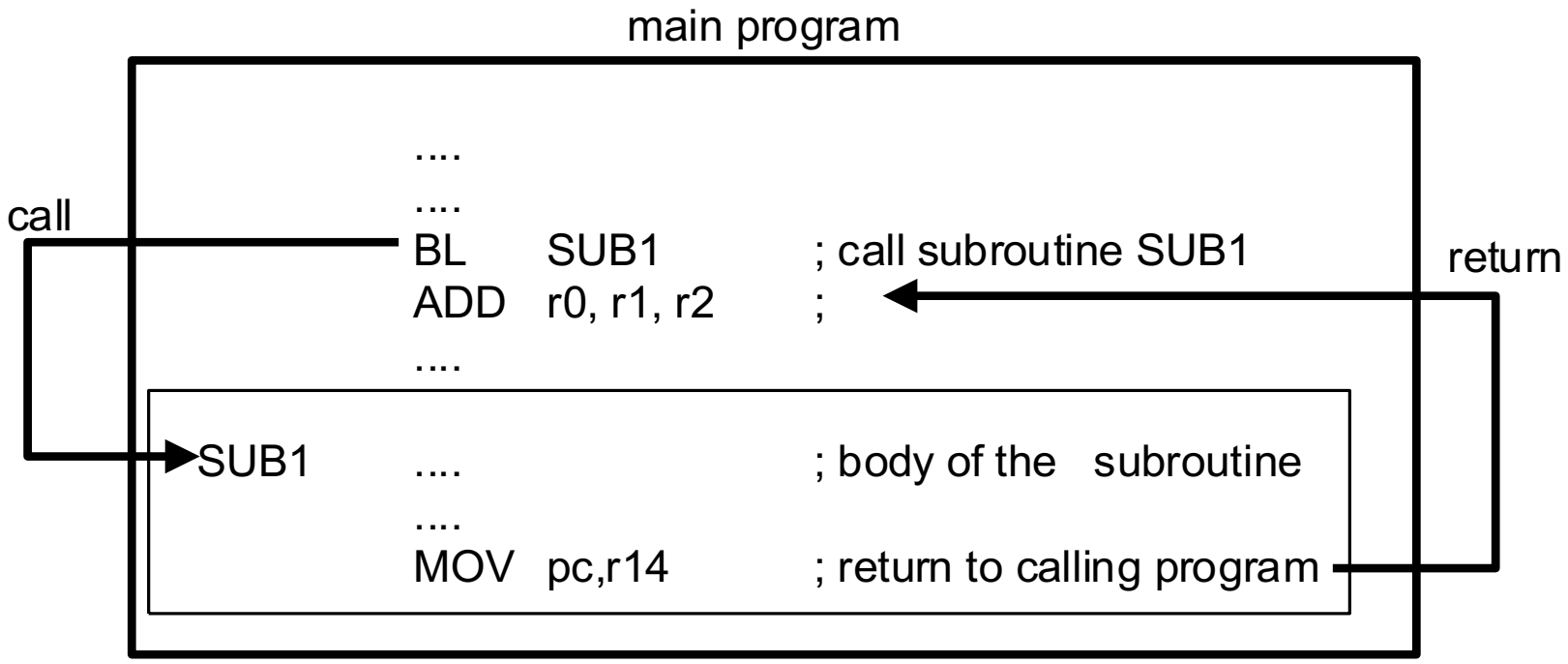
Subroutine

Dr. Muhammad Faeyz Karim

Subroutine (1)

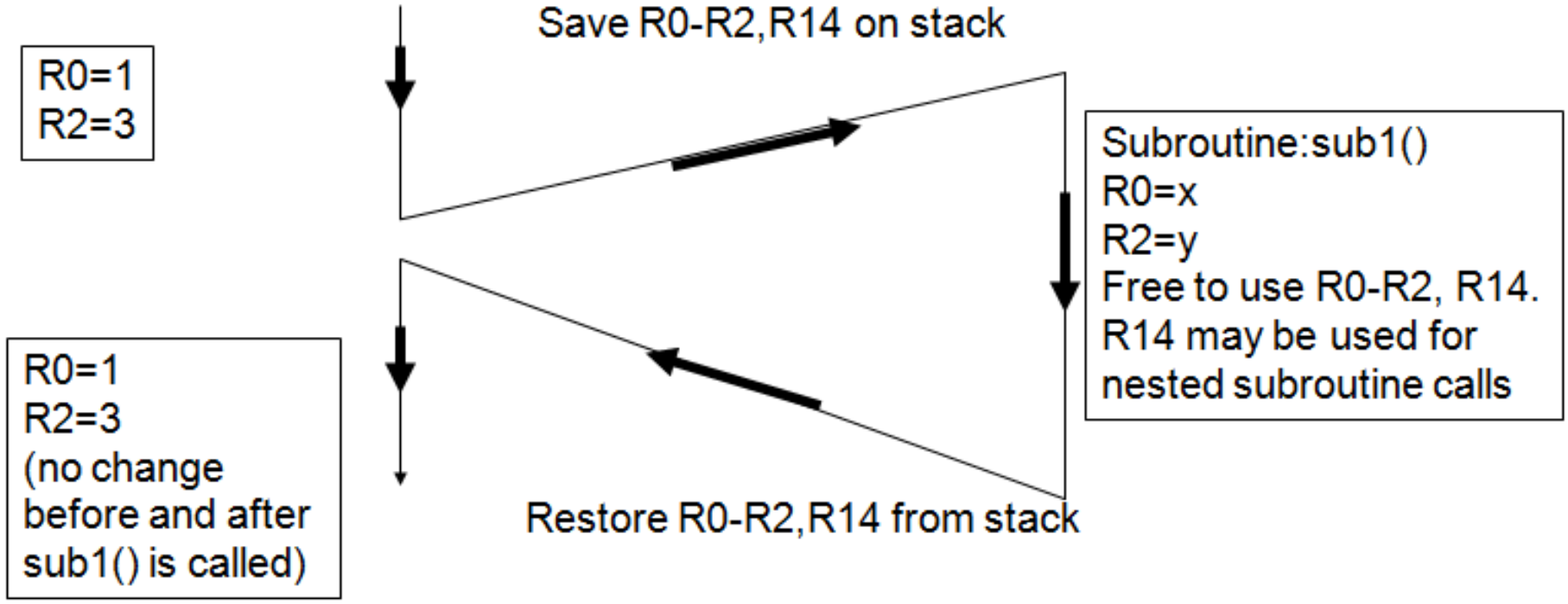
- Good software engineering strategy → divide and conquer
- Hence, large programs consist of many smaller subroutines
- Call with BL (branch and link) instruction
  - Transfers return address (address after the BL instruction) to link register lr (r14)
  - lr = pc – 4, why?
  - Transfers branch target (starting address of subroutine) to program counter pc (r15)

