

# 南京航空航天大学 计算机科学与技术系学 院 计算机组成原理 课程实验

学号：161630220

姓名：赵维康

## 1 PA1- 开天辟地的篇章:最简单的计算机

在进行本 PA 前，请在工程目录下执行以下命令进行分支整理

执行 `git commit --allow-empty -am "before starting pa1"` 命令的截图

```
root@zhaoweikang:/home/zhaoweikang/ics2017# git commit --allow-empty -am "before starting pa1"
error: unknown option 'allow-empty'
用法: git commit [<选项>] [--] <路径规格>...
```

<code>-q, --quiet</code>	提交成功后不显示概述信息
<code>-v, --verbose</code>	在提交说明模板里显示差异

提交说明选项

<code>-F, --file &lt;文件&gt;</code>	从文件中读取提交说明
<code>--author &lt;作者&gt;</code>	提交时覆盖作者
<code>--date &lt;日期&gt;</code>	提交时覆盖日期
<code>-m, --message &lt;说明&gt;</code>	提交说明
<code>-c, --reedit-message &lt;提交&gt;</code>	重用并编辑指定提交的提交说明
<code>-C, --reuse-message &lt;提交&gt;</code>	重用指定提交的提交说明
<code>--fixup &lt;提交&gt;</code>	使用 autosquash 格式的提交说明用以修正指定的提交
<code>--squash &lt;提交&gt;</code>	使用 autosquash 格式的提交说明用以压缩至指定的提交

执行 `git checkout master` 命令的截图

```
root@zhaoweikang:/home/zhaoweikang/ics2017# git checkout master
已经位于 'master'
您的分支领先 'origin/2017' 共 6 个提交。
（使用 "git push" 来发布您的本地提交）
```

执行 `git merge pa0` 命令的截图

```
root@zhaoweikang:/home/zhaoweikang/ics2017# git merge pa0
Merge made by the 'recursive' strategy.
 nemu/Makefile.git | 2 + -
 1 file changed, 1 insertion(+), 1 deletion(-)
```

执行 `git checkout -b pa1` 命令的截图

```
root@zhaoweikang:/home/zhaoweikang/ics2017# git checkout -b pa1
切换到一个新分支 'pa1'
```

## 在开始愉快的 PA 之旅之前

超级玛丽部分截图，因为本人不玩游戏，更多截图已省略



初识虚拟化

假设你在 Windows 中使用 Docker 安装了一个 GNU/Linux container, 然后在 container 中完成 PA, 通过 NEMU 运行 Hello World 程序. 在这样的情况下, 尝试画出相应的层次图.

```
"Hello World" program
  NEMU
    Container
      GNU/Linux
        Computer hardware
```

## 开天辟地的故事

思考题: 在 `cmd_c()` 函数中, 调用 `cpu_exec()` 的时候传入了参数 `-1`, 你知道这是什么意思吗?

答: 表示程序执行结束, 结束当前进程。

阅读 main 函数的截图

```
int init_monitor(int, char *[]);
void ui_mainloop(int);

int main(int argc, char *argv[]) {
    /* Initialize the monitor. */
    int is_batch_mode = init_monitor(argc, argv);

    /* Receive commands from user. */
    ui_mainloop(is_batch_mode);

    return 0;
}
```

阅读 init\_monitor()函数的截图

```
int init_monitor(int argc, char *argv[]) {
    /* Perform some global initialization. */

    /* Parse arguments. */
    parse_args(argc, argv);

    /* Open the log file. */
    init_log();

    /* Test the implementation of the 'CPU_state' structure. */
    reg_test();

#ifdef DIFF_TEST
    /* Fork a child process to perform differential testing. */
    init_diff_test();
#endif

    /* Load the image to memory. */
    load_img();

    /* Initialize this virtual computer system. */
    restart();
}
```

阅读 reg\_test()函数的截图

```
void reg_test() {
    srand(time(0));
    uint32_t sample[8];
    uint32_t eip_sample = rand();
    cpu.eip = eip_sample;

    int i;
    for (i = R_EAX; i <= R_EDI; i++) {
        sample[i] = rand();
        reg_l(i) = sample[i];
        assert(reg_w(i) == (sample[i] & 0xffff));
    }
}
```

