

Part E

CHAPTER 3

Architecture and Organization



1

These slides are provided with permission from the copyright for CS2208 use only. The slides must not be reproduced or provided to anyone outside the class.

All downloaded copies of the slides are for personal use only.

Students must destroy these copies within 30 days after receiving the course's final assessment.

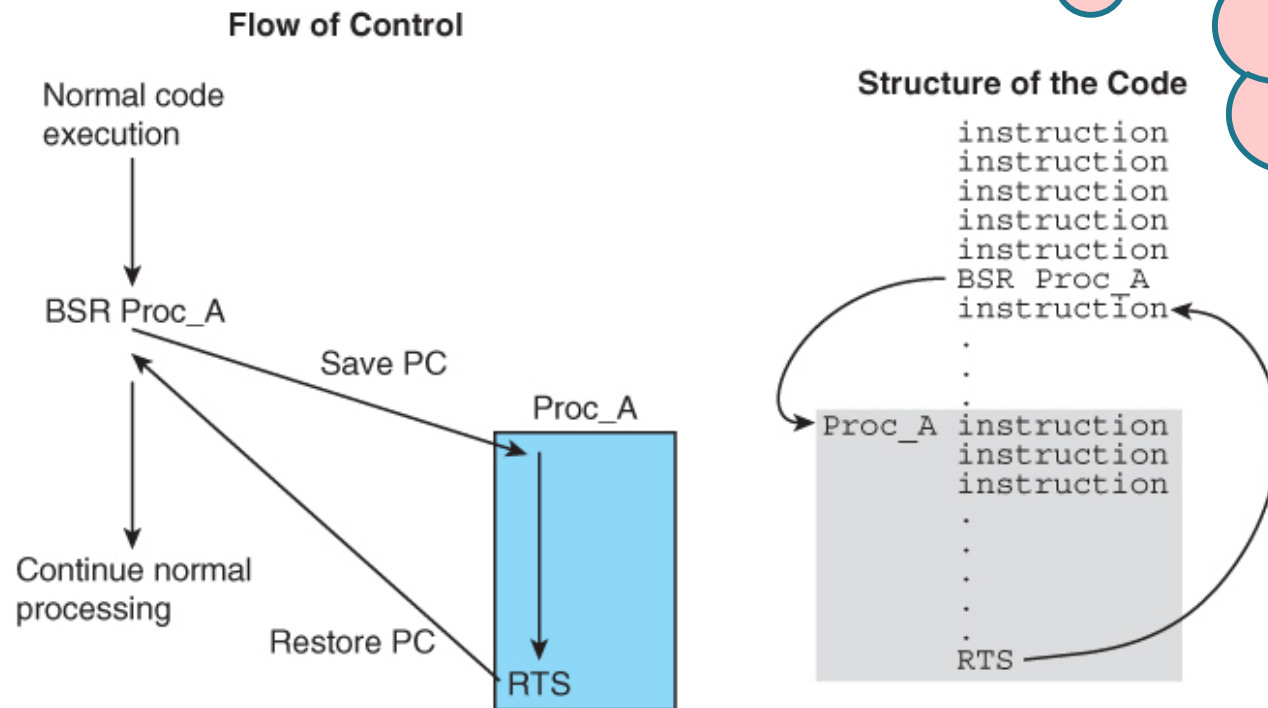
Subroutine Call and Return

- ❑ A *subroutine* (a.k.a. *function*, *procedure*, and *subprogram*) is *a set of instructions* that *may be repeatedly called* by a program to do a given function.
- ❑ A *subroutine* gives the simplest form of program abstraction.
- ❑ There are two main characteristics in any subroutine.
 1. A subroutine can be called from anywhere in the program.
 2. Once the subroutine is completed, it should return to the instruction directly after the subroutine calling location.

Subroutine Call and Return

- ❑ A *hypothetical* instruction *BSR Proc_A* calls subroutine *Proc_A*.
 - The processor **saves the address** of the next instruction to be executed in a safe place, and
 - **loads the program counter** with the address of the first instruction in the subroutine.
- ❑ At the end of the subroutine a *return from subroutine instruction*, *RTS*,
 - causes the processor to **return to the point immediately following the subroutine call**.

FIGURE 3.40 The subroutine call and return



BSR and *RTS*
are not ARM
instructions

ARM Support for Subroutines

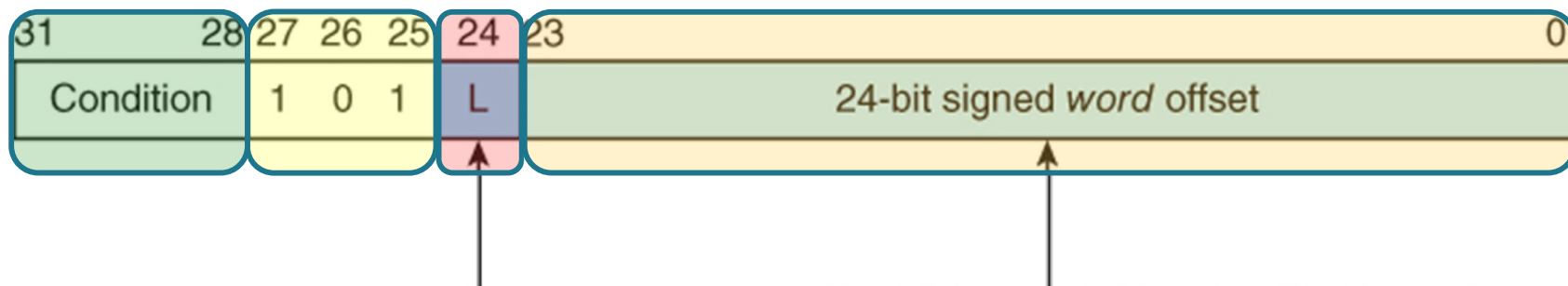
- ❑ **RISC** processors (including **ARM**) *do not provide* a *fully automatic* subroutine call/return mechanism like **CISC** processors.
- ❑ **ARM**'s *branch with link* instruction, **BL**,
 - automatically saves the return address in register **r14**.
- ❑ The branch instruction (Figure 3.41) has a 24-bit *signed* program counter relative offset (*word address offset*).

This is the main difference between B and BL

You may want to review slides 89 to 91 to remember how to encode and decode this 24-bit offset.

FIGURE 3.41

Encoding ARM's branch and branch-with-link instructions



The L-bit is 0 for a branch instruction and 1 for a branch with link instruction.