Subroutine (2)



Subroutine (3)

Example



Use stack to save/restore registers so as to preserve their contents before the call

Exercise On Stack Size

- For this stack size, how many nested subroutines (each sub uses 4x32bits=16 bytes) calls are allowed?
- Total stack size
- =0x488+1
  - $=4x16^2+8x16^1+8x16^0+1$
  - =1024+128+8+1
  - =1161 bytes.
- Total_size / each_call_size =1161/16 =72.6
- So 72 nested calls are allowed
- If you do 73 nested calls, it will result in stack overflow

Example: ARM7 memory map	
Addresses	AREA type
0x4000 FFFF- 0x4000 0489	Data
0x4000 0488- 0x4000 0000	**Stack**
0x0000 7FFF- 0x0000 0000	Code

Review – Branch instructions

- These instructions are used to:
  - branch backward to form loops → for, while loop
  - branch forward in conditional structure → jump
  - branch to subroutine with link option → subroutine call

Branch With Condition

- Signed numbers: B {EQ, NE, GE, LT, GT, LE}
- Unsigned numbers: B {EQ, NE, HS, LO, HI, LS}

Review Of Condition Codes – Signed Numbers

Field Mnemonic	Meaning
EQ	Equal ==
NE	Not equal !=
GE	Signed ≥
LT	Signed <
GT	Signed >
LE	Signed ≤

Review Of Condition Codes – Unsigned Numbers

Field Mnemonic	Meaning
EQ	Equal ==
NE	Not equal !=
CS/HS	Unsigned ≥
CC/LO	Unsigned <
HI	Unsigned >
LS	Unsigned ≤

Branch Link (BL) Instruction

To call a subroutine in ARM, use a Branch Link instruction. The syntax is:

- BL *label* where *label* is usually the label (target address) on the first instruction of the subroutine
- Actions by the BL instruction
  - Copy the return address (address of the instruction after the BL instruction in the calling program) to link register lr (=pc-4)
  - Copy to register pc the target address (label) of the subroutine

Registers Lr (R14) And Pc (R15)

Mode					
User / System	Supervisor	Abort	Undefined	Interrupt	Fast Interrupt
R0	R0	R0	R0	R0	R0
R1	R1	R1	R1	R1	R1
R2	R2	R2	R2	R2	R2
R3	R3	R3	R3	R3	R3
R4	R4	R4	R4	R4	R4
R5	R5	R5	R5	R5	R5
R6	R6	R6	R6	R6	R6
R7	R7	R7	R7	R7	R7
R8	R8	R8	R8	R8	R8_FIQ
R9	R9	R9	R9	R9	R9_FIQ
R10	R10	R10	R10	R10	R10_FIQ
R11	R11	R11	R11	R11	R11_FIQ
R12	R12	R12	R12	R12	R12_FIQ
R13	R13_SVC	R13_ABORT	R13_UNDEF	R13_IRQ	R13_FIQ
R14	R14_SVC	R14_ABORT	R14_UNDEF	R14_IRQ	R14_FIQ
PC	PC	PC	PC	PC	PC
CPSR	CPSR	CPSR	CPSR	CPSR	CPSR
	SPSR	SPSR_ABORT	SPSR_UNDEF	SPSR_IRQ	SPSR_FIQ

= banked register

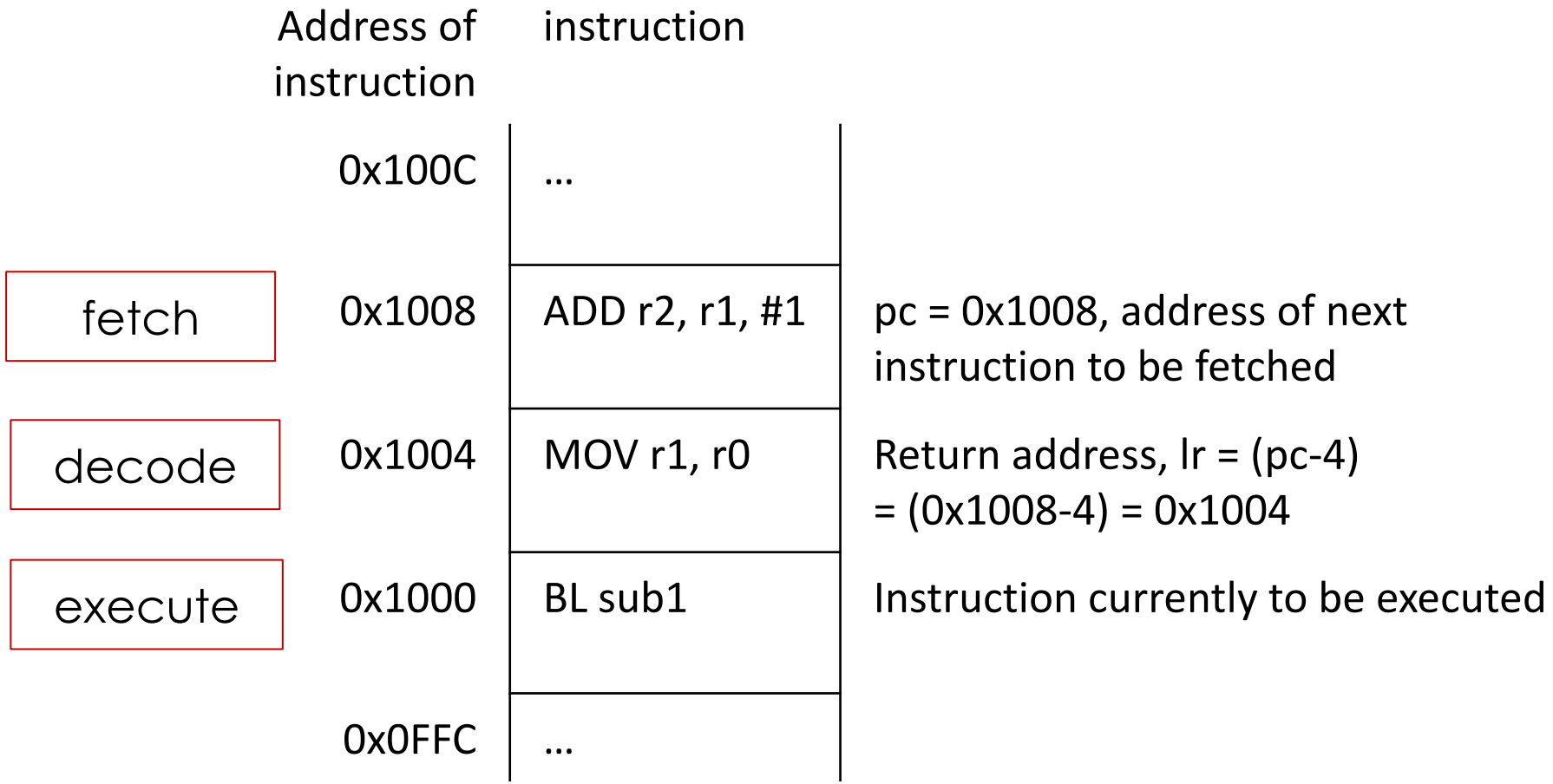
Note:

- There are SIX r14 (lr) registers available in ARM, one for each exception mode.
- There is only ONE register pc

ARM Uses Register Pc (R15) To Fetch The Next Instruction

- Register pc contains the address of the next instruction to be fetched
- The ARM processor uses it to fetch the next instruction
- Hence there is only ONE register pc!
- **By changing the content of register pc, we can change the flow of the program**

The 3-stage Fetch, Decode And Execute Pipeline



Note: each instruction is 4 bytes in size

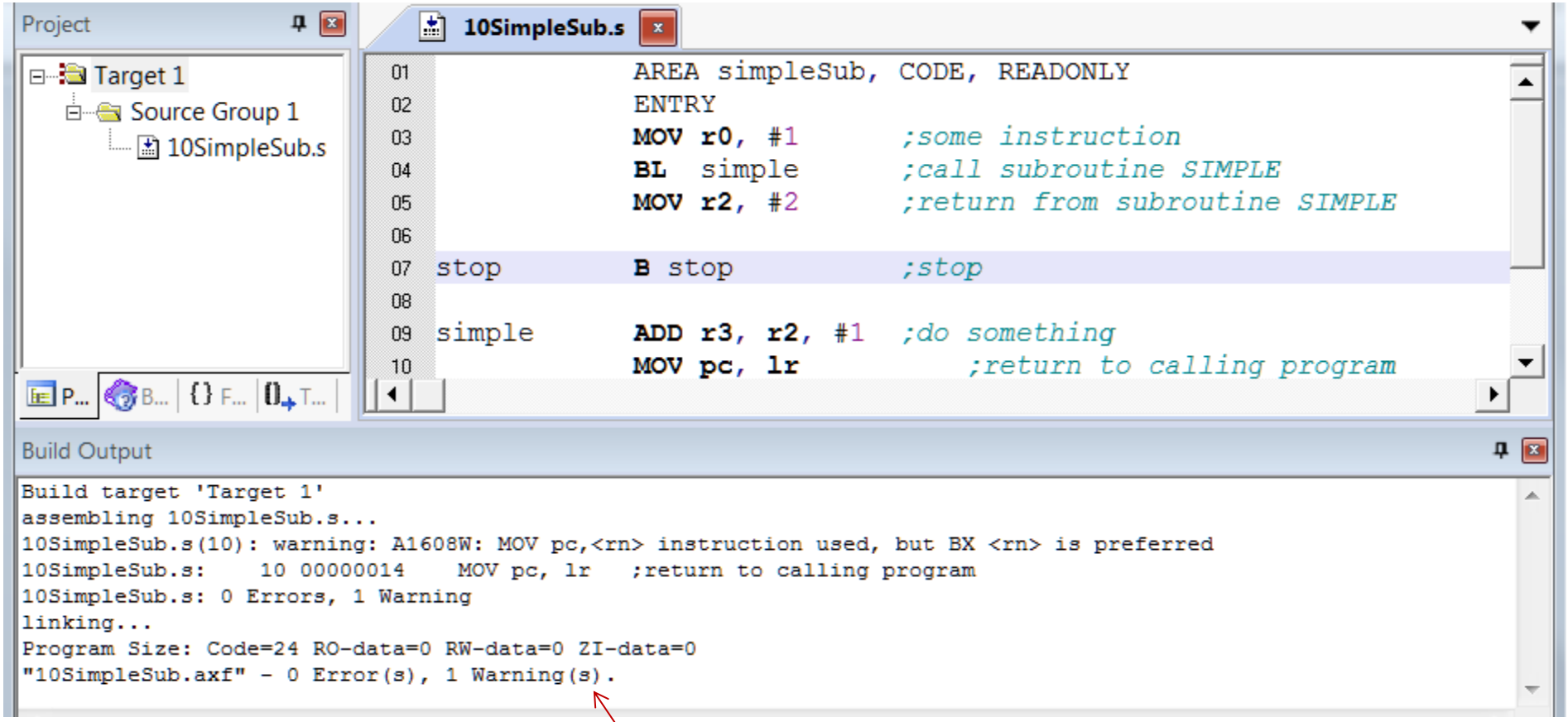
Assume that we have 5 instructions in our program (instr1 to instr5).

Time period	fetch (pc shows address of next instr to be fetched)	decode	execute
1	Instr1 (address=0x0FFC)	-	-
2	Instr2 (address=0x1000)	Instr1 (address=0x0FFC)	-
3	Instr3 (address=0x1004)	Instr2 (address=0x1000)	Instr1 (address=0x0FFC)
4	**Instr4 (address=0x1008)**	**Instr3 (address=0x1004)**	**Instr2 (address=0x1000)**
5	Instr5 (address=0x100C)	Instr4 (address=0x1008)	Instr3 (address=0x1004)
6	-	Instr5 (address=0x100C)	Instr4 (address=0x1008)
7	-	-	Instr5 (address=0x100C)