用于模拟寄存器的结构体 CPU\_state，以下是我实现寄存器结构体的代码截图

```
typedef struct {
    union {
        union{
            uint32_t _32;
            uint16_t _16;
            uint8_t _8[2];
        } gpr[8];

        /* Do NOT change the order of the GPRs' definitions. */

        /* In NEMU, rtlreg_t is exactly uint32_t. This makes RTL instructions
         * in PA2 able to directly access these registers.
         */
        struct{
            uint32_t eax, ecx, edx, ebx, esp, ebp, esi, edi;
        };
    };
    swaddr_t eip;
} CPU_state;
```

实现寄存器结构体之后，执行 make clean 的截图

```
root@zhaoweikang:/home/zhaoweikang/ics2017# make clean
make -C nemu clean
make[1]: Entering directory '/home/zhaoweikang/ics2017/nemu'
rm -rf ./build
make[1]: Leaving directory '/home/zhaoweikang/ics2017/nemu'
make -C nexus-am clean
make[1]: Entering directory '/home/zhaoweikang/ics2017/nexus-am'
make[2]: Entering directory '/home/zhaoweikang/ics2017/nexus-am/tests/asyetest'
Building asyetest []
make[2]: Leaving directory '/home/zhaoweikang/ics2017/nexus-am/tests/asyetest'
make[2]: Entering directory '/home/zhaoweikang/ics2017/nexus-am/tests/timetest'
Building timetest []
make[2]: Leaving directory '/home/zhaoweikang/ics2017/nexus-am/tests/timetest'
make[2]: Entering directory '/home/zhaoweikang/ics2017/nexus-am/tests/fuzz'
Building fuzz []
make[2]: Leaving directory '/home/zhaoweikang/ics2017/nexus-am/tests/fuzz'
make[2]: Entering directory '/home/zhaoweikang/ics2017/nexus-am/tests/quitest'
```

执行 make 命令的截图

```

root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# make
+ CC src/device/serial.c
+ CC src/device/vga.c
+ CC src/device/device.c
+ CC src/device/keyboard.c
+ CC src/device/timer.c
+ CC src/device/io/mmio.c
+ CC src/device/io/port-io.c
+ CC src/memory/memory.c
+ CC src/monitor/cpu-exec.c
+ CC src/monitor/monitor.c
+ CC src/monitor/debug/expr.c
+ CC src/monitor/debug/watchpoint.c
+ CC src/monitor/debug/ui.c
+ CC src/monitor/diff-test/diff-test.c
+ CC src/monitor/diff-test/gdb-host.c
+ CC src/monitor/diff-test/protocol.c
+ CC src/cpu/decode/modrm.c
+ CC src/cpu/decode/decode.c
+ CC src/cpu/reg.c
+ CC src/cpu/exec/cc.c
+ CC src/cpu/exec/arith.c
+ CC src/cpu/exec/control.c
--

```

执行 make run 命令的截图

```

root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# make run
./build/nemu -l ./build/nemu-log.txt
[src/monitor/monitor.c,47,load_default_img] No image is given. Use the default b
uild-in image.
Welcome to NEMU!
[src/monitor/monitor.c,30,welcome] Build time: 16:32:15, Mar 10 2018
For help, type "help"
(nemu) █

```

程序输出了以下内容

```

(nemu) c
nemu: HIT GOOD TRAP at eip = 0x00100026

```

说明成功实现了寄存器结构体

## 基础设施： 简易调试器

进入 nemu/src/monitor/debug 目录的过程截图

```

root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# ls
build include Makefile Makefile.git README.md runall.sh src
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# cd src/
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu/src# ls
cpu device main.c memory misc monitor
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu/src# cd monitor/
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu/src/monitor# ls
cpu-exec.c debug diff-test monitor.c
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu/src/monitor# cd debug/
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu/src/monitor/debug# ls
expr.c ui.c watchpoint.c
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu/src/monitor/debug# gedit ui.c

