

# **Лабораторная работа №9**

**Архитектура компьютера. Понятие подпрограммы. Отладчик GDB**

Сафиуллина Айлина Саяровна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>6</b>
<b>2</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
3.1	Реализация подпрограмм в NASM . . . . .	9
3.2	Отладка программ с помощью GDB . . . . .	12
3.3	Добавление точек останова . . . . .	16
3.4	Работа с данными программы в GDB . . . . .	18
3.5	Обработка аргументов командной строки в GDB . . . . .	20
3.6	Задание для самостоятельной работы . . . . .	23

# Список иллюстраций

3.1	Каталог lab09 . . . . .	9
3.2	Ввод текста из листинга 9.1 . . . . .	10
3.3	Запуск исполняемого файла . . . . .	10
3.4	Изменение текста программы . . . . .	11
3.5	Запуск исполняемого файла . . . . .	11
3.6	Создание файла lab09-2.asm . . . . .	12
3.7	Ввод текста из листинга 9.2. . . . .	12
3.8	Получение исполняемый файл . . . . .	13
3.9	Отладчик gdb . . . . .	13
3.10	run . . . . .	13
3.11	Установка брейкпоинта . . . . .	14
3.12	Дисассимилированный код . . . . .	14
3.13	Intel'овский синтаксис . . . . .	15
3.14	Режим псевдографики . . . . .	16
3.15	Информация о точках останова . . . . .	17
3.16	Установка точки останова . . . . .	17
3.17	Информация об установленных точках останова . . . . .	17
3.18	Команда si . . . . .	18
3.19	Значение переменной msg1 . . . . .	18
3.20	Значение переменной msg2 . . . . .	19
3.21	Изменение значения переменной msg1 . . . . .	19
3.22	Изменение значения переменной msg2 . . . . .	19
3.23	Изменение значения регистра ebx . . . . .	19
3.24	Завершение и выход из программы . . . . .	20
3.25	Копирование файла lab8-2.asm . . . . .	20
3.26	Создание исполняемого файла . . . . .	20
3.27	Загрузка исполняемого файла в отладчик . . . . .	21
3.28	Точка останова . . . . .	21
3.29	Адрес вершины стека . . . . .	22
3.30	Позиции стека . . . . .	22
3.31	Файл lab09-4.asm . . . . .	23
3.32	Измененная программа . . . . .	24
3.33	Запуск исполняемого файла . . . . .	25
3.34	Создание файла lab09-5.asm . . . . .	25
3.35	Ввод текста из листинга 9.3 . . . . .	26
3.36	Неправильный ответ программы . . . . .	26
3.37	Запуск программы с помощью отладчика GDB . . . . .	27

3.38 Анализ регистров . . . . .	28
3.39 Запуск исправленной программы . . . . .	29

## **Список таблиц**

# 1 Цель работы

Целью работы является приобретение навыков написания программ с использованием подпрограмм и знакомство с методами отладки при помощи GDB и его основными возможностями.

## 2 Теоретическое введение

Отладка — это процесс поиска и исправления ошибок в программе. В общем случае его можно разделить на четыре этапа:

- обнаружение ошибки;
- поиск её местонахождения;
- определение причины ошибки;
- исправление ошибки.

Можно выделить следующие типы ошибок:

- синтаксические ошибки — обнаруживаются во время трансляции исходного кода и вызваны нарушением ожидаемой формы или структуры языка;
- семантические ошибки — являются логическими и приводят к тому, что программа запускается, отрабатывает, но не даёт желаемого результата;
- ошибки в процессе выполнения — не обнаруживаются при трансляции и вызывают прерывание выполнения программы (например, это ошибки, связанные с переполнением или делением на ноль).

Второй этап — поиск местонахождения ошибки. Некоторые ошибки обнаружить довольно трудно. Лучший способ найти место в программе, где находится ошибка, это разбить программу на части и произвести их отладку отдельно друг от друга.

Третий этап — выяснение причины ошибки. После определения местонахождения ошибки обычно проще определить причину неправильной работы программы.

