PCS3432 - Laboratório de Processadores

Relatório - E9

Bancada B8

Bruno Mariz	11261826
Roberta Andrade	11260832

9-2-1

Os códigos foram compilados e linkados utilizando os comandos abaixo, e em seguida foi utilizado o GDB em um terminal separado para adicionar o breakpoint e executar o programa.

```
sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9$ eabi-gcc c_entry.c -o c_entry.o
sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9$ eabi-as startup.s -o startup.o
sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9$ eabi-ld -T vector_table.ld c_entry.o startup.o -o program.elf
sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9$ eabi-bin program.elf program.bin
sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9$ qemu program.bin
pulseaudio: set_sink_input_volume() failed
pulseaudio: Reason: Invalid argument
pulseaudio: Reason: Invalid argument
qemu-system-arm: terminating on signal 15 from pid 8012 ()
sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9$ qemu program.bin
pulseaudio: set_sink_input_volume() failed
pulseaudio: Reason: Invalid argument
pulseaudio: Reason: Invalid argument
qemu-system-arm: terminating on signal 15 from pid 8353 ()
sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9$
```

9-2-2

Foram compilados os códigos conforme indicado no enunciado, e então foi utilizado o GDB para executar o programa.

```
-Register group: general
                                                                 r1
r3
r5
r7
                                                                                  0x0
                                                                                            0
                            0
                                                                                            0
                  0x0
                                                                                  0x0
 r4
                                                                                            0
                  0x0
                                                                                  0x0
                            0
                                                                                            0
                  0x0
                                                                                  0x0
                            0
                  0x0
                                                                                  0x0
                                                                                            0
 r10
                                                                 r11
                                                                                  0x1094
                                                                                            4244
                  0x0
                            0
      -c_entry.c-
              void c_entry() {
               print uart0("Hello world!\n");
B+>
    13
                                                                                                           Line: 11
                                                                                                                      PC: 0x70
remote Thread 1 In: c_entry
c_entry c_entry.
(gdb) break c_entry
            c_entry.c
Breakpoint 1 at 0x70: file c_entry.c, line 11.
(gdb) c
Continuing.
Breakpoint 1, c_entry () at c_entry.c:11
(gdb)
```

```
-Register group: general
                                                                      r1
r3
r5
 r0
                   0x0
                              0
                                                                                        0 \times 0
 r2
r4
                   0x0
                              0
                                                                                        0x0
                   0x0
                                                                                        0x0
 r6
                   0x0
                              0
                                                                                        0x0
                              0
                                                                      r9
                   0x0
                                                                                        0x0
r10
                   0x0
                              0
                                                                      r11
                                                                                        0x1094
                                                                                                   4244
       -c entry.c
    10
              void c_entry() {
B+> 11
               print_uart0("Hello world!\n");
    12
13
     14
remote Thread 1 In: c entry
Breakpoint 1 at 0x70: file c_entry.c, line 11.
                                                                                                                    Line: 11
                                                                                                                                 PC: 0x70
(gdb) c
Continuing.
Breakpoint 1, c_entry () at c_entry.c:11
Continuing.
```

Ao rodar o comando de print na imagem acima, foi observada a saída "Hello, world!" no outro terminal, que pode ser observada na imagem abaixo:

```
    sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9/9-2-2$ eabi-gcc c_entry.c -o c_entry.o
    sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9/9-2-2$ eabi-as startup.s -o startup.o
    sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9/9-2-2$ eabi-ld -T vector_table.ld c_entry.o startup.o -o program.elf
    sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9/9-2-2$ eabi-bin program.elf program.bin
    sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9/9-2-2$ qemu program.bin
    pulseaudio: set_sink_input_volume() failed
    pulseaudio: Reason: Invalid argument
    pulseaudio: Reason: Invalid argument
    Hello world!
```

