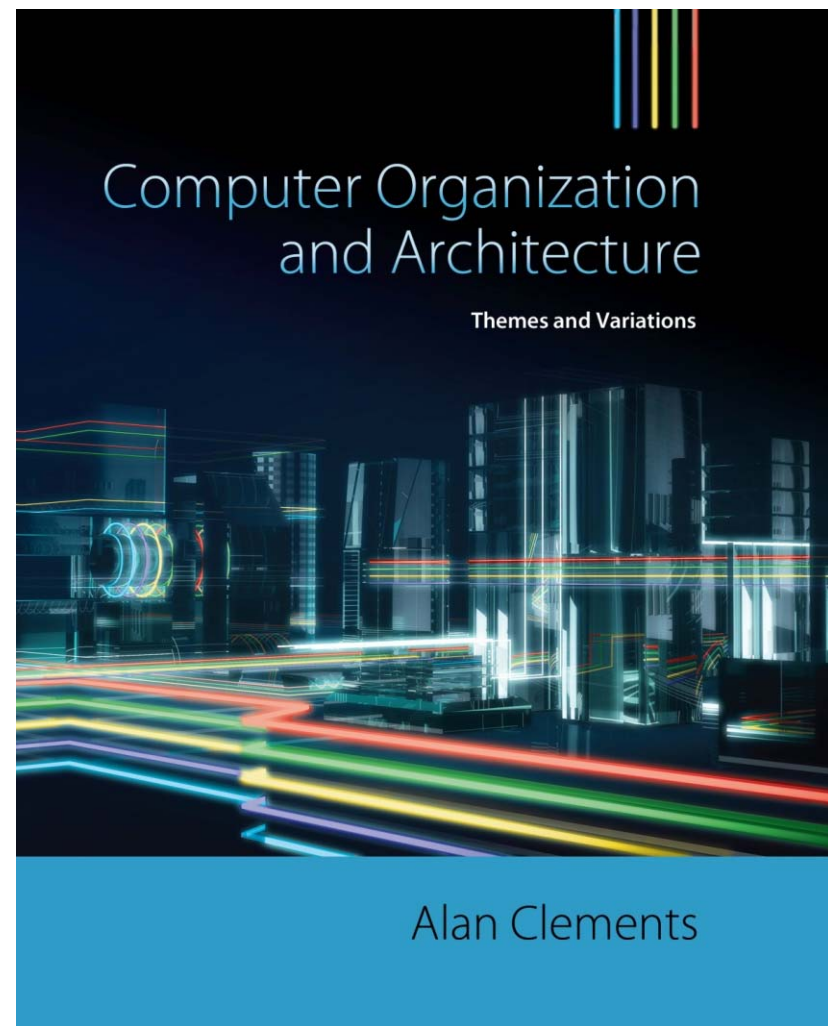


Part 0xC

CHAPTER 3

Architecture and Organization



1

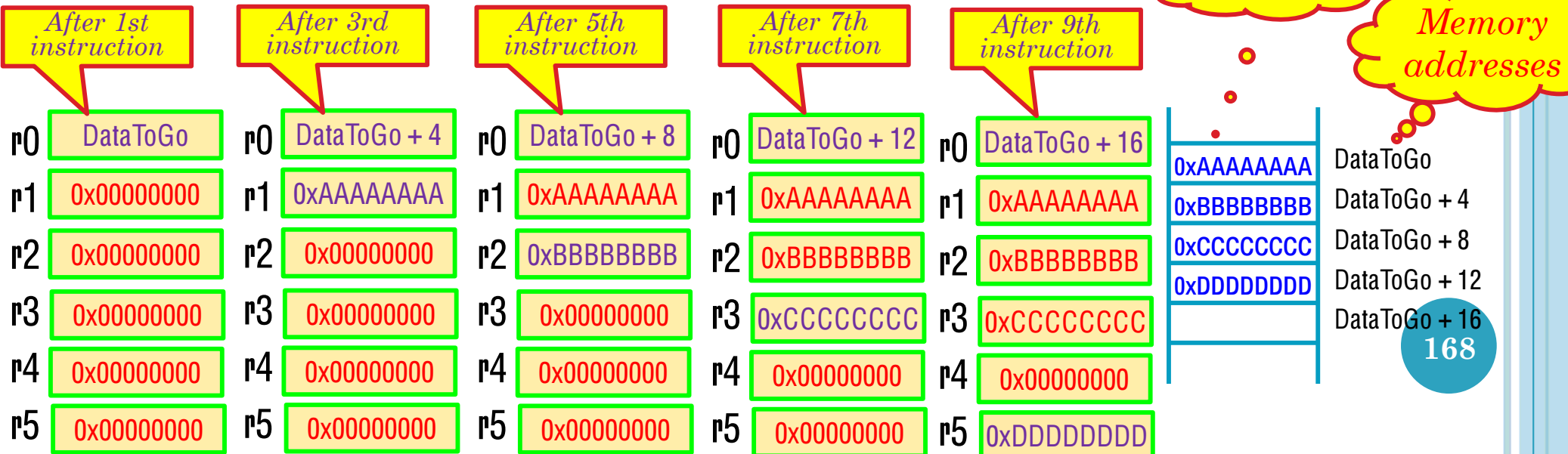
These slides are being provided with permission from the copyright for in-class (CS2208B) use only. The slides must not be reproduced or provided to anyone outside of the class.

All download copies of the slides and/or lecture recordings are for personal use only. Students must destroy these copies within 30 days after receipt of final course evaluations.

