

Отчёт по лабораторной работе №9

Дисциплина: Архитектура Компьютера

Курилко-Рюмин Е.М

Содержание

1	Цель работы	4
2	Задание	5
3	Теоретическое введение	6
4	Выполнение лабораторной работы	10
5	Выводы	27
	Список литературы	28

Список иллюстраций

4.1	Создание и запуск исполняемого файла	11
4.2	Редактирование файла	11
4.3	Создание и запуск исполняемого файла	12
4.4	Редактирование файла	12
4.5	Создание исполняемого файла, отладчик gdb	13
4.6	Отладчик gdb	14
4.7	Установка метки	14
4.8	Дисассимилированный код программы с синтаксисом intel	15
4.9	Режим псевдографики	16
4.10	Режим псевдографики	16
4.11	Проверка точек останова	16
4.12	Редактирование файла	17
4.13	Создание и запуск исполняемого файла	17
4.14	Изменение значений регистров и переменных	18
4.15	Изменение значений регистров и переменных	18
4.16	Содержимое регистров	19
4.17	Содержимое переменной, изменение в ней символов	19
4.18	Содержимое переменной, изменение в ней символов	20
4.19	Значения регистра edx	20
4.20	Изменение значений регистра	21
4.21	Загрузка файла в отладчик	21
4.22	Установка точки останова, запуск программы	22
4.23	Просмотр позиций стека	22
4.24	Копирование, редактирование файла	23
4.25	Создание и запуск исполняемого файла	23
4.26	Изменение значений регистров в gdb	24
4.27	Редактирование файла	24
4.28	Создание и запуск исполняемого файла	25

1 Цель работы

Целью данной работы является приобретение практического опыта в написании программ с использованием подпрограмм, а также знакомство с методами отладки при помощи gdb и его основными возможностями.

2 Задание

1. Общее ознакомление с подпрограммами в Nasm и отладкой при помощи gdb.
2. Реализация подпрограмм в NASM.
3. Отладка программ при помощи gdb.
4. Выполнение заданий для самостоятельной работы

3 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, отработывает, 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.

Отладчики позволяют управлять ходом выполнения программы, контролировать и изменять данные. Это помогает быстрее найти место ошибки в программе и ускорить её исправление. Наиболее популярные способы работы с отладчиком — это использование точек останова и выполнение программы по шагам. Пошаговое выполнение — это выполнение программы с остановкой после каждой строки, чтобы программист мог проверить значения переменных и выполнить другие действия. Точки останова — это специально отмеченные места в программе, в которых программа-отладчик приостанавливает выполнение программы и ждёт команд. Наиболее популярные виды точек останова:

- Breakpoint — точка останова (остановка происходит, когда выполнение доходит до определённой строки, адреса или процедуры, отмеченной программистом);
- Watchpoint — точка просмотра (выполнение программы приостанавливается, если программа обратилась к определённой переменной: либо считала её значение, либо изменила его).

Точки останова устанавливаются в отладчике на время сеанса работы с кодом программы, т.е. они сохраняются до выхода из программы-отладчика или до смены отлаживаемой программы. GDB (GNU Debugger — отладчик проекта GNU) [1] работает на многих UNIX-подобных системах и умеет производить отладку многих языков программирования. GDB предлагает обширные средства для слежения и контроля за выполнением компьютерных программ. Отладчик не содержит собственного графического пользовательского интерфейса и использует

стандартный текстовый интерфейс консоли. Однако для GDB существует несколько сторонних графических надстроек, а кроме того, некоторые интегрированные среды разработки используют его в качестве базовой подсистемы отладки. 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.

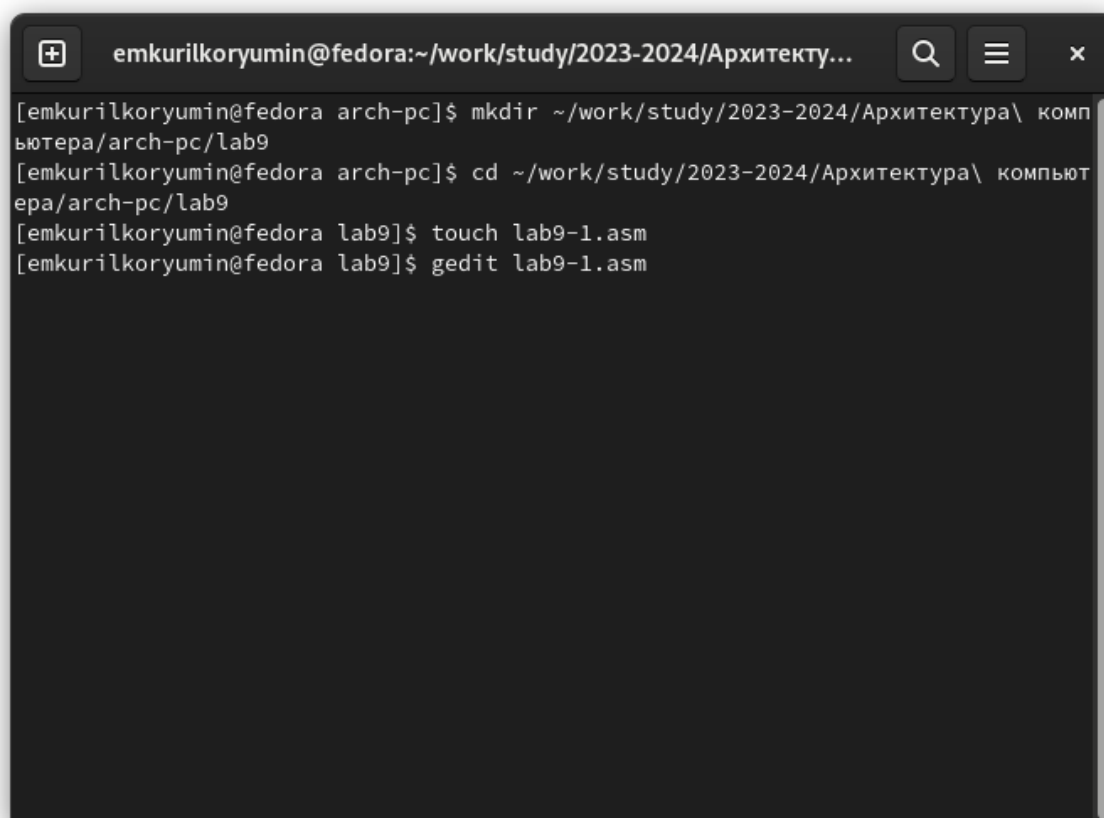
После запуска `gdb` выводит текстовое сообщение — так называемое «nice GDB logo». В следующей строке появляется приглашение (`gdb`) для ввода команд. Далее приведён список некоторых команд GDB. Команда `run` (сокращённо `r`) — запускает отлаживаемую программу в оболочке GDB. Если точки останова были заданы, то отладчик останавливается на соответствующей команде и выдаёт номер точки останова, адрес и дополнительную информацию — текущую строку, имя процедуры, и др. Команда `kill` (сокращённо `k`) прекращает отладку программы, после чего следует вопрос о прекращении процесса отладки. Если в ответ введено `y` (то есть «да»), отладка программы прекращается. Командой `run` её можно начать заново, при этом все точки останова (`breakpoints`), точки просмотра (`watchpoints`) и точки отлова (`catchpoints`) сохраняются. Для выхода из отладчика используется команда `quit` (или сокращённо `q`). 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`. Установить точку останова можно командой `break` (кратко `b`). Типич-