9-2-3

```
-Register group: general-
                                                                                                   0
0
                   0x0
                                                                      r1
r3
r5
r7
                                                                                         0x0
                   0x0
                                                                                         0x0
 r4
                   0x0
                                                                                         0x0
 r6
                                                                                         0x0
                   0x0
                   0x0
                                                                      r9
                                                                                         0x0
 r10
                   0x0
                                                                                         0x0
                                                                                                   0
               .global _Reset
                Reset:
                 B Reset_Handler /* Reset */
                 B Undefined_Handler /* Undefined */
                 B . /* SWI */
B . /* Prefetch Abort */
                                                                                                                     Line: 4
                                                                                                                                  PC: 0x0
remote Thread 1 In: Reset
Transfer rate: 1976 bits in <1 sec, 123 bytes/write. (gdb) b c
c_entry c_entry.c
(gdb) b c_entry
Breakpoint 1 at 0x98
             c_entry.c char
(gdb) b Undefined
Breakpoint 2 at 0xb4
(gdb)
```

```
Breakpoint 1, 0x00000098 in c_entry () (gdb) c
Continuing.

Breakpoint 2, 0x00000004 in Undefined () (gdb) c
Continuing.
```

Ao executar o código, foram executadas as funções Reset_Handler, primeiramente, que fez com que "Hello world!" fosse printado no terminal:

```
sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9/9-2-3$ qemu program.bin
pulseaudio: set_sink_input_volume() failed
pulseaudio: Reason: Invalid argument
pulseaudio: set_sink_input_mute() failed
pulseaudio: Reason: Invalid argument
Hello world!
```

Após o segundo comando "continue", foi executada a instrução inválida, o que fez o programa saltar para a subrotina Undefined_Handler, que por sua vez chamou a função Undefined, que printou "instrução inválida!" no terminal:

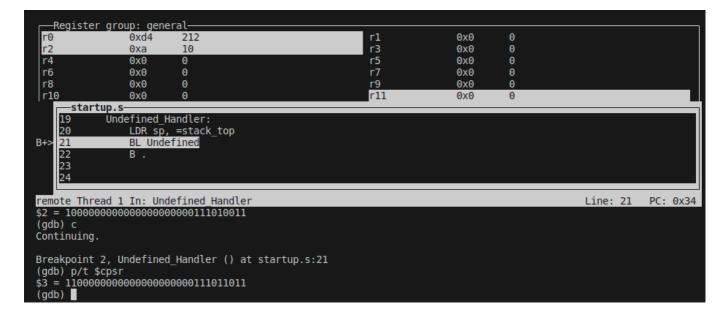
```
sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9/9-2-3$ qemu program.bin
pulseaudio: set_sink_input_volume() failed
pulseaudio: Reason: Invalid argument
pulseaudio: set_sink_input_mute() failed
pulseaudio: Reason: Invalid argument
Hello world!
instrução inválida!
```

9-2-4

Ao rodar o código, o programa vai para o Reset_Handler, que chama a função c_entry. Nesse momento, o modo do processador está em Supervisor (0b10011 nos ultimos 5 bits do CPSR):

```
-Register group: general-
 r0
                   0xd4
                              212
                                                                                      0x0
                                                                    r3
                   0x0
                                                                                      0x0
                                                                                                 0
 r2
 r4
                              0
                                                                     r5
                                                                                      0x0
                                                                                                 0
                   0x0
 r6
                   0x0
                              0
                                                                                      0x0
                                                                                                 0
 r8
                   0x0
                              0
                                                                                      0x0
                                                                                                 0
                              0
                                                                                      0x10f4
                                                                                                 4340
                   0x0
 r10
       c_entry.c
              void print_uart0(const char *s) {
               while(*s != '\0') { /* Loop until end of string */
                *UARTODR = (unsigned int)(*s); /* Transmit char
               s++; /* Next char */
remote Thread 1 In: print_uart0
Single stepping until exit from function c_entry,
                                                                                                                 Line: 4
                                                                                                                              PC: 0x50
which has no line number information.
print_uart0 (s=0xd4 "Hello world!\n") at c_entry.c:4
(gdb) p/x $cpsr
$1 = 0x400001d3
(gdb) p/t $cpsr
$2 = 10000000000000000000000111010011
(gdb)
```

