Chapter 3

Mandatory Content

In this section you will study the mandatory content of this lab which includes the development process, implementation of a simple, non-trivial example program as well as some basic programming constructs you will need within this lab. This chapter also contains the mandatory assignments. The manual is shaped in such a way that all the knowledge you need for an assignment is located before it so make sure to read everything in order so as to not be confused about what to do.

In the assignments you can borrow ideas from the example for your own programs but for now, the most important thing is that you will learn:

- what an assembly program looks like and how it is structured
- how to transform an idea into a good specification
- how to transform a specification into an assembly program
- how the basic programming constructs work in assembly (if/else, while, for, etc.)

3.1 Designing a Program

We will start by describing the program in plain English. We will then write the algorithm down more formally in *pseudocode*. Finally, we will translate the pseudocode into working assembly code and we will discuss that code in line by line detail.

Step 1: Description

The program we are going to write is quite simple: it will ask the user for an input number and increment it by 1 if it is even, otherwise return the same number. For simplicity, we will assume that the input will always be greater than or equal to 0. The following table illustrates some possible inputs and their outputs:

input	output
0	1
1	1
2	3
3	3
10	11
21	21
42	43
1041	1041

Step 2: Specification

Now that we are familiar with what our program is supposed to do, we will transform the description into a formal specification. Why do we have to do this? Well, because in the real world, there are many small, practical details that need to be considered before we can actually implement an algorithm. One such problem is the problem of representation: how will we represent the information in our program? Will we use a *linked list*[1] structure, an array, a map? Is a structure even needed? What implications will it have for the complexity of our program if we choose one representation over another? Resolving such questions is part of the creative challenge of programming, so usually you will have to decide on these matters for yourself. However, we will always expect you to formalise these decisions in the form of a good specification, before you start programming. As an example of what we consider to be a good specification, we present the specification of our program below.

Since this program is very simple, it does not actually require any structure to hold our data but simply a single variable on which we will perform the operations. Here is the pseudocode[2] that describes it:

```
main() {
        // print the welcome string
        print("Welcome to our program!")

        // call the inout subroutine
        inout()
}

inout() {
        // ask for the input
        int NUMBER = read(keyboard_input)

        // check whether the number is even
        if (NUMBER % 2 == 0) { // use modulo to determine divisibility by 2
                NUMBER = NUMBER + 1 // increment by 1
        }

        // print the outcome
        print(NUMBER)
}
```

The pseudocode above uses only simple operations on a simple data type (an integer) and an if statement which is a basic programming construct. These constructs can easily be translated to assembler programs, as we shall see in the next step.

Step 3: Implementation

The final step in our development process is to translate the specification into working assembler code. Here, we present the complete implementation of the program in working x86-64 assembler. In later exercises, you can use this program as a template for your own work. Try to read along and understand what happens, using the comments in the code and the subsequent explanations as a guide. Do not be intimidated if you do not understand all the details just yet, the following sections contain a detailed explanation of the language.

```
# ************************************************************************
# * Program: Oddifier                                                    *
# * Description: This program prints the closest >= odd number to the input *
# ************************************************************************

.text
welcome:        .asciz "\nWelcome to our program!\n"
prompt:         .asciz "\nPlease enter a positive number:\n"
```