ный аргумент этой команды — место установки. Его можно задать как имя метки или как адрес. Чтобы не было путаницы с номерами, перед адресом ставится «звёздочка». Для продолжения остановленной программы используется команда `continue (c)` (gdb). Выполнение программы будет происходить до следующей точки останова. В качестве аргумента может использоваться целое число \star , которое указывает отладчику проигнорировать $\star - 1$ точку останова (выполнение остановится на \star -й точке). Команда `stepi` (кратко `sI`) позволяет выполнять программу по шагам, т.е. данная команда выполняет ровно одну инструкцию. Как уже упоминалось, отладчик может показывать содержимое ячеек памяти и регистров, а при необходимости позволяет вручную изменять значения регистров и переменных. Посмотреть содержимое регистров можно с помощью команды `info registers` (или `i r`). 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. Если в программе встречается одинаковый участок кода, его можно оформить в виде подпрограммы, а во всех нужных местах поставить её вызов. При этом подпрограмма будет содержаться в коде в одном экземпляре, что позволит уменьшить размер кода всей программы. Для вызова подпрограммы из основной программы используется инструкция `call`, которая заносит адрес следующей инструкции в стек и загружает в регистр `esp` адрес соответствующей подпрограммы, осуществляя таким образом переход. Затем начинается выполнение подпрограммы, которая, в свою очередь, также может содержать подпрограммы. Подпрограмма завершается инструкцией `ret`, которая извлекает из стека адрес, занесённый туда соответствующей инструкцией `call`, и заносит его в `esp`. После этого выполнение основной программы возобновится с инструкции, следующей за инструкцией `call`.

4 Выполнение лабораторной работы

4.1) Реализация подпрограмм в NASM.

С помощью утилиты `mkdir` создаю директорию `lab9` для выполнения соответствующей лабораторной работы. Перехожу в созданный каталог с помощью утилиты `cd`. С помощью `touch` создаю файл `lab9-1.asm`. Копирую в текущий каталог файл `in_out.asm` с помощью утилиты `cp`, ибо он будет использоваться в дальнейшем. Открываю созданный файл `lab9-1.asm`, вставляю в него следующую программу: (рис.1).

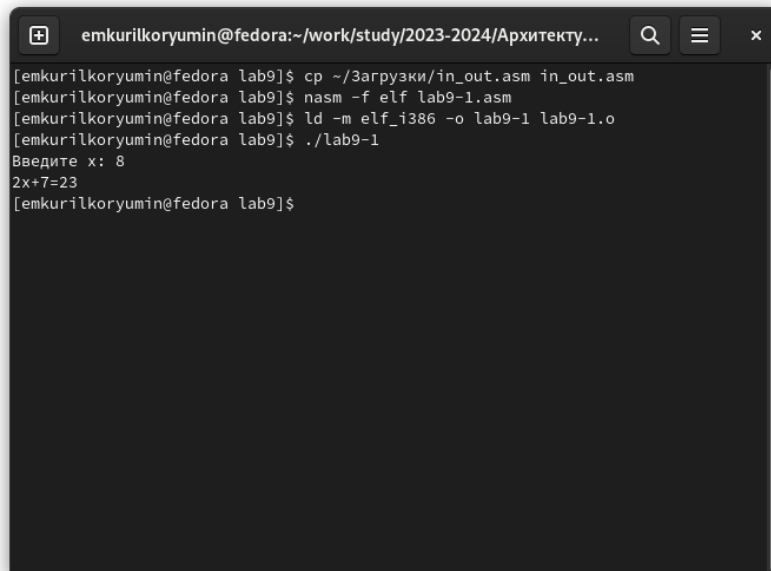


```
emkurilkoryumin@fedora:~/work/study/2023-2024/Архитекту...
[emkurilkoryumin@fedora arch-pc]$ mkdir ~/work/study/2023-2024/Архитектура\ комп
ьютера/arch-pc/lab9
[emkurilkoryumin@fedora arch-pc]$ cd ~/work/study/2023-2024/Архитектура\ комп
ьютера/arch-pc/lab9
[emkurilkoryumin@fedora lab9]$ touch lab9-1.asm
[emkurilkoryumin@fedora lab9]$ gedit lab9-1.asm
```