```

实现单步执行功能的函数 `cmd_si()`，实现打印寄存器功能的函数 `cmd_info()`，还有实现打印寄存器功能需要用到 `dump_reg()` 函数，因此加上了这一函数，以下是函数实现截图

```

static int cmd_si(char *args){
char *arg=strtok(NULL," ");
int n=0;
sscanf(arg,"%d",&n);
for(int j=0;j<n;j++){
cpu_exec(1);
}
return 0;
}
static void dump_regs(){
int i;
for(i=R_EAX;i<=R_EDI;i++){
printf("%s: 0x%08x\t%d\n",regsl[i],cpu.gpr[i]._32,cpu.g
}
printf("eip: 0x%08x\t%d\n",cpu.eip,cpu.eip);
}
static int cmd_info(char *args){
switch(*args){
case 'r':dump_regs();return 0;
default: return 1;
}
}
}

```

实现扫描内存功能的函数 cmd\_x(),以下是实现截图

```

static int cmd_x(char *args){
unsigned int addr,len,i;
sscanf(args,"%d 0x%x",&len,&addr);
printf("dump memory start addr: 0x%08x len: %d\n",addr,len);
for(i=0;i<len;++i){
if(!(i & 0xf))printf("\n0x%08x: ",addr+i*16);
printf("0x%02x ",*(unsigned char *)hwa_to_va(addr+i));
}
printf("\n");
return 0;
}
}

```

对结构体 cmd\_table[]进行补充完善,加入了用于实现单步执行、打印寄存器、扫描内存功能的命令, 以下是实现截图

```

static struct {
char *name;
char *description;
int (*handler) (char *);
} cmd_table [] = {
{ "help", "Display informations about all supported commands", cmd_help },
{ "c", "Continue the execution of the program", cmd_c },
{ "q", "Exit NEMU", cmd_q },

/* TODO: Add more commands */
{ "si", "Single step", cmd_si },
{ "info", "dump informations with option:r(register)", cmd_info },
{ "x", "dump memory: x length addr", cmd_x },
};

```

完成以上函数的实现后, 执行 make 以及 make run 命令的截图

```

root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# make
+ CC src/device/serial.c
+ CC src/device/vga.c
+ CC src/device/device.c
+ CC src/device/keyboard.c
+ CC src/device/timer.c
+ CC src/device/io/mmio.c
+ CC src/device/io/port-io.c
+ CC src/memory/memory.c
+ CC src/monitor/cpu-exec.c
+ CC src/monitor/monitor.c
+ CC src/monitor/debug/expr.c
+ CC src/monitor/debug/watchpoint.c
+ CC src/monitor/debug/ui.c
+ CC src/monitor/diff-test/diff-test.c

+ CC src/monitor/diff-test/gdb-host.c
+ CC src/monitor/diff-test/protocol.c
+ CC src/cpu/decode/modrm.c
+ CC src/cpu/decode/decode.c
+ CC src/cpu/reg.c
+ CC src/cpu/exec/cc.c
+ CC src/cpu/exec/arith.c
+ CC src/cpu/exec/control.c
+ CC src/cpu/exec/prefix.c
+ CC src/cpu/exec/logic.c
+ CC src/cpu/exec/system.c
+ CC src/cpu/exec/data-mov.c
+ CC src/cpu/exec/exec.c
+ CC src/cpu/exec/special.c
+ CC src/cpu/intr.c
+ CC src/main.c
+ CC src/misc/logo.c
+ LD build/nemu
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# make run
./build/nemu -l ./build/nemu-log.txt
[src/monitor/monitor.c,47,load_default_img] No image is given. Use the default build-in
image.
Welcome to NEMU!
[src/monitor/monitor.c,30,welcome] Build time: 20:47:16. Mar 10 2018

```

执行单步执行命令的截图

```

(nemu) si 10
100000: b8 34 12 00 00      movl $0x1234,%eax
100005: b9 27 00 10 00      movl $0x100027,%ecx
10000a: 89 01               movl %eax,(%ecx)
10000c: 66 c7 41 04 01 00   movw $0x1,0x4(%ecx)
100012: bb 02 00 00 00      movl $0x2,%ebx
100017: 66 c7 84 99 00 e0 ff ff 01 00   movw $0x1,-0x2000(%ecx,%ebx,4)
100021: b8 00 00 00 00      movl $0x0,%eax

nemu: HIT GOOD TRAP at eip = 0x00100026

100026: d6               nemu trap (eax = 0)

