Organizacion del Computador II

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Trabajo Práctico N°3

Grupo enifra

Integrante	LU	Correo electrónico
Serio, Franco	215/15	francoagustinserio@gmail.com

Reservado para la cátedra

Instancia	Docente	Nota
Primera entrega		
Segunda entrega		

Índice

1. Introduccion **3**

2. Modo Real **4**

3. Modo Protegido **5**

3.1. Segmentacion 5

3.2. Paginado 5

3.3. Manejo de Interrupciones 6

3.4. Tareas 8

3.5. Scheduler 9

3.6. modoDebug 10

1. Introduccion

Este trabajo práctico *Tierra Pirata* consiste en aplicar los conceptos de System Programming vistos en clase.

Construimos un sistema mínimo que permite correr hasta 16 tareas concurrentes a nivel de usuario.

El sistema es capaz de capturar cualquier problema que puedan generar las tareas y tomar las acciones necesarias para quitar a la tarea del sistema.

Algunas tareas podrán ser cargadas en el sistema de manera dinamica por medio de uso del teclado.

Con la realizacion de este trabajo, vamos a utilizar los mecanismos que posee el procesador para la programación desde el punto de vista del sistema operativo enfocados en dos aspectos: el sistema de protección y la ejecución concurrente de tareas.

El informe consta de varias secciones, en las cuales se explica lo realizado para poder hacer funcionar el sistema.

2. Modo Real

Cuando encendemos nuestra computadora, la misma inicia en *Modo Real*. En este modo tenemos una memoria disponible de 1mb, no disponemos de privilegios de ningun tipo, y debemos alinear la memoria a 16 bits para poder operar. Para manejar los distintos tipos de interrupciones, disponemos de rutinas de atencion a las mismas. Podemos acceder a instrucciones de cualquier tipo. Estando en Modo real, lo unico que vamos a hacer, es preparar el sistema para poder pasar a *Modo Protegido*, y realizar todo lo que necesitamos que haga nuestro sistema. Para nuestro sistema, definimos el código de *Modo Real* en el archivo *kernel.asm*:

```
BITS 16
start:
    ; Deshabilitar interrupciones
    cli

    ; Cambiar modo de video a 80 X 50
    mov ax, 0003h
    int 10h ; set mode 03h
    xor bx, bx
    mov ax, 1112h
    int 10h ; load 8x8 font

    ; Imprimir mensaje de bienvenida
    imprimir_texto_mr iniciando_mr_msg, iniciando_mr_len, 0x07, 0, 0
    ; Habilitar A20
    call habilitar_A20
    ; Cargar la GDT
    lgdt [GDT_DESC]

    ; Setear el bit PE del registro CR0
    mov eax, cr0
    or eax, 1
    mov cr0, eax

    ; Saltar a modo protegido
    jmp 0x58:mp
```

Mediante este set de instrucciones estamos preparando nuestro sistema para poder pasar a *Modo Protegido*. Dentro del codigo, estamos habilitando A20 que nos da accesos a direcciones superiores a los 2^{20} bits.
Cargamos la *GDT* (Global Descriptor Table). La *GDT* es una tabla ubicada en memoria que define los siguientes descriptores:

- Descriptores de segmento de memoria
- Descriptor de Task State Segment (TSS)

Luego seteamos el bit *PE* del registro *CR0*.
Una vez activado, vamos a saltar a *Modo Protegido*. Este salto lo realizamos utilizando un far jump al descriptor de segmento de código con nivel de privilegio de sistema. Es el jmp que realizamos en la última linea.

3. Modo Protegido

El *Modo Protegido*, es un poco mas completo que el *Modo Real*, tenemos 4GB de memoria disponible, 4 niveles de protección de memoria y rutinas de atenciión con privilegios.