Последний этап — исправление ошибки. После этого при повторном запуске

программы, может обнаружиться следующая ошибка, и процесс отладки начнётся заново.

Наиболее часто применяют следующие методы отладки:

- создание точек контроля значений на входе и выходе участка программы (например, вывод промежуточных значений на экран — так называемые диагностические сообщения);
- использование специальных программ-отладчиков.

Отладчик GDB (как и любой другой отладчик) позволяет увидеть, что происходит «внутри» программы в момент её выполнения или что делает программа в момент сбоя.

GDB может выполнять следующие действия:

- начать выполнение программы, задав всё, что может повлиять на её поведение;
- остановить программу при указанных условиях;
- исследовать, что случилось, когда программа остановилась;
- изменить программу так, чтобы можно было поэкспериментировать с устранением эффектов одной ошибки и продолжить выявление других.

Если есть файл с исходным текстом программы, а в исполняемый файл включена информация о номерах строк исходного кода, то программу можно отлаживать, работая в отладчике непосредственно с её исходным текстом. Чтобы программу можно было отлаживать на уровне строк исходного кода, она должна быть откомпилирована с ключом `-g`. Для продолжения остановленной программы используется команда `continue (c) (gdb) с [аргумент]`. Выполнение программы будет происходить до следующей точки останова. Подпрограмма — это, как правило, функционально законченный участок кода, который можно многократно вызывать из разных мест программы. В отличие от простых переходов из подпрограмм существует возврат на команду, следующую за вызовом.



## 3 Выполнение лабораторной работы

### 3.1 Реализация подпрограмм в NASM

Создадим каталог для выполнения лабораторной работы № 9, перейдем в него и создайте файл lab09-1.asm(рис. 3.1).

```
assafiullina@dk8n74 ~ $ mkdir ~/work/arch-pc/lab09
assafiullina@dk8n74 ~ $ cd ~/work/arch-pc/lab09
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ touch lab09-1.asm
assafiullina@dk8n74 ~/work/arch-pc/lab09 $
```

Рис. 3.1: Каталог lab09

В качестве примера рассмотрим программу вычисления арифметического выражения  $f(x) = 2x + 7$  с помощью подпрограммы `_calcul`. В данном примере  $x$  вводится с клавиатуры, а само выражение вычисляется в подпрограмме.(рис. 3.2).

```
lab09-1.asm      [----] 27 L:[ 14+21  35/ 35] *(707 / 707b) <EOF>  [*][X]
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
;-----
; Подпрограмма вычисления
; выражения "2x+7"
_calcul:
mov ebx, 2
mul ebx
add eax, 7
mov [res], eax
ret ; выход из подпрограммы
1Помощь 2Сохран 3Блок 4Замена 5Копия 6Пер~ть 7Поиск 8Уда~ть 9МенюМС10Выход
```

Рис. 3.2: Ввод текста из листинга 9.1

Создадим исполняемый файл и проверим его работу (рис. 3.3).

```
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ nasm -f elf lab09-1.asm
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-1 lab09-1.o
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ ./lab09-1
Введите x: 15
2x+7=37
assafiullina@dk8n74 ~/work/arch-pc/lab09 $
```

Рис. 3.3: Запуск исполняемого файла

Изменим текст программы, добавив подпрограмму `_subcalcul` в подпрограмму `_calcul`, для вычисления выражения  $f(g(x))$ , где  $x$  вводится с клавиатуры,  $f(x) = 2x + 7$ ,  $g(x) = 3x - 1$ . Т.е.  $x$  передается в подпрограмму `_calcul` из нее в подпрограмму `_subcalcul`, где вычисляется выражение  $g(x)$ , результат возвращается в `_calcul`