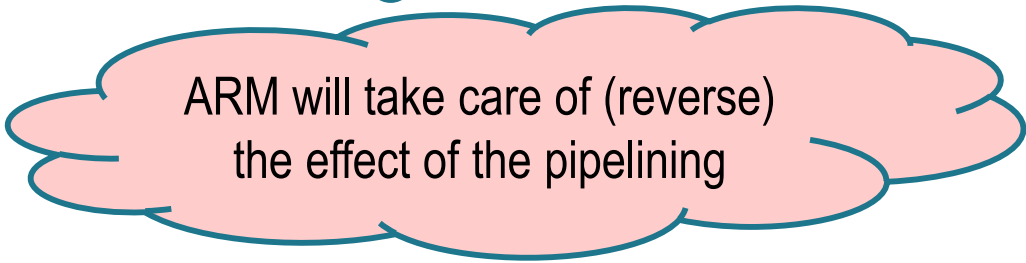
The 24-bit word offset is shifted left twice to create a 26-bit byte offset.

ARM Support for Subroutines

- ❑ The *branch with link* instruction behaves like the branch instruction but the processor also copies the return address (i.e., the address of the next instruction to be executed following a return) into the link register **r14**.

- ❑ If you execute:

```
BL      Sub_A      ;save return address in r14  
          ;branch to "Sub_A"
```



ARM will take care of (reverse)
the effect of the pipelining

- ❑ At the end of the subroutine, you return by
 - *copying the return address* in r14 to the program counter by executing:

```
MOV pc, lr
```

or

```
MOV r15, r14
```

ARM Support for Subroutines

- ❑ Suppose that you want to evaluate the following expression several times in a program.

if $x > 0$ then $x = 16*x + 1$ else $x = 32*x$

Should it be LT
or LE?

- ❑ Assuming that **x** is loaded into **r0**, we can write :

```
Func1 CMP    r0, #0           ;test for x > 0
      MOVGT  r0, r0, LSL #4    ;if x > 0 x = 16*x
      ADDGT  r0, r0, #1        ;if x > 0 then x = 16*x + 1
      MOVLT  r0, r0, LSL #5    ;ELSE if x < 0 THEN x = 32*x
      MOV    pc, lr           ;return by restoring saved PC
```

- ❑ Consider the following invocation of the above subroutine.

```
LDR    r0, [r4]    ;get P
BL     Func1       ;First call
                        ;P = (if P > 0 then 16*P + 1 else 32*P)
STR    r0, [r4]    ;save P
```

Later on ...

```
LDR    r0, [r5]    ;get Q
BL     Func1       ;Second call
                        ;Q = (if Q > 0 then 16*Q + 1 else 32*Q)
STR    r0, [r5]    ; save Q
```


ARM Support for Subroutines

```

01      AREA  BL_instruction, CODE, READWRITE
02      ENTRY
03
04      ADR    r4,P          ;register r4 points at P
05      ADR    r5,Q          ;register r5 points at Q
06
07      LDR    r0,[r4]       ; get P
08      BL     Func1         ; P = (if P > 0 then 16P + 1 else 32P)
09      STR    r0,[r4,#8]    ; save P
10      ;
11      ; some code
12      ;
13      LDR    r0,[r5]       ; get Q
14      BL     Func1         ; Q = (if Q > 0 then 16Q + 1 else 32Q)
15      STR    r0,[r5,#8]    ; save P
16
17      MOV    r0, #0x18     ; angel_SWIreason_ReportException
18      LDR    r1, =0x20026  ; ADP_Stopped_ApplicationExit
19      SVC    #0x123456     ; ARM semihosting (formerly SWI)
20
21
22      Func1  CMP    r0,#0   ;test for x > 0
23            MOVGT  r0,r0, LSL #4 ;if x > 0 x = 16x
24            ADDGT  r0,r0,#1   ;if x > 0 then x = 16x + 1
25            MOVLT  r0,r0, LSL #5 ;ELSE if x < 0 THEN x = 32x
26            MOV    pc,r14    ;return by restoring saved PC
27
28      AREA  BL_instruction, DATA, READWRITE
29      P
30      Q
31      DCD    0x00000003     ;P = 3
32      DCD    0xFFFFFFFF     ;Q = -1
33
34      SPACE  8

```

Register	Value
Current	
R0	0x00000018
R1	0x00020026
R2	0x00000000
R3	0x00000000
R4	0x00000044
R5	0x00000048
R6	0x00000000
R7	0x00000000
R8	0x00000000
R9	0x00000000
R10	0x00000000
R11	0x00000000
R12	0x00000000
R13 (SP)	0x00000000
R14 (LR)	0x0000001C
R15 (PC)	0x00000028
CPSR	0xA00000D3
SPSR	0x00000000
User/System	
Fast Interrupt	
Interrupt	
Supervisor	
Abort	
Undefined	
Internal	
PC \$	0x00000028
Mode	Supervisor
States	36
Sec	0.00000000

Memory 1	
Address:	0x44
0x00000044:	00 00 00 03 FF FF FF FF
0x0000004C:	00 00 00 31 FF FF FF E0
0x00000054:	00 00 00 00 00 00 00 00

Conditional Subroutine Calls

❑ **BL** instruction can be conditionally executed.

❑ **For example**

```
CMP r9,r4      ;if r9 < r4
```

```
BLLT ABC      ;then call subroutine ABC
```

❑ **BLLT** means

- **B**ranch
- with **L**ink
- execute on condition **L**ess **T**han

Subroutine Call and Return

- ❑ An important application of the stack is to save the address to return to after executing the subroutine.
 - A subroutine call can be implemented by
 - Pushing the return address onto the stack
 - Branching to the target address.
 - Once the execution of the subroutine code is completed, a *return from subroutine* instruction is executed
 - Popping the return address from the stack
 - Copy the return address to the **PC** register

This is another method to implement a subroutine call, other than using R14.

Subroutine Call and Return

Occupied memory

Grows up

Example

This is B. It is NOT BL

...
...
...

STR r15, [r13, #-4] !

B Target

...
...

The proper return address

The address pushed onto the stack.

; assume that the stack grows towards
; low addresses and the SP points at
; the top item on the stack.
; pre-decrement the stack pointer AND
; push the return address on the stack
; jump to the target address (B not BL)
; to return here

You need to re-map the memory to make the stack space read/write enabled (Debug/Memory Map).
The other option is to use a .ini file
You may want to review tutorial 7, slides 93-106.

