Отчет по лабораторной работе №9

Архитектура компьютера

Быкова Алина Александровна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Приобретение навыков написания программ с использованием подпрограмм. Знакомство с методами отладки при помощи GDB и его основными возможностями

2 Выполнение лабораторной работы

Создала каталог для выполнения лабораторной работы No 9, перешла в него и создала файл lab09-1.asm.

```
aabihkova@dk3n37 ~ $ mkdir ~/work/arch-pc/lab09
aabihkova@dk3n37 ~ $ cd ~/work/arch-pc/lab09
aabihkova@dk3n37 ~/work/arch-pc/lab09 $ touch lab09-1.asm
aabihkova@dk3n37 ~/work/arch-pc/lab09 $ ~
```

Рис. 2.1: Создала файл lab09-1.asm

Ввела в файл lab09-1.asm текст программы из листинга. f(x)=2x+7

```
%include 'in_out.asm'
SECTION .data
msg: DB 'Введите x: ',0
result: DB '2x+7=',0
SECTION .bss
x: RESB 80
res: RESB 80
SECTION .text
GLOBAL _start
_start:
;---------------------------------------------
; Основная программа
;---------------------------------------------
mov eax, msg
call sprint
mov ecx, x
mov edx, 80
call sread
mov eax,x
call atoi
call _calcul ; Вызов подпрограммы _calcul
mov eax,result
call sprint
mov eax,[res]
call iprintLF
call quit
_calcul:
mov ebx,2
mul ebx
add eax,7
mov [res],eax
ret ; выход из подпрограммы
```

Рис. 2.2: Программа из листинга 9.1

Создала исполняемый файл и проверила его работу.

```
aabihkova@dk3n37 ~/work/arch-pc/lab09 $ nasm -f elf lab09-1.asm
aabihkova@dk3n37 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-1 lab09-1.o
aabihkova@dk3n37 ~/work/arch-pc/lab09 $ ./lab09-1
Введите x: 1
2x+7=9
```

Рис. 2.3: Проверила работу файла для x=1

Изменила текст программы, добавив подпрограмму _subcalcul в подпрограмму _calcul, для вычисления выражения f(g(x)). f(x)=2x+7, g(x)=3x-1

```
 GNU nano 7.2
SECTION .text
GLOBAL _start
_start:
;-------------------------------------
; Основная программа
;-------------------------------------
mov eax, msg
call sprint
mov ecx, x
mov edx, 80
call sread
mov eax,x
call atoi
call _subcalcul
call _calcul
mov eax,result
call sprint
mov eax,[res]
call iprintLF
call quit
_calcul:
push ebx
mov ebx,2
mul ebx
add eax,7
pop ebx
ret ; выход из подпрограммы
_subcalcul:
push ebx
mov ebx, 3
mul ebx
dec ebx
mov [res],eax

pop ebx
ret
```

Рис. 2.4: Изменила программу

Создала исполняемый файл и проверила его работу.

```
aabihkova@dk3n37 ~/work/arch-pc/lab09 $ nasm -f elf lab09-1.asm
aabihkova@dk3n37 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-1 lab09-1.o
aabihkova@dk3n37 ~/work/arch-pc/lab09 $ ./lab09-1
Введите x: 1
f(g(x))=3
```

Рис. 2.5: Проверила работу файла для x=1

Создала файл lab09-2.asm с текстом программы из Листинга 9.2. (Программа печати сообщения Hello world!).