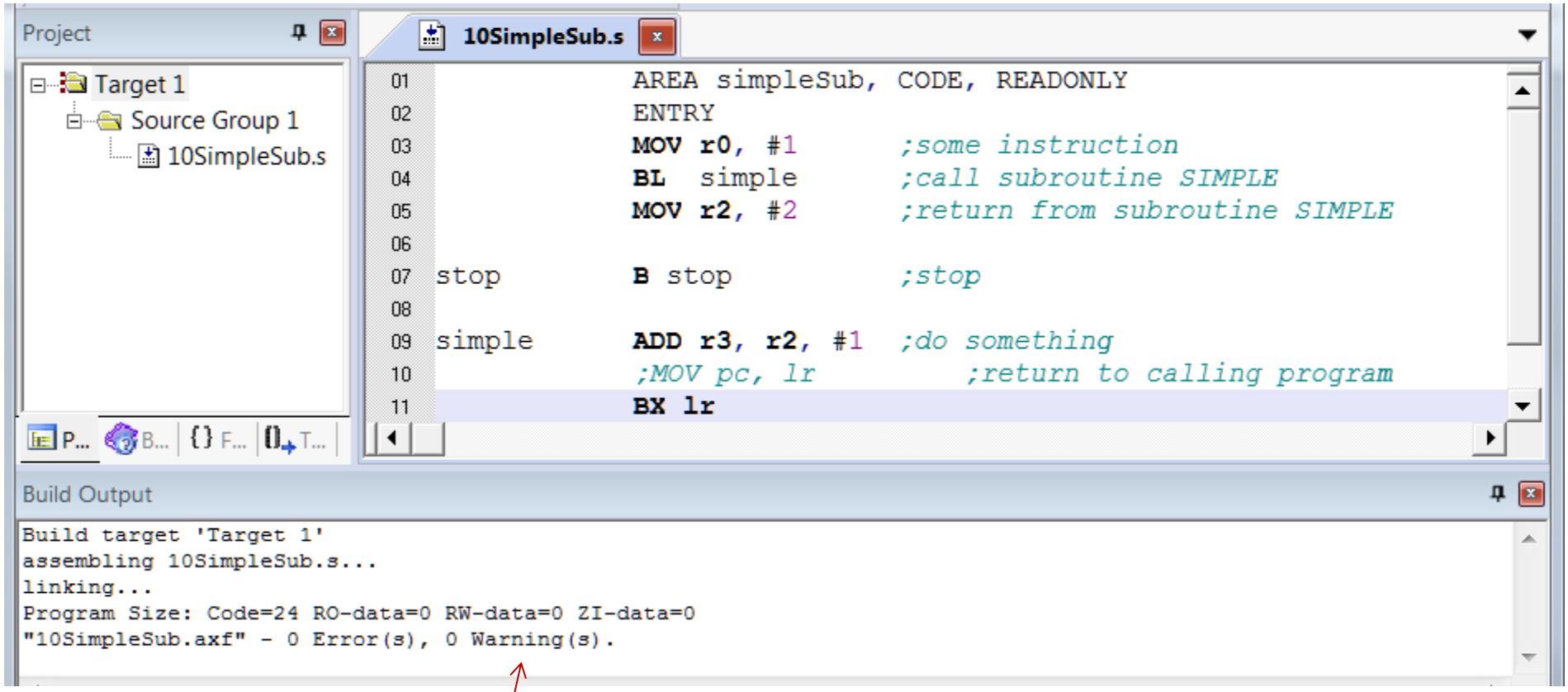
- Assume that Instr2 is our BL sub1 instruction (address = 0x1000).
- While executing this instruction, the processor is about to fetch Instr4 (address = 0x1008, +8 bytes away, 2 instructions away).
- So at this point, register pc = 0x1008 (compare with 0x1000, Instr2 address).
- After finishing the subroutine, we have to return to fetch Instr3 (address = 0x1004, +4 bytes away, 1 instruction away).
- 0x1004 is the return address and has to be stored in register lr before branching.
- Since we only have register pc for reference. Hence, return address is (=pc-4 =0x1008 - 4 =0x1004).
- Hence, before branching to the subroutine, register lr must store this return address, which is (pc-4)!

Return From Subroutine

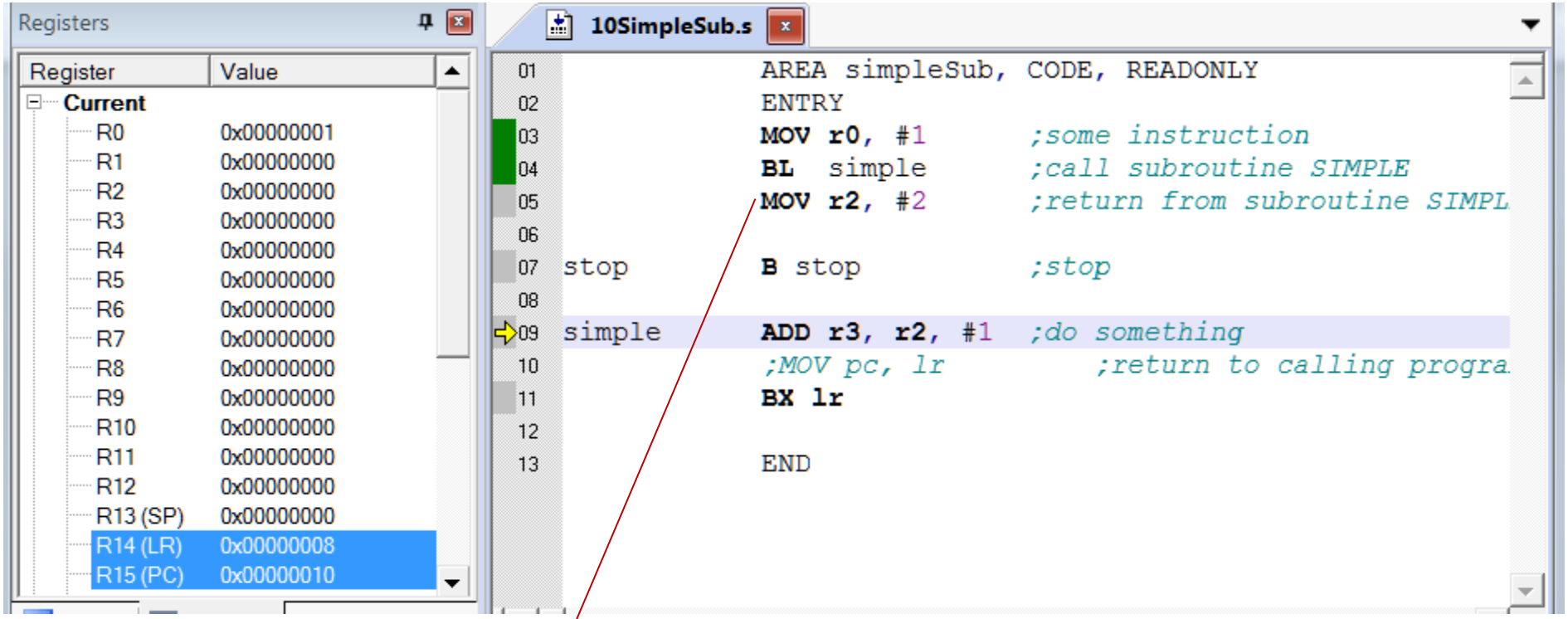
- To return from subroutine, we simply need to copy the content of register lr (r14) to register pc (r15)
- Recall that register lr contains the return address
- This will cause the next instruction to be fetched according to the address stored in pc, which is the return address
- We can use either one of the following instructions
  - MOV pc, lr ;OR
  - BX lr