Block Move Instructions

- ❑ The following conventional ARM code demonstrates how to load four registers from **consecutive** memory-locations.

1st *or LDR = r0*
`ADR r0, DataToGo ;load r0 with the address of the data area`
3rd
`LDR r1, [r0] ;load r1 with the word pointed at by r0`
`ADD r0, #4 ;update the pointer`
5th
`LDR r2, [r0] ;load r2 with the word pointed at by r0`
`ADD r0, #4 ;update the pointer`
7th
`LDR r3, [r0] ;load r3 with the word pointed at by r0`
`ADD r0, #4 ;update the pointer`
9th
`LDR r5, [r0] ;load r5 with the word pointed at by r0`
`ADD r0, #4 ;update the pointer`



Block Move Instructions

- ❑ *A more efficient way* to load four registers from consecutive memory-locations.

```

ADR r0, DataToGo ;load r0 with the address of the data area
LDR r1, [r0], #4 ;load r1 with the word pointed at by r0
                  ;and post-update the pointer
LDR r2, [r0], #4 ;load r2 with the word pointed at by r0
                  ;and post-update the pointer
LDR r3, [r0], #4 ;load r3 with the word pointed at by r0
                  ;and post-update the pointer
LDR r5, [r0], #4 ;load r5 with the word pointed at by r0
                  ;and post-update the pointer
  
```

- ❑ ARM has

- a *block move from memory to registers* instruction, **LDM**, and ^{multiple.}
- a *block move from registers to memory* instruction, **STM**

that can copy group of registers from and to memory.

This is even more efficient than the above solution.

- ❑ Both block move instructions take a **suffix** to describe *how* the data is accessed.

Block Move Instructions

- ❑ Think of block move instructions as if they are stack operations
 - *STM: to push a group of registers' content to memory*
 - *LDM: to pop values from memory and load them to a group of registers*

- ❑ Let's start by copying the contents of registers r1, r2, r3, and r5, into *sequential* memory-locations with

ADR r0, DataToGo .

STMIA r0!, {r1-r3, r5} ;note the syntax of this instruction

increment
after.

update

order
doesn't
matter.

;the register list is put between
;curly braces and it can have a range

This is a different example. It is an STM and the example in the previous two slides was LDM.

- ❑ This instruction copies registers r1 to r3, and r5, into sequential memory-locations, using r0 as a pointer with auto-indexing (indicated by the ! suffix).
- ❑ The suffix **IA** indicates that index register r0 is *incremented after* the transfer, with data transfer in the order of increasing addresses.
- ❑ Although ARM's block move instructions have several variations, *ARM always stores the lowest numbered register first at the lowest memory address*, followed by the next lowest numbered register, and so on, regardless of the order in the instruction.
For example, "STMIA r0!, {r5, r1-r3}" and "STMIA r0!, {r2, r3, r5, r1}" have the same effect as "STMIA r0!, {r1-r3, r5}"

Block Move Instructions

Registers

Register	Value
R0	0x00000048
R1	0x11111111
R2	0x22222222
R3	0x33333333
R4	0x00000000
R5	0x55555555
R6	0x00000000
R7	0x00000000
R8	0x00000000
R9	0x00000000
R10	0x00000000
R11	0x00000000
R12	0x00000000
R13 (SP)	0x00000000
R14 (LR)	0x00000000
R15 (PC)	0x00000018
CPSR	0x000000D3
SPSR	0x00000000

MoveMultiple.asm

```

01 AREA MoveMultiple, CODE, READWRITE
02 ENTRY
03 0x00000000 LDR r1,=0x11111111 ;Let's set up some nice simple values that we can track
04 0x00000004 LDR r2,=0x22222222
05 0x00000008 LDR r3,=0x33333333
06 0x0000000C LDR r5,=0x55555555
07 0x00000010 ADR r0, Stack ;let's have a stack to put data on
08 0x00000014 STMIA r0!,{r1-r3, r5} ;Now move the data
09 0x00000018 MOV r0, #0x18 ;angel_SWIreason_ReportException
10 0x0000001C LDR r1, =0x20026 ;ADP_Stopped_ApplicationExit
11 0x00000020 SVC #0x123456 ;ARM semihosting (formerly SWI)
12 0x00000024 SPACE 20 ;leave 20 spaces
13 Stack SPACE 20 ;leave 20 more spaces
14 END
  
```

Memory 1

Address	Value
0x0000001C	E5 9F 10 38
0x00000020	EF 12 34 56
0x00000024	00 00 00 00
0x00000028	00 00 00 00
0x0000002C	00 00 00 00
0x00000030	00 00 00 00
0x00000034	00 00 00 00
0x00000038	11 11 11 11
0x0000003C	22 22 22 22
0x00000040	33 33 33 33
0x00000044	55 55 55 55
0x00000048	00 00 00 00
0x0000004C	11 11 11 11
0x00000050	22 22 22 22
0x00000054	33 33 33 33
0x00000058	55 55 55 55

Annotations:

- Registers preloaded with data
- Registers loaded in the constant pool before execution
- Registers saved on the stack
- r0 contains 0x48 which is the value after the data has been stored.