```

执行打印寄存器命令的截图

```
(nemu) info r
eax: 0x0037b4b1 3650737
ecx: 0x38ac7eb1 950828721
edx: 0x7836e810 2016864272
ebx: 0x57fdb53a 1476244794
esp: 0x647d1411 1685918737
ebp: 0x0cd173a9 215053225
esi: 0x523e3319 1379808025
edi: 0x7f9ee3d8 2141119448
eip: 0x00100000 1048576
```

执行扫描内存命令的截图

```
(nemu) x 10 0x100000
dump memory start addr: 0x00100000 len: 10

0x00100000: 0x100000 0x100001 0x100002 0x100003 0x100004 0x100005 0x100006 0x100007
0x100008 0x100009
```

git 记录

使用 git init 命令进行初始化的截图

```
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# git init
已初始化空的 Git 仓库于 /home/zhaoweikang/ics2017/nemu/.git/
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# git log
fatal: 您的当前分支 'master' 尚无任何提交
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# git status
位于分支 master
```

初始提交

未跟踪的文件:

(使用 "git add <文件>..." 以包含要提交的内容)

```
.gitignore
Makefile
Makefile.git
README.md
include/
runall.sh
```

使用 git status 命令查看未追踪文件, 以及 git add -A 加入追踪的截图



src/

提交为空，但是存在尚未跟踪的文件（使用 "git add" 建立跟踪）  
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# git add -A  
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# git status  
位于分支 master

初始提交

要提交的变更：  
（使用 "git rm --cached <文件>..." 以取消暂存）

```
新文件:   .gitignore
新文件:   Makefile
新文件:   Makefile.git
新文件:   README.md
新文件:   include/common.h
新文件:   include/cpu/decode.h
新文件:   include/cpu/exec.h
新文件:   include/cpu/reg.h
新文件:   include/cpu/rtl.h
新文件:   include/debug.h
新文件:   include/device/mmio.h
新文件:   include/device/port-io.h
新文件:   include/macro.h
新文件:   include/memory/memory.h
新文件:   include/memory/mmu.h
新文件:   include/monitor/expr.h
新文件:   include/monitor/monitor.h
新文件:   include/monitor/watchpoint.h
新文件:   include/nemu.h
新文件:   runall.sh
新文件:   src/cpu/decode/decode.c
新文件:   src/cpu/decode/modrm.c
新文件:   src/cpu/exec/all-instr.h
新文件:   src/cpu/exec/arith.c
新文件:   src/cpu/exec/cc.c
新文件:   src/cpu/exec/control.c
新文件:   src/cpu/exec/data-mov.c
新文件:   src/cpu/exec/exec.c
新文件:   src/cpu/exec/logic.c
新文件:   src/cpu/exec/prefix.c
新文件:   src/cpu/exec/special.c
新文件:   src/cpu/exec/system.c
新文件:   src/cpu/intr.c
新文件:   src/cpu/reg.c
新文件:   src/device/device.c
新文件:   src/device/io/mmio.c
```

执行 git commit 命令的截图

---

```
新文件:  src/device/io/port-io.c
新文件:  src/device/keyboard.c
新文件:  src/device/serial.c
新文件:  src/device/timer.c
新文件:  src/device/vga.c
新文件:  src/main.c
新文件:  src/memory/memory.c
新文件:  src/misc/logo.c
新文件:  src/monitor/cpu-exec.c
新文件:  src/monitor/debug/expr.c
新文件:  src/monitor/debug/ui.c
新文件:  src/monitor/debug/watchpoint.c
新文件:  src/monitor/diff-test/diff-test.c
新文件:  src/monitor/diff-test/gdb-host.c
新文件:  src/monitor/diff-test/protocol.c
新文件:  src/monitor/diff-test/protocol.h
新文件:  src/monitor/monitor.c
```

```
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# git commit
```

```
[master (根提交) 2102be6] fix bug for pa1.1
```

```
53 files changed, 3658 insertions(+)
```

```
create mode 100644 .gitignore
```

```
create mode 100644 Makefile
```

```
create mode 100644 Makefile.git
```