(image/1.1.p

width=70%}

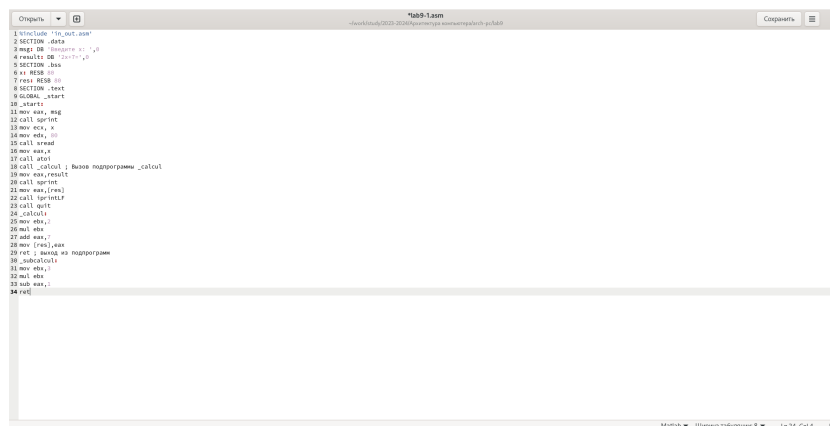
Создаю исполняемый файл и запускаю его. (рис.2).



```
emkurilkoryumin@fedora:~/work/study/2023-2024/Архитекту...
[emkurilkoryumin@fedora lab9]$ cp ~/Загрузки/in_out.asm in_out.asm
[emkurilkoryumin@fedora lab9]$ nasm -f elf lab9-1.asm
[emkurilkoryumin@fedora lab9]$ ld -m elf_i386 -o lab9-1 lab9-1.o
[emkurilkoryumin@fedora lab9]$ ./lab9-1
Введите x: 8
2x+7=23
[emkurilkoryumin@fedora lab9]$
```

Рис. 4.1: Создание и запуск исполняемого файла

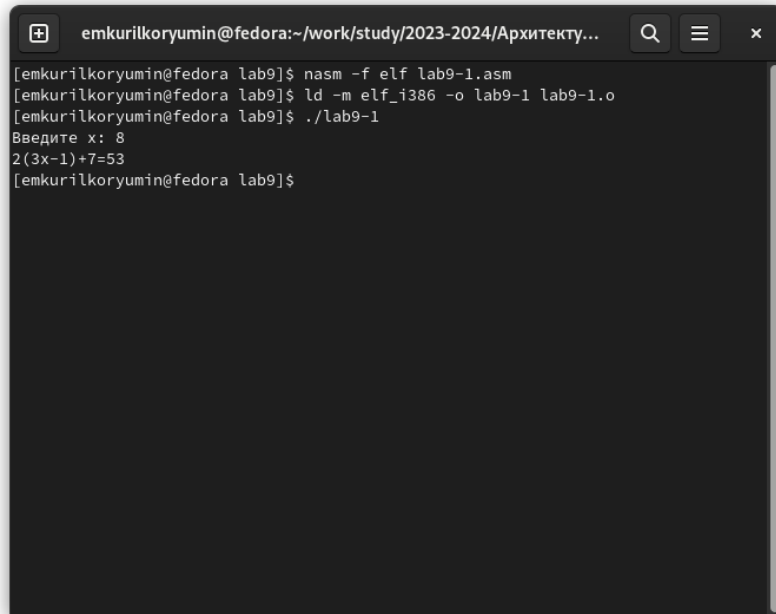
Добавляю подпрограмму subcalcul_, чтобы программа вычисляла значение $f(g(x))$. (рис.3).



```
Открыть 1 lab9-1.asm
1 include "in_out.asm"
2 SECTION .data
3     msg DB "Введите x: ",0
4     result DB "2x+7=",0
5 SECTION .bss
6     RESB 10
7     RESB 10
8 SECTION .text
9 GLOBAL _start
10 _start:
11     mov eax, msg
12     call printf
13     mov ecx, x
14     mov edx, 0
15     call readf
16     mov eax, x
17     call atoi
18     call _calcul ; вызов подпрограммы _calcul
19     mov eax, result
20     call printf
21     mov eax, [eax]
22     call sprintf
23     call quit
24     call _calcul
25     mov ebx, 1
26     mov ebx, 1
27     add eax, 1
28     mov [eax],eax
29     ret ; выход из подпрограммы
30 _calcul:
31     mov ebx, 1
32     mov ebx, 1
33     sub eax, 1
34     ret
```

Рис. 4.2: Редактирование файла

Создаю исполняемый файл и убеждаюсь в правильности его работы. (рис.4).



```
emkurilkoryumin@fedora:~/work/study/2023-2024/Архитекту...
[emkurilkoryumin@fedora lab9]$ nasm -f elf lab9-1.asm
[emkurilkoryumin@fedora lab9]$ ld -m elf_i386 -o lab9-1 lab9-1.o
[emkurilkoryumin@fedora lab9]$ ./lab9-1
Введите x: 8
2(3x-1)+7=53
[emkurilkoryumin@fedora lab9]$
```

Рис. 4.3: Создание и запуск исполняемого файла

4.2) Отладка программ при помощи gdb.