- ❑ In LDM/STM, the access happens in the order of increasing register numbers,
 - ❑ the lowest numbered register occupies the lowest memory address and
 - ❑ the highest numbered register occupies the highest memory address

Block Moves and Stack Operations

TABLE 3.5 Stack Types and the ARM Block Move Instruction Suffixes

Stack type	1	2	3	4
Stack growth	Descending	Ascending	Descending	Ascending
Class	Full	Full	Empty	Empty
Stack suffix	FD	FA	ED	EA
Load suffix	IA (increment after) <i>operation</i>	DA (decrement after)	IB (increment before)	DB (decrement before)
Store suffix	DB (decrement before)	IB (increment before)	DA (decrement after)	IA (increment after)

Similar to PUSH, i.e., PUSH from registers to memory

Similar to POP, i.e., POP from memory to these registers

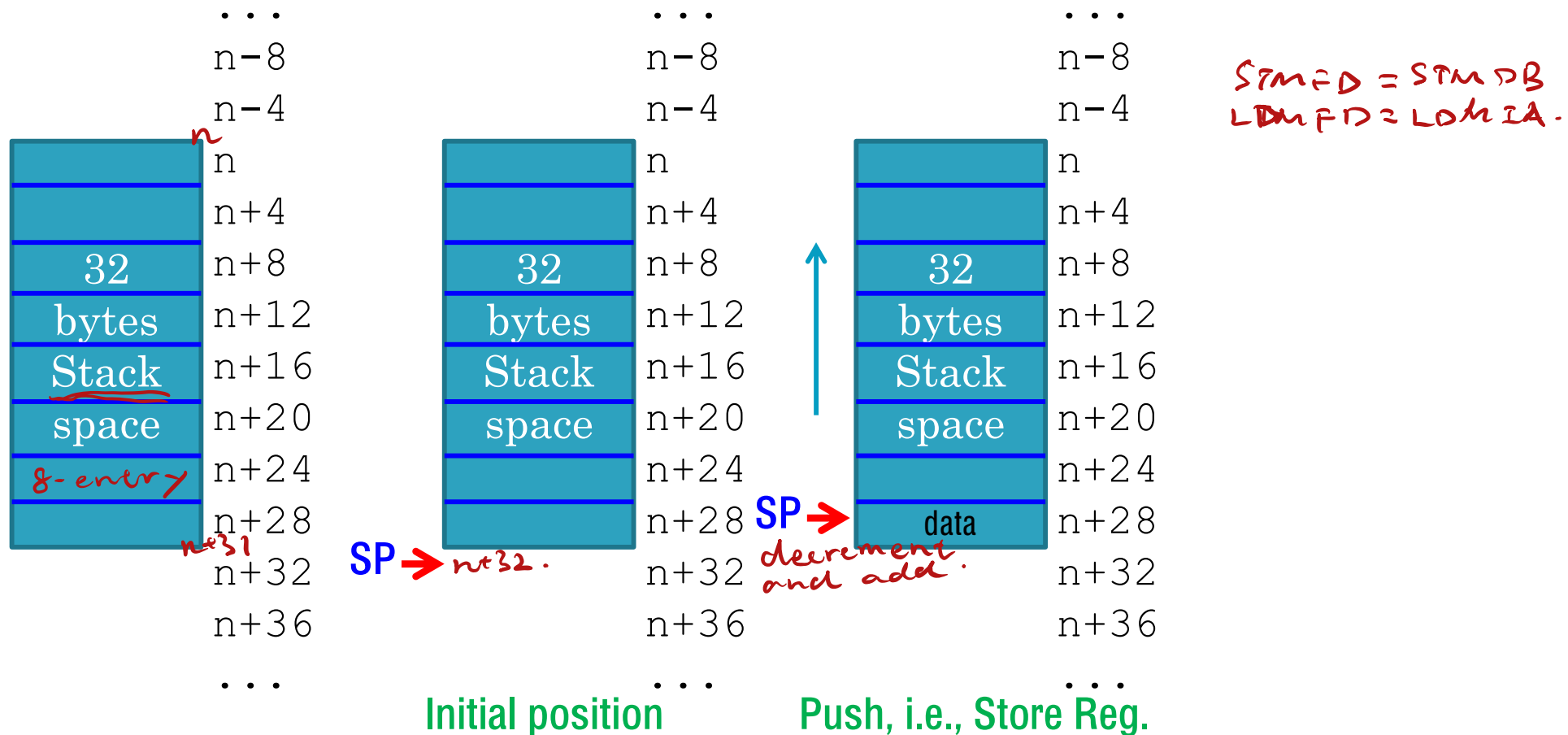