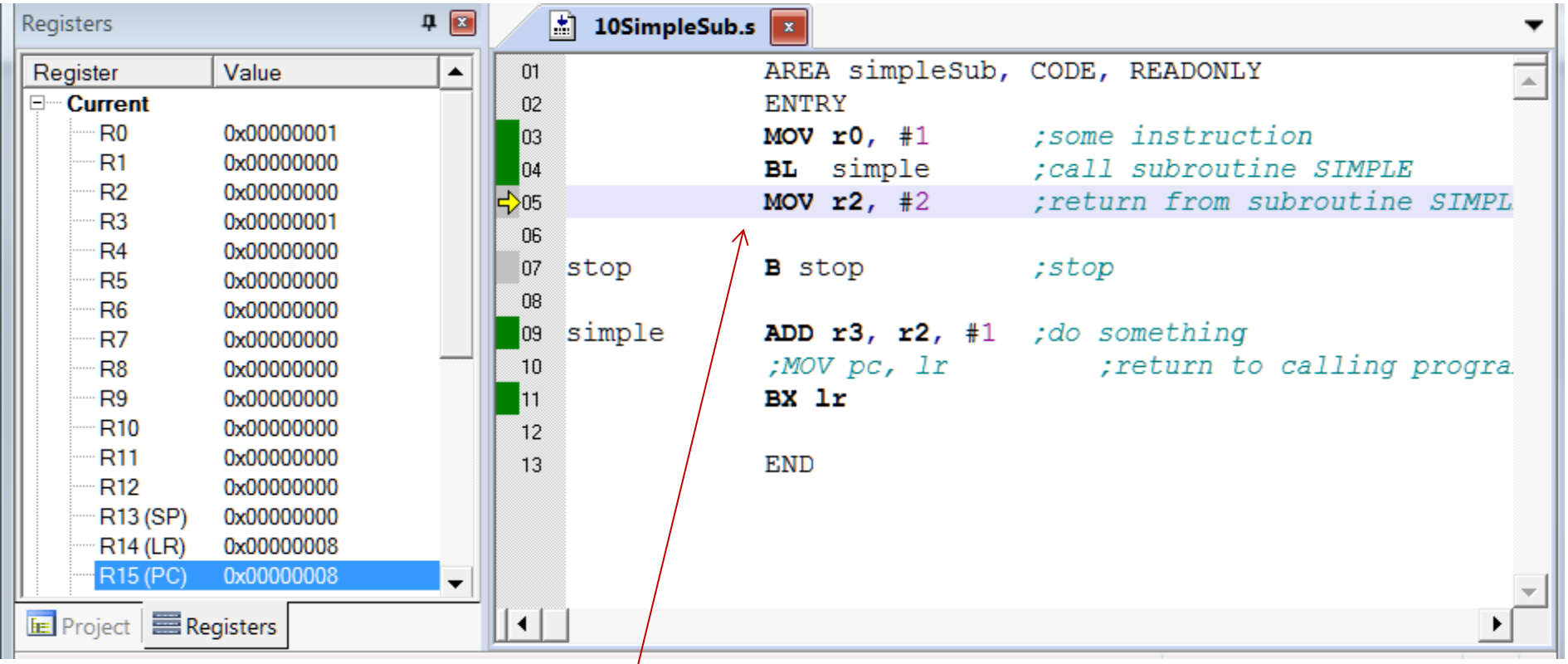
Note the warning!
However, it can still assemble and execute



No warning! If we use BX lr



Return address to lr



Return from subroutine

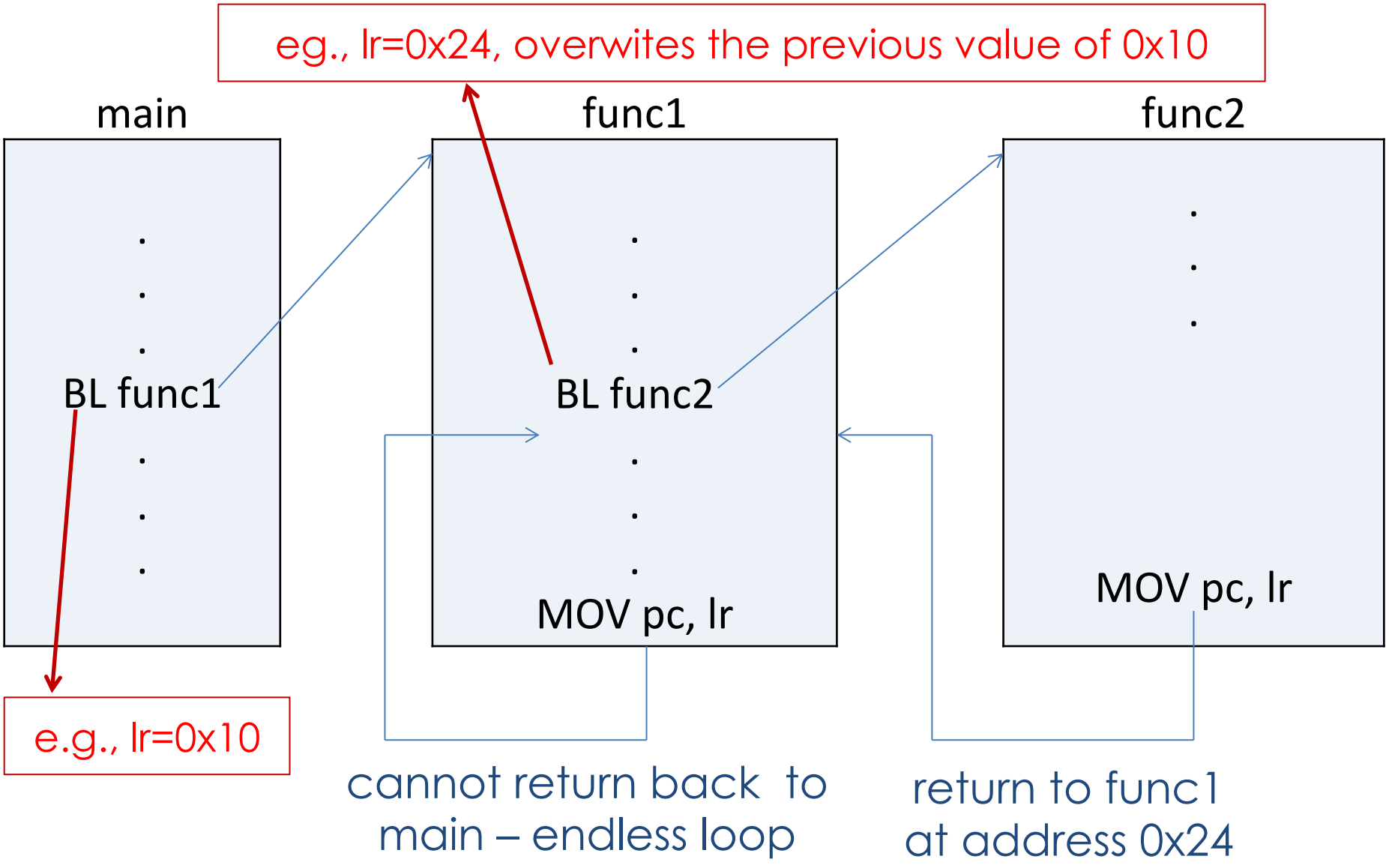
IMPORTANT!!!

