PA2.5

1. 理解mainargs参数是如何传递给hello程序的:
   1. 首先要明确，这个hello程序是要被nemu加载的程序，因此在hello被编译的时候，就需要把这个参数传递给hello里面的main函数了。因此我们可以定位这个参数是在编译的时候。但是目前只能找到makefile中关于把这个参数作为预定义的宏传给了hello.c函数。那么hello是如何根据这个宏来得到参数的呢？？？这个地方不理解！
   2. 补充a) 找到了这个宏在哪里被引用了！！！在abstract-machine/am/src/platform/nemu/trm.c这个函数下面！这个trm.c里面的内容还是非常重要的。他直接定义了halt、heap、以及trm的启动函数\_trm\_init。在\_trm\_init函数中，调用了宏mainargs并传递给了main函数！

另外，在start.S汇编文件中，定义了程序的入口\_start，并且从\_start启动进入\_trm\_init。

1. 在始终update这一块的代码似乎是有BUG的！只有把高低位都拼接起来才能正确让us读出时间，但是只读地位却不行，us一直是0.这就非常奇怪了，因为地位肯定有数的呀！！所以可能是我的低32位数据的指令有BUG？？
   1. 进一步探索发现，只要把RTC\_ADDR的高位和地位都读出来就没有这个BUG。。。。。莫不着头脑～～。
   2. !!!原来这就是框架代码埋下的大坑！！！！他是通过寄存器来模拟MMIO的，所以他需要通过回调函数来更新，而回调函数只有在你读时钟外设高地址的时候才会更新。所以读取顺序要从高到低。。。。。。太难了！！！

进入到ysyx基础阶段 B线

1. 又遇到了ALU的问题。重新思考了以下关于无符号数比较的问题。觉得可以类比一个12小时制的时钟。利用减法来比较时，对一个点取反相当于他在时钟上对称了一下，即时钟针到0/12点的距离在之前和之后都是一样的。这就像一个头尾连在一起的一个结构。因此无符号数利用减法比较时，当结果的carry有进位的时候，那么就说明他们相加溢出了！溢出就说明被减的那个时钟针在减数的后面或者相等！！非常巧妙好理解，尝试在纸上画一个12小时制的时钟就明白了。
2. 对于补码运算的符号溢出问题。 加法减法都转换为加法运算，而且数据以补码的形式进行运算，得出的结果就是补码形式，不论以有符号数还是无符号数的角度看，计算结果都是正确的！ 对于加法来说，只有正数+正数，负数+负数这两种情况会发生溢出问题，因此只需要特殊处理这两类。
3. 比较运算这个地方感觉实验讲义上有点麻烦。在不溢出的情况下，直接看符号为判断；在溢出的情况下，说明A，B肯定不同号，这个时候直接判断A、B的符号位不就行了吗？ 但是判断结果的符号位确实更省逻辑资源一些： 那么这样只剩两种情况： 正-负 ->正+正溢出，那么结果符号位肯定是1,这时候A为正， A>B;另一种情形就是负-正 ->负+负溢出，那么结果符号位肯定是0,这时候A<B；

B线

1. PA3.0
2. nanos的代码和NEMU的代码是分离的，互不影响。Nanos运行在AM之上
3. AM给的栈空间有多大呢？ 这一点应该根据连接器的脚本可以查询到。在AM目录下的link.ld文件查询，他在链接的时候通过-T被引用，可以看到栈空间的大小是0x8000，并且是0x1000字节对齐的。



8. PA3.1
9. 这一部分简直就是之前学习过的汪老师教的内容：异常上下文的保存已经跳转处理。总体的思路是这样的：软件通过ecall除法异常，这时候需要保存相应的寄存器，如mstatus，并把当前指针写入mepc中，然后跳转到mtvec，即中断向量地址，这个一般都是由操作系统控制的，也即操作系统此时获得控制权来处理异常。首先保存上下文，包括gpr，及一些csr到栈里，然后跳转到相应的中断处理函数处理中断，然后返回。最后从栈中恢复上下文，使用mret指令返回保存在mepc中的地址。其中有个问题，mepc的地址+4是软件控制的，因此需要操作系统自己判断什么时候+4，比如异常的时候不加，中断的时候+4.
10. 因此实现上述功能，需要添加和寄存器操作相关的指令，目前只需要csrrw、csrrs、mret这三个
11. 重新组织结构体比较容易，只需要看汇编里面的数据保存顺序就行了。因此另一个问题迎刃而解，上下文指针c是从汇编代码里面来的，由于RV的规范，参数传递都使用a0开始的寄存器，所以a0就是c，而a0指向的sp，sp指向的是刚才保存数据的栈顶，那么显而易见，他就是上下文结构体的指针，因此C里面都是上下文的数据。
12. 为什么RISC指令中mepc+4与否是由软件来控制，而CICS指令都是由硬件控制的？我的理解是减少硬件复杂度。软件可以自己判断来的是异常还是中断等。比如发生了分页错误等，那么处理完之后还需要返回原指令再检查看是否还出错，而中断的话，再处理完之后就可以直接跳到下条语句运行。那么如果把异常、中断的判断机制交给硬件，会需要更大的芯片面积和复杂的逻辑。
13. 必答题(需要在实验报告中回答) - 理解穿越时空的旅程
14. 解答如下：yield（）会触发ecall指令，那么NEMU中就会运行ecall，触发异常机制，会把相应的触发号等写入相应csr中，然后跳转到mtvec保存的异常向量表地址。这个地址在AM中被设置为\_\_am\_asm\_trap（）这个函数的地址，因此之后会保存上下文，跳转到中断处理函数，他会先识别出中断号，然后交给操作系统来处理。处理完成后返回一个上下文的结构体，（我的理解是为了给以后多程序运行切换使用的），然后回到trap里面恢复上下文，此时这个上下文有可能是另一个程序的哦！




20. PA3.2
21. 踩坑踩坑！！！此处img文件的program段的第一个可load的项，他的offset竟然是0！！看了很多遍手册，发现没有问题，就是从文件头开始的！！那么只有一个可能，就是程序的起始地址另有地方！！果然，是e\_entry!!
22. 在C语言中，## 是一种特殊的预处理器运算符，用于在宏定义中连接两个标识符或标记（tokens）
23. 必答题(需要在实验报告中回答) - hello程序是什么, 它从而何来, 要到哪里去
24. 这个问题我想已经很好回答了！hello程序就是一段被操作系统加载并执行的二进制文件数据。他由navy程序编译而来，在编译时由-T选项都被链接到0x83000000的地址，并且编译链接后得到相应的ELF文件。该文件里存放了所有的信息，比如可执行文件的开始地址，program header，section header信息等。之后os操作系统的程序被编译链接，在链接过程中，会把ramdisk，也就是hello程序的ELF文件数据都链接到ramdisk\_start到ramdisk\_end这段内存中。之后我们会首先开始运行操作系统，然后解析ramdisk的信息，并把需要加载的数据加载到0x8300000这个起始地址，并通过program entry地址找到hello程序的第一条指令地址。那么操作系统就可以跳转到这个地址运行hello程序拉！至于打印字符串这个行为，就是一个系统调用过程而以。