3.1. Segmentacion

Para el mecanismo de segmentación necesitamos inicializar la GDT. El primer descriptor de la tabla siempre es *nulo*. También al principio tenemos otros 4 segmentos. 1 de código nivel kernel, 1 de código nivel usuario, 1 de datos nivel usuario y 1 de datos nivel kernel. Los segmentos de user tienen dpl 3 y los de sistema 0. A su vez, el límite de los segmentos de la gdt se saca porque en el TP dice que se direccionan los primeros 500MB de memoria. Eso significa que tenemos que usar granularidad de a 4KB de lo contrario no llegamos a los 500MB pedidos. El limite se calcula de hacer (500MB / 4KB) - 1. Esto es porque granularity como dijimos está seteado. El dpl es 3 si se trata de usuario y 0 si se trata de kernel. El tipo es 10 si se trata de de código y 2 si se trata de datos. Hay otro descriptor al comienzo de nuestro sistema para el video. Aquí la base es 0xB8000 a diferencia del cero de las demás entradas. Ésto lo dice la página 2 del enunciado del TP. Todos los segmentos se ponen en presentes.
Nos encargamos de setear los offset de los descriptores de los selectores de segmentos. Luego seteamos la pila del kernel en la dirección 0x27000 que indica el enunciado del TP. Al primer ax le cargamos el indice de la gdt de los datos de nivel 0 y al segundo el indice de la gdt del segmento de video, que son el 9 y el 12 respectivamente.

```
BITS 32
mp:
    ; Establecer selectores de segmentos
    xor eax, eax
    mov ax, 1001000b
    mov ds, ax
    mov ss, ax
    mov es, ax
    mov gs, ax
    mov ax, 1100000b
    mov fs, ax
    ; Establecer la base de la pila
    mov esp, 0x27000
    mov ebp, 0x27000
```

Luego de esto imprimimos en pantalla un mensaje de bienvenida a nuestro sistema e inicializamos la pantalla y el juego.

```
    ; Imprimir mensaje de bienvenida
    imprimir_texto_mp iniciando_mp_msg, iniciando_mp_len, 0x07, 2, 0
    call game_inicializar
    call screen_inicializar
    call screen_pintar_nombre
    call screen_pintar_puntajes
```

Las funciones *screen_inicializar*, *screen_pintar_nombre* estan definidas en **screen.h** y desarrolladas en **screen.c**. Estos métodos se encargan de pintar la pantalla, según lo pedido en el enunciado. La función *game_inicializar* esta definida en **game.c** que inicializa los 2 jugadores y el reloj de cada pirata.

3.2. Paginado

Habilitamos la paginación en nuestro sistema de la siguiente manera:

```
    ; Cargar directorio de paginas
    ; Inicializar el directorio de paginas
    call mmu_inicializar
    call mmu_inicializar_dir_kernel
    xor eax, eax
```

```
mov eax, 0x27000
mov cr3, eax
; Habilitar paginacion
xor eax, eax
mov eax, cr0
or eax, 0x80000000
mov cr0, eax
```

Para mappear y unmapear definimos métodos en el archivo *mmu.c*, para ser mas preciso, mmu_mapear_pagina que devuelve void y recibe una direccion virtual y fisica para el que tiene que mapear, un cr3 que es nuestra dirección de comienzo del page_directory_address y flags de read-write y user-supervisor. Durante el mapeo, lo que se hace es lo siguiente:

- Se saca el índice del page directory shifteando la virtual para la derecha 22 bits.
- Se saca el índice del page table shifteando la virtual 10 bits para la izquierda y despues 22 para la derecha (así nos quedamos con lo del medio).
- Se busca si el page directory en ese índice está presente. Si no lo está se lo pone presente y se pide una pagina libre para el page table. Se establece como base_address del page directory esta nueva página pedida shifteada 12 its para la derecha y en éste nuevo page table se pone como base_address la fisica que nos pasan como parámetro shifteada 12 bits para la derecha.
- Si el page directory en ese índice sí esta presente, sólo se pide el page table al que apunta el base_address de ese page directory. A éste último se le establece como base_address la física que nos pasaron como parámetro shifteada 12 bits para la derecha.
- Luego sólo resta poner los bits correspondientes prendidos, apagados, o los read-write y user-supervisor que nos pasan como parámetro.

Finalmente, mara desmapear una pagina, usamos mmu_unmapear_pagina que toma una dirección virtual y un cr3. Lo que se hace para esto es:

- Se shiftea 22 bits a la derecha la virtual pasada por parámetro para sacar el índice dle page directory.
- Se shiftea 10 bits para la izquierda y 22 para la derecha para quedarse con el índice del page table de la dirección virtual pasada por parámetro.
- Se va al page table de esa dirección virtual sacando lo que apunta la base_address del page directory en el primer índice resuelto y se la pone como no presente.