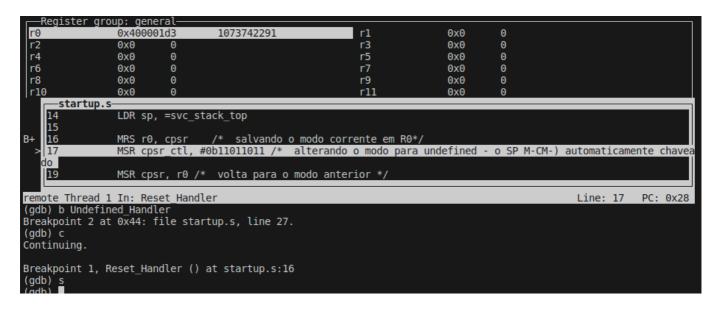
Após executar a instrução indefinida do Reset_Handler, o programa pula para a subrotina Undefined_Handler, e é possível observar que o modo do processador nesse momento está em Undefined (0b11011):



O programa então entra em loop infinito e permanece nesse modo.

9-2-5

Foi executado o código utilizando o gdb e foi possível observar o registrador CPSR salvo em r0:



A mudança de modo, e o SP_undef com o valor 0x0:

```
-Register group: general-
 r0
                   0x400001d3
                                       1073742291
                                                                    r1
r3
r5
r7
                                                                                      0x0
 r2
r4
                   0 \times 0
                                                                                      0x0
                   0x0
                              0
                                                                                      0x0
 r6
                   0x0
                              0
                                                                                      0x0
                                                                                                 0
                                                                    r9
                                                                                                 0
                   0x0
                                                                                      0x0
r10
                   0x0
                              0
                                                                    r11
                                                                                      0x0
                                                                                                 0
       startup.s
B+
                   MRS r0, cpsr
                                          salvando o modo corrente em R0*/
                                   #0b11011011 /* alterando o modo para undefined - o SP M-CM-) automaticamente chave
    17
                   MSR cpsr ctl,
                  LDR sp, =undefined stack top /* a pilha de undefined M-CM-) setada */
MSR cpsr, r0 /* volta para o modo anterior */
    18
    19
    20
                   BL c_entry
remote Thread 1 In: Reset Handler
                                                                                                                 Line: 18
                                                                                                                              PC: 0x2c
(gdb) s
(gdb) s
Reset_Handler () at startup.s:18
(gdb) p/t $cpsr
$1 = 1000000000000000000000111011011
(gdb) p/x $sp
$2 = 0x0
(dbp)
```

A alteração do valor de SP_undef para 0x2000:

```
-Register group: general
                                                                        r1
r3
r5
r7
                    0x400001d3
                                          1073742291
                                                                                            0x0
                                                                                                       0
 r0
                    0x0
                               0
                                                                                            0x0
                                                                                                       0
                    0x0
                                                                                            0x0
 r6
                    0x0
                                                                                            0x0
 r8
                    0x0
                               0
                                                                         r9
                                                                                            0x0
                                                                                                       0
                    0x0
                                                                                            0x0
       startup.s
                    MRS r0, cpsr
B+
                                             salvando o modo corrente em R0*/
                    MSR cpsr_ctl, #0b11011011 /* alterando o modo para undefined - o SP M-CM-) automaticamente chave LDR sp, =undefined_stack_top /* a pilha de undefined M-CM-) setada */
     17
     18
                   MSR cpsr, r0 /* volta para o modo anterior */
     19
     20
                    BL c_entry
remote Thread 1 In: Reset_Handler
                                                                                                                        Line: 19
                                                                                                                                      PC: 0x30
$1 = 10000000000000000000000111011011
(gdb) p/x $sp
$2 = 0x0 (gdb) s
Reset_Handler () at startup.s:19
(gdb) p/x $sp
$3 = 0x2000
(gdb)
```

A saída do modo Undefined e o valor de SP svc em 0x1000:

```
-Register group: general
                                                                     r1
r3
r5
r7
 r0
                   0x400001d3
                                        1073742291
                                                                                        0x0
                                                                                                   0
                                                                                                   0
 r2
r4
                   0x0
                                                                                        0x0
                   0x0
                              0
                                                                                        0x0
                   0x0
                                                                                        0x0
                   0x0
                              0
                                                                      r9
                                                                                        0x0
                                                                                                   0
 r10
                   0x0
                                                                                        0x0
       startup.s
                   MSR cpsr, r0 /* volta para o modo anterior */
     20
                   BL c_entry
.word 0xffffffff
     21
     22
23
                   В.
remote Thread 1 In: Reset Handler
                                                                                                                                PC: 0x34
                                                                                                                   Line: 21
$3 = 0x2000
(gdb) s
Reset_Handler () at startup.s:21
(gdb) p/t $cpsr
$4 = 100000000000000000000111010011
(gdb) p/x $sp
$5 = 0x1000
(gdb)
```

