

Project 1: Introduction to Linux Kernel Modules

I. Kernel Modules Overview

II. Loading and Removing Kernel Modules

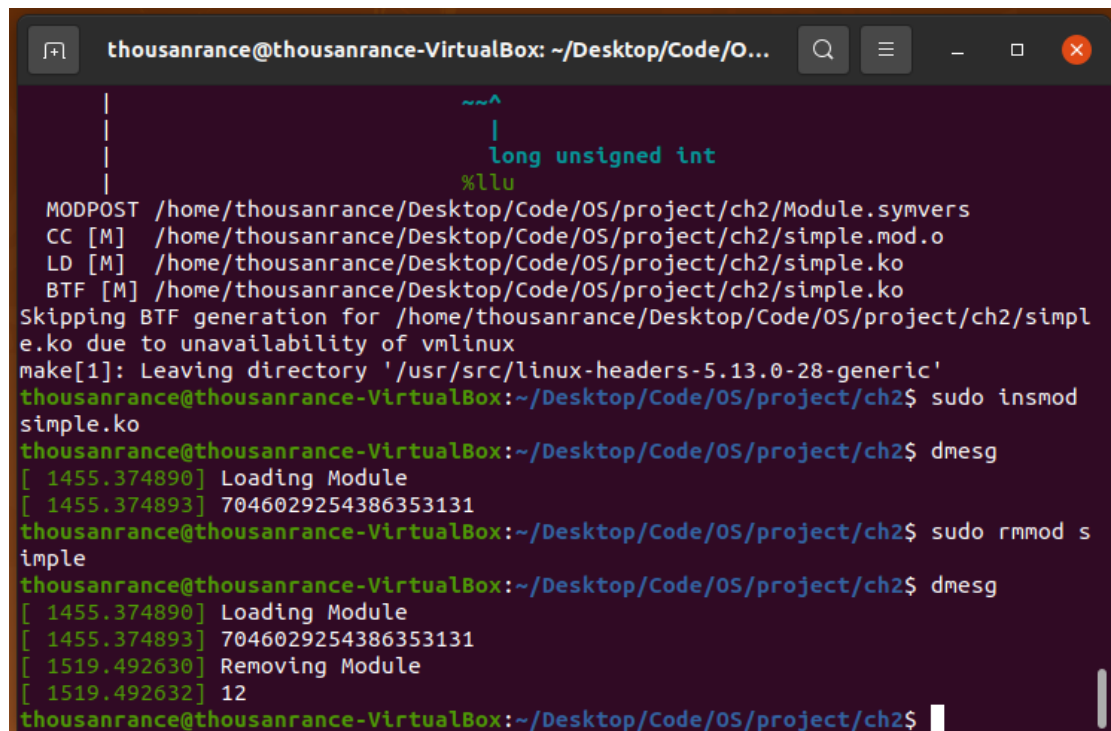
1. Print out the value of GOLDEN RATIO PRIME in the `simple_init()` function.
2. Print out the greatest common divisor of 3,300 and 24 in the `simple_exit()` function.

实现细节:

<linux/hash.h>: `printk(KERN_INFO "%lu\n", GOLDEN_RATIO_PRIME);`

<linux/gcd.h>: `unsigned long gcd(unsigned long a, unsigned b);`

按照书上的提示，导入库，然后将上述代码分别加入到 `simple_init()` 与 `simple_exit()` 函数中。



```
thousanrance@thousanrance-VirtualBox: ~/Desktop/Code/O...
|                                     ~~~^
|                                     |
|                                     long unsigned int
|                                     %llu
MODPOST /home/thousanrance/Desktop/Code/OS/project/ch2/Module.symvers
CC [M] /home/thousanrance/Desktop/Code/OS/project/ch2/simple.mod.o
LD [M] /home/thousanrance/Desktop/Code/OS/project/ch2/simple.ko
BTF [M] /home/thousanrance/Desktop/Code/OS/project/ch2/simple.ko
Skipping BTF generation for /home/thousanrance/Desktop/Code/OS/project/ch2/simple.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.13.0-28-generic'
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ sudo insmod simple.ko
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ dmesg
[ 1455.374890] Loading Module
[ 1455.374893] 7046029254386353131
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ sudo rmmod simple
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ dmesg
[ 1455.374890] Loading Module
[ 1455.374893] 7046029254386353131
[ 1519.492630] Removing Module
[ 1519.492632] 12
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$
```