Рис. 2.6: Программа из листинга 9.2

Получила исполняемый файл; Загрузила исполняемый файл в отладчик gdb; Проверила работу программы, запустив ее в оболочке GDB с помощью команды run; Для более подробного анализа программы установила брейкпоинт на метку _start, с которой начинается выполнение любой ассемблерной программы, и

запустила её; Посмотрела дисассимилированный код программы с помощью команды disassemble; Переключилась на отображение команд с Intel'овским синтаксисом, введя команду set disassembly-flavor intel; Включила режим псевдографики для более удобного анализа программы.

```
aabihkova@dk3n65 ~/work/arch-pc/lab09 $ nasm -f elf -g -l lab09-2.lst lab09-2.asm
aabihkova@dk3n65 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-2 lab09-2.o
aabihkova@dk3n65 ~/work/arch-pc/lab09 $ gdb lab09-2
GNU gdb (Gentoo 12.1 vanilla) 12.1
Copyright (C) 2022 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-pc-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://bugs.gentoo.org/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab09-2...
(gdb) run
Starting program: /afs/.dk.sci.pfu.edu.ru/home/a/a/aabihkova/work/arch-pc/lab09/lab09-2
Hello, world!
[Inferior 1 (process 4155) exited normally]
(gdb) break _start
Breakpoint 1 at 0x8049000: file lab09-2.asm, line 9.
(gdb) run
Starting program: /afs/.dk.sci.pfu.edu.ru/home/a/a/aabihkova/work/arch-pc/lab09/lab09-2

Breakpoint 1, _start () at lab09-2.asm:9
9       mov eax, 4
(gdb)
```

Рис. 2.7: Исполнение файла

```
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x08049000 <+0>:     mov    $0x4,%eax
   0x08049005 <+5>:     mov    $0x1,%ebx
   0x0804900a <+10>:    mov    $0x804a000,%ecx
   0x0804900f <+15>:    mov    $0x8,%edx
   0x08049014 <+20>:    int    $0x80
   0x08049016 <+22>:    mov    $0x4,%eax
   0x0804901b <+27>:    mov    $0x1,%ebx
   0x08049020 <+32>:    mov    $0x804a008,%ecx
   0x08049025 <+37>:    mov    $0x7,%edx
   0x0804902a <+42>:    int    $0x80
   0x0804902c <+44>:    mov    $0x1,%eax
   0x08049031 <+49>:    mov    $0x0,%ebx
   0x08049036 <+54>:    int    $0x80
End of assembler dump.
(gdb) set disassembly-flavor intel
(gdb) disassemble _start
```

