Xiaobin Zhuang - 300519184
ECEN301 Lab 6
22/09/2020

Objectives

The purpose of this lab session is to study the debug capabilities of JTAG.

Methodology

Step 4: I changed the value of R0 from 0x00000000 to 0x00000001, which shown in figure 1.

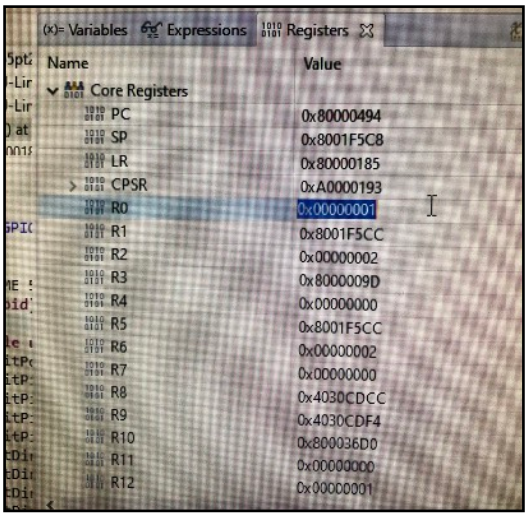

fig. 1

Step 5: found “Memory browser”, searched the value of the SP (0x8001F328). Shown in the figure below with red underline.

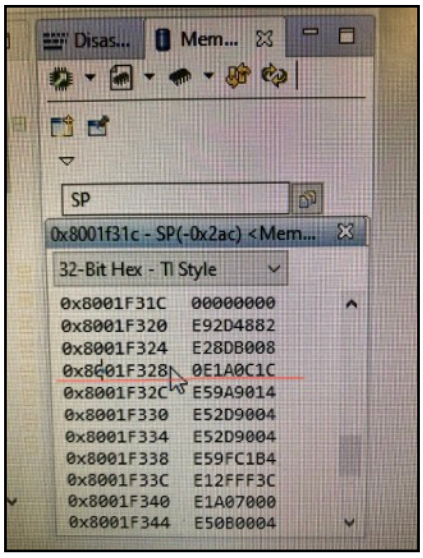

fig. 2

Step 6: I clicked on the small green arrow which means step into one single instruction. Then the green bar has moved down one step in the disassembler window. Also, the yellow highlighting in

the resisters window indicated the PC and SP resisters and memory have altered. They are shown in figure 3.

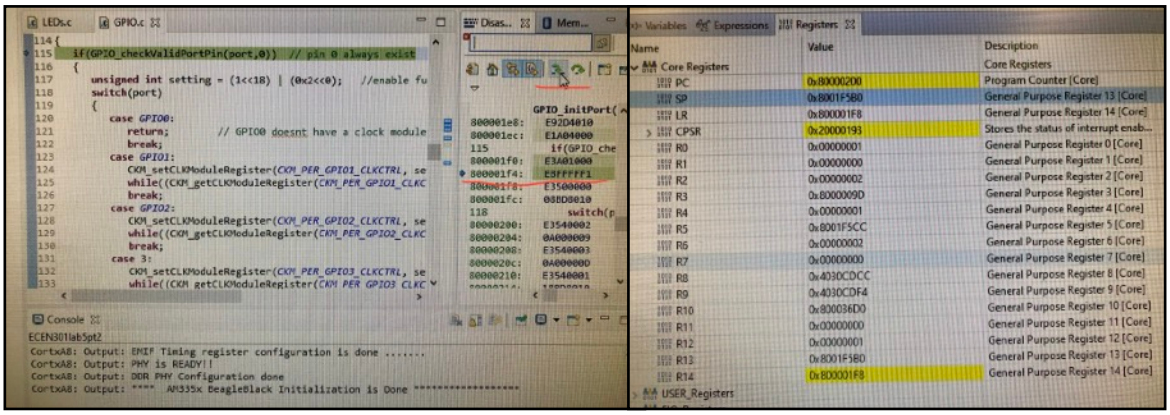

fig .3

Step 7: I changed the value of memory 0x8001F328 in the memory view window, changed from 0E1A0C1C to 0E1A0C2C. Shown in the figure below.

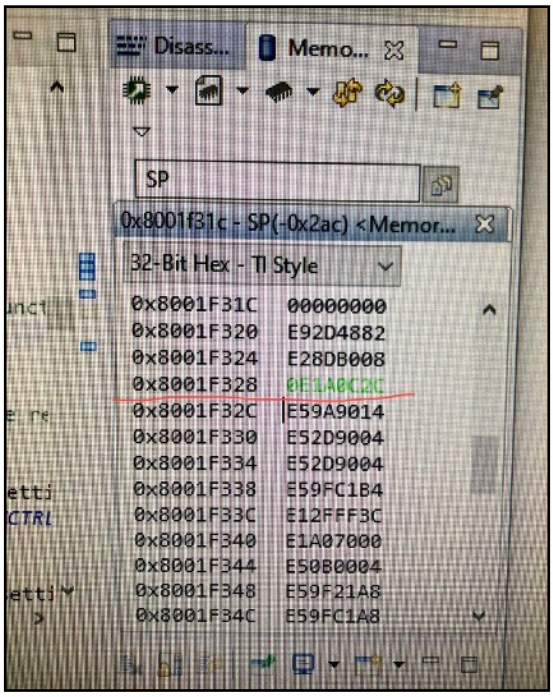

fig .4

Step 9: when I executed the code in the zip file, the “Z” flag remain 0. After changing the ADDS instruction to ADD, the “Z” flag changed from 0 to 1.