1. Print out the values of `jiffies` and `HZ` in the `simple_init()` function.
2. Print out the value of `jiffies` in the `simple_exit()` function.

实现细节:

按照书上提示导入库 `<asm/param.h>` `<linux/jiffies.h>`，然后在 `simple_init()` 与 `simple_exit()` 函数中通过 `printk()` 语句打印要求的值。

```

thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ dmesg
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ sudo insmod
simple.ko
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ dmesg
[ 2205.855150] Loading Module
[ 2205.855154] 7046029254386353131
[ 2205.855156] 4295443747
[ 2205.855157] 250
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ sudo rmmod s
imple
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ dmesg
[ 2205.855150] Loading Module
[ 2205.855154] 7046029254386353131
[ 2205.855156] 4295443747
[ 2205.855157] 250
[ 2224.892265] Removing Module
[ 2224.892269] 12
[ 2224.892270] 4295448507
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$

```

模块自加载到删除经过的秒数 = (删除时的 jiffies 值 - 加载时的 jiffies 值) / HZ 的值

III The /proc File System

这部分原本只需要按照书上步骤操作完成，但是可能由于 linux 内核版本更新，proc_create() 函数的最后一个参数类型不再是像书上写的那样是 file_operation 结构体指针，而是一个 proc_ops 结构体指针，原本的示例代码 hello.c 在 make 时反而会报错。

```

thousanrance@thousanrance-VirtualBox: ~/Desktop/Cod...
efile
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ make
make -C /lib/modules/5.13.0-28-generic/build M=/home/thousanrance/Desktop/Cod
e/OS/project/ch2 modules
make[1]: Entering directory '/usr/src/linux-headers-5.13.0-28-generic'
  CC [M] /home/thousanrance/Desktop/Code/OS/project/ch2/hello.o
/home/thousanrance/Desktop/Code/OS/project/ch2/hello.c: In function 'proc_int
t':
/home/thousanrance/Desktop/Code/OS/project/ch2/hello.c:46:41: error: passing
argument 4 of 'proc_create' from incompatible pointer type [-Werror=incompati
ble-pointer-types]
   46 |         proc_create(PROC_NAME, 0, NULL, &proc_ops);
      |                                     ^
      |                                     |
      |                                     struct file_operations *
In file included from /home/thousanrance/Desktop/Code/OS/project/ch2/hello.c:
16:
./include/linux/proc_fs.h:110:24: note: expected 'const struct proc_ops *' bu
t argument is of type 'struct file_operations *'
   110 | struct proc_dir_entry *proc_create(const char *name, umode_t mode, st
ruct proc_dir_entry *parent, const struct proc_ops *proc_ops);
      |                                     ^
/home/thousanrance/Desktop/Code/OS/project/ch2/hello.c: In function 'proc_rea
d':
/home/thousanrance/Desktop/Code/OS/project/ch2/hello.c:93:9: warning: ignorin
g return value of 'copy_to_user', declared with attribute warn_unused_result
[-Wunused-result]
   93 |         copy_to_user(usr_buf, buffer, rv);
      |         ^
cc1: some warnings being treated as errors
make[2]: *** [scripts/Makefile.build:281: /home/thousanrance/Desktop/Code/OS/
project/ch2/hello.o] Error 1
make[1]: *** [Makefile:1879: /home/thousanrance/Desktop/Code/OS/project/ch2]
Error 2
make[1]: Leaving directory '/usr/src/linux-headers-5.13.0-28-generic'
make: *** [Makefile:3: all] Error 2
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$

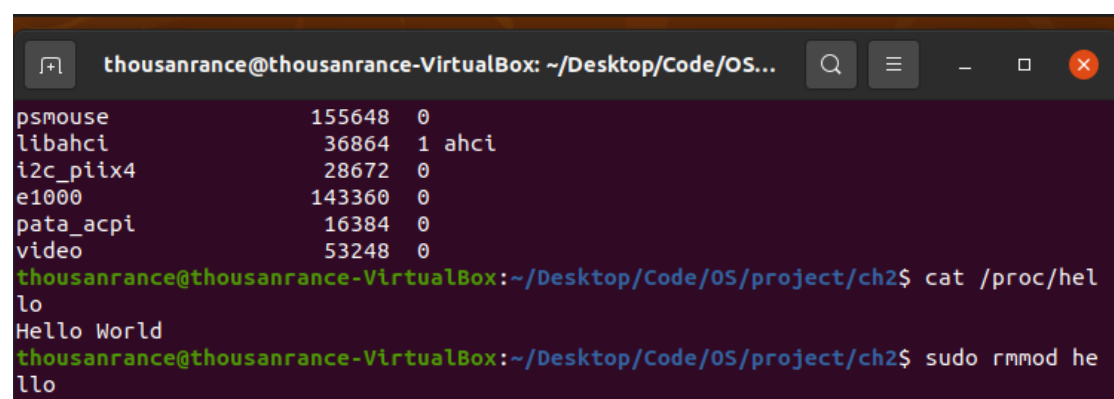
```