Рис. 2.8: Исполнение файла

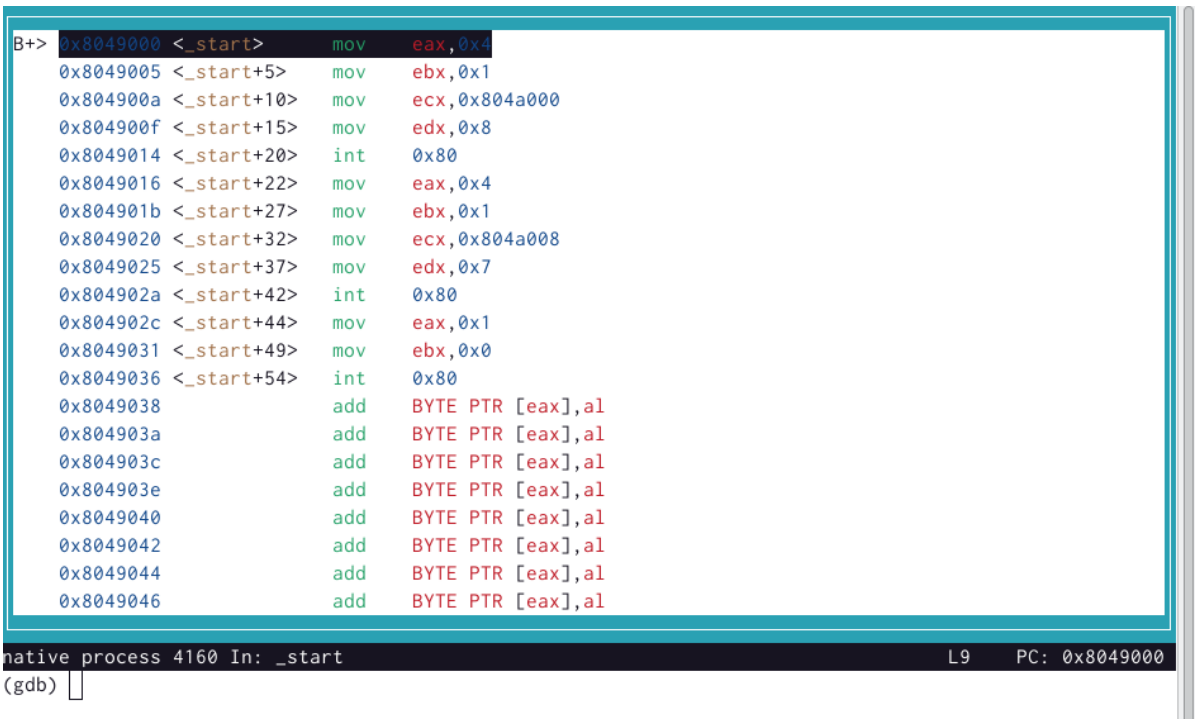

Рис. 2.9: Исполнение файла

Рис. 2.10: Исполнение файла

На предыдущих шагах была установлена точка останова по имени метки (_start). Проверила это с помощью команды info breakpoints.

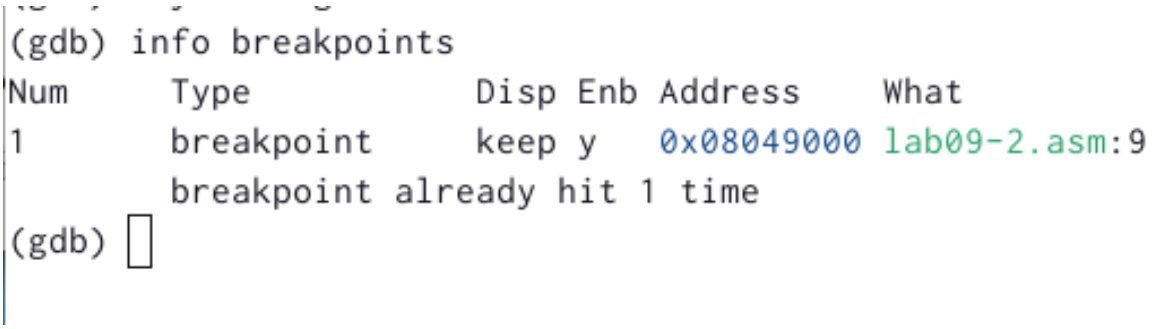

Рис. 2.11: Проверка

Установила еще одну точку останова по адресу инструкции. Посмотрела информацию о всех установленных точках останова.

```
(gdb) break *0x8049031
Breakpoint 2 at 0x8049031: file lab09-2.asm, line 20.
(gdb) i b
Num     Type           Disp Enb Address    What
1       breakpoint     keep y   0x08049000 lab09-2.asm:9
        breakpoint already hit 1 time
2       breakpoint     keep y   0x08049031 lab09-2.asm:20
(gdb)
```

Рис. 2.12: Выполнение команд

Посмотрела содержимое регистров с помощью команды info registers.

```
ebx            0x0                0
esp            0xffffc430         0xffffc430
ebp            0x0                0x0
esi            0x0                0
edi            0x0                0
--Type <RET> for more, q to quit, c to continue without paging--eip            0x8049000          0x8049000 <_start>
eflags         0x202              [ IF ]
cs             0x23               35
ss             0x2b               43
ds             0x2b               43
es             0x2b               43
fs             0x0                0
gs             0x0                0
(gdb)
```

Рис. 2.13: Информацию о всех установленных точках останова

Посмотрела значение переменной msg1 по имени.

```
native process 3427 In: _start
(gdb) x/1sb &msg1
0x804a000 <msg1>:       "Hello, "
(gdb)
```

Рис. 2.14: Посмотрела значение переменной msg1 по имени

Посмотрела значение переменной msg2 по адресу.

```
(gdb) layout regs
(gdb) x/1sb 0x804a008
0x804a008 <msg2>:       "world!\n\034"
(gdb)
```