Создаю файл lab09-2.asm и вношу в него следующий текст программы: (рис.5).



```
lab9-2.asm
1 SECTION .data
2 msg1 db "hello", 0x00
3 msg2len equ $ - msg1
4 msg2 db "world", 0x00
5 msg2len equ $ - msg2
6 SECTION .text
7 global _start
8 _start:
9     mov     eax, 4
10    mov     ebx, 1
11    mov     ecx, msg1
12    mov     edx, msg2len
13    int     0x40
14    mov     ecx, 4
15    mov     ebx, 1
16    mov     ecx, msg2
17    mov     edx, msg2len
18    int     0x40
19    mov     ebx, 1
20    mov     ecx, 0
21    int     0x80
```

Рис. 4.4: Редактирование файла

Создаю исполняемый файл и загружаю его в отладчик gdb, запускаю программу с помощью команды run. (рис.6).

```
emkurilkoryumin@fedora:~/work/study/2023-2024/Архитектура компьютера/arch-pc/lab...
[emkurilkoryumin@fedora lab9]$ nasm -f elf lab9-2.asm
[emkurilkoryumin@fedora lab9]$ ld -m elf_i386 -o lab9-2 lab9-2.o
[emkurilkoryumin@fedora lab9]$ gdb lab9-2
GNU gdb (GDB) Fedora Linux 13.2-6.fc38
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-redhat-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
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 lab9-2...
(gdb) r
Starting program: /home/emkurilkoryumin/work/study/2023-2024/Архитектура компьютера/arch-pc/lab9/lab9-2

This GDB supports auto-downloading debuginfo from the following URLs:
<https://debuginfod.fedoraproject.org/>
Enable debuginfod for this session? (y or [n]) y
Debuginfod has been enabled.
To make this setting permanent, add 'set debuginfod enabled on' to .gdbinit.
Downloading separate debug info for system-supplied DSO at 0xf7ffc000
Hello, world!
[Inferior 1 (process 3469) exited normally]
(gdb)
```

Рис. 4.5: Создание исполняемого файла, отладчик gdb

Убеждаюсь в правильности работы программы. (рис.7).

```
emkurilkoryumin@fedora:~/work/study/2023-2024/Архитекту...
[emkurilkoryumin@fedora lab9]$ touch lab9-2.asm
[emkurilkoryumin@fedora lab9]$ gedit lab9-2.asm
[emkurilkoryumin@fedora lab9]$ nasm -f elf lab9-2.asm
[emkurilkoryumin@fedora lab9]$ ld -m elf_i386 -o lab9-2 lab9-2.o
[emkurilkoryumin@fedora lab9]$ ./lab9-2
Hello, world!
[emkurilkoryumin@fedora lab9]$
```

Рис. 4.6: Отладчик gdb

Устанавливаю метку `_start` и запускаю программу, также увидим работу метки.
(рис.8).

```
emkurilkoryumin@fedora:~/work/study/2023-2024/Архитекту...
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

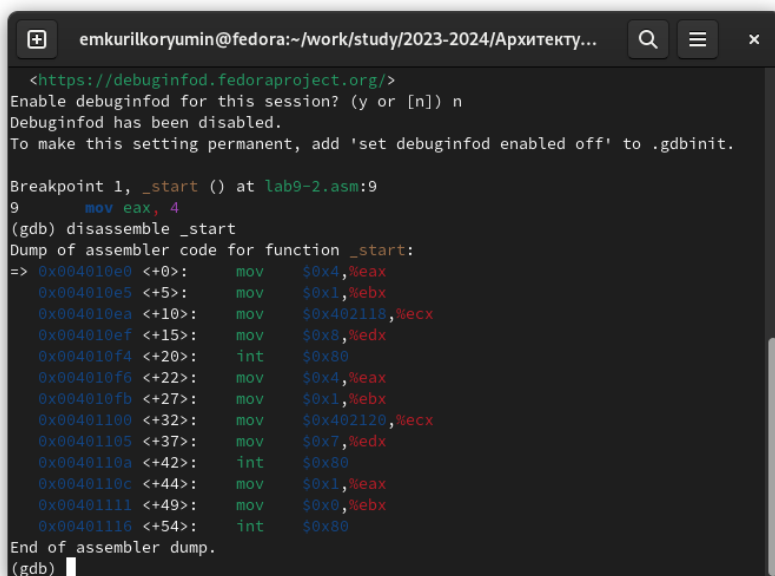
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab9-2...
(gdb) break _start
Breakpoint 1 at 0x4010e0: file lab9-2.asm, line 9.
(gdb) r
Starting program: /home/emkurilkoryumin/work/study/2023-2024/Архитектура компьютер/arch-pc/lab9/lab9-2

This GDB supports auto-downloading debuginfo from the following URLs:
<https://debuginfod.fedoraproject.org/>
Enable debuginfod for this session? (y or [n]) n
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.

Breakpoint 1, _start () at lab9-2.asm:9
9      mov eax, 4
(gdb)
```

Рис. 4.7: Установка метки

Смотрю дисассимилированный код программы сначала обычный, потом с синтаксисом intel. (рис.9).



```
emkurilkoryumin@fedora:~/work/study/2023-2024/Архитекту...
<https://debuginfod.fedoraproject.org/>
Enable debuginfod for this session? (y or [n]) n
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.

Breakpoint 1, _start () at lab9-2.asm:9
9      mov eax, 4
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x004010e0 <+0>:    mov     $0x4,%eax
0x004010e5 <+5>:    mov     $0x1,%ebx
0x004010ea <+10>:   mov     $0x402118,%ecx
0x004010ef <+15>:   mov     $0x8,%edx
0x004010f4 <+20>:   int     $0x80
0x004010f6 <+22>:   mov     $0x4,%eax
0x004010fb <+27>:   mov     $0x1,%ebx
0x00401100 <+32>:   mov     $0x402120,%ecx
0x00401105 <+37>:   mov     $0x7,%edx
0x0040110a <+42>:   int     $0x80
0x0040110c <+44>:   mov     $0x1,%eax
0x00401111 <+49>:   mov     $0x0,%ebx
0x00401116 <+54>:   int     $0x80
End of assembler dump.
(gdb)
```