经过资料搜索，两结构体在头文件<linux/proc_fs.h>中的声明如下：

```
1 struct proc_ops {
2     unsigned int proc_flags;
3     int (*proc_open)(struct inode *, struct file *);
4     ssize_t (*proc_read)(struct file *, char __user *, size_t, loff_t *);
5     ssize_t (*proc_write)(struct file *, const char __user *, size_t, loff_t *);
6     loff_t (*proc_lseek)(struct file *, loff_t, int);
7     int (*proc_release)(struct inode *, struct file *);
8     __poll_t (*proc_poll)(struct file *, struct poll_table_struct *);
9     long (*proc_ioctl)(struct file *, unsigned int, unsigned long);
10 #ifndef CONFIG_COMPAT
11     long (*proc_compat_ioctl)(struct file *, unsigned int, unsigned long);
12 #endif
13     int (*proc_mmap)(struct file *, struct vm_area_struct *);
14     unsigned long (*proc_get_unmapped_area)(struct file *, unsigned long, unsigned long, unsigned long, unsigned long);
15 } __randomize_layout;
```

```
1 struct file_operations {
2
3     struct module *owner; // 拥有该结构的模块的指针，一般为THIS_MODULE
4
5
6     loff_t (*llseek) (struct file *, loff_t, int); // 用来修改文件当前的读写位置
7
8     ssize_t (*read) (struct file *, char __user *, size_t, loff_t *); // 从设备中同步读取数据
9
10    ssize_t (*write) (struct file *, const char __user *, size_t, loff_t *); // 向设备发送数据
11
12    ssize_t (*aio_read) (struct kiocb *, const struct iovec *, unsigned long, loff_t); // 初始化一个异步的读取操作
13
14    ssize_t (*aio_write) (struct kiocb *, const struct iovec *, unsigned long, loff_t); // 初始化一个异步的写入操作
15
16    int (*readdir) (struct file *, void *, filldir_t); // 仅用于读取目录，对于设备文件，该字段为NULL
17
18    unsigned int (*poll) (struct file *, struct poll_table_struct *); // 轮询函数，判断目前是否可以进行非阻塞的读写或写入
19
20    int (*ioctl) (struct inode *, struct file *, unsigned int, unsigned long); // 执行设备I/O控制命令
21
22    long (*unlocked_ioctl) (struct file *, unsigned int, unsigned long); // 不使用BLK文件系统，将使用此种函数指针代替ioctl
23    ...
24 }
```