и вычисляется выражение  $f(g(x))$ . Результат возвращается в основную программу для вывода результата на экран.(рис. 3.4).

```
lab09-1.asm      [-M--] 23 L:[ 1+ 5  6/ 42] *(137 / 642b) 0010 0x00A  [*][X]
%include 'in_out.asm'
SECTION .data
msg: DB 'Введите x:',0
prim1: DB 'f(x)=2x+7',0
prim2: DB 'g(x)=3x-1',0
result: DB 'f(g(x))=',0
SECTION .bss
x: RESB 80
res: RESB 80
SECTION .text
GLOBAL _start
_start:
mov eax,prim1
call sprintf
mov eax,prim2
call sprintf
mov eax, msg
call sprintf
mov ecx, x
mov edx, 80
call read
mov eax,x
1Помощь 2Сохран 3Блок 4Замена 5Копия 6Пер~ть 7Поиск 8Уда~ть 9МенюМС10Выход
```

Рис. 3.4: Изменение текста программы

Создадим исполняемый файл и проверим его работу(рис. 3.5).

```
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ nasm -f elf lab09-1.asm
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-1 lab09-1.o
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ ./lab09-1
f(x)=2x+7
g(x)=3x-1
Введите x:19
f(g(x))=119
assafiullina@dk8n74 ~/work/arch-pc/lab09 $
```