Due to the pipeline effect, the PC value will not be the address of the current instruction. Instead, it will be current address +12. Yes, it is +12, not +8, as it is STR instruction

- Because ARM does not support a stack-based subroutine return mechanism, you would have to write:

LDR r12, [r13], #+4

; get saved PC and post-increment

; stack pointer

SUB r15, r12, #4

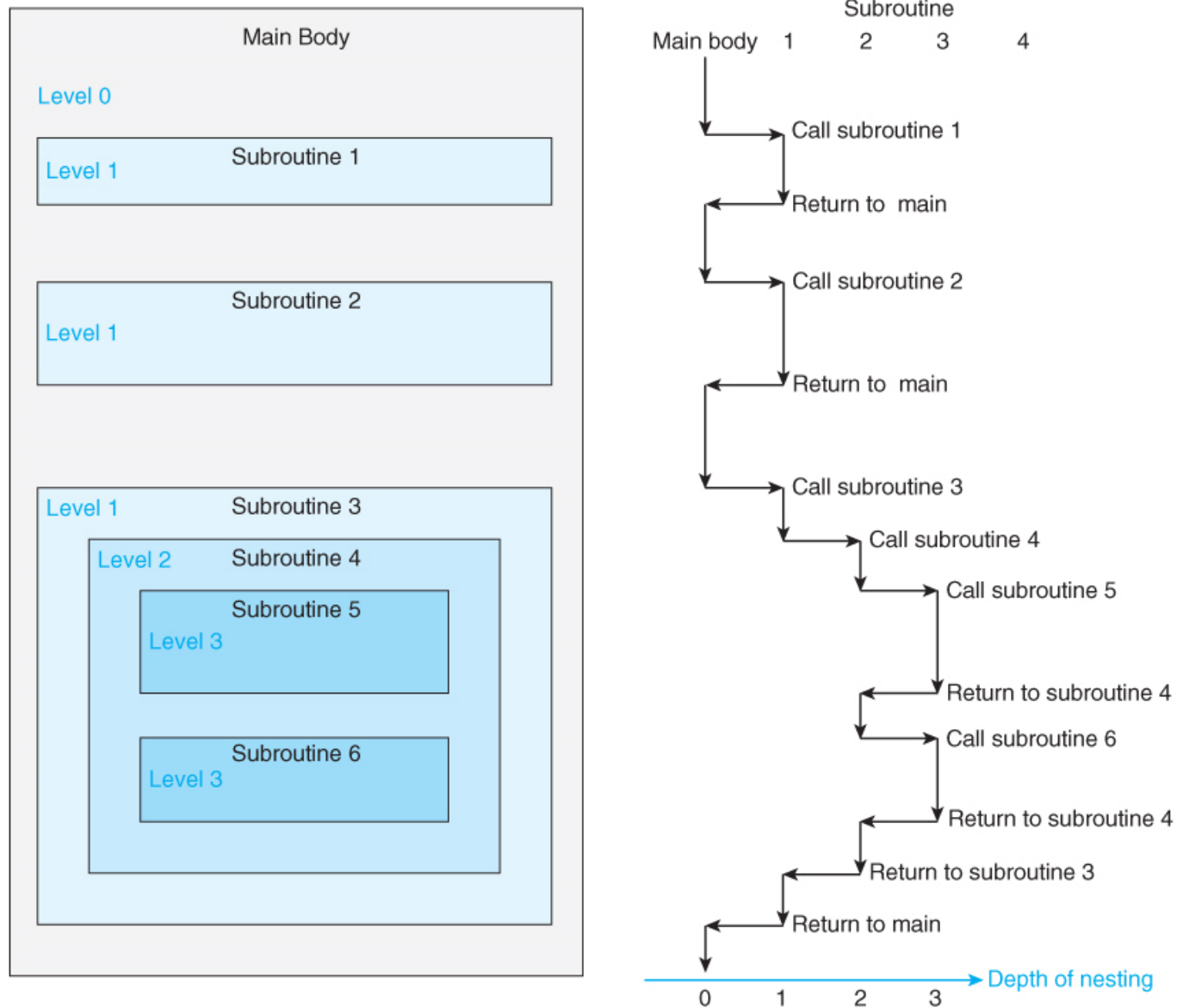
; fix PC and load into r15 to return

Why did not we copy the stack content directory to r15?

The 4 is subtracted to make the popped address pointing to the proper return address.