据此对示例代码 hello.c 进行了修改，注释掉原本的 file_operation 结构体，补写了 proc_ops 结构体，最终编译成功。



```
thousanrance@thousanrance-VirtualBox: ~/Desktop/Code/OS...
psmouse          155648  0
libahci           36864  1 ahci
i2c_piix4         28672  0
e1000             143360  0
pata_acpi         16384  0
video             53248  0
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ cat /proc/hello
Hello World
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ sudo rmmod hello
```

proc_ops 结构体的缺点是，不再有 struct module *owner 这个参数，没有指向该结构体所属模块的指针，所以在逻辑上是一个不属于这个模块的结构体。

```
thousanrance@thousanrance-VirtualBox: ~/Desktop/Code/OS...
arser"
[ 4.813326] audit: type=1400 audit(1646043584.903:6): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/bin/evince" pid=506 comm="apparmor_parser"
[ 4.813331] audit: type=1400 audit(1646043584.903:7): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/bin/evince//sanitized_helper" pid=506 comm="apparmor_parser"
[ 4.813332] audit: type=1400 audit(1646043584.903:8): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/bin/evince-previewer" pid=506 comm="apparmor_parser"
[ 4.813334] audit: type=1400 audit(1646043584.903:9): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/bin/evince-previewer//sanitize_d_helper" pid=506 comm="apparmor_parser"
[ 4.813335] audit: type=1400 audit(1646043584.903:10): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/bin/evince-thumbnailer" pid=506 comm="apparmor_parser"
[ 5.820759] kauditd_printk_skb: 21 callbacks suppressed
[ 5.820761] audit: type=1400 audit(1646043585.907:32): apparmor="DENIED" operation="capable" profile="/usr/sbin/cups-browsed" pid=614 comm="cups-browsed" capability=23 capname="sys_nice"
[ 6.485671] e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
[ 6.486995] IPv6: ADDRCONF(NETDEV_CHANGE): enp0s3: link becomes ready
[ 8.456761] loop13: detected capacity change from 0 to 8
[ 11.565122] rfkill: input handler disabled
[ 322.813931] rfkill: input handler enabled
[ 329.832955] rfkill: input handler disabled
[ 613.945807] hello: loading out-of-tree module taints kernel.
[ 613.945870] hello: module verification failed: signature and/or required key missing - tainting kernel
[ 613.945954] /proc/hello created
[ 698.734020] /proc/hello removed
thousanrance@thousanrance-VirtualBox: ~/Desktop/Code/OS/project/ch2$
```

IV. Assignment

1、Design a kernel module that creates a /proc file named /proc/jiffies that reports the current value of jiffies when the /proc/jiffies file is read, such as with the command

```
cat /proc/jiffies
```

Be sure to remove /proc/jiffies when the module is removed.