Рис. 2.15: Посмотрела значение переменной msg2 по адресу

Изменила первый символ переменной msg1.

```
(gdb) set {char}&msg1='h'
(gdb) x/1sb &msg1
0x804a000 <msg1>:       "hello, "
(gdb)
```

Рис. 2.16: Изменение символа

Заменила w на W во второй переменной msg2.

```
(gdb) set {char}&msg2='W'
(gdb) x/1sb &msg2
0x804a008 <msg2>:       "World!\n\034"
(gdb)
```

Рис. 2.17: Замена символа

Вывела в различных форматах (в шестнадцатеричном формате, в двоичном

формате и в символьном виде) значение регистра edx.

```
(gdb) p/s $edx
$1 = 0
(gdb) p/x
$2 = 0x0
(gdb) p/t
$3 = 0
(gdb)
```

Рис. 2.18: Вывод значений

С помощью команды set изменила значение регистра ebx.

```
(gdb) set $ebx='2'
(gdb) p/s $ebx
$4 = 50
(gdb) set $ebx=2
(gdb) p/s $ebx
$5 = 2
```

Рис. 2.19: Изменение значение регистра

Завершила выполнение программы с помощью команды continue и вышла из GDB с помощью команды quit.

Рис. 2.20: Завершила выполнение программы и вышла из GDB

Скопировала файл lab8-2.asm, созданный при выполнении лабораторной работы No8, с программой выводящей на экран аргументы командной строки в файл с именем lab09-3.asm и создала исполняемый файл.

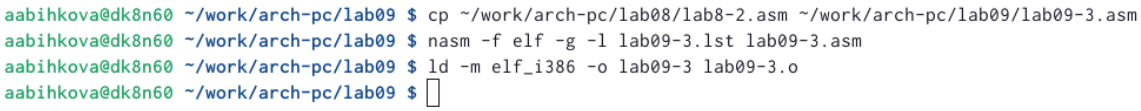

Рис. 2.21: Создала исполняемый файл

Загрузила исполняемый файл в отладчик, указав аргументы.

```
aabihkova@dk8n60 ~/work/arch-pc/lab09 $ gdb --args lab09-3 аргумент1 аргумент 2 'аргумент 3'
GNU gdb (Gentoo 12.1 vanilla) 12.1
Copyright (C) 2022 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-pc-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://bugs.gentoo.org/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab09-3...
```

Рис. 2.22: Загрузила исполняемый файл в отладчик

Установила точку останова и запустила ее.

```
(gdb) b _start
Breakpoint 1 at 0x80490e8: file lab09-3.asm, line 5.
(gdb) run
```

Рис. 2.23: Установка точки и ее запуск

Посмотрела адрес вершины стека, который хранится в регистре esp, число аргументов 5. Посмотрела остальные позиции стека (по адесу [esp+4] располагается адрес в памяти где находиться имя программы, по адесу [esp+8] храниться адрес первого аргумента, по аресу [esp+12] – второго и т.д.).

```
(gdb) x/x $esp
0xffffc3f0:     0x00000005
(gdb) x/s *(void**)($esp + 4)
0xffffc654:     "/afs/.dk.sci.pfu.edu.ru/home/a/a/aabihkova/work/arch-pc/lab09/lab09-3"
(gdb) x/s *(void**)($esp + 8)
0xffffc69a:     "аргумент1"
(gdb) x/s *(void**)($esp + 12)
0xffffc6ac:     "аргумент"
(gdb) x/s *(void**)($esp + 16)
0xffffc6bd:     "2"
(gdb) x/s *(void**)($esp + 20)
0xffffc6bf:     "аргумент 3"
(gdb) x/s *(void**)($esp + 24)
0x0:    <error: Cannot access memory at address 0x0>
```

