# 實驗二 ARM Assembly II

#### 0610032 林仲偉

1. What 實驗要做什麼

熟悉基本 ARMv7 組合語言語法使用。

- 2. How 實驗要怎麼做
  - I. Postfix arithmetic (50%)

操作 stack 來完成 postfix 的加減法運算

每次都讀入一個字元(R2, in asci value),依照該字元決定操作。

```
load:

ldrb r2, [r0, r1] //r2: byte loader cmp r2, #0 //0: end of string? beq save cmp r2, #32 //verifying the space beq next cmp r2, #43 //+ beq ad cmp r2, #45 //-| beq sub_or_neg // check '-' is number or operation?
```

● R2 不觸發上述任何 branch: 默認為數字,把 ascii 轉 int 後再 push

```
atoi:
//TODO: implement a "convert string to integer"
ldrb r2, [r0, r1]
cmp r2, #32
beq back
mul r3, r3, r5
sub r2, r2, #48
add r3, r3, r2
add r1, r1, #1
b atoi
back:
bx lr //bx: branch by reg context
```

讀到空白字元時 branch back,否則就一直讀新值&舊值<=舊值\*10+新值 記得 ascii 要 -48 就能轉成單一字元表示的數字(0:9 = ascii(48:57))。

● R2=0: 讀到 end of string,就把 stack 內結果(應該只會剩一個)pop 並存入 result。

```
save:
   pop {r7}
   str r7, [r4]
```

● R2=32: 讀到 space,直接繼續讀下一個。

```
next:
    add r1, r1, #1 //skipping the space
    b load
```

● R2=43: operation +: pop 兩個數字做運算再 push

```
ad: //add and push back result
pop {r8}
pop {r7}
add r7, r7, r8
push {r7}
b next
```

● R2=45: 需要先看是 operation 還是 sign:

再 load 下一個字元,如果是空格就是 operation; 否則是 sign

```
sub_or_neg:
   add r1, r1, #1
   ldrb r2, [r0, r1] //loading next byte to determine
   cmp r2, #32
   beq sb //it's sub
```

Operation:和+一樣,pop 兩個數字做運算再 push

```
sb:

pop {r8}

pop {r7}

sub r7, r7, r8

push {r7}
```

Sign: 和把 ascii 轉 int 後再 push 一樣,只是多了一個 RSB 來反轉正負

```
//otherwise it's neg
bl atoi // bl: update lr
rsb r3, r3, #0 //reverse
push {r3}
mov r3, #0
b next
```

● 每個區塊最後都要跳下一個字元: branch to "next"

```
next:
   add r1, r1, #1 //skipping the space
   b load
```

最後結果:

```
main.s 🛭
          .syntax unified
                                                                                                                                                             Monitors

        • × *
        0x200000000 : 0x200000000 < Signed Interest</td>

    0x20000000
    0x80001c8
    0x20017ff4

                                                                                                                                                                                                           Address
                                                                                                                                                                                                            99999999999999
           user_stack: .zero 128
expr_result:.word 0
postfix_expr: .asciz = -100 10 20 + - 10 + "// no minus temporarily
.text
                                                                                                                                                                 0x20000080
                                                                                                                                                                                                             0000000020000020
                                                                                                                                                                 0x20000080
                                                                                                                                                                                                            0000000020000030

    0×20000080

         .text
.global main
main:
LDR R0, =postfix_expr //r0: postfix_expr_ptr
ldr r4, =expr_result //r4: expr_result_ptr
mov r6, #0 //r6: result reg
mov r6, #10 //r6: constant (for MUL)
TOOD: Satur stack pointer to and of user stack and calculate the
                                                                                                                                                                                                            0000000020000060
                                                                                                                                                                                                             0000000020000070
                                                                                                                                                                                                            000000020000080 -120
000000020000090 824192288
```

# II. 求最大公因數並計算最多用了多少 stack size (50%)

## • Code:

```
1.syntax unified
2.cpu cortex-m4
3.thumb
  5.data
 6 result: .word 0
7 max size: .word
       max_size: .word 0
  8.text
9 m: .word 0x0C
10 n: .word 0x24
 11.global main
 12
13
 14 exita:
15 mov r6, r1
16 pop {r7}
      pop {pc}
18
19 exitb:
20 mov r6, r0
21 pop {r7}
22 pop {pc}
 23
24 gcd:
     mov r5, #1
      cmp r0, #0
beq exita
 26
                       // a == 0
 27
      29
 31
 35
 37
      beg state2
      subs r4, r0, r1 // abs(a - b)
cmp r4, #0
it lt
 39
40
      neglt r4, r4
42
43
      cmp r0, r1
it lt
                          // min(a, b)
      movlt r1, r0
      mov r0, r4
b next
45
46
48 state1:
49
     lsr r0, #1
      cmp r3, #0
50
51
      moveq r5, #2
     beq state2
b next
53
54
56 state2:
57 lsr r1, #1
58 b next
60 next:
61 push {lr}
      push {r5}
      add r8, r8, #2
      bl gcd
64
65
66 right:
67 mul r6, r6, r7
68 pop {r7}
69 pop {pc}
70
71
72 main:
      ldr r0, m
      ldr r1, n
      mov r8, #0
mov r9, #8
bl gcd
mul r6, r6, r7
75
76
     mul r8, r8, r9
ldr r10, =result
ldr r11, =max_size
82 str r6, [r10]
83 str r8, [r11]
84 L: b L
```