Рис. 4.8: Дисассимилированный код программы с синтаксисом intel

Различия отображения синтаксиса можно наблюдать в правой части окна. Затем я включаю режим псевдографики (рис.10).(рис.11).

```
emkurilkoryumin@fedora:~/work/study/2023-2024/Архитекту...
b+ 0x4010e0 <_start>    mov     eax,0x4
    0x4010e5 <_start+5>  mov     ebx,0x1
    0x4010ea <_start+10> mov     ecx,0x402118
    0x4010ef <_start+15> mov     edx,0x8
    0x4010f4 <_start+20> int     0x80
    0x4010f6 <_start+22> mov     eax,0x4
    0x4010fb <_start+27> mov     ebx,0x1
    0x401100 <_start+32> mov     ecx,0x402120
    0x401105 <_start+37> mov     edx,0x7
    0x40110a <_start+42> int     0x80
    0x40110c <_start+44> mov     eax,0x1
    0x401111 <_start+49> mov     ebx,0x0
    0x401116 <_start+54> int     0x80

exec No process In:                               L??  PC: ??
(gdb)
```

Рис. 4.9: Режим псевдографики

```
[ Register Values Unavailable ]

B+> 0x4010e0 <_start>    mov     eax,0x4
    0x4010e5 <_start+5>  mov     ebx,0x1
    0x4010ea <_start+10> mov     ecx,0x402118
    0x4010ef <_start+15> mov     edx,0x8
    0x4010f4 <_start+20> int     0x80
    0x4010f6 <_start+22> mov     eax,0x4

native process 3849 In: _start                       L9  PC: 0x4010e0
(gdb) layout regs
(gdb)
```

Рис. 4.10: Режим псевдографики

Проверяю точки останова. (рис.12).

```
Breakpoint 1 at 0x4010e0: file lab9-2.asm, line 9.
(gdb) info breakpoints
Num   Type       Disp Enb Address      What
1     breakpoint keep y  0x004010e0 lab9-2.asm:9
(gdb) 
```

Рис. 4.11: Проверка точек остановки

Устанавливаю точку останова в последней инструкции. (рис.13).

```
(gdb) b *0x401111
Breakpoint 2 at 0x401111: file lab9-2.asm, line 20.
(gdb)
```

Рис. 4.12: Редактирование файла

Опять же, смотрю информацию обо всех установленных точках останова. (рис.14).

```
emkurilkoryumin@fedora:~/work/study/2023-2024/Архитекту...
Reading symbols from lab9-2...
(gdb) r
Starting program: /home/emkurilkoryumin/work/study/2023-2024/Архитектура компьютерной архитектуры/lab9/lab9-2

This GDB supports auto-downloading debuginfo from the following URLs:
  <https://debuginfod.fedoraproject.org/>
Enable debuginfod for this session? (y or [n]) y
Debuginfod has been enabled.
To make this setting permanent, add 'set debuginfod enabled on' to .gdbinit.
Hello, world!
[Inferior 1 (process 3020) exited normally]
(gdb) break _start
Breakpoint 1 at 0x4010e0: file lab9-2.asm, line 9.
(gdb) info breakpoints
Num      Type             Disp Enb Address            What
1        breakpoint      keep y   0x004010e0  lab9-2.asm:9
(gdb) b *0x401111
Breakpoint 2 at 0x401111: file lab9-2.asm, line 20.
(gdb) i b
Num      Type             Disp Enb Address            What
1        breakpoint      keep y   0x004010e0  lab9-2.asm:9
2        breakpoint      keep y   0x00401111  lab9-2.asm:20
(gdb)
```

Рис. 4.13: Создание и запуск исполняемого файла

Вручную изменяю значений регистров и переменных с помощью инструкции si. (рис.15).

```
emkurilkoryumin@fedora:~/work/study/2023-2024/Архитекту...
b+ 0x4010e0 <_start>    mov    eax,0x4
    0x4010e5 <_start+5>  mov    ebx,0x1
    0x4010ea <_start+10> mov    ecx,0x402118
    0x4010ef <_start+15> mov    edx,0x8
    0x4010f4 <_start+20> int     0x80
    0x4010f6 <_start+22> mov    eax,0x4
    0x4010fb <_start+27> mov    ebx,0x1
    0x401100 <_start+32> mov    ecx,0x402120
    0x401105 <_start+37> mov    edx,0x7
    0x40110a <_start+42> int     0x80
    0x40110c <_start+44> mov    eax,0x1
b+ 0x401111 <_start+49> mov    ebx,0x0
    0x401116 <_start+54> int     0x80

exec No process In: L?? PC: ??
1 breakpoint keep y 0x004010e0 lab9-2.asm:9
(gdb) b *0x401111
Breakpoint 2 at 0x401111: file lab9-2.asm, line 20.
(gdb) i b
Num    Type             Disp Enb Address      What
1      breakpoint       keep y 0x004010e0 lab9-2.asm:9
2      breakpoint       keep y 0x00401111 lab9-2.asm:20
(gdb)
```

Рис. 4.14: Изменение значений регистров и переменных

Выполняю 5 инструкций si, и последовательно замечаю изменение значений регистров на экране соответственно. (рис.16).

```
--Register group: general--
eax      0x8              8
ecx      0x402118        4202776
edx      0x8              8
ebx      0x1              1
esp      0xffffd1c0      0xffffd1c0
ebp      0x0              0x0

0x4010ea <_start+10>  mov    $0x402118,%ecx
0x4010ef <_start+15>  mov    $0x8,%edx
0x4010f4 <_start+20>  int     $0x80
> 0x4010f6 <_start+22> mov    $0x4,%eax
0x4010fb <_start+27>  mov    $0x1,%ebx
0x401100 <_start+32>  mov    $0x402120,%ecx

native process 4234 In: _start L14 PC: 0x4010f6
(gdb) layout asm
(gdb) layout regs
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb)
```