Step 10: to set “N” and “GE” bits, we have to know that the “N” bit set if result is negative, the “GE” bit set if result is greater or equal.
The figure below showed the code and bits values.

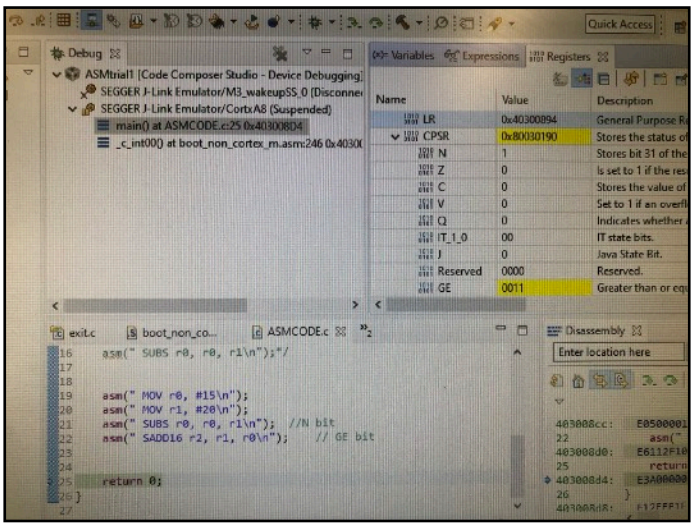

fig .5

The explanation of code:

MOV r0, #15\n: move R0 to 15 *MOV r1, #20*\n: move R1 to 20

SUBS r0, r0, r1\n: R0 = R0 - R1, the result was negative, so the “N” bit has been set to 1.

SADD16 r2, r1, r0\n: R2 = R1 + R0, the result (R2) was greater than R1 and R0, so the “GE” bit has been set to 0011.

There was an issue when I set “GE” bits. I initially used CMP instruction to compare R0 and R1, if R1 > R0, the “GE” bit should be set. However, it didn’t work.

Step 12: set a breakpoint at line 28 of the C code as shown in figure 6, then run the program. The four LEDs lighted up, but the program halted execution at the breakpoint.

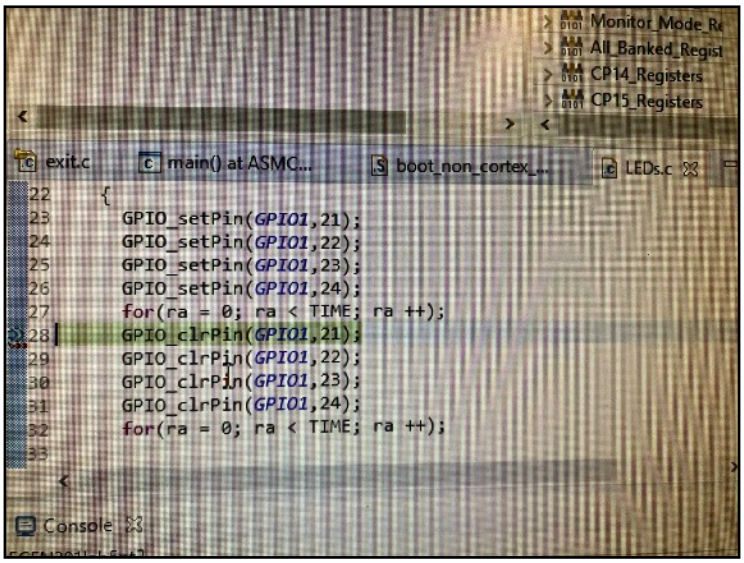

fig. 6

Then clicked the step over arrow (F6), the program jumped over the breakpoint. When I pressed F6 a few times, the program kept running and the LEDs turned off one by one.

Questions:

Q1: 80000494: E52DE004 str lr, [sp, #-4]!
First line of the code means push a link resists on the stack pointer after subtract the stack pointer by a 4 bytes. The ! Indicates that the change in the stack pointer is to be kept.
80000498: E24DD00C sub sp, sp, #0xc
Allocating 0xc bytes of stack space for local variables.

Q2: the flag can be set by using ADDS, while ADD can't achieve this. Because data processing instructions do not affect the condition code flags but the flags can be optionally set by using "S".

Q3:

Abbreviation	Signal	Description
TCK	Test Clock	Synchronizes the internal state machine operations.
TMS	Test Mode Select	Sampled at the rising edge of TCK to determine the next state.
TDI	Test Data In	Represents the data shifted into the device's test or programming logic. It is sampled at the rising edge of TCK when the internal state machine is in the correct state.
TDO	Test Data Out	Represents the data shifted out of the device's test or programming logic and is valid on the falling edge of TCK when the internal state machine is in the correct state.
TRST	Test Reset	An optional pin which, when available, can reset the TAP controller's state machine.