Des
filled IA/DB
empty IB/DA

Asc
DA/IB
DB/IA

Grows up

Occupied memory

Block Moves and Stack Operations

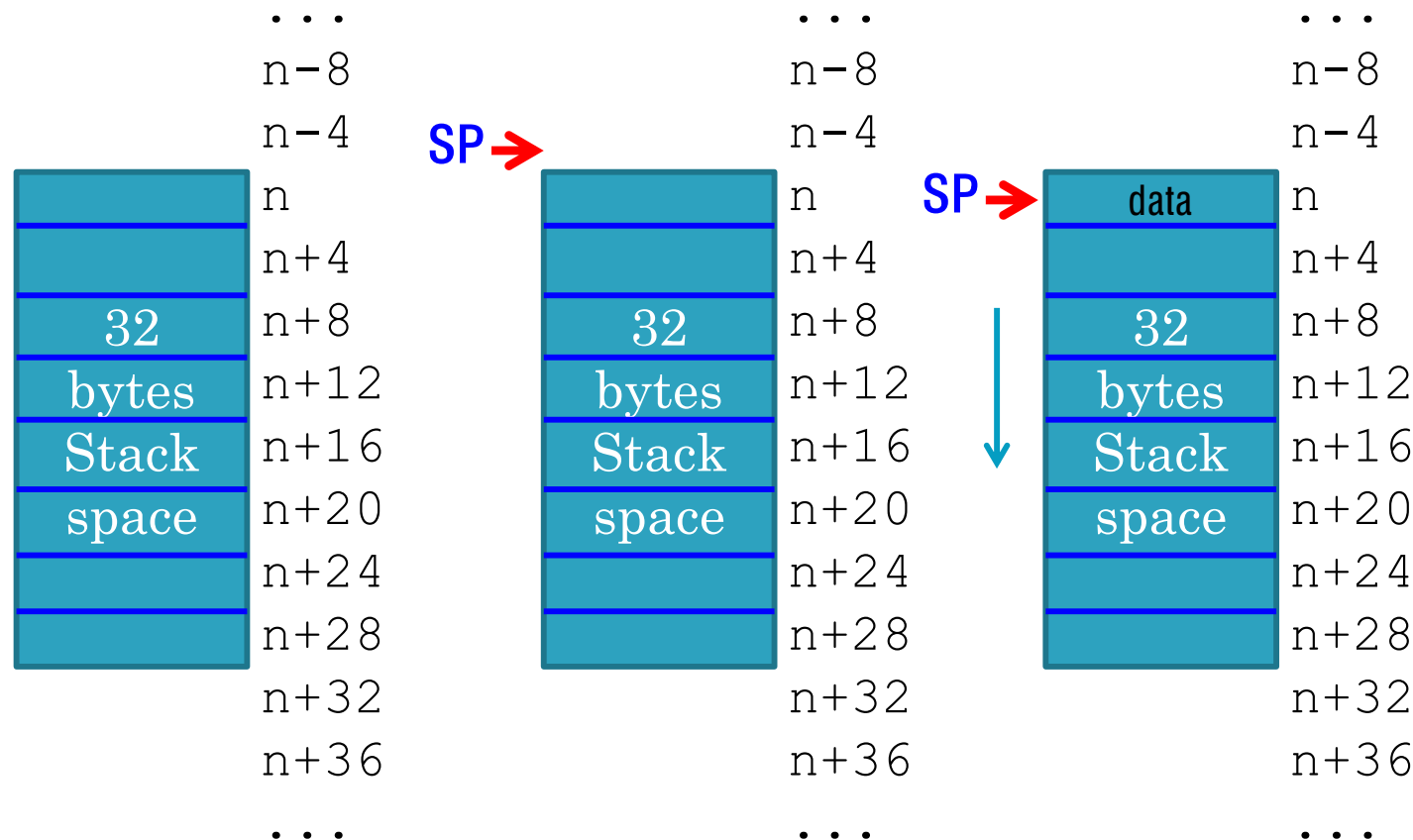


□ Stack type: **FD** (i.e., Class=**F**ull and Stack growth=**D**escending)
(**STMFD** and **LDMFD**)

- Empty stack → SP points to just after the stack space
- Pushing on the stack → SP to be **D**ecrement **B**efore (**STMDB**)
- Popping off the stack → SP to be **I**ncrement **A**fter (**LDMIA**)

Handwritten notes: $\text{SP} \rightarrow \text{not in the stack}$, $\text{SP} \rightarrow \text{after the stack}$, $\text{SP} \rightarrow \text{currently point to the item} \Rightarrow \text{pop the item}$, $\text{update the pointer}$.

Block Moves and Stack Operations



STMFA = STMIB
LDMFA = LDMDA

Initial position

Push, i.e., Store Reg.