#### ● 主程式部分

1. 本程式使用了r0~rll的register,功能如下。

r0	儲存並運算m的值
rl	儲存並運算n的值
r2	m % 2 的結果
r3	n % 2 的結果
r4	abs(m, n)
r5	要儲存的乘數 (1 或 2)
r6	gcd 的結果
r7	被取出的乘數
r8	stack size
r9	儲存數字8
r10	儲存 result 的位置
r11	儲存 max_size 的位置

- 2. 將 m 和 n 值讀入 r 0 和 r 1, 跳至 gcd 進行運算。
- 3. Stein's algorithm 可被判斷式分為 6 種情況,其中 4 種須再次呼叫 gcd,在此介紹根據判斷式所跳至的區塊及其需進行的工作。
- **若**r0 == 0,跳至 exita: 將 rl 的值放入象徵 result 的 r6,將之前存的 位置由 stack pop 出至 pc。
- 若 r1 == 0, 跳至 exitb: 將 r0 的值放入象徵 result 的 r6, 將之前存的 位置由 stack pop 出至 pc。。
- **若** r0 % 2 == 0, 跳至 state1: 將 r0 除以 2, 判斷 r1 是不是同時也是偶數,若是,將乘數 r5 設定為 2, 跳至 state2, 若非,則跳至 next。
- 若 r1 % 2 == 0, 跳至 state2: 將 r1 除以 2, 然後跳至 next。
- 若以上情況皆不符合,則將 r0 和 r1 設為 abs(r1-r0)和 min(r1, r0)
- abs(r1-r0)的作法:將兩者相減的結果與 0 比較,若小於 0 則使之 neg。
- min(rl,r0)的作法:將兩者相比,若r0較小則移入rl,反之則不處理。
- next: 進入此區塊表示需進行下次 gcd。將 lr 及乘數 r5 push 至 stack,並將紀錄 stack size 的 r8 加 2,利用 bl 重新跳至 gcd。
- right:由於right 位於 next 下方,因此當 exita 或 exitb pop 出位置至 pc 後,便會跳至此區塊。將 r6 與乘數 r7 相乘,再 pop 出下次需要的位置和乘數。
- 4. 由於最初紀錄的乘數與返回 main 的位置同時被取出,未被計算到,因此返回 main 後,先將最後一次取出的乘數與 r6 相乘,得到正確的結果。再將記錄 stack size 的 r8 乘上 8 已表示 byte。最後再將此兩項存入 result 與 max\_size 的位置即可完成。



## 3. Feedback 實驗心得或建議

Lab2 PDF 內,把 ascii 放在 text section(程式文字檔區)會被誤認為是 instruction.

```
6 expr_result:.word 0
7 .text
8 .global main
9 postfix_expr:.asciz "100 10 20 + - 10 +" // no minus temporarily
10 main:
11 LDR R0, =postfix_expr
12
13//TODO: Setup stack pointer to end of user_stack and calculate the
14//expression using PUSH, POP operators, and store the result into expr_result
15 mov r1, #0 //an ASCII is 18 wide
16 ldr r2, [r0]
17 b atoi

CONSOLE ** Tasks ** Problems ** Executables ** Debugger Console
CDT Build Console [Lab2-2]
arm-none-eabi-gcc -mcpu=cortex-m4 -mthumb -mfloat-abi=hard -mfpu=fpv4-sp-d16 -T"D:/微處理應系統實驗/Lab2/Lab2-2/LinkerScript.ld" -W1,-startup/startup_stm32.o: In function 'LoopFillZerobss':
D:\微處理應系統實驗/Lab2/Lab2-2/Debug/../startup/startup_stm32.s:83: undefined reference to `main' collect2.exe: error: ld returned 1 exit status
```

#### Solution on StackOverflow:

on Ubuntu 16.04 aarch64-linux-gnu-gcc 5.4.0.

Now, if you remove the references to the msg variable:

```
.text
.global _start
_start:
asm_main_after_prologue:
    /* exit */
    mov x0, #0
    mov x8, #93
    svc #0
msg:
    .ascii "hello syscall v8\n"
len = . - msg
```

it starts failing with:

```
hello.S: Assembler messages:
hello.S: Error: unaligned opcodes detected in executable segment
```

So somehow, when references are removed, it must be thinking that the  $$\tt hello$$  syscall v8 string is an instruction instead of data.