Рис. 2.24: Просмотр позиций стека

3 Задание для самостоятельной работы

1. Преобразовала программу из лабораторной работы №8 (задание №1 для самостоятельной работы), реализовав вычисление значения функции f(x) как подпрограмму.

```
%include 'in_out.asm'
SECTION .data
f_x db "функция: 10(x - 1)",0h
msg db 10,13,'результат: ',0h
SECTION .text
global _start
_f:
push ebx
dec eax
mov ebx, 10
mul ebx
pop ebx
ret
_start:
pop ecx
pop edx
sub ecx, 1
mov esi, 0
next:
cmp ecx,0h
jz _end
pop eax
call atoi
call _f
add esi, eax
loop next
_end:
mov eax, f_x
call sprint
mov eax, msg
call sprint
mov eax, esi
call iprintLF
call quit
```

Рис. 3.1: Изменение программы

Создала исполняемый файл и проверила его работу.

```
aabihkova@dk3n38 ~/work/arch-pc/lab09 $ ./lab9-4 1 2 3 4
функция: 10(x - 1)
результат: 60
```

Рис. 3.2: Проверка исполняемого файла

Ввела программу из листинга вычисления выражения (3 + 2) * 4 + 5

```
 GNU nano 7.2
%include 'in_out.asm'
SECTION .data
div: DB 'Результат: ',0
SECTION .text
GLOBAL _start
_start:
; ---- Вычисление выражения (3+2)*4+5
mov ebx,3
mov eax,2
add ebx,eax
mov ecx,4
mul ecx
add ebx,5
mov edi,ebx
; ---- Вывод результата на экран
mov eax,div
call sprint
mov eax,edi
call iprintLF
call quit
```

Рис. 3.3: Ввела программу из листинга

Создала исполняемый файл и проверила его работу. При запуске данная программа дает неверный результат.

```
aabihkova@dk2n24 ~/work/arch-pc/lab09 $ nasm -f elf -g -l lab9-5.lst lab9-5.asm
aabihkova@dk2n24 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab9-5 lab9-5.o
aabihkova@dk2n24 ~/work/arch-pc/lab09 $ gdb lab9-5
GNU gdb (Gentoo 13.2 vanilla) 13.2
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-pc-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://bugs.gentoo.org/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab9-5...
(gdb) run
Starting program: /afs/.dk.sci.pfu.edu.ru/home/a/a/aabihkova/work/arch-pc/lab09/lab9-5
Результат: 10
[Inferior 1 (process 4118) exited normally]
(gdb)
```

Рис. 3.4: Проверка работы программы

Изменила текст программы для верного результата.

```
%include 'in_out.asm'
SECTION .data
div: DB 'Результат: ',0
SECTION .text
GLOBAL _start
_start:
; ---- Вычисление выражения (3+2)*4+5
mov ebx,3
mov eax,2
add eax,ebx
mov ecx,4
mul ecx
add eax,5
mov edi,eax
; ---- Вывод результата на экран
mov eax,div
call sprint
mov eax,edi
call iprintLF
call quit
```

Рис. 3.5: Изменение программы

Создала исполняемый файл и проверила его работу. Вывел верный результат.

```
aabihkova@dk2n24 ~/work/arch-pc/lab09 $ nasm -f elf -g -l lab9-5.lst lab9-5.asm
aabihkova@dk2n24 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab9-5 lab9-5.o
aabihkova@dk2n24 ~/work/arch-pc/lab09 $ gdb lab9-5
GNU gdb (Gentoo 13.2 vanilla) 13.2
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-pc-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://bugs.gentoo.org/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab9-5...
(gdb) run
Starting program: /afs/.dk.sci.pfu.edu.ru/home/a/a/aabihkova/work/arch-pc/lab09/lab9-5
Результат: 25
[Inferior 1 (process 3992) exited normally]
(gdb)
```

Рис. 3.6: Проверка работы программы

4 Выводы

Приобрела навыки написания программ с использованием подпрограмм. Познакомилась с методами отладки при помощи GDB и его основными возможностями