Continuando o programa, é possível observar o comportamento esperado após encontrar a instrução inválida do Reset Handler:

```
-Register group: general-
                   0xf4
                              244
                                                                    r1
r3
r5
r7
 r2
                   0x21
                              33
                                                                                      0x0
                                                                                                 0
 r4
                   0x0
                                                                                      0x0
                   0 \times 0
                              Θ
                                                                                      0 \times 0
                   0x0
                              0
                                                                    r9
                                                                                      0x0
                                                                                                 0
r10
                   0x0
                              0
                                                                                      0x0
                                                                                                 0
      -startup.s-
              Undefined Handler:
                  BL Undefined
B+> 27
     28
    29
remote Thread 1 In: Undefined_Handler
                                                                                                                 Line: 27
                                                                                                                             PC: 0x44
(gdb) p/x $sp
$5 = 0x1000
(gdb) n
Undefined_Handler () at startup.s:26
(adb) n
Breakpoint 2, Undefined_Handler () at startup.s:27
(gdb)
```

```
sexta@bancada8:~/projects/labproc/src/e9/relatorio/src_e9/9-2-5$ qemu program.bin
pulseaudio: set_sink_input_volume() failed
pulseaudio: Reason: Invalid argument
pulseaudio: set_sink_input_mute() failed
pulseaudio: Reason: Invalid argument
Hello world!
instrução inválida!
```

9-2-6

Código utilizado na questão:

```
.section INTERRUPT_VECTOR, "x"
.global _Reset
_Reset:
  B Reset_Handler /* Reset */
  B Undefined_Handler /* Undefined */
  B . /* SWI */
  B . /* Prefetch Abort */
  B . /* Data Abort */
  B . /* reserved */
  B . /* IRQ */
  B . /* FIO */
Reset_Handler:
    LDR sp, =svc_stack_top
    MRS r0, cpsr /* salvando o modo corrente em R0*/
    MSR cpsr_ctl, #0b11011011 /* alterando o modo para undefined - o SP é
automaticamente chaveado ao chavear o modo*/
    LDR sp, =undefined_stack_top /* a pilha de undefined é setada */
    MSR cpsr, r0 /* volta para o modo anterior */
    .word 0xffffffff
```

```
BL c_entry
B .

Undefined_Handler:
STMFD sp!, {r0-r12,lr}
BL Undefined
vesaida:
LDMFD sp!, {r0-r12,pc}^
```