Durante el juego, debemos poder paginar de manera dinámica las direcciones de los piratas que se agregan, para poder realizarlo utilizamos el siguiente método:

```
unsigned int mmu_proxima_pagina_fisica_libre()
    unsigned int pagina_libre = proxima_pagina_libre;
    proxima_pagina_libre += PAGE_SIZE;
    return pagina_libre;
```

3.3. Manejo de Interrupciones

Para poder atender los distintos tipos de interrupciones, definimos las tareas de atención en *isr.asm* Definimos una rutina para atender las interrupciones del reloj:

```
global _isr32
_isr32:
    ; PRESERVAR REGISTROS
    pushad
    call fin_intr_pic1
```

```
cmp byte [modoDebugPantalla], 1
je .fin
call sched_tick
str cx
cmp ax, cx
je .fin
mov [sched_tarea_selector], ax
jmp far [sched_tarea_offset]
.fin:
; RESTAURAR REGISTROS
popad
iret
```

Luego, para ateneder las interrupciones correspondientes al teclado lo hacemos de la siguiente manera:

```
global_isr33
    _isr33:
    pushad
    call fin_intr_pic1
    xor ax, ax
    in al, 0x60
    push eax
    call game_atender_teclado
    pop eax
    popad
    iret
```

El método *game_atender_teclado* esta definido en nuestro archivo *game.c*. Este método lo que hace, es imprimir en el rincon derecho superior de la pantalla la tecla que se presionó. Cuenta con un switch, que evalua el caso de cada tecla posible, y en base a esto imprime lo que corresponde.

La interrupción del software la realizamos con

```
global _isr70
_isr70:
    cmp eax, 3
    je .posicion
    pushad
    push ecx
    push eax
    call game_syscall_manejar
    call sched_intercambiar_por_idle
    mov ax, 13<<3
    mov [sched_tarea_selector], ax
    jmp far [sched_tarea_offset]
    pop eax
    pop ecx
    jmp .fin
.posicion:
    mov edi, eax
    push ecx
    push edi
    call game_syscall_manejar
    pop ecx
    pop edi
    jmp .fin2
.fin:
    popad
.fin2:
    iret
```

Ésto compara si la interrupción es por la función posición, en cuyo caso se hace aparte para poder devolver el resultado en eax. En el otro caso, llamamos a manejar e intercambiamos por idle. Después hacemos el jmp far para cambiar la tarea.

Para atender las interrupciones de excepciones que describe el ejercicio 2 del TP, definimos una macro:

```
% macro ISR 1
global _isr%1
_isr%1:
    mov eax, %1
    imprimir_texto_mp desc_%1, desc_len_%1, 0x07, 3, 0
    jmp $
```

De esta manera, podemos definir el mensaje correspondiente para cada interrupcion, y utilizando la macro, no tenemos que repetir el código, ya que para todas las interrupciones va a trabajar de la misma manera. Va a imprimir en pantalla el nombre de la interrupción que acaba de ocurrir. Por ejemplo, cuando queremos identificar la interrupción de "Divide Error", definimos el mensaje de la siguiente maner:

```
desc_0 db 'Divide Error'
desc_len_0 equ $ - desc_0
```

De esta misma manera definimos todos los mensajes correspondientes a las interrupciones, en nuestro archivo *isr.asm*.
En el kernel.asm las interrupciones están representadas por el siguiente código:

```
call idt_inicializar
lidt[IDT_DESC]
call resetear_pic
call habilitar_pic
```

Donde lo que se hace es inicializar las entries de la idt, inclusive la entry de la syscall que necesita otro dpl (en este caso 3, de usuario) a diferencia del 0 que es kernel. Por eso hay IDT_entry y IDT_entry_syscall en **idt.c**. La IDT se carga con la instrucción lidt con la dirección de la idt y se resetea y habilita el Programmable Interrupt Controller, que es el mismo al cual le avisamos en las isr's cuando se atiende cada una de las interrupciones. La linea *sti* activa las interrupciones (set interrupts). Ésto lo hacemos después de cargar la tarea inicial.

3.4. Tareas

Completamos las TSS utilizando código c, en el archivo *tss.c*. Se necesita un idle que va a hacer como pivot en todo cambio de tareas y una inicial para que el primer context switch pueda tirar sus datos en algún lado, por eso no es importante qué tiene y se llena toda con ceros (o basura).

Debemos agregar los *descriptores de TSS* correspondientes a la tarea *idle* y la tarea *inicial* a nuestra *GDT*, para poder realizar esto, definimos un método llamado *tss_agregar_a_gdt*

Luego necesitamos completar la TSS correspondiente a cada pirata.

En el kernel.asm que es lo que se corre en bochs, las tareas estan representadas por el siguiente código:

```
call tss_inicializar
call tss_agregar_a_gdt
```

Esto lo que hace es inicializar los valores de las tss_idle y tss_inicial que están declaradas en **tss.h** y agregar sus respectivos descriptores a la GDT. El código

```
mov ax, 0x70
ltr ax
```

carga la tarea inicial y

```
jmp 0x68:0
```

cambia a la tarea idle. Ésta tarea tiene como cr3, base de la pila y stack el 0x27000, el eip de 0x16000 que es donde

está el código de la tarea.