Рис. 4.15: Изменение значений регистров и переменных

Просматриваю содержимое регистров. (рис.17).

```
Register group: general
eax      0x8      8
ecx      0x402118 4202776
edx      0x8      8
ebx      0x1      1
esp      0xffffd1c0 0xffffd1c0
ebp      0x0      0x0

0x4010ea <_start+10> mov $0x402118,%ecx
0x4010ef <_start+15> mov $0x8,%edx
0x4010f4 <_start+20> int $0x80
> 0x4010f6 <_start+22> mov $0x4,%eax
0x4010fb <_start+27> mov $0x1,%ebx
0x401100 <_start+32> mov $0x402120,%ecx

native process 4234 In: _start L14 PC: 0x4010f6
eax      0x8      8
ecx      0x402118 4202776
edx      0x8      8
ebx      0x1      1
esp      0xffffd1c0 0xffffd1c0
ebp      0x0      0x0
esi      0x0      0
--Type <RET> for more, q to quit, c to continue without paging--
```

Рис. 4.16: Содержимое регистров

Затем я просматриваю содержимое переменной msg1 и изменяю в ней символ с помощью команды {char}. (рис.18).

```
Register group: general
eax      0x8      8
ecx      0x402118 4202776
edx      0x8      8
ebx      0x1      1
esp      0xffffd1c0 0xffffd1c0
ebp      0x0      0x0

0x4010ea <_start+10> mov ecx,0x402118
0x4010ef <_start+15> mov edx,0x8
0x4010f4 <_start+20> int 0x80
> 0x4010f6 <_start+22> mov eax,0x4
0x4010fb <_start+27> mov ebx,0x1
0x401100 <_start+32> mov ecx,0x402120

native process 5190 In: _start L14 PC: 0x4010f6
(gdb) x/lsb &msg1
0x402118 <msg1>: "Hello, "
(gdb) x/lsb 0x402120
0x402120 <msg2>: "world!\n\034"
(gdb) set {char}&msg1='h'
(gdb) x/lsb &msg1
0x402118 <msg1>: "hello, "
(gdb)
```

Рис. 4.17: Содержимое переменной, изменение в ней символов

Аналогичные действия проделываю с переменной msg2. (рис.19).

```

Register group: general
eax      0x8      8
ecx      0x402118 4202776
edx      0x8      8
ebx      0x1      1
esp      0xffffd1c0 0xffffd1c0
ebp      0x0      0x0

0x4010ea <_start+10> mov ecx,0x402118
0x4010ef <_start+15> mov edx,0x8
0x4010f4 <_start+20> int 0x80
> 0x4010f6 <_start+22> mov eax,0x4
0x4010fb <_start+27> mov ebx,0x1
0x401100 <_start+32> mov ecx,0x402120

native process 5190 In: _start L14 PC: 0x4010f6
0x402120 <msg2>: "world!\n\034"
(gdb) set {char}&msg1='h'
(gdb) x/lsb &msg1
0x402118 <msg1>: "hello, "
(gdb) set {char}0x402120 ='E'
(gdb) x/lsb 0x402120
0x402120 <msg2>: "Eorld!\n\034"
(gdb)

```

Рис. 4.18: Содержимое переменной, изменение в ней символов

Ввожу в различных форматах значение регистра edx. (рис.20).

```

Register group: general
eax      0x8      8
ecx      0x402118 4202776
edx      0x8      8
ebx      0x1      1
esp      0xffffd1c0 0xffffd1c0
ebp      0x0      0x0

0x4010ea <_start+10> mov ecx,0x402118
0x4010ef <_start+15> mov edx,0x8
0x4010f4 <_start+20> int 0x80
> 0x4010f6 <_start+22> mov eax,0x4
0x4010fb <_start+27> mov ebx,0x1
0x401100 <_start+32> mov ecx,0x402120

native process 5190 In: _start L14 PC: 0x4010f6
0x402120 <msg2>: "Eorld!\n\034"
(gdb) p/s $edx
$1 = 8
(gdb) p/t $edx
$2 = 1000
(gdb) p/x $edx
$3 = 0x8
(gdb)

```

Рис. 4.19: Значения регистра edx

Изменяю значение регистра ebx с помощью команды set. (рис.21).

```

Register group: general
eax      0x8      8
ecx      0x402118  4202776
edx      0x8      8
ebx      0x2      2
esp      0xffffd1c0 0xffffd1c0
ebp      0x0      0x0

0x4010ea <_start+10> mov ecx,0x402118
0x4010ef <_start+15> mov edx,0x8
0x4010f4 <_start+20> int 0x80
> 0x4010f6 <_start+22> mov eax,0x4
0x4010fb <_start+27> mov ebx,0x1
0x401100 <_start+32> mov ecx,0x402120

native process 5190 In: _start L14 PC: 0x4010f6
$3 = 0x8
(gdb) set $ebx = '2'
(gdb) p/s $ebx
$4 = 50
(gdb) set $ebx=2
(gdb) p/s $ebx
$5 = 2
(gdb)

```

Рис. 4.20: Изменение значений регистра

Разница в выводе команд объясняется в значении: при бескавычном значении 2, мы её и получаем в итоге, а в другом случае переменная воспринимается иначе, и на выходе мы видим значение 50.

Завершаю выполнение программы с помощью continue и выхожу из gdb с помощью quit.