Nested subroutines

FIGURE 3.48 An example of nested subroutines



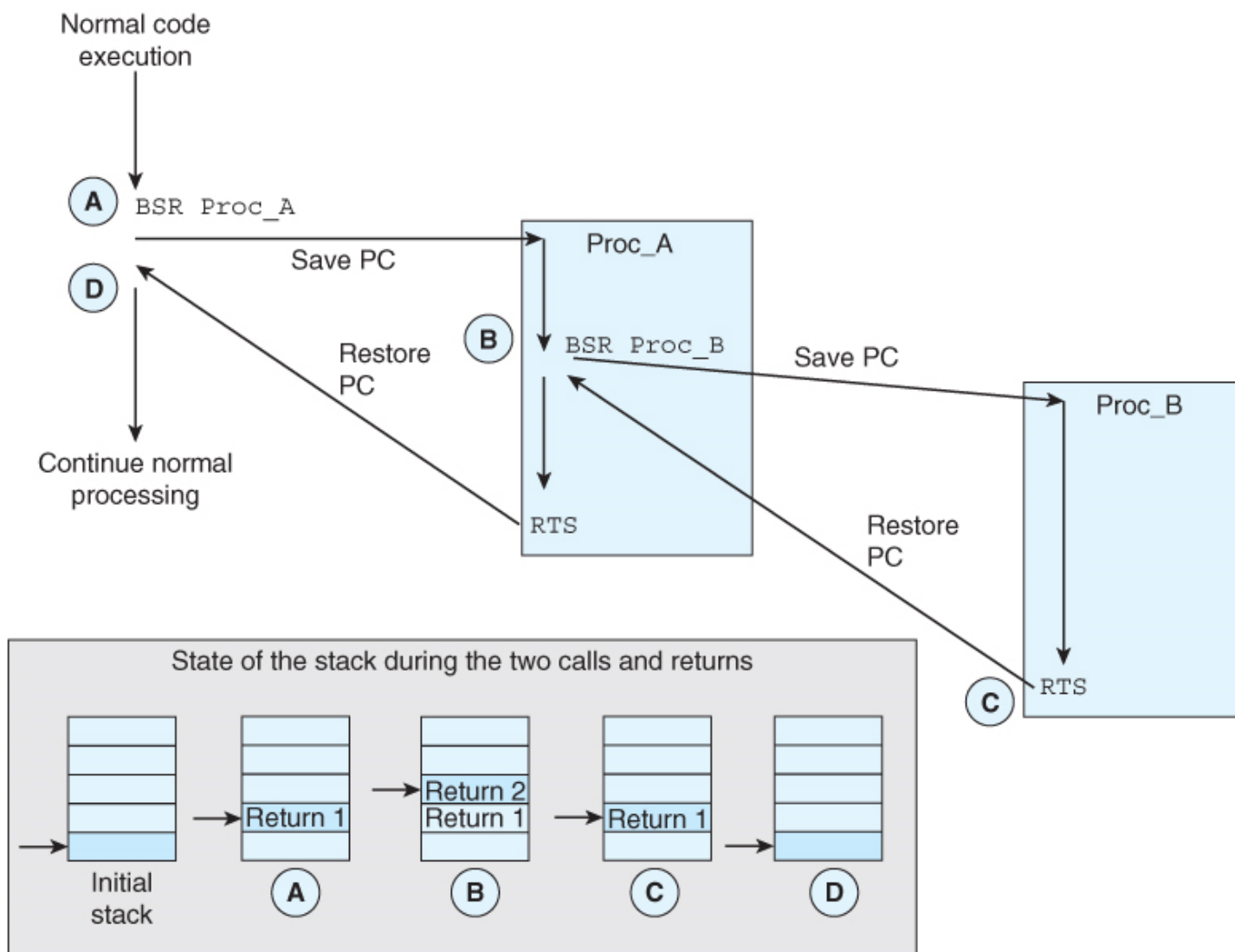
© Cengage Learning 2014

Occupied
memory

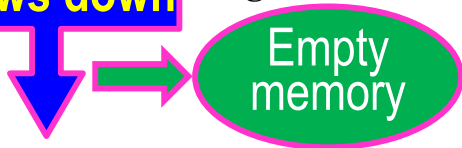
Example of nested subroutine

FIGURE 3.49

The stack and nested subroutines (CISC processors)



© Cengage Learning 2014



Leaf routines

- ❑ A *leaf routine* doesn't call another routine; it's at the end of the tree.
- ❑ If you call a *leaf routine* with **BL**,
 - the return address is saved in link register **r14**.
- ❑ A return to the calling point is made with a MOV **pc**, lr.
- ❑ If the routine is *not a leaf routine*, you *cannot* call another routine *without* first saving the link register.

```
ADR sp, STACK
```

```
BL Fun_1 ;call a simple leaf routine
```

```
BL Fun_2 ;call a routine that calls a nested routine
```

```
Loop B Loop
```

```
Fun_1 NOP ;this is a leaf routine
      MOV pc, lr ;return by copying the LR value into PC
```

```
Fun_2 NOP ;this is a non-leaf routine
      STR lr, [sp], #4 ;save link register
      BL Fun_1 ;call Fun_1 - overwrites the old LR
      LDR pc, [sp, #-4]! ;return by copying the LR value (from
                        ;the stack) into PC
```

```
STACK SPACE 0x10
```

What kind of stack is used here?

200

What is the maximum depth that can be called using this stack?

Leaf routines

- ❑ Subroutine Fun_1 is a leaf subroutine that does not call any other subroutine and, therefore, we don't have to worry about saving the link register, **r14**, and we can return by executing `MOV pc, lr`.
- ❑ Subroutine Fun_2 contains a call to another subroutine (i.e., nested subroutine) and we have to save the link register in order to return from Fun_2.
- ❑ The simplest way of *saving* the link register is to *push* it onto the stack.
- ❑ To return from Fun_2, we *restore the pushed* **r14** into the program counter.

Leaf routines

The screenshot shows the uVision4 IDE with the following components:

- Registers Panel:**

Register	Value
R0	0x00000000
R1	0x00000000
R2	0x00000000
R3	0x00000000
R4	0x00000000
R5	0x00000000
R6	0x00000000
R7	0x00000000
R8	0x00000000
R9	0x00000000
R10	0x00000000
R11	0x00000000
R12	0x00000000
R13 (SP)	0x00000000
R14 (LR)	0x00000000
R15 (PC)	0x00000000
CPSR	0x000000D3
SPSR	0x00000000
- Disassembly Panel:**

```

3:      ADR sp,STACK
4:
0x00000000 E28FD020 ADD    R13,PC,#0x00000020
5:      BL Fun_1      ;call a simple leaf routine
0x00000004 EB000001 BL     0x00000010
6:      BL Fun_2      ;call a routine that calls a nested routine
0x00000008 EB000002 BL     0x00000018
7: Loop B Loop
8: ;-----
0x0000000C EAffffFE B      0x0000000C
9: Fun_1 NOP          ;this is a leaf routine
0x00000010 E1A00000 NOP
10:      MOV pc,lr     ;return by moving the LR value into PC
  
```
- Source File (ex1.asm):**

```

1  AREA function_calls, CODE, READONLY
2  ENTRY
3  ADR sp,STACK
4
5  BL Fun_1      ;call a simple leaf routine
6  BL Fun_2      ;call a routine that calls a nested routine
7 Loop B Loop
8 ;-----
9 Fun_1 NOP      ;this is a leaf routine
  
```
- Command Window:**

```

*** Restricted Version with 32768 Byte Cc
*** Currently used: 56 Bytes (0%)
  
```
- Memory Window:**

Address: 0x0

0x00000000:	E2 8F D0 20 EB 00 00 01 EB 00 00 02 EA FF FF FE E1 A0 00 00
0x00000014:	E1 A0 F0 0E E1 A0 00 00 E4 8D E0 04 EB FF FF FA E5 3D F0 04
0x00000028:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0000003C:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00000050:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

A red callout bubble points to the instruction `ADD R13, PC, #0x00000020` with the text: "What is the value to be stored in r13?"