[1] http://en.wikipedia.org/wiki/Linked_list
[2] https://en.wikipedia.org/wiki/Pseudocode

```
input:          .asciz "%ld"
output:         .asciz "The␣result␣is:␣%ld.\n\n"

.global main

main:
        movq    %rsp, %rbp                  # initialize the base pointer
        movq    $0, %rax                    # no vector registers in use for printf
        movq    $welcome, %rdi              # first parameter: welcome string
        call    printf                      # call printf to print welcome
        call    inout                       # call the subroutine inout

end:    # this loads the program exit code and exits the program

        movq    $0, %rdi
        call    exit

# ************************************************************************
# * Subroutine: inout                                                    *
# * Description: this subroutine takes an integer as input from a user,  *
# * increments it by 1 if it is even, and prints it out                  *
# * Parameters: there are no parameters and no return value              *
# ************************************************************************
inout:
        # prologue
        pushq   %rbp                        # push the base pointer
        movq    %rsp , %rbp                 # copy stack pointer value to base pointer

        movq    $0, %rax                    # no vector registers in use for printf
        movq    $prompt, %rdi               # param1: prompt string
        call    printf                      # call printf to print prompt

        subq    $8, %rsp                    # reserve space in stack for the input
        movq    $0, %rax                    # no vector registers in use for scanf
        movq    $input, %rdi                # param1: input format string
        leaq    -8(%rbp), %rsi              # parameter2: address of the reserved space
        call    scanf                       # call scanf to scan the users input

        popq    %rsi                        # pop the input value into RSI
                                            # (RSI is the second parameter register)

        movq    %rsi, %rax                  # copy the input to RAX
        movq    $2, %rbx                    # move the value 2 to RBX
        movq    $0, %rdx                    # clear the contents of RDX
        divq    %rbx                        # divide the content of RDX:RAX by the
                                            # content of RB (result stored
                                            # in RAX and remainder in RDX)
        cmpq    $0, %rdx                    # compare RDX to 0
        jne     odd                         # if they are not equal (input is odd),
                                            # don't increment
even:
        incq    %rsi                        # increment the input value

odd:
        movq    $0, %rax                    # no vector registers in use for printf
        movq    $output, %rdi               # param1: output string
                                            # param2: number (in RSI)
        call    printf                      # call printf to print the output

        # epilogue
        movq    %rbp , %rsp                 # clear local variables from stack
        popq    %rbp                        # restore base pointer location

        ret                                 # return from subroutine
```

3.2 Assembler Directives

The commands that start with a period (e.g. `.bss`, `.text`, `.global`, `.skip`, `.asciz`, etc.) are *assembler directives*. Assembler directives have special functions in an assembler program. For instance, the `.text` directive at the beginning of the file tells the assembler to put all the subsequent code in a specific *section*. Other assembler directives, like `.global`, make certain labels visible to the outside world. The following is a description of the most commonly used assembler directives or *pseudo-instructions* as they are sometimes called. The directives are grouped by functionality. For a full reference, see the official documentation of the GNU assembler[3].

Section directives: `.text`, `.data`, `.bss`

```
.text
.data
.bss
```

The memory space of a program is divided into three different *sections*. These directives tell the assembler in which section it should put the subsequent code.

The `.text` segment is intended to hold all instructions. The `.text` segment is read-only. It is perfectly fine to include constants and ASCII strings in this segment.

The `.data` segment is used for initialised variables (variables that receive an initial value at the time you write your program, such as those created with the `.word` directive).

The `.bss` segment is intended to hold uninitialised variables (variables that receive a value only at runtime). Therefore, this section is not part of the executable file after compilation, unlike the other two sections.

Defining constants: `.equ`

```
.equ NAME, EXPRESSION
```

The `.equ` directive can be used to define symbolic names for expressions, such as numeric constants. An example of usage is given below:

```
.equ FOO, 1024

pushq $FOO  # push 1024
```

Declaring variables: `.byte`, `.word`, `.long`, `.quad`

```
.byte VALUE
.word VALUE
.long VALUE
.quad VALUE
```

The `.byte`, `.word`, `.long` and `.quad` directives can be used to reserve and initialise memory for variables and/or constants. Just as the assembler translates instructions into bits of memory contents directly (as explained in subsection 1.2), these directives will be transformed into memory contents as well, i.e. there is no special magic involved here. `.byte` reserves one byte of memory, `.word` reserves two bytes of memory `.long` reserves four bytes and `.quad` reserves 8 bytes. Whether these bytes will actually be writable depends on the section in which you define them (see above for a description of the sections). Each directive allows you to define more than one value in a comma separated list.