Копирую файл lab8-2.asm, полученный во время выполнения лабораторной работы №8, содержащий программу для вывода аргументов командной строки. Загружаю исполняемый файл в отладчик, указав нужные аргументы. (рис.22).

```

GNU gdb (GDB) Fedora Linux 13.2-6.fc38
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-redhat-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
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. 4.21: Загрузка файла в отладчик

Устанавливаю точку останова перед первой инструкцией и запускаю программу. (рис.23).

```
This GDB supports auto-downloading debuginfo from the following URLs:
<https://debuginfod.fedoraproject.org/>
Enable debuginfod for this session? (y or [n]) n
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.

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

Рис. 4.22: Установка точки останова, запуск программы

Далее просматриваю позиции стека. (рис.24).

```
(gdb) x/x $esp
0xffffd190: 0x00000005
(gdb) x/s *(void**)(esp + 4)
0xffffd34d:
(gdb) x/s *(void**)(esp + 8)
0xffffd377: "argument1"
(gdb) x/s *(void**)(esp + 12)
0xffffd381: "argument"
(gdb) x/s *(void**)(esp + 16)
0xffffd38a: "2"
(gdb) x/s *(void**)(esp + 20)
0xffffd38c: "argument 3"
(gdb) x/s *(void**)(esp + 24)
0x0: <error: Cannot access memory at address 0x0>
```

Рис. 4.23: Просмотр позиций стека

Шаг изменения равен 4, т.к. каждый следующий адрес на стеке находится на расстоянии в 4 байта от предыдущего.

4.3) Выполнение заданий для самостоятельной работы

Копирую файл задания для самостоятельной работы, и реализую вычисление значения функции через подпрограмму. (рис.25).

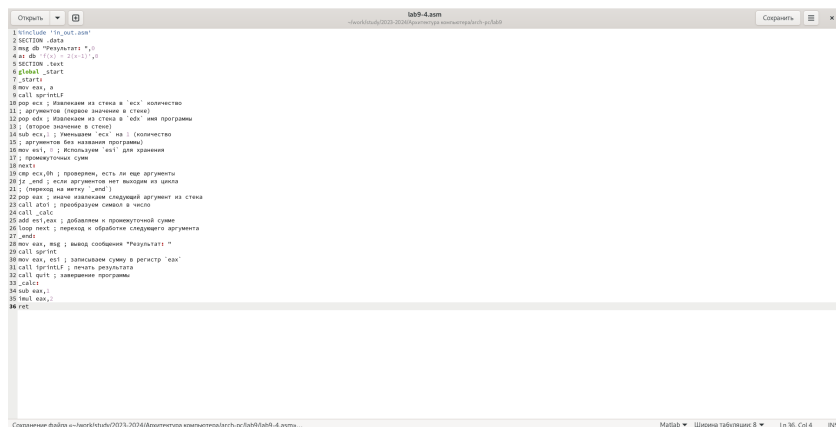


Рис. 4.24: Копирование, редактирование файла

Создаю исполняемый файл и убеждаюсь в правильности работы программы.
(рис.26).

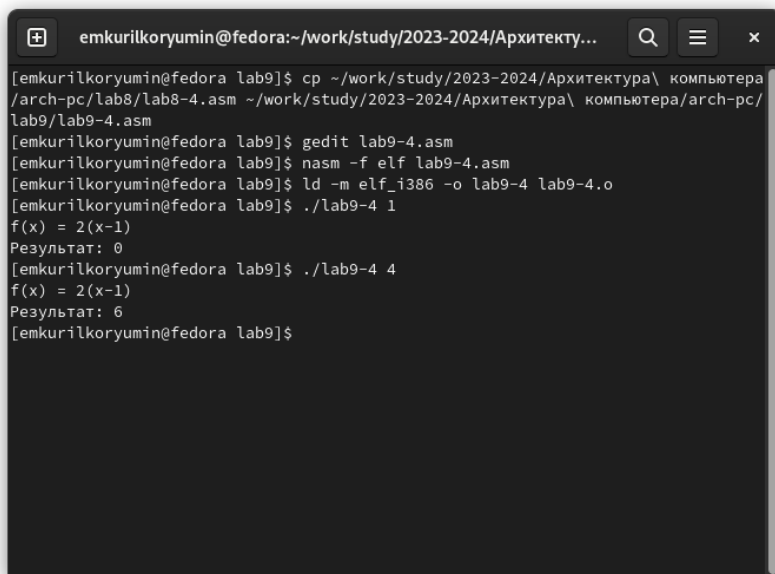


Рис. 4.25: Создание и запуск исполняемого файла

Создаю файл lab9-5.asm и вношу в него программу из последнего листинга. При запуске программа дает неверный результат, и чтобы исправить эту ситуацию, нужно проанализировать изменения значений регистров. (рис.27).

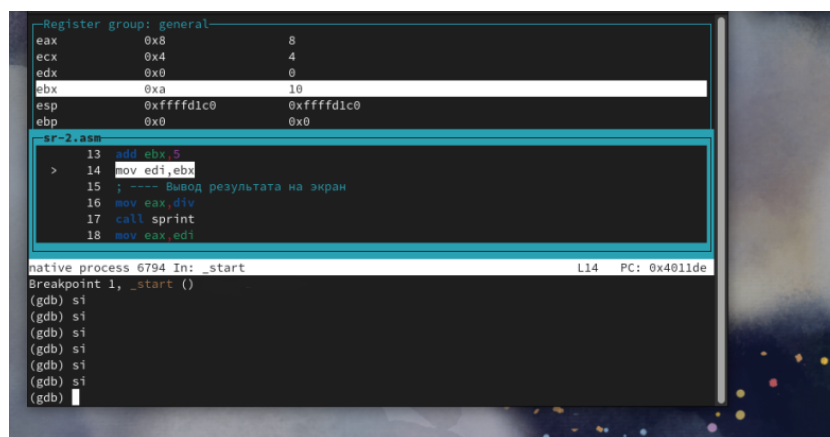


Рис. 4.26: Изменение значений регистров в gdb

Благодаря этому мне удалось вычислить ошибку и исправить её в тексте программы. (рис.28).