Ao executar o programa acima, e foram feitos os prints em cada etapa, observando ao fim que a função Undefined foi executada e depois o código retornou ao ponto onde estava em Reset_Handler, onde foi chamado c_entry:

```
-Register group: general
0 0x400001d3
                                        1073742291
 r0
                                                                     r1
r3
r5
r7
                                                                                       0x0
                                                                                                 0
                   0x0
                              Θ
                                                                                       0x0
 r4
                   0x0
                              0
                                                                                       0x0
 r6
                   0x0
                              0
                                                                                       0x0
 r8
                                                                     r9
                                                                                                 0
                   0x0
                              0
                                                                                       0x0
                   0x0
                                                                                       0x0
       startup.s
     16
17
18
                                           salvando o modo corrente em R0*/
                   MSR cpsr_ctl, #0b11011011 /* alterando o modo para undefined - o SP M-CM-) automaticamente chave
                   LDR sp, =undefined stack top /* a pilha de undefined M-CM-) setada */
MSR cpsr, r0 /* volta para o modo anterior */
    19
     20
                    .word 0xffffffff
remote Thread 1 In: Reset_Handler
                                                                                                                 Line: 19
                                                                                                                              PC: 0x30
(gdb) s
Reset_Handler () at startup.s:16
(gdb) s
(gdb) s
Reset_Handler () at startup.s:18
(gdb) s
Reset_Handler () at startup.s:19
(gdb)
```

```
Register group: general
                 0x400001d3
 r0
                                    1073742291
                                                               r1
r3
r5
r7
                                                                                0x0
 r2
r4
                                                                                          0
                 0x0
                                                                                0x0
                           0
                                                                                          0
                 0x0
                           0
                                                                                0x0
                 0x0
                                                                                0x0
                 0x0
                                                               r9
                                                                                0x0
 r10
                 0x0
                                                                                0x0
       startup.s
    25
             Undefined_Handler:
                 STMFD sp!, {r0-r12,lr}
    26
    27
28
                 BL Undefined
                 LDMFD sp!, {r0-r12,pc}^
remote Thread 1 In: Undefined Handler
                                                                                                                     PC: 0x40
                                                                                                         Line: 26
(gdb) s
(gdb) s
Reset_Handler () at startup.s:18
(gdb)
Reset_Handler () at startup.s:19
Undefined Handler () at startup.s:26
(gdb)
```

```
Register group: general
                  0x400001d3
                                      1073742291
                                                                 r1
r3
r5
r7
                                                                                   0x0
                                                                                             0
0
0
0
 r2
                  0 \times 0
                            0
                                                                                   0x0
 r4
r6
                  0x0
                                                                                   0x0
                  0x0
                                                                                   0x0
 r8
                  0x0
                                                                                   0x0
                  0x0
      startup.s
                   .word 0xffffffff
    22
                  BL c entry
    23
24
             Undefined Handler:
remote Thread 1 In: Reset Handler
                                                                                                            Line: 22
                                                                                                                        PC: 0x38
Reset_Handler () at startup.s:19
(qdb) s
Undefined_Handler () at startup.s:26
(gdb) s
(gdb)
(gdb)
Reset_Handler () at startup.s:22
   -Register group: general
```

```
0xe8
                            232
                                                                r3
r5
r7
                            10
                                                                                            0
                  0xa
                                                                                 0x0
                                                                                            0
 r4
                  0x0
                                                                                 0x0
 r6
                                                                                            0
                  0x0
                                                                                 0x0
 r8
                            0
                                                                                            0
                  0x0
                                                                r9
                                                                                 0x0
 r10
                  0x0
                            0
                                                                                 0x0
                                                                                            0
      -startup.s-
                  .word 0xffffffff
    22
                  BL c entry
    23
                 В.
     24
    25
             Undefined_Handler:
remote Thread 1 In: Reset Handler
                                                                                                           Line: 23
                                                                                                                       PC: 0x3c
Undefined Handler () at startup.s:26
(gdb) s
(gdb)
(gdb)
Reset Handler () at startup.s:22
```

```
sexta@bancada8:~/projects/labproc/src/e9/tarefa/src$ qemu program.bin
pulseaudio: set_sink_input_volume() failed
pulseaudio: Reason: Invalid argument
pulseaudio: set_sink_input_mute() failed
pulseaudio: Reason: Invalid argument
instrução inválida!Hello world!
```

a) Por que tem um chapeuzinho "^" no final da instrução? Para que serve isso?

O acento circunflexo no fim da instrução serve para que o registrador de status seja carregado com o status salvo simultaneamente.

b) Por que essa instrução não salva os registradores sp (ou r13) e r14?

O sp não é salvo pela instrução pois ele é usado como registrador de base para apontar para a pilha, e o r14 (LR) não é salvo pois seu valor não precisa ser recuperado, mas sim transferido para o PC, ou seja, em vez de inserir LR na lista de registradores, é inserido PC, colocando assim o valor antigo do LR em PC e retornando ao ponto do programa onde foi encontrada a instrução indefinida.

c) O sp do modo Undefined já deve ter sido inicializado logo no reset, quando a placa é inicializada usando a instrução MSR para chavear o modo e inicializar o sp.

Isso se deve à necessidade de se manter o valor de SP_undef entre diferentes chamadas de Undefined_Handler, o que não seria possível se SP_undef fosse reinicializado dentro de Undefined_Handler toda vez que a subrotina fosse chamada.