

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: set_sink_input_mute() failed
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: set_sink_input_mute() failed
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
r0      0x0    0          r1      0x0    0
r2      0x0    0          r3      0x0    0
r4      0x0    0          r5      0x0    0
r6      0x0    0          r7      0x0    0
r8      0x0    0          r9      0x0    0
r10     0x0    0         r11     0x1094 4244

c_entry.c
9
10 void c_entry() {
11 print_uart0("Hello world!\n");
12 }^?
13
14

remote Thread 1 In: c_entry Line: 11 PC: 0x70
c_entry c_entry.c char
(gdb) break c_entry
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
r0      0x0      0
r2      0x0      0
r4      0x0      0
r6      0x0      0
r8      0x0      0
r10     0x0      0
r1      0x0      0
r3      0x0      0
r5      0x0      0
r7      0x0      0
r9      0x0      0
r11     0x1094   4244

c_entry.c
9
10 void c_entry() {
11 print_uart0("Hello world!\n");
12 }^?
13
14

remote Thread 1 In: c_entry Line: 11 PC: 0x70
Breakpoint 1 at 0x70: file c_entry.c, line 11.
(gdb) c
Continuing.

Breakpoint 1, c_entry () at c_entry.c:11
(gdb) c
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: set_sink input mute() failed
pulseaudio: Reason: Invalid argument
Hello world!

```

9-2-3

```

Register group: general
r0      0x0      0
r2      0x0      0
r4      0x0      0
r6      0x0      0
r8      0x0      0
r10     0x0      0
r1      0x0      0
r3      0x0      0
r5      0x0      0
r7      0x0      0
r9      0x0      0
r11     0x0      0

2 .global _Reset
3 Reset:
> 4 B Reset Handler /* Reset */
5 B Undefined Handler /* Undefined */
6 B . /* SWI */
7 B . /* Prefetch Abort */

remote Thread 1 In: Reset Line: 4 PC: 0x0
Transfer rate: 1976 bits in <1 sec, 123 bytes/write.
(gdb) b c
c entry c_entry.c char
(gdb) b c_entry
Breakpoint 1 at 0x98
(gdb) b Undefined
Breakpoint 2 at 0xb4
(gdb)

```

```

remote Thread 1 In: Undefined
Breakpoint 1, 0x00000098 in c_entry ()
(gdb) c
Continuing.

Breakpoint 2, 0x000000b4 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 últimos 5 bits do CPSR):

[illegible]

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):

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

```
Register group: general
r0      0xf4      244      r1      0x0        0
r2      0x21       33      r3      0x0        0
r4      0x0         0      r5      0x0        0
r6      0x0         0      r7      0x0        0
r8      0x0         0      r9      0x0        0
r10     0x0         0     r11     0x0        0

startup.s
24
25     Undefined_Handler:
26     BL Undefined
B+> 27     B .
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
(gdb) 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 . /* FIQ */

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
r0      0x400001d3      1073742291  r1      0x0          0
r2      0x0            0          r3      0x0          0
r4      0x0            0          r5      0x0          0
r6      0x0            0          r7      0x0          0
r8      0x0            0          r9      0x0          0
r10     0x0            0         r11     0x0          0

--startup.s
16      MRS r0, cpsr /* salvando o modo corrente em R0*/
17      MSR cpsr_ctl, #0b11011011 /* alterando o modo para undefined - o SP M-CM-) automaticamente chave
18      LDR sp, =undefined stack top /* a pilha de undefined M-CM-) setada */
> 19      MSR cpsr, r0 /* volta para o modo anterior */
20
21      .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
r0      0x400001d3      1073742291  r1      0x0          0
r2      0x0            0          r3      0x0          0
r4      0x0            0          r5      0x0          0
r6      0x0            0          r7      0x0          0
r8      0x0            0          r9      0x0          0
r10     0x0            0         r11     0x0          0

--startup.s
24
25      Undefined_Handler:
> 26      STMFD sp!, {r0-r12,lr}
27      BL Undefined
28      LDMFD sp!, {r0-r12,pc}^
29

remote Thread 1 In: Undefined_Handler                           Line: 26   PC: 0x40
(gdb) s
(gdb) s
Reset_Handler () at startup.s:18
(gdb) s
Reset_Handler () at startup.s:19
(gdb) s
Undefined_Handler () at startup.s:26
(gdb) █
```

```

Register group: general
r0      0x400001d3  1073742291  r1      0x0      0
r2      0x0      0      r3      0x0      0
r4      0x0      0      r5      0x0      0
r6      0x0      0      r7      0x0      0
r8      0x0      0      r9      0x0      0
r10     0x0      0      r11     0x0      0

startup.s
20
21      .word 0xffffffff
> 22      BL c_entry
23      B .
24
25      Undefined Handler:

remote Thread 1 In: Reset_Handler                               Line: 22  PC: 0x38
Reset_Handler () at startup.s:19
(gdb) s
Undefined_Handler () at startup.s:26
(gdb) s
(gdb) s
(gdb) s
Reset_Handler () at startup.s:22
(gdb)

```

```

Register group: general
r0      0xe8      232      r1      0x0      0
r2      0xa      10      r3      0x0      0
r4      0x0      0      r5      0x0      0
r6      0x0      0      r7      0x0      0
r8      0x0      0      r9      0x0      0
r10     0x0      0      r11     0x0      0

startup.s
20
21      .word 0xffffffff
22      BL c_entry
> 23      B .
24
25      Undefined Handler:

remote Thread 1 In: Reset_Handler                               Line: 23  PC: 0x3c
(gdb) s
Undefined_Handler () at startup.s:26
(gdb) s
(gdb) s
(gdb) s
Reset_Handler () at startup.s:22
(gdb) n
(gdb)

```

```

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.