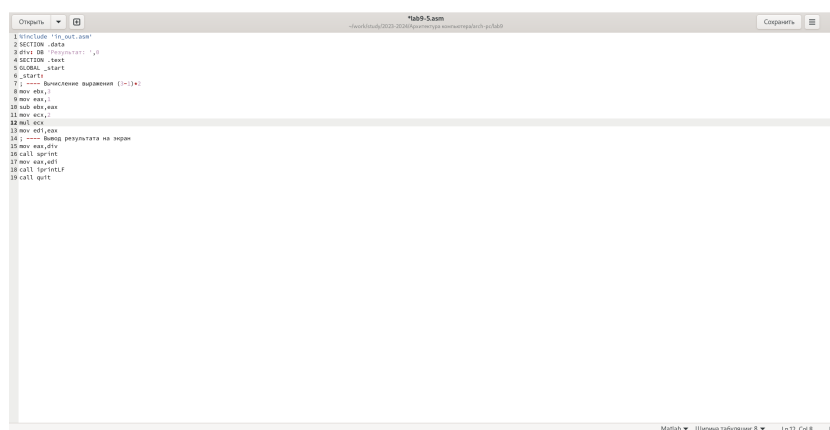
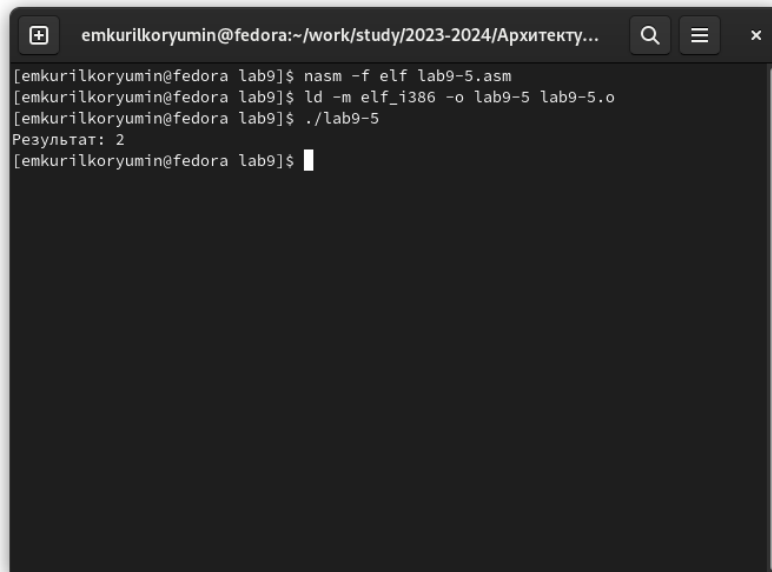


Рис. 4.27: Редактирование файла

Создаю исполняемый файл, и, выполнив устную проверку, убеждаемся в правильности работы программы. (рис.29).



```
emkurilkoryumin@fedora:~/work/study/2023-2024/Архитекту...
[emkurilkoryumin@fedora lab9]$ nasm -f elf lab9-5.asm
[emkurilkoryumin@fedora lab9]$ ld -m elf_i386 -o lab9-5 lab9-5.o
[emkurilkoryumin@fedora lab9]$ ./lab9-5
Результат: 2
[emkurilkoryumin@fedora lab9]$
```

Рис. 4.28: Создание и запуск исполняемого файла

Листинг 4.1 - Преобразованная программа из лабораторной работы №8.

```
%include 'in_out.asm' SECTION .data msg db "Результат: ",0 a:
db 'f(x) = 2(x-1)',0 SECTION .text global _start _start: mov eax,
a call sprintLF pop ecx ; Извлекаем из стека в `ecx` количество ;
аргументов (первое значение в стеке) pop edx ; Извлекаем из стека в
`edx` имя программы ; (второе значение в стеке) sub ecx,1 ; Уменьшаем
`ecx` на 1 (количество ; аргументов без названия программы) mov esi,
0 ; Используем `esi` для хранения ; промежуточных сумм next: cmp
ecx,0h ; проверяем, есть ли еще аргументы jz _end ; если аргументов
нет выходим из цикла ; (переход на метку `_end`) pop eax ; иначе
извлекаем следующий аргумент из стека call atoi ; преобразуем символ
в число call _calc add esi,eax ; добавляем к промежуточной сумме loop
next ; переход к обработке следующего аргумента _end: mov eax, msg ;
вывод сообщения "Результат: " call sprint mov eax, esi ; записываем
сумму в регистр `eax` call iprintLF ; печать результата call quit
; завершение программы _calc: sub eax,1 imul eax,2 ret
```

Листинг 4.2 -

Исправленная программа для вычисления значения выражения.

```
““%include 'in_out.asm' %include 'in_out.asm' SECTION .data div: DB 'Результат:',0
SECTION .text GLOBAL _start _start: ; -- Вычисление выражения (3-1)*2 mov ebx,3
mov eax,1 sub ebx,eax mov ecx,2 mul ecx,2 mov edi,eax ; -- Вывод результата на
экран mov eax,div call sprint mov eax,edi call iprintLF call quit
```

5 Выводы

При выполнении лабораторной работы я приобрел практический опыт в написании программ в написании программ с использованием подпрограмм, а также ознакомился с методами отладки при помощи gdb и его основными возможностями.

Список литературы

Архитектура компьютера и ЭВМ