- Need to PUSH the content of the link register (lr) to the stack at the start of a subroutine and POP it back to pc before return to calling program for nested subroutine calls that are more than 2 level deep.
- WHY?

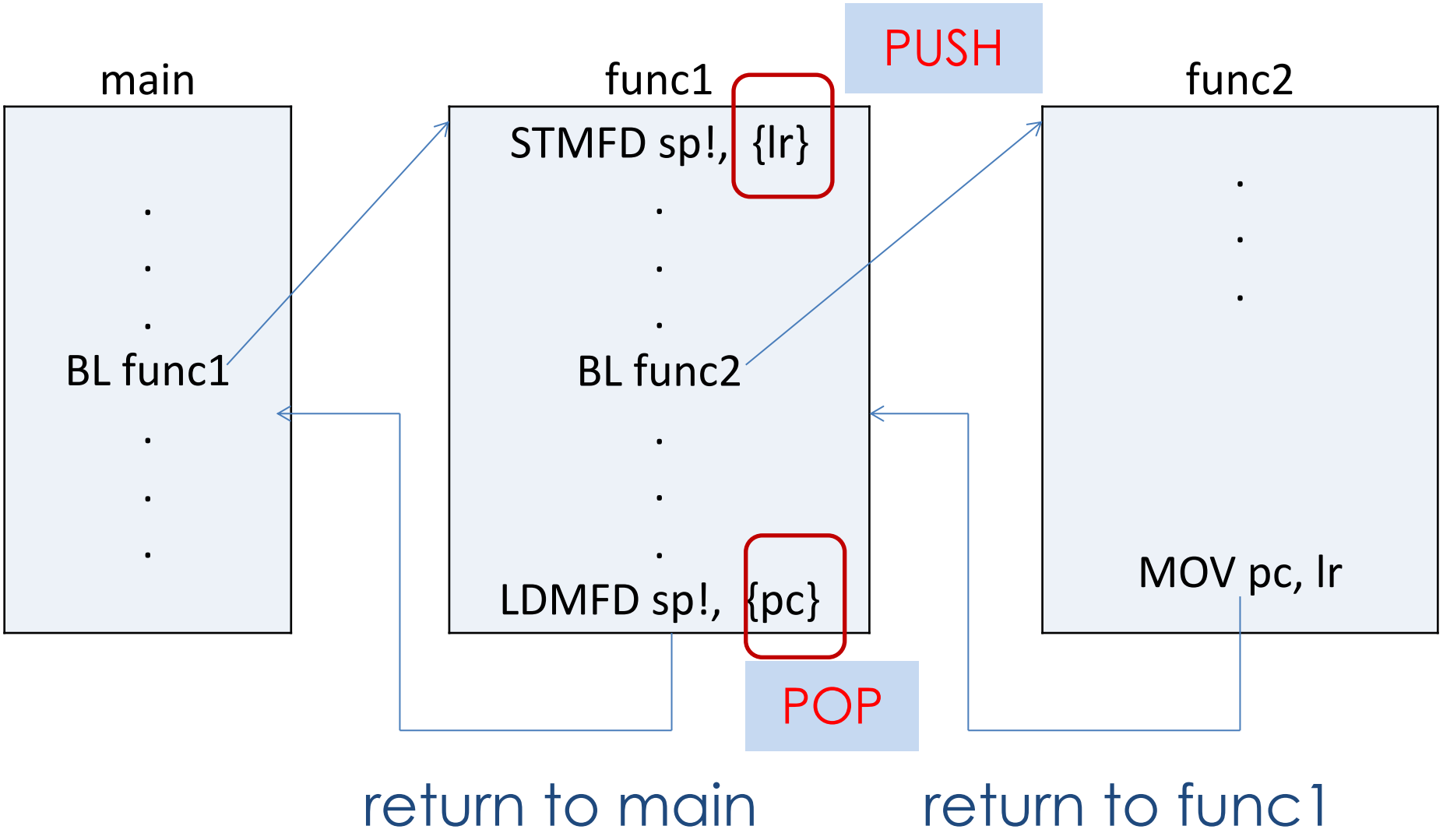
Reason: Else Result In Endless Loop

- Subroutine can call another subroutine
- Next figure shows two nested subroutines, func1 and func2
- If not careful we can get stuck in an infinite loop
- If func1 does not save the content of the link register (lr) at the start, lr will be overwritten when BL func2 is executed (call to func2) within func1
- Upon return from func2 to func1, content in lr is used as return address (address after the BL func2 instruction)
- **When func1 reach the end and wants to return back to main, it cannot return properly!**
- **Instead the instruction after BL func2 will be fetched again**
- **This will result in an endless loop**
- Solve easily by pushing the content of the link register lr at the start of subroutine func1 and pop it to pc at the end of subroutine func1!