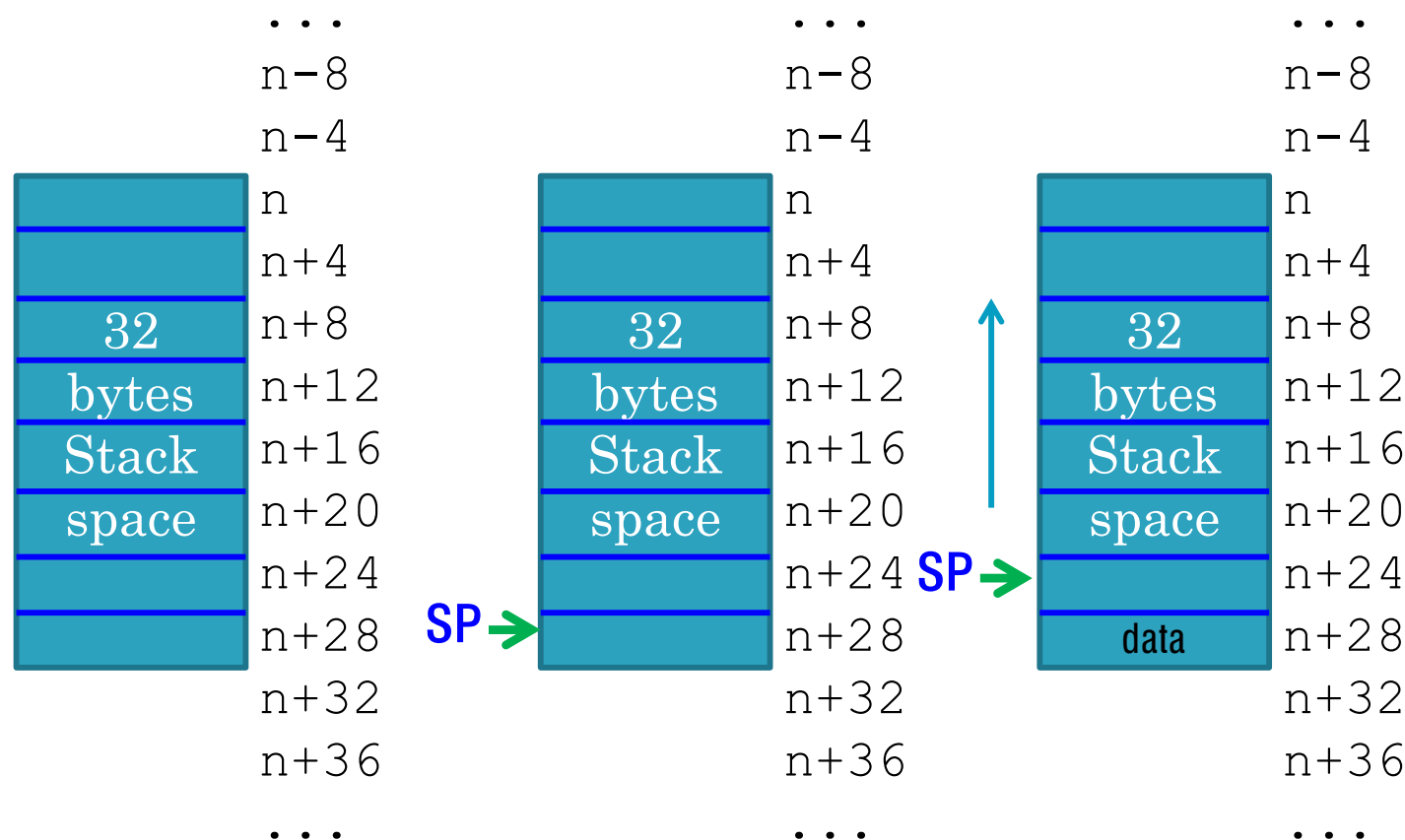
□ Stack type: **FA** (i.e., Class=**F**ull and Stack growth=**A**scending)

(**STMFA** and **LDMFA**)

- Empty stack → SP points to just before the stack space
- Pushing on the stack → SP to be **I**ncremented **B**efore (**STMIB**)
- Popping off the stack → SP to be **D**ecremented **A**fter (**LMDA**)