A few examples:

[3] `https://sourceware.org/binutils/docs-2.25/as/Pseudo-Ops.html#Pseudo-Ops`

```
FOO: .byte 0xAA, 0xBB, 0xCC    # three bytes starting at address FOO
BAR: .word 2718, 2818          # a couple of words
BAZ: .long 0xDEADBEEF          # a single long
BAK: .quad 0xDEADBEEFBAADF00D  # a single quadword
```

Note that the x86-64 is a *little-endian* machine, which means that a value like `.long 0x01234567` will actually end up in memory as `67 45 23 01`. Of course, you normally do not notice this since the `movl`-instruction will automatically reverse the byte order while it loads the long back into memory. Taking endianness into account, it should be clear that the following three statements are completely equivalent:

```
FOO: .byte 0x0D, 0xF0, 0xAD, 0xBA, 0xEF, 0xBE, 0xAD, 0xDE
FOO: .word 0xF00D, 0xBAAD, 0xBEEF, 0xDEAD
FOO: .long 0xBADF00D, 0xDEADBEEF
FOO: .quad 0xDEADBEEFBAADF00D
```

Reserving memory: `.skip`

```
.skip AMOUNT
```

Sometimes it is necessary to reserve memory in bigger chunks than bytes, words, longs or quads. The `.skip` directive can be used to reserve blocks of memory of arbitrary size:

```
BUFFER: .skip 1024 # reserve 1024 bytes of memory
```

Placing this directive in the `.data` section will initialize all bytes with zero, while placing it in `.bss` will leave the data uninitialized (and will thus contain “random” data from previous programs).

Strings variables: `.ascii`, `.asciz`

```
STRING:  .ascii string
STRINGZ: .asciz string
```

These directives can be used to reserve and initialise blocks of ASCII encoded characters. In many higher-level programming languages, including C, strings are simply blocks of ASCII codes terminated by a zero byte (`0x00`). The `.asciz` directive adds such a zero byte automatically. The following two examples are thus equivalent:

```
WELCOME: .ascii "Hello!!"  # A string..
         .byte 0x00        # ..followed by a 0-byte.

WELCOME: .asciz "Hello!!"  # A string followed by a 0-byte.
```

Global symbols: `.global`

```
.global label
```

This directive enters a label into the symbol table. The symbol table is a table of contents of sorts which is contained in the binary assembled file. Publishing labels in the symbol table is useful if you want other programs to have access to your labels, e.g. if you want the labels to be visible in the debugger or if you want other programs to use your subroutines[4]. One very important use of the symbol table is to export the `main` label. This label *must* be exported because the operating system needs to know where to start running your program.

```
.global main
```

[4]Sharing subroutines is not part of this lab course, but if you are interested you can have a look at subsection 4.8

3.3 x86-64 Assembly Language

This subsection contains a short language reference for the x86-64 assembly language. Apart from a list of commonly used instructions, there is a short rundown of the differences between the so called “AT&T syntax” and the “Intel syntax”. This course uses the GNU *assembler*[5]. Because this assembler only supports the AT&T syntax, we use this syntax throughout the course. If you are also interested in the Intel syntax, you can find it in the official Intel x86-64 platform manual.

3.3.1 About the AT&T Syntax

If you have examined some of the x86-64 assembler examples in the book of Hamacher et al., you will have noticed that there is a difference between the x86 assembler they use and the one we use during the lab course. An explanation is in order here. First of all, there is of course no such thing as an “official” x86-64 assembly language. In theory, you could write your own x86-64 assembler and come up with a new syntax of your own. In practice however, there are only two flavors of x86-64 assembly language which are in actual use. There are good arguments for using either, but we have chosen to use the AT&T syntax for the lab course, while the book has chosen to use the Intel syntax. While this is really all you need to know regarding the subject, we provide a short background on the issue for the sake of completeness:

The Intel syntax, as used in the book, is the preferred syntax that was used and developed by the Intel Corporation - the designers of the x86-64 architecture. The Intel syntax is what you will see in the official x86-64 reference manual and platform definition. If anything, this could be considered the “official” x86-64 syntax. Long before the Intel Corporation introduced the x86-64 however, there was the UNIX operating system and the programming language C, both of which were developed at Bell Labs, the R&D department of the American phone company AT&T. Bell Labs and others had ported the UNIX operating system to a variety of different architectures before the x86-64 even existed, and thus the AT&T-style of assembly languages was widespread long before the x86-64 came along. While Intel may favour its own syntax, it is much more beneficial for the rest of us to learn AT&T syntax, as there are many other AT&T-style assemblers available for other hardware platforms. In addition, most compilers generate AT&T-style output and it is, arguably, more elegant than Intel syntax.