Рис. 3.5: Запуск исполняемого файла

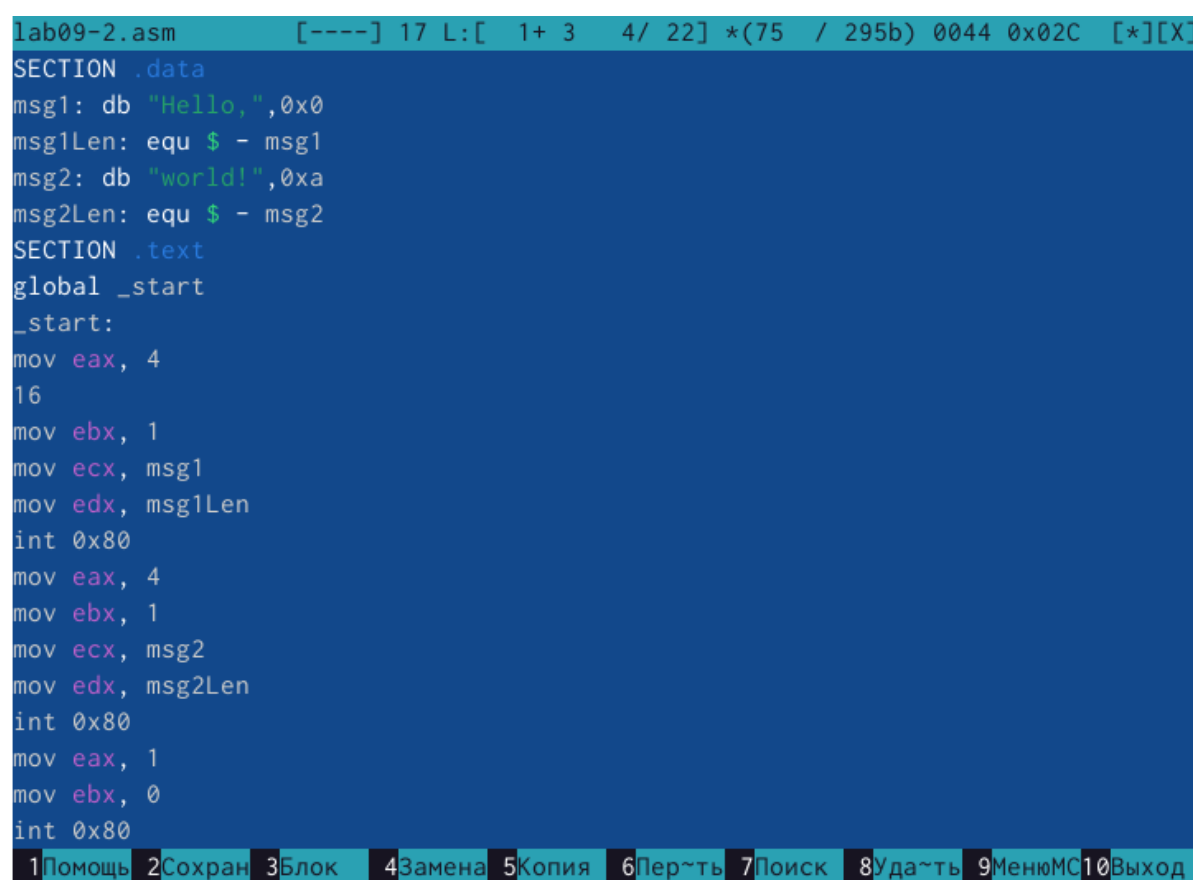
## 3.2 Отладка программ с помощью GDB

Создадим файл lab09-2.asm с текстом программы из Листинга 9.2. (Программа печати сообщения Hello world!): (рис. 3.6).

```
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ touch lab09-2.asm
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ mc
```

Рис. 3.6: Создание файла lab09-2.asm

(рис. 3.7).



```
lab09-2.asm [----] 17 L:[ 1+ 3 4/ 22] *(75 / 295b) 0044 0x02C [*][X]
SECTION .data
msg1: db "Hello,",0x0
msg1Len: equ $ - msg1
msg2: db "world!",0xa
msg2Len: equ $ - msg2
SECTION .text
global _start
_start:
mov eax, 4
int 0x80
mov ebx, 1
mov ecx, msg1
mov edx, msg1Len
int 0x80
mov eax, 4
mov ebx, 1
mov ecx, msg2
mov edx, msg2Len
int 0x80
mov eax, 1
mov ebx, 0
int 0x80
1Помощь 2Сохран 3Блок 4Замена 5Копия 6Переть 7Поиск 8Уда-ть 9МенюМС10Выход
```

Рис. 3.7: Ввод текста из листинга 9.2.

Получим исполняемый файл. Для работы с GDB в исполняемый файл необходимо добавить отладочную информацию, для этого трансляцию программ необходимо проводить с ключом ‘-g’ (рис. 3.8).

```
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ nasm -f elf -g -l lab09-2.lst lab09-2.asm
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-2 lab09-2.o
assafiullina@dk8n74 ~/work/arch-pc/lab09 $
```

---

Рис. 3.8: Получение исполняемый файл

Загрузим исполняемый файл в отладчик gdb (рис. 3.9).

```
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ gdb lab09-2
GNU gdb (Gentoo 14.2 vanilla) 14.2
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 lab09-2...
(gdb) █
```

---

Рис. 3.9: Отладчик gdb

Проверим работу программы, запустив ее в оболочке GDB с помощью команды `run` (сокращённо `r`)(рис. 3.10).

```
(gdb) run
Starting program: /afs/.dk.sci.pfu.edu.ru/home/a/s/assafiullina/work/arch-pc/lab09/lab09-2
Hello,world!
[Inferior 1 (process 7239) exited normally]
(gdb) █
```

---

Рис. 3.10: run

Для более подробного анализа программы установим брейкпоинт на метку `_start`, с которой начинается выполнение любой ассемблерной программы, и запустим её(рис. 3.11).

```

(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/s/assafiullina/work/arch-pc/lab09/lab09-2

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

```

---

Рис. 3.11: Установка брейкпоинта

Посмотрим дисассимилированный код программы с помощью команды `disassemble` начиная с метки `_start`(рис. 3.12).

```

(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     $0x7,%edx
    0x08049014 <+20>:     int     $0x80
    0x08049016 <+22>:     mov     $0x4,%eax
    0x0804901b <+27>:     mov     $0x1,%ebx
    0x08049020 <+32>:     mov     $0x804a007,%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) █