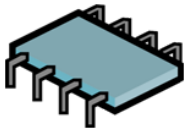
Endless Loop In Nested Subroutine Calls



PUSH The Link Register Lr In Nested Subroutine Calls



Demo – Endless Loop in Nested Subroutine Calls



Registers

Register	Value
Current	
R0	0x00000002
R1	0x00000004
R2	0x000019A1
R3	0x00000051
R4	0x00000000
R5	0x00000000
R6	0x00000000
R7	0x00000000
R8	0x00000000
R9	0x00000000
R10	0x00000000
R11	0x00000000
R12	0x00000000
R13 (SP)	0x00000000
R14 (LR)	0x00000010
R15 (PC)	0x00000018

Project | Registers

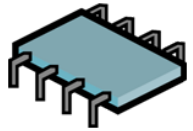
10NestedSubEndlessLoop.s

```
01              AREA NestedSubEL, CODE, READONLY
02              ENTRY
03  main        ;compute (x^3 + 1)^4
04              MOV r0, #2   ;x=2
05              BL  func1    ;call subroutine func1
06  stop        B   stop     ;return from func1
07  func1       ;computer (func2+1)^4
08              BL  func2        ;call subroutine fun
09              ADD r2, r2, #1   ;return from func2, r2=func2+1
10              MUL r3, r2, r2
11              MUL r2, r3, r3   ;r2=(func2+1)^4
12              MOV pc, lr       ;return to main
13  func2       ;computer x^3
14              MUL r1, r0, r0
15              MUL r2, r1, r0   ;r2=x^3
16              MOV pc, lr       ;return to func1
17              END
```

endless loop
cannot return back to main

Demo – SOLVED!

1. PUSH lr to stack at the beginning
2. POP from stack to pc at the end



Registers

Register	Value
Current	
R0	0x00000002
R1	0x00000004
R2	0x000019A1
R3	0x00000051
R4	0x00000000
R5	0x00000000
R6	0x00000000
R7	0x00000000
R8	0x00000000
R9	0x00000000
R10	0x00000000
R11	0x00000000
R12	0x00000000
R13 (SP)	0x40000100
R14 (LR)	0x00000018
R15 (PC)	0x0000000C
CPSR	0x000000D3
SPSR	0x00000000
User/System	

Project | Registers

10NestedSub.s

```
01 ram_base EQU 0x40000000
02          AREA NestedSub, CODE, READONLY
03          ENTRY
04 main     ;compute (x^3 + 1)^4
05          LDR sp, =ram_base + 0x100
06          MOV r0, #2   ;x=2
07          BL  func1    ;call subroutine func1
08 stop     B   stop     ;return from func1
09 func1    ;computer (func2+1)^4
10          STMFD sp!, {lr} ;PUSH lr to stack
11          BL  func2       ;call subroutine fun
12          ADD r2, r2, #1  ;return from func2, r2=func2+1
13          MUL r3, r2, r2
14          MUL r2, r3, r3  ;r2=(func2+1)^4
15          LDMFD sp!, {pc} ;return to main by POP to pc
16 func2    ;computer x^3
17          MUL r1, r0, r0
18          MUL r2, r1, r0  ;r2=x^3
19          MOV pc, lr      ;return to func1
20          END
```

1

2

Passing Parameters To Subroutine

- Subroutines are written as general as possible
- Data or addresses need to be able to move in/out of subroutines → parameters for the subroutine
- Parameters can be passed through registers or stack or a mixture of both
- By convention
  - registers r0-r3 are used to pass input parameters to subroutine
  - register r0 to return result back to the caller
- Use of any other registers (r4-r12) in subroutine
  - PUSH to stack before use → save environment
  - POP from stack before return to caller → restore environment

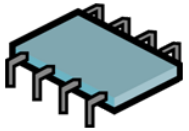
Passing Parameters Through Registers

Calling program	Subroutine
1) Sets some registers to contain inputs	
2) Calls subroutine	
	3) Extract contents from registers that contains inputs
	4) Performs the action of the subroutine
	5) Places the outputs in some registers and return
6) Read from those registers containing outputs	

Passing Parameters Through Registers

- Example: in a subroutine
  - r0 = option: "0" → shift left; "1" → shift right
  - r1 = operand to be shifted
  - r2 = shift m bits
  - r3 = result
  - r4 = temporary register
- 3 parameters (r0, r1, r2) need to be passed to the subroutine
- So its value need to be defined before calling subroutine
- r4 is used as a temporary register in the subroutine, so it must first be stacked before it is used in the subroutine, else the previous value before the call will be corrupted by the subroutine

Demo - Passing Parameters Through Registers (1)



```
ram_base EQU 0x40000000
     AREA PassParaReg, CODE, READONLY
    ENTRY
main
    LDR  sp, =ram_base + 0x100
    MOV r0, #0   ;shift left
    LDR  r1, =0x00012340   ;operand
    MOV r2, #4   ;shift 4 bits
    BL     shiftfunc     ;call subroutine shiftfunc
stop B   stop      ;return from shiftfunc
```

Demo - Passing Parameters Through Registers (2)

```
shiftfunc
    STMFD  sp!, {r4, lr}    ;PUSH r4, lr to stack
    MOV      r4, #0   ;r4 - temporary register
    CMP      r0, r4
    MOVEQ r3, r1, LSL r2    ;r0=0 implies shift left
    MOVNE r3, r1, LSR r2    ;else shift right
    LDMFD  sp!, {r4, pc}    ;POP r4 to restore r4 and
        ;POP lr to pc to return
    END
```

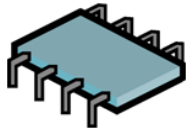
Passing Parameters Through The Stack

- Data is PUSH before the subroutine call
- Subroutine grabs the data from the stack for processing
- Results are stored back into the stack to be retrieved later by the calling program

Passing Parameters through the Stack

Calling program	Subroutine
1) Pushes inputs onto the Stack 2) Calls subroutine	
	3) Extract inputs from the stack (pops) 4) Performs the action of the subroutine 5) Pushes outputs on the stack and return
6) Stack contain outputs (pop) 7) Balance stack	

Demo - Passing Parameters Through The Stack (1)



