Exception Handler 实验报告

- 容逸朗 2020010869

1. 实验目的

- 了解 MIPS 异常处理流程和相关机制。

2. 实验原理

运行如下代码：

```
.globl  main
main:
        lw $v0, 1($0)   # AdEL
        sw $v0, 1($0)   # AdES
        lui $7, 32767   # R7 = 0x7fff0000
        ori $7, 65535   # R7 = 0x7fffffff
        addi $7, 1      # Ov
        nop
```

2.1 AdEL

当程序运行至带有 `# AdEL` 标记的一行时，EPC、cause、status 寄存器的值如下：

```
EPC      = 400024
Cause    = 10
Status   = 3000ff12
```

`EPC` 表示当前出现错误的代码地址。

对于 `Cause` = `0x10` = `0000 0000 0000 0000 0000 0000 0001 0000`：

- Branch delay = `0` ，表示程序不是在 delay slot 中出现异常。
- Pending interrupts 中没有 `1` ，表示没有中断需要处理。
- Exception code = `00100` （十进制中为 `4` ），表示 AdEL 错误。

对于 `Status` = `0x3000ff12` = `0011 0000 0000 0000 1111 1111 0001 0010`：

- Interrupt mask = `11111111` ，表示所有中断都被允许。
- User mode = `1` ，表示程序运行于用户态。
- Exception level = `1` ，表示异常发生，没有完成处理。
- Interrupt enable = `0` ，即禁止中断处理。

2.2 AdES

当程序运行至带有 `# AdES` 标记的一行时，EPC、cause、status 寄存器的值如下：

```
EPC      = 400028
Cause    = 14
Status   = 3000ff13
```

2.3 Ov

```
    lui $7, 32767   # R7 = 0x7fff0000
    ori $7, 65535   # R7 = 0x7fffffff
    addi $7, 1      # Ov
```

`32` 位带符号整数的最大值为 `0x7fffffff` ，由此可以先在 `R7` 寄存器的高 `16` 位中放入 `0x7fff` ，然后在 `R7` 寄存器的低 `16` 位中存入 `0xffff` ，最后把 `R7` 寄存器的值加 `1` 便会导致溢出。

当程序运行至最后一行时，EPC、cause、status 寄存器的值如下：

```
EPC      = 400034
Cause    = 30
Status   = 3000ff13
```

3. 实验截图