```

---

Рис. 3.12: Дисассимилированный код

Переключимся на отображение команд с Intel'овским синтаксисом, введя команду `set disassembly-flavor intel`(рис. 3.13).

```

(gdb) set disassembly-flavor intel
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x08049000 <+0>:      mov     eax,0x4
    0x08049005 <+5>:      mov     ebx,0x1
    0x0804900a <+10>:     mov     ecx,0x804a000
    0x0804900f <+15>:     mov     edx,0x7
    0x08049014 <+20>:     int     0x80
    0x08049016 <+22>:     mov     eax,0x4
    0x0804901b <+27>:     mov     ebx,0x1
    0x08049020 <+32>:     mov     ecx,0x804a007
    0x08049025 <+37>:     mov     edx,0x7
    0x0804902a <+42>:     int     0x80
    0x0804902c <+44>:     mov     eax,0x1
    0x08049031 <+49>:     mov     ebx,0x0
    0x08049036 <+54>:     int     0x80
End of assembler dump.
(gdb)

```

---

Рис. 3.13: Intel'овский синтаксис

Различия отображения синтаксиса машинных команд в режимах АТТ и Intel заключаются в командах. В диссасилированном отображении в командах используются “%” и “\$” , а в Intel этих символов нет. На это отображение удобнее смотреть. Включим режим псевдографики для более удобного анализа программы с помощью команд: (gdb) layout asm (gdb) layout regs (рис. 3.14).

```
Register group: general
eax      0x0      0
ecx      0x0      0
edx      0x0      0
ebx      0x0      0
esp      0xffffc440 0xffffc440
ebp      0x0      0x0

B> 0x8049000 <_start> mov eax,0x4
    0x8049005 <_start+5> mov ebx,0x1
    0x804900a <_start+10> mov ecx,0x804a000
    0x804900f <_start+15> mov edx,0x7
    0x8049014 <_start+20> int 0x80
    0x8049016 <_start+22> mov eax,0x4

native process 7620 In: _start L9 PC: 0x8049000
(gdb) layout regs
(gdb) run
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /afs/.dk.sci.pfu.edu.ru/home/a/s/assafiullina/work/arch-pc/lab09/lab09-2

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

Рис. 3.14: Режим псевдографики

В этом режиме есть три окна:

- В верхней части видны названия регистров и их текущие значения;
- В средней части виден результат дисассимилирования программы;
- Нижняя часть доступна для ввода команд.

### 3.3 Добавление точек останова

На предыдущих шагах была установлена точка останова по имени метки (`_start`). Проверим это с помощью команды `info breakpoints` (кратко `i b`)(рис. 3.15).



```

Breakpoint 1, _start () at lab09-2.asm:9
(gdb) info breakpoints
Num      Type           Disp Enb Address      What
1        breakpoint     keep y   0x08049000 lab09-2.asm:9
          breakpoint already hit 1 time
(gdb)

```

Рис. 3.15: Информация о точках останова

Установим еще одну точку останова по адресу инструкции (рис. 3.16).

```

Register group: general
eax      0x4          4
ecx      0x0          0
edx      0x0          0
ebx      0x0          0
esp      0xffffc440   0xffffc440
ebp      0x0          0x0

B+ 0x8049000 <_start>      mov     eax,0x4
>0x8049005 <_start+5>     mov     ebx,0x1
0x804900a <_start+10>     mov     ecx,0x804a000
0x804900f <_start+15>     mov     edx,0x7
0x8049014 <_start+20>     int     0x80
0x8049016 <_start+22>     mov     eax,0x4

native process 7620 In: _start L10 PC: 0x8049005
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) si
(gdb)

```

Рис. 3.16: Установка точки останова

Посмотрим информацию о всех установленных точках останова (рис. 3.17).

```

(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. 3.17: Информация об установленных точках останова

## 3.4 Работа с данными программы в GDB

Отладчик может показывать содержимое ячеек памяти и регистров, а при необходимости позволяет вручную изменять значения регистров и переменных. С помощью команды `si` посмотрим регистры и изменим их.