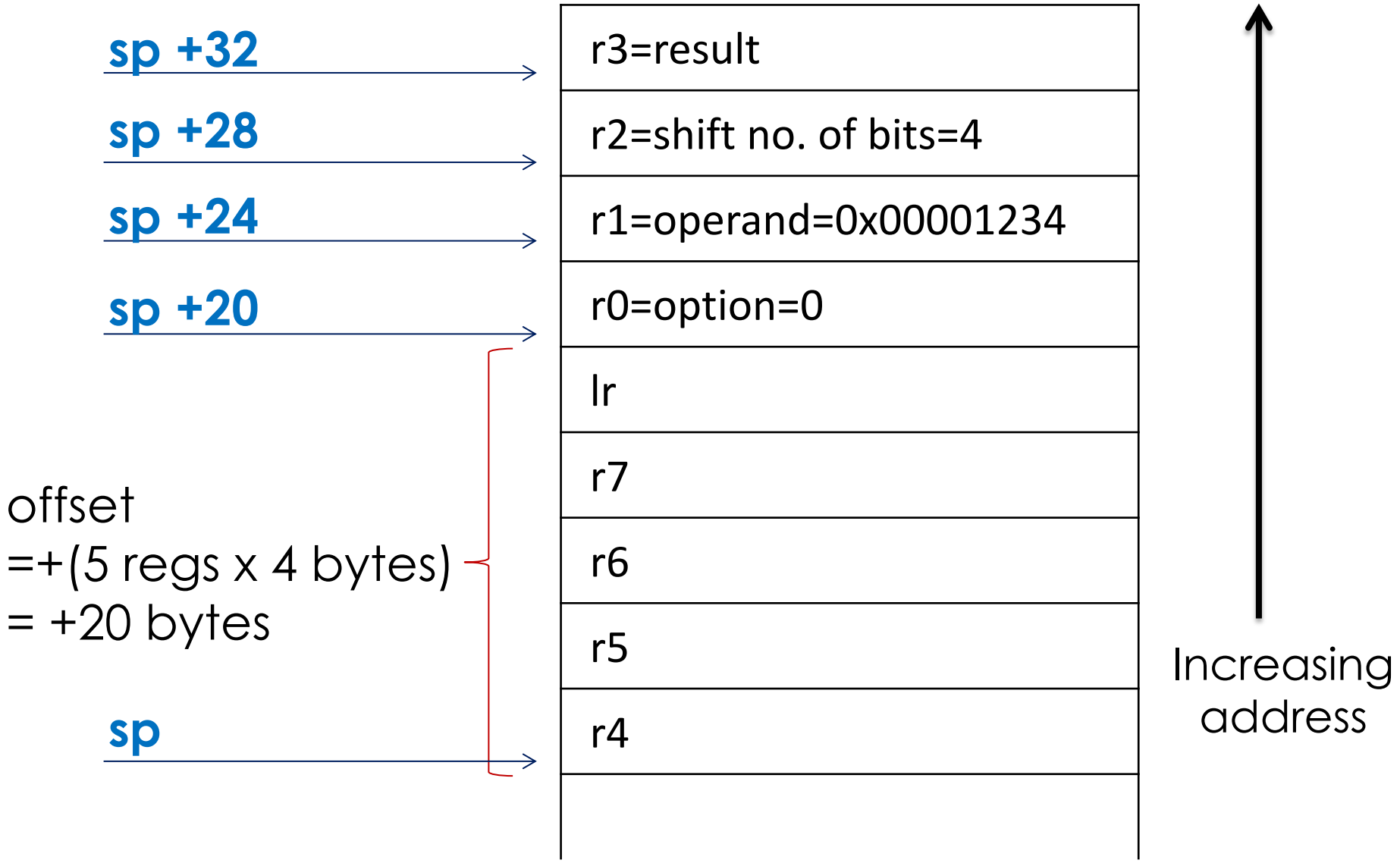
```
ram_base EQU 0x40000000
     AREA PassParaStack, CODE, READONLY
    ENTRY
main
    LDR  sp, =ram_base + 0x100
    MOV r0, #0   ;option=0 implies shift left
    LDR  r1, =0x00001234   ;operand
    MOV r2, #4   ;shift 4 bits

    STMFD sp!, {r0-r3}    ;PUSH in/out parameters to stack
    BL     shiftfunc     ;call subroutine shiftfunc
    LDMFD sp!, {r0-r3}   ;POP in/out parameters from stack
         ;result in r3
stop B   stop      ;return from shiftfunc
```

Demo - Passing Parameters Through The Stack (2)

```
shiftfunc
    STMFD sp!, {r4-r7, lr};PUSH r4-r7, lr to stack (5 regs)
    LDR      r4, [sp, #20]     ;r4=option, offset=5*4=20 bytes
    LDR      r5, [sp, #24]     ;r5=operand
    LDR      r6, [sp, #28]     ;r6=shift no. of bits
    MOV      r7, #0   ;r7 - temporary register
    CMP      r4, r7
    MOVEQ r7, r5, LSL r6    ;r0=0 implies shift left
    MOVNE r7, r5, LSR r6    ;else shift right
    STR      r7, [sp, #32] ;store result in stack
    LDMFD sp!, {r4-r7, pc}  ;POP r4-r7 to restore them and
         ;pop lr to pc to return
    END
```

Content Of Stack In Shiftfunc After 1st Instruction, STMFD Sp!, {R4-r7, Lr}



The ARM APCS (AAPCS)

- Application Procedure Call Standard → a standard
- Defines how subroutines can be separately written, separately compiled and separately assembled
- Contract between subroutine callers and callees
- Standard specifies
  - how parameters be passed to subroutines
  - which registers must have their content preserved (which are corruptible)
  - special roles for certain registers
  - a Full Descending stack pointed by r13 (sp) etc

AAPCS Simplified Specifications

Register	Notes
r0 – r3	Parameters to and results from subroutines. Otherwise may be corrupted.
r4 – r11	Variables. Must be preserved.
r12	Scratch register (corruptible), use by linkers
r13	Stack pointer (sp)
r14	Link register (lr)
r15	Program counter (pc)

Summary

- LDM/STM instructions
- Stacks – FD, FA, ED, EA
- Implementation of PUSH, POP operations using STM and LDM instructions
- Subroutine, calls and return
  - Call instruction – BL label
  - Return instructions
  - Registers sp, pc, lr
- Nested subroutine call
- Parameters Passing
  - Through registers
  - Through stack
  - Standards, AAPCS