---

```
create mode 100644 README.md
create mode 100644 include/common.h
create mode 100644 include/cpu/decode.h
create mode 100644 include/cpu/exec.h
create mode 100644 include/cpu/reg.h
create mode 100644 include/cpu/rtl.h
create mode 100644 include/debug.h
create mode 100644 include/device/mmio.h
create mode 100644 include/device/port-io.h
create mode 100644 include/macro.h
create mode 100644 include/memory/memory.h
create mode 100644 include/memory/mmu.h
create mode 100644 include/monitor/expr.h
create mode 100644 include/monitor/monitor.h
create mode 100644 include/monitor/watchpoint.h
create mode 100644 include/nemu.h
create mode 100644 runall.sh
create mode 100644 src/cpu/decode/decode.c
create mode 100644 src/cpu/decode/modrm.c
create mode 100644 src/cpu/exec/all-instr.h
create mode 100644 src/cpu/exec/arith.c
create mode 100644 src/cpu/exec/cc.c
create mode 100644 src/cpu/exec/control.c
create mode 100644 src/cpu/exec/data_mov.c
```

---

```
create mode 100644 src/cpu/exec/exec.c
create mode 100644 src/cpu/exec/logic.c
create mode 100644 src/cpu/exec/prefix.c
create mode 100644 src/cpu/exec/special.c
create mode 100644 src/cpu/exec/system.c
create mode 100644 src/cpu/intr.c
create mode 100644 src/cpu/reg.c
create mode 100644 src/device/device.c
create mode 100644 src/device/io/mmio.c
create mode 100644 src/device/io/port-io.c
create mode 100644 src/device/keyboard.c
create mode 100644 src/device/serial.c
create mode 100644 src/device/timer.c
create mode 100644 src/device/vga.c
create mode 100644 src/main.c
create mode 100644 src/memory/memory.c
create mode 100644 src/misc/logo.c
create mode 100644 src/monitor/cpu-exec.c
create mode 100644 src/monitor/debug/expr.c
create mode 100644 src/monitor/debug/ui.c
create mode 100644 src/monitor/debug/watchpoint.c
create mode 100644 src/monitor/diff-test/diff-test.c
create mode 100644 src/monitor/diff-test/gdb-host.c
create mode 100644 src/monitor/diff-test/protocol.c
```

---

fix bug for pa1.1

# 请为您的变更输入提交说明。以 '#' 开始的行将被忽略，而一个空的提交

# 说明将会终止提交。

# 位于分支 master

#

# 初始提交

#

# 要提交的变更：

# 新文件： .gitignore

# 新文件： Makefile

# 新文件： Makefile.git

# 新文件： README.md

# 新文件： include/common.h

# 新文件： include/cpu/decode.h

# 新文件： include/cpu/exec.h

# 新文件： include/cpu/reg.h

# 新文件： include/cpu/rtl.h

# 新文件： include/debug.h

# 新文件： include/device/mmio.h

# 新文件： include/device/port-io.h

# 新文件： include/macro.h

# 新文件： include/memory/memory.h

# 新文件： include/memory/mmu.h

:wq

---

root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# git log

commit 2102be6e3d0198ff9df91608a4b6e55b8f5ce6e4

Author: 161630220-Zhao Weikang <2875206963@qq.com>

Date: Sat Mar 10 21:00:27 2018 +0800

fix bug for pa1.1

```
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# git commit --allow-empty
[master 06207a4] fix bug for pa1.1
root@zhaoweikang:/home/zhaoweikang/ics2017/nemu# git log
commit 06207a4af5cfe850cefc6cff4ee0acba6baa4d84
Author: 161630220-Zhao Weikang <2875206963@qq.com>
Date: Sat Mar 10 21:15:36 2018 +0800
```

fix bug for pa1.1

```
commit 2102be6e3d0198ff9df91608a4b6e55b8f5ce6e4
Author: 161630220-Zhao Weikang <2875206963@qq.com>
Date: Sat Mar 10 21:00:27 2018 +0800
```

fix bug for pa1.1

-