(рис. 3.18).

```
Register group: general
eax      0x4      4
ecx      0x0      0
edx      0x0      0
ebx      0x0      0
esp      0xffffc440 0xffffc440
ebp      0x0      0x0

B+ 0x8049000 <_start>      mov     eax,0x4
>0x8049005 <_start+5>     mov     ebx,0x1
0x804900a <_start+10>     mov     ecx,0x804a000
0x804900f <_start+15>     mov     edx,0x7
0x8049014 <_start+20>     int     0x80
0x8049016 <_start+22>     mov     eax,0x4

native process 7620 In: _start L10 PC: 0x8049005
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) si
(gdb)
```

Рис. 3.18: Команда `si`

Для отображения содержимого памяти можно использовать команду `x`, которая выдаёт содержимое ячейки памяти по указанному адресу. Формат, в котором выводятся данные, можно задать после имени команды через косую черту: `x/NFU`. С помощью команды `x &` также можно посмотреть содержимое переменной. Посмотрим значение переменной `msg1` по имени (рис. 3.19).

```
(gdb) x/1sb &msg1
0x804a000 <msg1>:      "Hello,"
(gdb)
```

Рис. 3.19: Значение переменной `msg1`

Посмотрим значение переменной msg2 по адресу (рис. 3.20).

```
(gdb) x/lsb 0x804a008
0x804a008:      "orld!\n\034"
(gdb) █
```

Рис. 3.20: Значение переменной msg2

Изменить значение для регистра или ячейки памяти можно с помощью команды set, задав ей в качестве аргумента имя регистра или адрес. При этом перед именем регистра ставится префикс \$, а перед адресом нужно указать в фигурных скобках тип данных. Изменим первый символ переменной msg1 (рис. 3.21).

```
(gdb) set {char}&msg1='h'
(gdb) set {char}0x804a001='h'
(gdb) x/lsb &msg1
0x804a000 <msg1>:      "hh1lo,"
(gdb) █
```

Рис. 3.21: Изменение значения переменной msg1

Изменим символ переменной msg2 (рис. 3.22).

```
(gdb) set {char}0x804a008='L'
(gdb) set {char}0x804a00b=' '
(gdb) x/lsb &msg2
0x804a007 <msg2>:      "wLr1 !\n\034"
(gdb) █
```

Рис. 3.22: Изменение значения переменной msg2

С помощью команды set изменим значение регистра ebx (рис. 3.23).

```
(gdb) set $ebx='2'
(gdb) p/s $ebx
$1 = 50
(gdb) set $ebx=2
(gdb) p/s $ebx
$2 = 2
(gdb) █
```

Рис. 3.23: Изменение значения регистра ebx

Команда выводит два разных значения, потому что в первый раз мы вносим значение 2, а во второй - регистр равен двум, поэтому значения отличаются. Завершим выполнение программы с помощью команды `continue` (сокращенно `c`) или `stepi` (сокращенно `si`) и выйдем из GDB с помощью команды `quit` (сокращенно `q`) (рис. 3.24).

```
Breakpoint 2, _start () at lab09-2.asm:20
(gdb) quit
A debugging session is active.

    Inferior 1 [process 7620] will be killed.

Quit anyway? (y or n) █
```

Рис. 3.24: Завершение и выход из программы

## 3.5 Обработка аргументов командной строки в GDB

Скопируем файл `lab8-2.asm`, созданный при выполнении лабораторной работы №8, с программой выводящей на экран аргументы командной строки (Листинг 8.2) в файл с именем `lab09-3.asm` (рис. 3.25).

```
end of assembler dump.
(gdb) layout asm
assafiullina@dk8n74 ~/work/arch-pc/lab09 $ cp ~/work/arch-pc/lab08/lab8-2.asm ~/work/arch-pc/lab09/lab09-3.asm
assafiullina@dk8n74 ~/work/arch-pc/lab09 $
```

Рис. 3.25: Копирование файла `lab8-2.asm`

Создадим исполняемый файл (рис. 3.26).

```
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ nasm -f elf -g -l lab09-3.lst lab09-3.asm
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-3 lab09-3.o
assafiullina@dk4n65 ~/work/arch-pc/lab09 $
```

Рис. 3.26: Создание исполняемого файла

Для загрузки в gdb программы с аргументами необходимо использовать ключ `-args`. Загрузим исполняемый файл в отладчик, указав аргументы (рис. 3.27).

```
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ gdb --args lab09-3 аргумент1 аргумент2 'аргумент 3'
GNU gdb (Gentoo 14.2 vanilla) 14.2
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 lab09-3...
(gdb)
```