Leaf routines

Registers

Register	Value
R0	0x00000000
R1	0x00000000
R2	0x00000000
R3	0x00000000
R4	0x00000000
R5	0x00000000
R6	0x00000000
R7	0x00000000
R8	0x00000000
R9	0x00000000
R10	0x00000000
R11	0x00000000
R12	0x00000000
R13 (SP)	0x00000028
R14 (LR)	0x00000000
R15 (PC)	0x00000004
CPSR	0x000000D3
SPSR	0x00000000
User/System	
Fast Interrupt	
Interrupt	
Supervisor	

Disassembly

```

3:      ADR sp, STACK
4:
0x00000000 E28FD020 ADD    R13, PC, #0x00000020
5:      BL Fun_1          ;call a simple leaf routine
0x00000004 EB000001 BL     0x00000010
6:      BL Fun_2          ;call a routine that calls a nested routine
0x00000008 EB000002 BL     0x00000018
7: Loop B Loop
8: ;-----
0x0000000C EAffffFE B      0x0000000C
9: Fun_1 NOP              ;this is a leaf routine
0x00000010 E1A00000 NOP
10:     MOV pc, lr         ;return by copying the LR value into PC

```

ex1.asm

```

3      ADR sp, STACK
4
5      BL Fun_1          ;call a simple leaf routine
6      BL Fun_2          ;call a routine that calls a nested routine
7 Loop B Loop
8 ;-----
9 Fun_1 NOP              ;this is a leaf routine
10     MOV pc, lr         ;return by copying the LR value into PC
11 ;-----

```

Memory 1

Address: 0x0

0x00000000:	E2 8F D0 20 EB 00 00 01 EB 00 00 02 EA FF FF FE E1 A0 00 00
0x00000014:	E1 A0 F0 0E E1 A0 00 00 E4 8D E0 04 EB FF FF FA E5 3D F0 04
0x00000028:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0000003C:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00000050:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Simulation t1: 0.00000000 s

How is this offset encoded?

Leaf routines

The screenshot displays the uVision4 IDE interface with the following components:

- Registers:** A list of registers (R0-R15, CPSR, SPSR) with their current values. R14 (LR) is highlighted with a value of 0x00000008.
- Disassembly:** Shows assembly instructions with comments. The instruction at address 0x00000010 is highlighted in yellow: `0x00000010 E1A00000 NOP`. The comment indicates it is a leaf routine.
- ex1.asm:** Shows the source code for Fun_1 and Fun_2. Fun_1 is highlighted in green, showing a NOP instruction and a return statement: `9 Fun_1 NOP ;this is a leaf routine` and `10 MOV pc,lr ;return by copying the LR value into PC`.
- Command:** Displays a message: `*** Restricted Version with 32768 Byte Cc` and `*** Currently used: 56 Bytes (0%)`.
- Memory:** Shows a memory dump starting at address 0x0. The first few lines of memory are: `0x00000000: E2 8F D0 20 EB 00 00 01 EB 00 00 02 EA FF FF FE E1 A0 00 00`, `0x00000014: E1 A0 F0 0E E1 A0 00 00 E4 8D E0 04 EB FF FF FA E5 3D F0 04`, `0x00000028: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00`, `0x0000003C: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00`, and `0x00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00`.

Leaf routines

The screenshot displays the uVision4 IDE interface for a project named 'C:\Users\elsakka2\Desktop\ARM\ex1.uvproj'. The main window is divided into several panes:

- Registers:** A list of registers (R0-R15, CPSR, SPSR) with their current values. R15 (PC) is highlighted with a value of 0x00000014.
- Disassembly:** A list of instructions with their addresses and comments. Instruction 11, 'MOV PC, LR' at address 0x00000014, is highlighted in yellow. Comments indicate that this is a leaf routine that returns by copying the LR value into the PC.
- ex1.asm:** The source assembly code is shown below the disassembly. It includes instructions for calling leaf routines (Fun_1, Fun_2), a loop, and return instructions (NOP, MOV PC, LR).
- Command:** A text area showing memory usage statistics: '*** Restricted Version with 32768 Byte Cc' and '*** Currently used: 56 Bytes (0%)'.
- Memory:** A memory dump window showing the contents of memory starting at address 0x0. The dump shows a sequence of bytes, including the instruction 'E1 A0 F0 0E' at address 0x00000014.

The status bar at the bottom indicates the simulation is running, with a timer showing 't1: 0.00000000 s'.

Leaf routines

The screenshot shows the uVision4 IDE with the following components:

- Registers Panel:** Shows the current state of registers. R15 (PC) is highlighted with the value 0x00000008.
- Disassembly Panel:** Shows assembly code. Line 6 is highlighted: `0x00000008 EB000002 BL 0x00000018`. A red callout bubble points to the offset 0x00000018 with the text "How is this offset encoded?".
- Source Panel (ex1.asm):** Shows the corresponding assembly source code. Line 6 is highlighted: `BL Fun_2 ;call a routine that calls a nested routine`.
- Memory Panel:** Shows memory contents starting at address 0x0. The first two lines of memory are highlighted: `0x00000000: E2 8F D0 20 EB 00 00 01 EB 00 00 02 EA FF FF FE E1 A0 00 00` and `0x00000014: E1 A0 F0 0E E1 A0 00 00 E4 8D E0 04 EB FF FF FA E5 3D F0 04`.
- Command Panel:** Shows the command `ASSIGN BreakDisable BreakEnable BreakKill`.

Leaf routines

The screenshot displays the uVision4 IDE interface for a project named 'ex1.uvproj'. The 'Registers' window on the left shows the current state of registers, with R14 (LR) at 0x0000000C and R15 (PC) at 0x00000018. The 'Disassembly' window shows the following code:

```

0x00000008 EB000002 BL      0x00000018
           7: Loop B      Loop
           8: ;-----
0x0000000C EAffffff B      0x0000000C
           9: Fun_1 NOP      ;this is a leaf routine
0x00000010 E1A00000 NOP
          10:      MOV pc,lr      ;return by copying the LR value into PC
          11: ;-----
0x00000014 E1A0F00E MOV      PC,R14
          12: Fun_2 NOP      ;this is a non-leaf routine
→ 0x00000018 E1A00000 NOP
          13:      STR lr,[sp],#4 ;save link register
0x0000001C E48DE004 STR      R14,[R13],#0x0004
  
```

The 'ex1.asm' source file window shows the corresponding assembly code:

```

6      BL      Fun_2      ;call a routine that calls a nested routine
7 Loop B      Loop
8 ;-----
9 Fun_1 NOP      ;this is a leaf routine
10      MOV pc,lr      ;return by copying the LR value into PC
11 ;-----
12 Fun_2 NOP      ;this is a non-leaf routine
13      STR lr,[sp],#4 ;save link register
14      BL      Fun_1      ;call Fun_1 - overwrites the old link register
15      LDR pc,[sp,#-4]! ;return by copying the LR value (from the stack) into
  