Grows up

Block Moves and Stack Operations

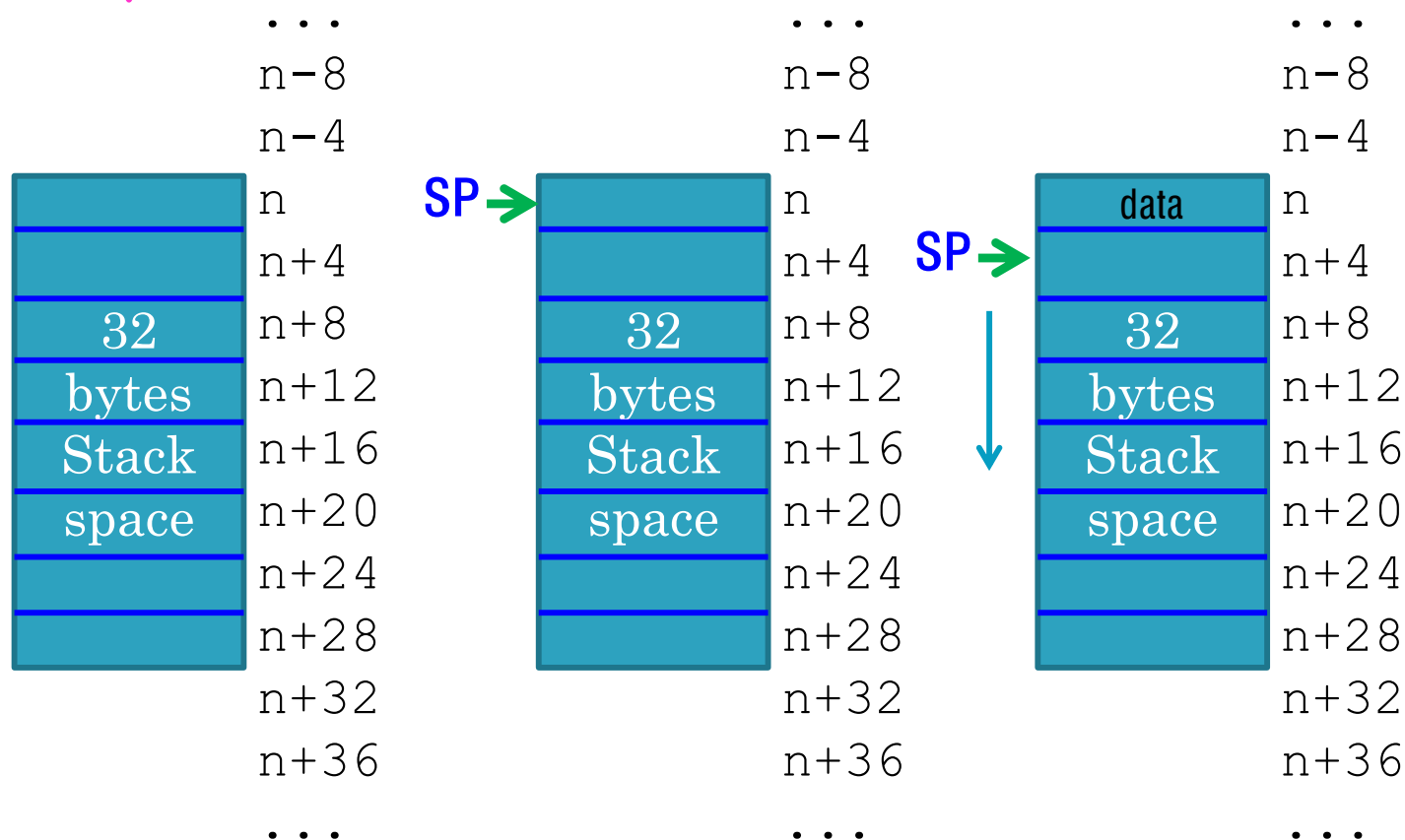


STMED = STMDA
LDMED = LDMIB.

□ Stack type: **ED** (i.e., Class=**E**mpy and Stack growth=**D**escending)
(**STMED** and **LDMED**)

- Empty stack → SP points to the last memory word in the stack
- Pushing on the stack → SP to be **D**ecremented **A**fter (**STMDA**)
- Popping off the stack → SP to be **I**ncremented **B**efore (**LDMIB**)

Block Moves and Stack Operations



$STMEA = STMIA$
 $LDMEA = LDMDB$

□ Stack type: **EA** (i.e., Class=**E**Empty and Stack growth=**A**scending)
 (**STMEA** and **LDMEA**)

- Empty stack → SP points to the first memory word in the stack
- Pushing on the stack → SP to be **I**ncrement **A**fter (**STMIA**)
- Popping off the stack → SP to be **D**ecrement **B**efore (**LDMDB**)

Block Moves and Stack Operations

□ A stack operation can be described either by

▪ *what* it does

- *FD Full Descending*
- *FA Full Ascending*
- *ED Empty Descending*
- *EA Empty Ascending*

▪ *how* it does

- *DB Decrement Before*
- *DA Decrement After*
- *IB Increment Before*
- *IA Increment After*

FD, FA, ED, and EA
are *pseudo* notation.

The assembler will translate
these *pseudo* notation to the
IA, DB, DA, and IB
notation.

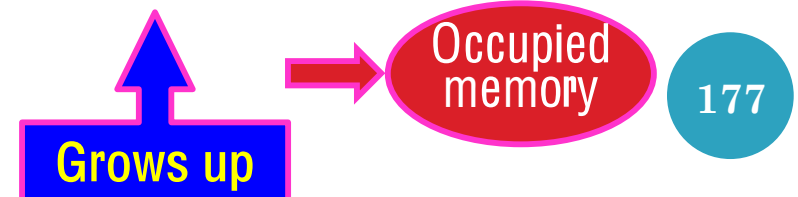
For example,

□ We can write **STMFD sp!, {r0, r1}** when pushing r0 and r1 onto the stack,

▪ Also can be written as **STMDB sp!, {r0, r1}**

□ We can write **LDMFD sp!, {r0, r1}** when popping r0 and r1 off the stack.

▪ Also can be written as **LDMIA sp!, {r0, r1}**



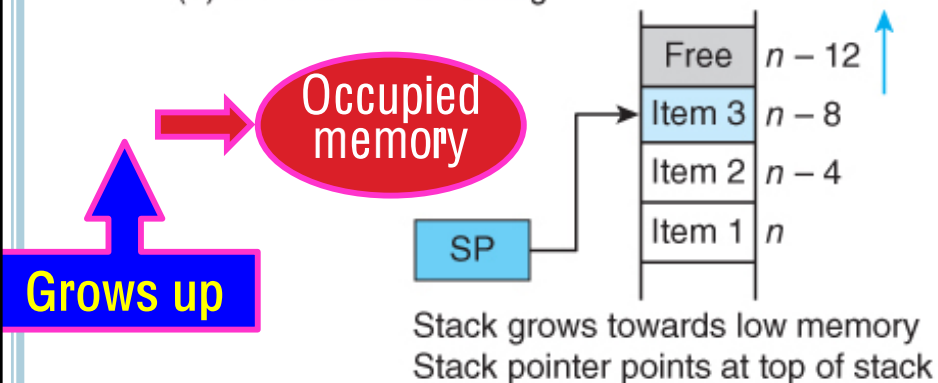
Block Moves and Stack Operations

❑ The ARM's literature uses four terms to describe stacks:

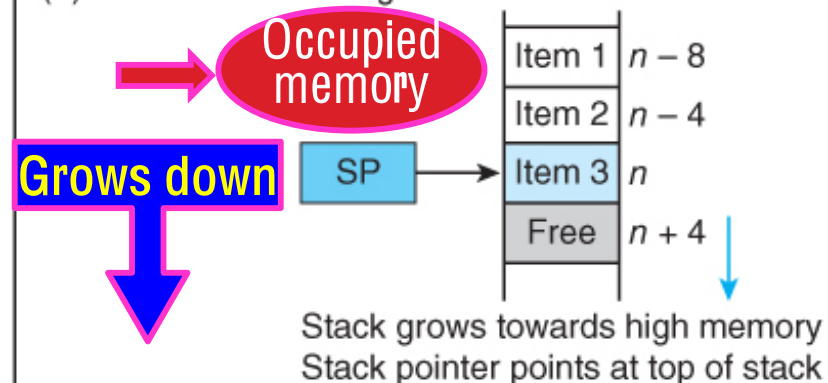
- | | | | | |
|-------|-------------------------|--------------|----|---------|
| a) FD | <i>full descending</i> | Figure 3.52a | DB | $F = B$ |
| b) FA | <i>full ascending</i> | Figure 3.52b | LB | $E = A$ |
| c) ED | <i>empty descending</i> | Figure 3.52c | DA | |
| d) EA | <i>empty ascending</i> | Figure 3.52d | LA | |