Рис. 3.27: Загрузка исполняемого файла в отладчик

При запуске программы аргументы командной строки загружаются в стек. Исследуем расположение аргументов командной строки в стеке после запуска программы с помощью gdb. Для начала установим точку останова перед первой инструкцией в программе и запустим ее (рис. 3.28).

```
(gdb) b _start
Breakpoint 1 at 0x80490e8: file lab09-3.asm, line 5.
(gdb) run
Starting program: /afs/.dk.sci.pfu.edu.ru/home/a/s/assafiullina/work/arch-pc/lab09/lab09-3 аргумент1 аргумент2 аргумент\ 3

Breakpoint 1, _start () at lab09-3.asm:5
5      pop ecx ; Извлекаем из стека в 'ecx' количество
(gdb)
```

Рис. 3.28: Точка останова

Адрес вершины стека храниться в регистре esp и по этому адресу располагается число равное количеству аргументов командной строки (включая имя программы)(рис. 3.29).

```
(gdb) x/x $esp
0xfffffc410:    0x00000004
(gdb)
```

Рис. 3.29: Адрес вершины стека

Как видно, число аргументов равно 5 – это имя программы lab09-3 и непосредственно аргументы: аргумент1, аргумент, 2 и ‘аргумент 3’. Посмотрим остальные позиции стека(рис. 3.30).

```
(gdb) x/x $esp
0xfffffc410:    0x00000004
(gdb) x/x $esp
0xfffffc410:    0x00000004
(gdb) x/s *(void**)(esp + 8)
0xfffffc699:    "аргумент1"
(gdb) x/s *(void**)(esp + 12)
0xfffffc6ab:    "аргумент2"
(gdb) x/s *(void**)(esp + 16)
0xfffffc6bd:    "аргумент 3"
(gdb) x/s *(void**)(esp + 20)
0x0:    <error: Cannot access memory at address 0x0>
(gdb)
```

Рис. 3.30: Позиции стека

Элементы расположены с интервалом в 4 единицы, потому что стек может хранить до 4 байт, и для того, чтобы данные сохранялись нормально и без помех, компьютер использует новый стек для новой информации.

## 3.6 Задание для самостоятельной работы

Преобразуем программу из лабораторной работы №8 (Задание №1 для самостоятельной работы).(рис. 3.31).

```
assafiullina@dk4n65 ~ $ cp ~/work/arch-pc/lab08/lab8-4.asm ~/work/arch-pc/lab09/lab09-4.asm
assafiullina@dk4n65 ~ $ █
```

Рис. 3.31: Файл lab09-4.asm

Реализуем вычисление значения функции  $f(x)$  как подпрограмму(рис. 3.32).

```
lab09-4.asm      [----]  0 L:[ 1+ 0  1/ 29] *(0  / 341b) 0037 0x025[*][X]
%include 'in_out.asm'
SECTION .data
prim db 'f(x)=15x-9',0
otv db 'Ответ: ',0
SECTION .text
GLOBAL _start
_start:
pop ecx
pop edx
sub ecx,1
mov esi,0
mov eax,prim
call sprintfLF
next:
cmp ecx,0
jz _end
mov ebx,15
pop eax
call atoi
mul ebx
add eax,-9
add esi,eax
loop next
_end:
mov eax,otv
call sprintf
mov eax,esi
call iprintLF
call quit
```

1Помощь 2Сохран 3Блок 4Замена 5Копия 6Печать 7Поиск 8Удалить 9МенюМС10Выход

Рис. 3.32: Измененная программа

Создадим исполняемый файл и запустим его. (рис. 3.33).



```
assafiullina@dk4n65 ~ $ cd ~/work/arch-pc/lab09
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ nasm -f elf lab09-4.asm
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-4 lab09-4.o
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ ./lab09-4 5 7 18 9
f(x)=15x-9
Ответ: 549
assafiullina@dk4n65 ~/work/arch-pc/lab09 $
```