Cada pirata es una tarea distinta y tienen cada uno un cr3 distinto. Cuando se lanza una tarea lo primero que se hace es agregar el descriptor de tss de ese pirata a la GDT y despues se completa la tss. Ésto se hace con los métodos tss_agregar_pirata_a_gdt y completarTssPirata, respectivamente. Ambos estan en el archivo **tss.c**

3.5. Scheduler

Decidimos representar al *Scheduler* de la siguiente manera:

```
int tareaActualA;
int tareaActualB;
uint proximaTareaA; //indice 0-7
uint proximaTareaB; //indice 0-7
uchar turnoPirata; //0 A, 1 B
uchar turnoPirataActual; //0 A, 1 B
uchar estaEnIdle; // 0 NO, 1 SI
uint modoDebugPantalla;
uint modoDebugActivado;
int proxTareaAMuerta;
int proxTareaBMuerta;
```

Para inicializar estos valores, definimos el siguiente método:

```
void sched_inicializar(){
turnoPirata = 0;
proximaTareaA = 0;
estaEnIdle = 1;
proximaTareaB = 0;
modoDebugActivado = 1;
tareaActualA = 0;
tareaActualB = 0;
turnoPirataActual = 0;
proxTareaAMuerta = 0;
proxTareaBMuerta = 0;
modoDebugPantalla = 0;
}
```

El jugador que empieza el es A, la primera tarea que empieza a correr es la idle por eso está seteado. Ambos jugadores tienen como primer tarea a correr la 0 o sea la primera. El modoDebugActivado está seteado porque el enunciado dice que la primer excepción del procesador ya tiene que lanzar la pantalla y hay dos flags porque uno indica si está la pantalla debug y otra si está el debug activado. proximaTareaA y proximaTareaB indican las proximas tarea a correr de cada jugador. Por último, la proxTareaAMuerta y proxTareaBMuerta indican cuales son los indices de los piratas de cada jugador que van a ser usados en caso de que se lance un pirata verde o azul, respectivamente.

Para atender a la proxima tarea, vamos a reutilizar la función que cambia las tareas de acuerdo al tick del clock, utilizamos a la función:

```
unsigned int sched_proxima_a_ejecutar(){
    return sched_tick();
}
```

Luego, para realizar lo correspondiente al tick del clock usamos sched_tick, que a su vez llama a game_tick que sólo actualiza todos los relojes, en concordancia a lo que pide el ejercicio

Por último, otros métodos que definimos en nuestro *sched.c*

```
void sched_intercambiar_por_idle(){
    estaEnIdle = 1;
}
void sched_nointercambiar_por_idle(){
```

```
        estaEnIdle = 0;
    }
    void sched_toggle_debug(){
        if (modoDebugPantalla) {
            game_modoDebug_close();
            modoDebugPantalla = FALSE;
        } else {
            if (modoDebugActivado) {
                modoDebugActivado = TRUE;
            } else {
                modoDebugActivado = FALSE;
            }
        }
    }
```

Éste último método se llama cuando se aprieta la tecla "y". Lo que hace es preguntar si está la pantalla del debug en el juego, en este caso la cierra y vuelve al juego, poniendo el flag en FALSE, que esta definido como cero. Si no está la pantalla cheque si ya se apretó la tecla "y" y el modoDebugActivado está activado o no, haciendo un simple toggle de éste último valor.
A su vez, el scheduler se tiene que encargar de sacar una tarea cuando ésta muere y agregar una tarea cuando se lanza. Ésto se hace con sched_sacar y sched_agregar, respectivamente. Lo que hace el primero es fijarse cual es la próxima tarea muerta del jugador en cuestión y actualiza si la tarea que se murió viene antes. El sched_agregar se fija cual esta muerto de las tareas del jugador y actualiza su variable próxima tarea muerta.
El scheduler si inicialize en el kernel.asm cuando se hace

```
call sched_inicializar
```

3.6. modoDebug

Para el modo debug usamos 2 flags que están en la estructura del scheduler, modoDebugActivado y modoDebug-Pantalla.

```
    pushad
    call game_pirata_explotoisr
    cmp byte [modoDebugActivado], 1
    jne .fin
    mov eax, cr0
    push eax
    mov eax, cr2
    push eax
    mov eax, cr3
    push eax
    mov eax, cr4
    push eax
    push cs ; push segmentos
    push ds
    push es
    push fs
    push gs
    push ss
    push esp ; push array con toda la info de los registros
    call game_modoDebug_open
.fin:
    jmp 0x68:0 ;jumpeo a la idle
```