```

The 'Command' window shows the status: '*** Restricted Version with 32768 Byte Cc', '*** Currently used: 56 Bytes (0%)', and 'ASSIGN BreakDisable BreakEnable BreakKill'. The 'Memory 1' window shows the memory dump starting at address 0x0:

```

0x00000000: E2 8F D0 20 EB 00 00 01 EB 00 00 02 EA FF FF FE E1 A0 00 00
0x00000014: E1 A0 F0 0E E1 A0 00 00 E4 8D E0 04 EB FF FF FA E5 3D F0 04
0x00000028: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  
```


Grows down

Empty
memory

Leaf routines

Registers

Register	Value
R0	0x00000000
R1	0x00000000
R2	0x00000000
R3	0x00000000
R4	0x00000000
R5	0x00000000
R6	0x00000000
R7	0x00000000
R8	0x00000000
R9	0x00000000
R10	0x00000000
R11	0x00000000
R12	0x00000000
R13 (SP)	0x00000028
R14 (LR)	0x0000000C
R15 (PC)	0x0000001C
CPSR	0x000000D3
SPSR	0x00000000
User/System	
Fast Interrupt	
Interrupt	
Supervisor	
Abort	

Disassembly

```
7: Loop B Loop
8: ;-----
0x0000000C EAffffff B 0x0000000C
9: Fun_1 NOP ;this is a leaf routine
0x00000010 E1A00000 NOP
10: MOV pc,lr ;return by copying the LR value into PC
11: ;-----
0x00000014 E1A0F00E MOV PC,R14
12: Fun_2 NOP ;this is a non-leaf routine
0x00000018 E1A00000 NOP
13: STR lr,[sp],#4 ;save link register
0x0000001C E48DE004 STR R14,[R13],#0x0004
14: BL Fun_1 ;call Fun_1 - overwrites the old link register
```

ex1.asm

```
6 BL Fun_2 ;call a routine that calls a nested routine
7 Loop B Loop
8 ;-----
9 Fun_1 NOP ;this is a leaf routine
10 MOV pc,lr ;return by copying the LR value into PC
11 ;-----
12 Fun_2 NOP ;this is a non-leaf routine
13 STR lr,[sp],#4 ;save link register
14 BL Fun_1 ;call Fun_1 - overwrites the old link register
15 LDR pc,[sp,#-4]! ;return by copying the LR value (from the stack) into
```

Memory 1

Address: 0x0

0x00000000:	E2 8F D0 20 EB 00 00 01 EB 00 00 02 EA FF FF FE E1 A0 00 00
0x00000014:	E1 A0 F0 0E E1 A0 00 00 E4 8D E0 04 EB FF FF FA E5 3D F0 04
0x00000028:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Command

*** Restricted Version with 32768 Byte Cc
*** Currently used: 56 Bytes (0%)

ASSIGN BreakDisable BreakEnable BreakKill

Simulation t1: 0.00000000 se

Which type of stack
is it?

Leaf routines

The screenshot shows the uVision4 IDE with the following components:

- Registers Window:**

Register	Value
R0	0x00000000
R1	0x00000000
R2	0x00000000
R3	0x00000000
R4	0x00000000
R5	0x00000000
R6	0x00000000
R7	0x00000000
R8	0x00000000
R9	0x00000000
R10	0x00000000
R11	0x00000000
R12	0x00000000
R13 (SP)	0x0000002C
R14 (LR)	0x0000000C
R15 (PC)	0x00000020
CPSR	0x000000D3
SPSR	0x00000000
- Disassembly Window:**

```

0x00000010 E1A00000 NOP
10:      MOV pc,lr      ;return by copying the LR value into PC
11: ;-----
0x00000014 E1A0F00E MOV      PC,R14
12: Fun_2 NOP          ;this is a non-leaf routine
0x00000018 E1A00000 NOP
13:      STR lr,[sp],#4  ;save link register
0x0000001C E48DE004 STR      R14,[R13],#0x0004
14:      BL  Fun_1      ;call Fun_1 - overw
0x00000020 EBFFFFFFA BL      0x00000010
15:      LDR pc,[sp,#-4]! ;return by copying the LR value (from the stack) into
0x00000024 E53DF004 LDR      PC,[R13,#-0x0004]!
0x00000028 0000000C ANDEQ    R0,R0,R12

```
- Source Window (ex1.asm):**

```

6      BL  Fun_2      ;call a routine that calls a nested routine
7 Loop B      Loop
8 ;-----
9 Fun_1 NOP          ;this is a leaf routine
10     MOV pc,lr      ;return by copying the LR value into PC
11 ;-----
12 Fun_2 NOP          ;this is a non-leaf routine
13     STR lr,[sp],#4  ;save link register
14     BL  Fun_1      ;call Fun_1 - overwrites the old link register
15     LDR pc,[sp,#-4]! ;return by copying the LR value (from the stack) into

```
- Memory Window:**

Address: 0x0

```

0x00000000: E2 8F D0 20 EB 00 00 01 EB 00 00 02 EA FF FF FE E1 A0 00 00
0x00000014: E1 A0 F0 0E E1 A0 00 00 E4 8D E0 04 EB FF FF FA E5 3D F0 04
0x00000028: 00 00 00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

A red callout bubble points to the instruction `BL 0x00000010` in the disassembly window with the text: "How is this offset encoded?". A blue arrow points from the `R14 (LR)` register value to the memory view at address `0x00000028`.

Leaf routines

The screenshot displays the uVision4 IDE interface for an ARM project. The main window shows the disassembly of the current routine, with the following instructions:

```

0x00000010 E1A00000 NOP
10: MOV pc,lr ;return by copying the LR value into PC
11: ;-----
0x00000014 E1A0F00E MOV PC,R14
12: Fun_2 NOP ;this is a non-leaf routine
0x00000018 E1A00000 NOP
13: STR lr,[sp],#4 ;save link register
0x0000001C E48DE004 STR R14,[R13],#0x0004
14: BL Fun_1 ;call Fun_1 - overwrites the old link register
0x00000020 EBFFFFFFA BL 0x00000010
15: LDR pc,[sp,#-4]! ;return by copying the LR value (from the stack) into
0x00000024 E53DF004 LDR PC,[R13,#-0x0004]!
0x00000028 0000000C ANDEQ R0,R0,R12
  
```

The Registers window shows the current state of the registers:

Register	Value
R0	0x00000000
R1	0x00000000
R2	0x00000000
R3	0x00000000
R4	0x00000000
R5	0x00000000
R6	0x00000000
R7	0x00000000
R8	0x00000000
R9	0x00000000
R10	0x00000000
R11	0x00000000
R12	0x00000000
R13 (SP)	0x0000002C
R14 (LR)	0x00000024
R15 (PC)	0x00000010
CPSR	0x000000D3
SPSR	0x00000000

The ex1.asm source window shows the assembly code for the routines:

```

6 BL Fun_2 ;call a routine that calls a nested routine
7 Loop B Loop
8 ;-----
9 Fun_1 NOP ;this is a leaf routine
10 MOV pc,lr ;return by copying the LR value into PC
11 ;-----
12 Fun_2 NOP ;this is a non-leaf routine
13 STR lr,[sp],#4 ;save link register
14 BL Fun_1 ;call Fun_1 - overwrites the old link register
15 LDR pc,[sp,#-4]! ;return by copying the LR value (from the stack) into
  
```

The Command window shows the status of the simulation:

```

*** Restricted Version with 32768 Byte Code
*** Currently used: 56 Bytes (0%)
  
```

The Memory window shows the memory contents at address 0x0:

```

0x00000000: E2 8F D0 20 EB 00 00 01 EB 00 00 02 EA FF FF FE E1 A0 00 00
0x00000014: E1 A0 F0 0E E1 A0 00 00 E4 8D E0 04 EB FF FF FA E5 3D F0 04
0x00000028: 00 00 00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  
```

The bottom status bar indicates the simulation is running at t1: 0.00000000 seconds.

Leaf routines

The screenshot displays the uVision4 IDE interface with the following components:

- Registers Window:** Shows the current state of registers. R15 (PC) is highlighted with a value of 0x00000014.
- Disassembly Window:** Shows the disassembled instructions. The instruction at address 0x00000014 is highlighted in yellow: `MOV PC, R14`. Comments indicate this is a non-leaf routine.
- Source Window (ex1.asm):** Shows the assembly code. The instruction `MOV pc,lr` at line 10 is highlighted in green, corresponding to the disassembly.
- Command Window:** Shows the command `ASSIGN BreakDisable BreakEnable BreakKill`.
- Memory Window:** Shows the memory dump starting at address 0x00000000.

Disassembly Details:

Address	Instruction	Comment
0x00000010	E1A00000 NOP	
10:	MOV pc,lr	;return by copying the LR value into PC
11:	;	
0x00000014	E1A0F00E MOV PC, R14	
12:	Fun_2 NOP	;this is a non-leaf routine
0x00000018	E1A00000 NOP	
13:	STR lr, [sp], #4	;save link register
0x0000001C	E48DE004 STR R14, [R13], #0x0004	
14:	BL Fun_1	;call Fun_1 - overwrites the old link register
0x00000020	EBFFFFFFA BL 0x00000010	
15:	LDR pc, [sp, #-4]!	;return by copying the LR value (from the stack) into PC
0x00000024	E53DF004 LDR PC, [R13, #-0x0004]!	
0x00000028	0000000C ANDEQ R0, R0, R12	

Source Code (ex1.asm) Details:

Line	Instruction	Comment
6	BL Fun_2	;call a routine that calls a nested routine
7	Loop B Loop	
8	;	
9	Fun_1 NOP	;this is a leaf routine
10	MOV pc,lr	;return by copying the LR value into PC
11	;	
12	Fun_2 NOP	;this is a non-leaf routine
13	STR lr, [sp], #4	;save link register
14	BL Fun_1	;call Fun_1 - overwrites the old link register
15	LDR pc, [sp, #-4]!	;return by copying the LR value (from the stack) into PC

Memory Dump:

Address	Hex Data
0x00000000	E2 8F D0 20 EB 00 00 01 EB 00 00 02 EA FF FF FE E1 A0 00 00
0x00000014	E1 A0 F0 0E E1 A0 00 00 E4 8D E0 04 EB FF FF FA E5 3D F0 04
0x00000028	00 00 00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Leaf routines

The screenshot displays the uVision4 IDE interface for an ARM project. The main window shows the disassembly of the code, highlighting the leaf routine Fun_1 and the non-leaf routine Fun_2. The Registers window on the left shows the current state of the registers, with R15 (PC) highlighted. The ex1.asm source window shows the assembly code for the routines. The Command window at the bottom shows the status of the project, and the Memory window shows the memory dump.

Registers:

Register	Value
R0	0x00000000
R1	0x00000000
R2	0x00000000
R3	0x00000000
R4	0x00000000
R5	0x00000000
R6	0x00000000
R7	0x00000000
R8	0x00000000
R9	0x00000000
R10	0x00000000
R11	0x00000000
R12	0x00000000
R13 (SP)	0x0000002C
R14 (LR)	0x00000024
R15 (PC)	0x00000024
CPSR	0x000000D3
SPSR	0x00000000

Disassembly:

```

0x0000000C EAfffffe B 0x0000000C
9: Fun_1 NOP ;this is a leaf routine
0x00000010 E1A00000 NOP
10: MOV pc,lr ;return by copying the LR value into PC
11: ;-----
0x00000014 E1A0F00E MOV PC,R14
12: Fun_2 NOP ;this is a non-leaf routine
0x00000018 E1A00000 NOP
13: STR lr,[sp],#4 ;save link register
0x0000001C E48DE004 STR R14,[R13],#0x0004
14: BL Fun_1 ;call Fun_1 - overwrites the old link register
0x00000020 EBfffffa BL 0x00000010
15: LDR pc,[sp,#-4]! ;return by copying the LR value (from the stack) into
0x00000024 E53DF004 LDR PC,[R13,#-0x0004]!
  
```

ex1.asm:

```

10 MOV pc,lr ;return by copying the LR value into PC
11 ;-----
12 Fun_2 NOP ;this is a non-leaf routine
13 STR lr,[sp],#4 ;save link register
14 BL Fun_1 ;call Fun_1 - overwrites the old link register
15 LDR pc,[sp,#-4]! ;return by copying the LR value (from the stack) into
16 ;-----
17 STACK SPACE 0x10
18 ;-----
  
```

Command:

```

*** Restricted Version with 32768 Byte Cc
*** Currently used: 56 Bytes (0%)
  
```

Memory 1:

Address: 0x0

```

0x00000000: E2 8F D0 20 EB 00 00 01 EB 00 00 02 EA FF FF FE E1 A0 00 00
0x00000014: E1 A0 F0 0E E1 A0 00 00 E4 8D E0 04 EB FF FF FA E5 3D F0 04
0x00000028: 00 00 00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  
```

Simulation: t1: 0.00000000 s

Leaf routines

The screenshot shows the uVision4 IDE with the following components:

- Registers Window:** Lists registers R0 through R15. R13 (SP) is at 0x00000028, R14 (LR) is at 0x00000024, and R15 (PC) is at 0x0000000C. A blue arrow points from R15 to the memory window.
- Disassembly Window:** Shows assembly code for Fun_1 and Fun_2. Fun_1 is a leaf routine (NOP, MOV pc, lr). Fun_2 is a non-leaf routine (NOP, STR lr, [sp], #4, BL Fun_1, LDR pc, [sp, #-4]!).
- ex1.asm Window:** Shows the source assembly code for Fun_1 and Fun_2, matching the disassembly.
- Memory Window:** Shows memory addresses 0x00000000 to 0x00000028. The value at 0x00000028 is 00 00 00 0C, which is the address of R15 (PC).
- Command Window:** Shows the status of the simulation: "Restricted Version with 32768 Byte Code Memory", "Currently used: 56 Bytes (0%)", and "ASSIGN BreakDisable BreakEnable BreakKill".
- Simulation Status:** The bottom status bar indicates "Simulation" and "t1: 0.00000000 s".

Leaf routines

The screenshot displays the uVision4 IDE interface with the following components:

- Registers Panel:** Shows the current state of registers R0 through R15, CPSR, and SPSR. R13 (SP) is at 0x00000028, R14 (LR) is at 0x00000024, and R15 (PC) is at 0x0000000C.
- Disassembly Panel:** Shows the disassembled code for the current address range.
 - Address 0x0000000C: `EAF FFF FE B 0x0000000C` (NOP) - Comment: `;this is a leaf routine`
 - Address 0x00000010: `E1A 00 00 00` (NOP)
 - Address 0x00000011: `MOV pc,lr` - Comment: `;return by copying the LR value into PC`
 - Address 0x00000014: `E1A 0F 00 E` (NOP) - Comment: `;this is a non-leaf routine`
 - Address 0x00000018: `E1A 00 00 00` (NOP)
 - Address 0x0000001C: `E48 DE 00 4` (STR) - Comment: `;save link register`
 - Address 0x0000001D: `BL Fun_1` - Comment: `;call Fun_1 - overwrites the old link register`
 - Address 0x00000020: `EB FFF FFA` (BL) - Comment: `;return by copying the LR value (from the stack) into PC`
 - Address 0x00000024: `E53 DF 00 4` (LDR) - Comment: `;return by copying the LR value (from the stack) into PC`
- Source Panel (ex1.asm):** Shows the corresponding assembly source code.
 - Line 6: `BL Fun_2` - Comment: `;call a routine that calls a nested routine`
 - Line 7: `Loop B Loop`
 - Line 9: `Fun_1 NOP` - Comment: `;this is a leaf routine`
 - Line 10: `MOV pc,lr` - Comment: `;return by copying the LR value into PC`
 - Line 12: `Fun_2 NOP` - Comment: `;this is a non-leaf routine`
 - Line 13: `STR lr, [sp], #4` - Comment: `;save link register`
 - Line 14: `BL Fun_1` - Comment: `;call Fun_1 - overwrites the old link register`
- Command Panel:** Shows the command `*** Restricted Version with 32768 Byte Code Memory *** Currently used: 56 Bytes (0%)`.
- Memory Panel:** Shows the memory dump starting at address 0x0.
 - 0x00000000: `E2 8F D0 20 EB 00 00 01 EB 00 00 02 EA FF FF FE E1 A0 00 00`
 - 0x00000014: `E1 A0 F0 0E E1 A0 00 00 E4 8D E0 04 EB FF FF FA E5 3D F0 04`
 - 0x00000028: `00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00`
- Bottom Panel:** Includes the `ASSIGN BreakDisable BreakEnable BreakKill` command and the `Simulation` status bar.

Subroutines and Block Move Instructions

- ❑ All subroutines commonly use the same set of registers to save values, and this might cause problems.
 - Assume that a program used **R1** to store a temporary value.
 - Later, this program called a function.
 - The function also used **R1** to store a different value.
 - After returning from the function, the program will not have access to the original **R1** value that was there before calling the function.

- ❑ To solve this issue, the followings need to be done:
 - At the beginning of the function, the values of all registers that will be used in the function must be pushed onto a stack.
 - Just before returning from the function, all pushed values must be popped and loaded to the same registers.

Subroutines and Block Move Instructions

- ❑ The **ARM**'s block move instructions can be used to
 - save register values once entering a subroutine and
 - restore registers just before returning from a subroutine.
- ❑ Consider the following ARM code:

```
BL      test                ;call test, save return
                                ;address in r14

...

test STMFD r13!, {r0-r4,r10} ;subroutine test, save working
                                ;registers

. body of code

.
LDMFD r13!, {r0-r4,r10}      ;subroutine completes,
                                ;restore the registers

MOV     pc, r14              ;copy the return address in
                                ;r14 to the PC
```

You need to re-map the memory to make the stack
space read/write enabled (Debug/Memory Map).
The other option is to use a .ini file
You may want to review tutorial 7, slides 93-106.

Subroutines and Block Move Instructions

- ❑ If you are using block move STM/LDM instructions to store/load multiple registers to/from the stack, you may also want to store the link register (R14) as well and then load its value directly into the program counter (R15) to save an instruction.

We can write:

```
test STMFD r13!, {r0-r4, r10, r14} ;save working registers
                                   ;and return address in r14
:
LDMFD r13!, {r0-r4, r10, r15} ;restore working registers
                               ;and put r14 in the PC
```

- ❑ At the beginning of the subroutine, we push the *link register r14* containing the return address onto the stack, and then at the end we pull the saved register values, including the value of the return address which is placed into the *PC*, to make the return.
 - By doing so, we reduced the size of this code by one instruction

You need to re-map the memory to make the stack space read/write enabled (Debug/Memory Map).
The other option is to use a .ini file
You may want to review tutorial 7, slides 93-106.