FIGURE 3.59 ARM's four stack modes

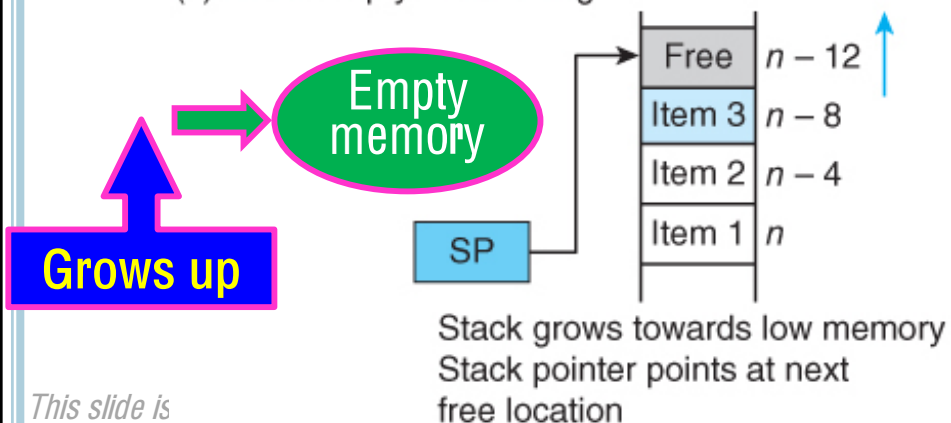
(a) Stack full descending



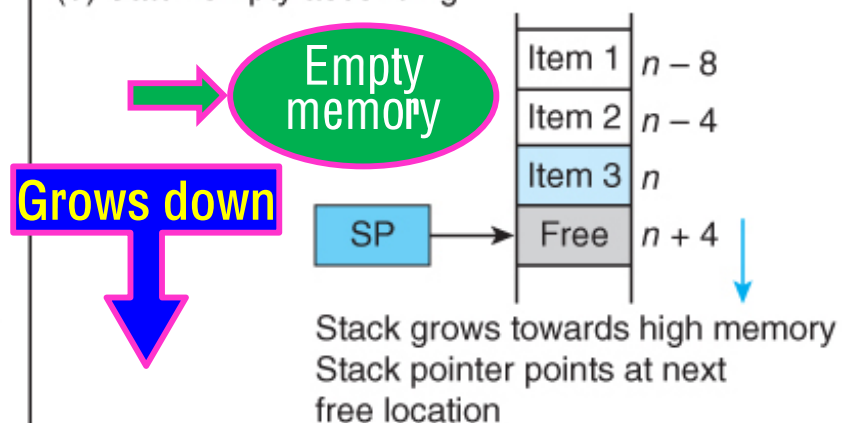
(b) Stack full ascending



(c) Stack empty descending



(d) Stack empty ascending

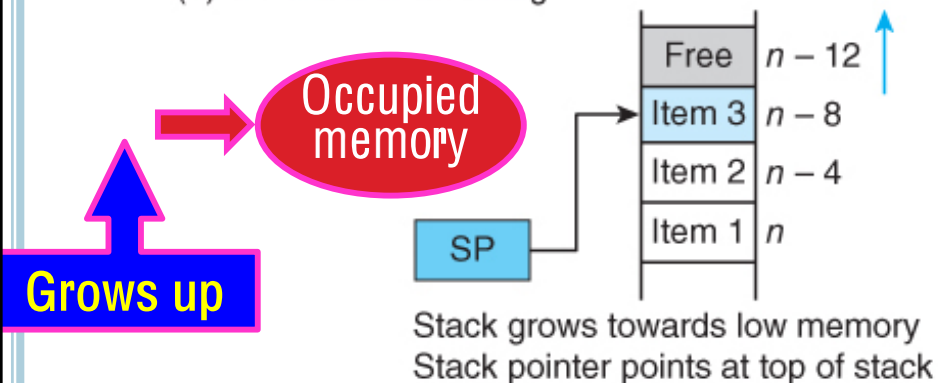


Block Moves and Stack Operations

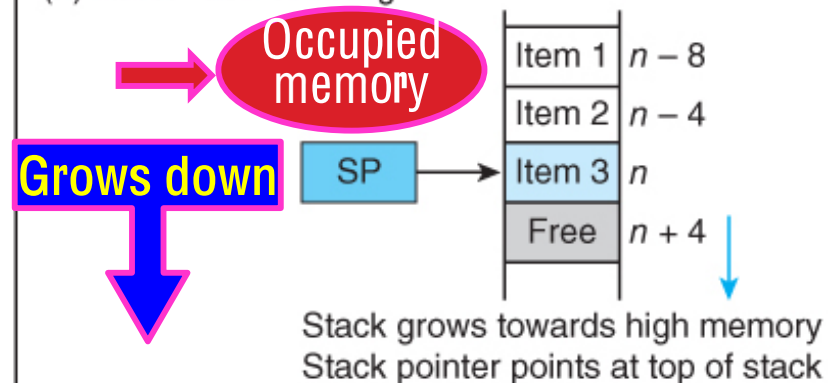
- ❑ A stack is described as *full* if the stack pointer *points to the top element* of the stack.
- ❑ If the stack pointer *points to the next free* element in the stack, then the stack is called *empty*.