实现细节：基本仿照 hello.c，导入库<linux/jiffies.h>，然后只需要对 proc_read() 函数中的 printf() 的参数进行修改，输出要求的 jiffies 的值即可。


```
thousanrance@thousanrance-VirtualBox: ~/Desktop/Code/OS...
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ make clean
make -C /lib/modules/5.13.0-28-generic/build M=/home/thousanrance/Desktop/Code/OS/project/ch2 clean
make[1]: Entering directory '/usr/src/linux-headers-5.13.0-28-generic'
CLEAN /home/thousanrance/Desktop/Code/OS/project/ch2/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-5.13.0-28-generic'
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ make
make -C /lib/modules/5.13.0-28-generic/build M=/home/thousanrance/Desktop/Code/OS/project/ch2 modules
make[1]: Entering directory '/usr/src/linux-headers-5.13.0-28-generic'
CC [M] /home/thousanrance/Desktop/Code/OS/project/ch2/jiffies.o
/home/thousanrance/Desktop/Code/OS/project/ch2/jiffies.c: In function 'proc_read':
/home/thousanrance/Desktop/Code/OS/project/ch2/jiffies.c:69:9: warning: ignoring return value of 'copy_to_user', declared with attribute warn_unused_result [-Wunused-result]
   69 |         copy_to_user(usr_buf, buffer, rv);
      |         ^~~~~~
MODPOST /home/thousanrance/Desktop/Code/OS/project/ch2/Module.symvers
CC [M] /home/thousanrance/Desktop/Code/OS/project/ch2/jiffies.mod.o
LD [M] /home/thousanrance/Desktop/Code/OS/project/ch2/jiffies.ko
BTF [M] /home/thousanrance/Desktop/Code/OS/project/ch2/jiffies.ko
Skipping BTF generation for /home/thousanrance/Desktop/Code/OS/project/ch2/jiffies.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.13.0-28-generic'
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ sudo insmod jiffies.ko
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ dmesg
[ 1244.781548] /proc/jiffies created
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ cat /proc/jiffies
Now the jiffies vlaue is 4295209379
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$

Now the jiffies vlaue is 4295209379
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ sudo rmmod jiffies
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ dmesg
[ 1244.781548] /proc/jiffies created
[ 1359.901507] /proc/jiffies removed
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$
```

2、Design a kernel module that creates a proc file named /proc/seconds that reports the number of elapsed seconds since the kernel module was loaded. This will involve using the value of jiffies as well as the HZ rate. When a user enters the command

```
cat /proc/seconds
```

your kernel module will report the number of seconds that have elapsed since the kernel module was first loaded. Be sure to remove /proc/seconds when the module is removed.

实现细节：基本仿照 hello.c，导入库<asm/param.h><linux/jiffies.h>，然后只需要对 proc_read() 函数中的 printf() 的参数进行修改，利用公式“模块自加载到删除经过的秒数 = (删除时的 jiffies 值 - 加载时的 jiffies 值) / HZ 的值”，输出要求的值即可。

```
thousanrance@thousanrance-VirtualBox: ~/Desktop/Code/OS...  
-Wformat=]  
72 |         rv = sprintf(buffer, "%d seconds have elapsed.\n", (r_jiffies-fl_  
jiffies)/hz);  
|  
|  
|  
|  
|         long unsigned int  
|  
|         %ld  
/home/thousanrance/Desktop/Code/OS/project/ch2/seconds.c:75:9: warning: ignoring  
return value of 'copy_to_user', declared with attribute warn_unused_result [-Wunu  
sed-result]  
75 |         copy_to_user(usr_buf, buffer, rv);  
|  
MODPOST /home/thousanrance/Desktop/Code/OS/project/ch2/Module.symvers  
CC [M] /home/thousanrance/Desktop/Code/OS/project/ch2/seconds.mod.o  
LD [M] /home/thousanrance/Desktop/Code/OS/project/ch2/seconds.ko  
BTF [M] /home/thousanrance/Desktop/Code/OS/project/ch2/seconds.ko  
Skipping BTF generation for /home/thousanrance/Desktop/Code/OS/project/ch2/second  
s.ko due to unavailability of vmlinux  
make[1]: Leaving directory '/usr/src/linux-headers-5.13.0-28-generic'  
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ ls  
hello.c      Makefile      Module.symvers  seconds.ko      seconds.mod.c  seconds.o  
jiffies.c    modules.order  seconds.c        seconds.mod     seconds.mod.o  simple.c  
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ sudo insmod s  
econds.ko  
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ dmesg  
[ 1519.824424] /proc/seconds created  
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ cat /proc/sec  
onds  
14 seconds have elapsed.  
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$
```

```
14 seconds have elapsed.  
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ sudo rmmmod se  
conds  
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$ dmesg  
[ 1519.824424] /proc/seconds created  
[ 1565.242440] /proc/seconds removed  
thousanrance@thousanrance-VirtualBox:~/Desktop/Code/OS/project/ch2$
```