Рис. 3.33: Запуск исполняемого файла

Создадим файл для решения №2 самостоятельной работы (рис. 3.34).

```
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ touch lab09-5.asm
assafiullina@dk4n65 ~/work/arch-pc/lab09 $
```

Рис. 3.34: Создание файла lab09-5.asm

В листинге 9.3 приведена программа вычисления выражения  $(3+2)*4+5$ . При запуске данная программа дает неверный результат.(рис. 3.35).

```

lab09-5.asm      [----] 7 L:[ 1+ 5 6/ 21] *(103 / 350b) 0010 0x00A[*][X]
#include 'in_out.asm'
SECTION .data
div: DB 'Результат:',0
SECTION .text
GLOBAL _start
_start:
; -- Вычисление выражения (3+2)*4+5
35
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. 3.35: Ввод текста из листинга 9.3

Проверим, что программа выводит неправильный ответ.(рис. 3.36)

```

assafiullina@dk4n65 ~/work/arch-pc/lab09 $ nasm -f elf lab09-5.asm
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-5 lab09-5.o
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ ./lab09-5
Результат:10
assafiullina@dk4n65 ~/work/arch-pc/lab09 $

```

Рис. 3.36: Неправильный ответ программы

С помощью отладчика GDB запустим программу(рис. 3.37)

```

assafiullina@dk4n65 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-5 lab09-5.o
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ gdb lab09-5
GNU gdb (Gentoo 14.2 vanilla) 14.2
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 lab09-5...
(No debugging symbols found in lab09-5)
(gdb) r
Starting program: /afs/.dk.sci.pfu.edu.ru/home/a/s/assafiullina/work/arch-pc/lab09/lab09-5
Результат:10
[Inferior 1 (process 4840) exited normally]
(gdb) b_start
Undefined command: "b_start". Try "help".
(gdb) r
Starting program: /afs/.dk.sci.pfu.edu.ru/home/a/s/assafiullina/work/arch-pc/lab09/lab09-5
Результат:10
[Inferior 1 (process 4857) exited normally]
(gdb) █

```

Рис. 3.37: Запуск программы с помощью отладчика GDB

Проанализировав изменения значений регистров, понятно, что некоторые регистры стоят не на своих местах.(рис. 3.38)

```
Register group: general
eax      0x0      0
ecx      0x0      0
edx      0x0      0
ebx      0x0      0
esp      0xffffc440 0xffffc440
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0

[ No Source Available ]

native process 5123 In: _start L?? PC: 0x80490e8
ab09/lab09-5

Breakpoint 1, 0x080490e8 in _start ()
(gdb) run
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /afs/.dk.sci.pfu.edu.ru/home/a/s/assafiullina/work/arch-pc/1
ab09/lab09-5

Breakpoint 1, 0x080490e8 in _start ()
(gdb)
```

Рис. 3.38: Анализ регистров

Исправив регистры, запустим программу(рис. 3.39)

```

lab09-5.asm      [----] 10 L:[ 1+13 14/ 20] *(231 / 347b) 0120 0x0
#include 'in_out.asm'
SECTION .data
div: DB 'Результат:',0
SECTION .text
GLOBAL _start
_start:
; -- Вычисление выражения (3+2)*4+5
mov eax,3
mov ebx,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. 3.39: Запуск исправленной программы

Теперь программа действительно выводит правильный ответ. Программа работает верно.(рис. ??)

```

assafiullina@dk4n65 ~/work/arch-pc/lab09 $ nasm -f elf -g -l lab09-5.lst lab09-5.asm
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ ld -m elf_i386 -o lab09-5 lab09-5.o
assafiullina@dk4n65 ~/work/arch-pc/lab09 $ ./lab09-5
Результат:25
assafiullina@dk4n65 ~/work/arch-pc/lab09 $

```

#### # Выводы

В процессе выполнения лабораторной работы я получила навыки написания программ с использованием подпрограмм и ознакомилась с методами отладки

при помощи GDB, его основными возможностями.