As a final note, it is important to stress that the Intel syntax uses a different order for source and destination, e.g. if you read the Intel manual, `mov A B` will copy a value from B to A, whereas in AT&T syntax the equivalent `movl A B` will copy the value from A to B.

3.3.2 Instructions and Operands

The lines of code in an assembly program using AT&T syntax consist of an *instruction* (what should happen) and possibly some *operands* (the data to act with). This paragraph explains how to use the different kinds of operands.

Operand Prefixes: Registers and Literal Values

The AT&T syntax uses a number of prefixes for operands. You have probably seen them already:

- Register names are prefixed by the `%` character (e.g. `%rax`, `%rsp`).
- Literal values are prefixed with the `$` character (e.g. `$3`).

Instruction Postfixes (Specifying Operand Size)

Many instructions in AT&T syntax need to be postfixed with a `b`, `w`, `l` or `q` modifier. This postfix specifies the size of the operands, where `b` stands for “byte”, `w` stands for “word” (2 bytes), `l`

[5]An assembler is a program that translates an assembly code file into machine language. See: `https://sourceware.org/binutils/docs-2.25/as/index.html`

stands for "long" (4 bytes) and `q` stand for "quadword" (8 bytes). As an example, take a look at four different uses of the `push` instruction:

```
pushb $3 # Push one byte onto the stack (0x03)
pushw $3 # Push two bytes onto the stack (0x0003)
pushl $3 # Push four bytes onto the stack (0x00000003)
pushq $3 # Push eight bytes onto the stack (0x0000000000000003)
```

All four instructions in the example push the literal value '3' onto the stack, but the actual size of the operand is different in each situation. We will do assembly in 64-bit, so mostly you will have to use the `q` postfix.

In our instruction set reference table in section 3.3.3, we do not list these suffixes explicitly. The Intel manual does not list them either.

Partial Registers

The size suffix is especially important when you use *partial registers*. The x86-64 allows you to address smaller parts of the 64-bits registers through special names. By replacing the initial `R` with an `E` on the first eight registers, it is possible to access the lower 32 bits. If we use the `RAX` register as an example, you can address the least significant 32 bits of this register by using the name `EAX`. To access the lower 16 bits the initial R should be removed (`AX` for `RAX`). In a similar fashion, the highest and lowest order bytes in this `AX` register can be addressed by the names `AH` and `AL` respectively. Again, we present a few examples using the `mov` instruction:

```
movl %eax, %ebx # Copy 32 bits values between registers
movq %rax, %rbx # Copy 64 bits values between registers
movw %ax, %bx   # Copy only the lowest order 16 bits
movb %al, %bl   # Copy only the lowest order 8 bits
movb %ah, %al   # Copy 8 bits within a single register
```

The following table shows how you can access the lower X bytes of each register:

8-byte	4-byte	2-byte	1-byte
%rax	%eax	%ax	%al
%rcx	%ecx	%cx	%cl
%rdx	%edx	%dx	%dl
%rbx	%ebx	%bx	%bl
%rsi	%esi	%si	%sil
%rdi	%edi	%di	%dil
%rsp	%esp	%sp	%spl
%rbp	%ebp	%bp	%bpl
%r8	%r8d	%r8w	%r8b
%r9	%r9d	%r9w	%r9b
%r10	%r10d	%r10w	%r10b
%r11	%r11d	%r11w	%r11b
%r12	%r12d	%r12w	%r12b
%r13	%r13d	%r13w	%r13b
%r14	%r14d	%r14w	%r14b
%r15	%r15d	%r15w	%r15b

Addressing Memory

There are several ways of addressing the memory in AT&T syntax:

- **Immediate addressing:**
  - Directly using a label will yield the value at the address of the label. (e.g. `label`)
  - Prefixing a label with a `$` will yield the address of the label. (e.g. `$label`)

- **Indirect addressing:**
  - Surrounding a *register* with parentheses will yield the value at the memory address stored in the register. (e.g. `(%RAX)`)
  - Prefixing the left parenthesis with a *displacement* will yield the value at the memory address stored in the register plus the displacement (e.g. `-8(%RBP)`).
  - *Advanced:* Accessing memory with *displacement*`(`*base*`,` *index*`,` *scale*`)` will yield the value at memory address "*displacement* + *base* + *index* × *scale*" Here, *displacement* is a constant expression (may include labels), *base* and *index* are registers, and *scale* is either 1, 2, 4, or 8. (e.g. `table(%RDI, %RCX, 8)`)

  Indirect addressing is explained in more detail in the GNU assembler documentation [6].