FIGURE 3.59 ARM's four stack modes

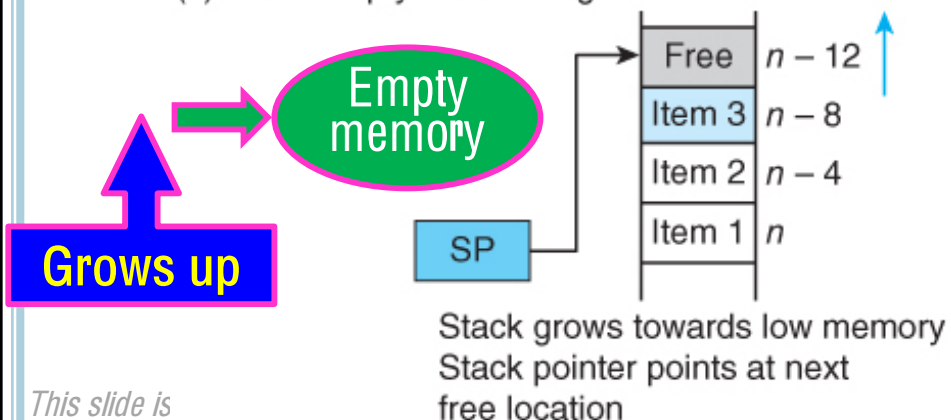
(a) Stack full descending



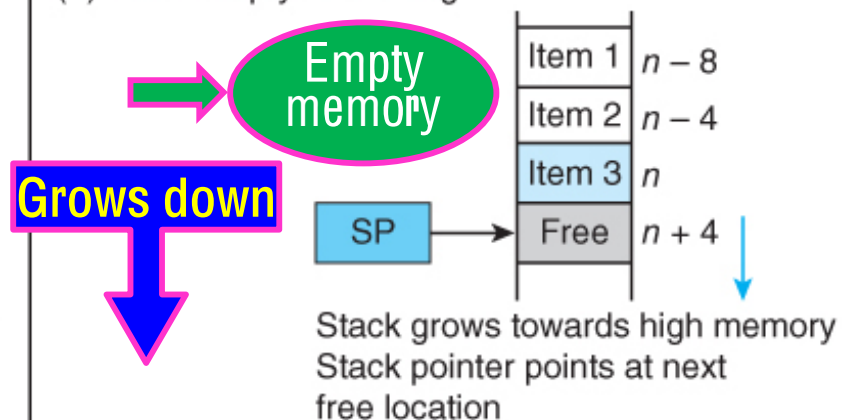
(b) Stack full ascending



(c) Stack empty descending



(d) Stack empty ascending



Block Moves and Stack Operations

❑ ARM's block move instruction is useful because it supports **four** possible **stack types**.

❑ The differences among these four types are

- the **direction** in which the stack grows
 - up (i.e., descending toward lower addresses), or
 - down (i.e., ascending toward higher addresses)

Bit#23 (Up/down)

ARM uses the terms **ascending** and **descending** to describe the growth of the stack toward **higher** or **lower** addresses, respectively.

- whether the **stack pointer points at**
 - the item currently at the **top of the stack** or
 - the **next free item** on the stack.

Bit#24 (Pre-post)

Block Move Example

- ❑ The block move provides a convenient means of copying data between memory regions. ***This is NOT a stack application.***

ADR r0, Table1

- ❑ In the next example we copy 256 words (1024 bytes) from Table 1 to Table 2.

32 x 8

```

ADR    r0, Table1    ; r0 points to source
                        ; (note pseudo-op ADR)

ADR    r1, Table2    ; r1 points to the destination

MOV    r2, #32 counter ; 32 blocks of 8 = 256 words to move
                        ; 4x8

Loop LDMEA r0!, {r3-r10} ; REPEAT Load 8 registers (r3 to r10)
      STMFA r1!, {r3-r10} ; store the registers at
each loop for one block ; their destination

SUBS   r2, r2, #1    ; decrement loop counter
BNE    Loop          ; UNTIL all 32 blocks of
                        ; 8 registers moved
  
```

Is it right to
use LDMFD and STMFD?

memory → r0 → r1 → memory

- ❑ The two block move instructions above allow us to move eight registers (i.e., 32 bytes) at once.

Block Move Example

- ❑ The block move provides a convenient means of copying data between memory regions. ***This is NOT a stack application.***
- ❑ In the next example we copy 256 words (1024 bytes) from Table 1 to Table 2.

```

ADR    r0, Table1    ; r0 points to source
                        ; (note pseudo-op ADR)
ADR    r1, Table2    ; r1 points to the destination
MOV    r2, #32        ; 32 blocks of 8 = 256 words to move
Loop   LDMIA r0!, {r3-r10} ; REPEAT Load 8 registers (r3 to r10)
      STMIA r1!, {r3-r10} ; store the registers at
                        ; their destination
      SUBS r2, r2, #1    ; decrement loop counter
      BNE Loop          ; UNTIL all 32 blocks of
                        ; 8 registers moved

```

LDMIA and **STMIA**,
not **LD~~R~~FD** and **ST~~R~~FD**
Not correct in the book page 220

- ❑ The two block move instructions above allow us to move eight registers (i.e., 32 bytes) at once.