3.3.3 Instruction Set

The example program uses a number of commonly used instructions, such as `mov`, `push`, `cmp` and `jmp`. The next page contains a list of commonly used x86-64 instructions. It should be sufficient to get you through the lab course, but you may always study the official Intel manual [7] to obtain more instructions. Some important notes:

- The instructions are all case insensitive.
- In the table we denote the necessity of a `b`, `w`, `l` or `q` postfix with a period ('`.`').
- Most of the instructions with two operands require at least one of their operands to be a register. The other operand may be either a register or a memory location. This may differ per instruction and is specified in detail in the official Intel manual [7].
- The multiplication and division instructions require their operands to be in special registers[8]. The multiplication instruction will store the result in both `%RDX` and `%RAX` (denoted in the table by `%RDX:%RAX`), while the division instructions will require the dividend to be in these two registers. The higher-order bits should be in `%RDX` while the lower-order bits should be in `%RAX`. Note that the division operator also stores the remainder of the division in `%RDX`.

[6]`https://sourceware.org/binutils/docs-2.25/as/i386_002dMemory.html#i386_002dMemory`

[7]`http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html`, specifically volume 2, the instruction set reference

[8]Other forms of these instructions also exist, but they are not listed here.

Mnemonic	Operands	Action	Description
			Data Transfer
`mov.`	SRC, DST	DST = SRC	Copy.
`pushq`	SRC	`%RSP` -= 8, (`%RSP`) = SRC	Push a value onto the stack.
`popq`	DST	DST = (`%RSP`) , `%RSP` += 8	Pop a value from the stack.
`xchg.`	A, B	TMP = A, A = B, B = TMP	Exchange two values.
`movzb.`	SRC, DST	DST = SRC (one byte only)	Move byte, zero extended.
`movzw.`	SRC, DST	DST = SRC (one word only)	Move word, zero extended.
			Arithmetic
`add.`	SRC, DST	DST = DST + SRC	Addition.
`sub.`	SRC, DST	DST = DST - SRC	Subtraction.
`inc.`	DST	DST = DST + 1	Increment by one.
`dec.`	DST	DST = DST - 1	Decrement by one.
`mul.`	SRC	`%RDX:%RAX` = `%RAX` * SRC	Unsigned multiplication.
`imul.`	SRC	`%RDX:%RAX` = `%RAX` * SRC	Signed multiplication.
`div.`	SRC	`%RAX` = `%RDX:%RAX` / SRC	Unsigned division.
		`%RDX` = `%RDX:%RAX` % SRC	
`idiv.`	SRC	`%RAX` = `%RDX:%RAX` / SRC	Signed division.
		`%RDX` = `%RDX:%RAX` % SRC	
			Branching
`jmp`	ADDRESS		Jump to address (or label).
`je`	ADDRESS		Jump if equal.
`jne`	ADDRESS		Jump if not equal.
`jg`	ADDRESS		Jump if greater than.
`jge`	ADDRESS		Jump if greater or equal.
`jl`	ADDRESS		Jump if less than.
`jle`	ADDRESS		Jump if less or equal.
`call`	ADDRESS		Jump and push return address.
`ret`			Pop address and jump to it.
`loop`			`decq %RCX`, jump if not zero.
			Logic and Shifting
`cmp.`	A, B	`sub` A B (Only set flags)	Compare and set condition flags.
`xor.`	SRC, DST	DST = SRC ˆ DST	Bitwise exclusive or.
`or.`	SRC, DST	DST = SRC | DST	Bitwise inclusive or.
`and.`	SRC, DST	DST = SRC & DST	Bitwise and.
`shl.`	A, DST	DST = DST << A	Shift left by one bit.
`shr.`	A, DST	DST = DST >> A	Shift right by one bit
			Other
lea.	A, DST	DST = &A	Load effective address.
int	INT_NR		Software interrupt.

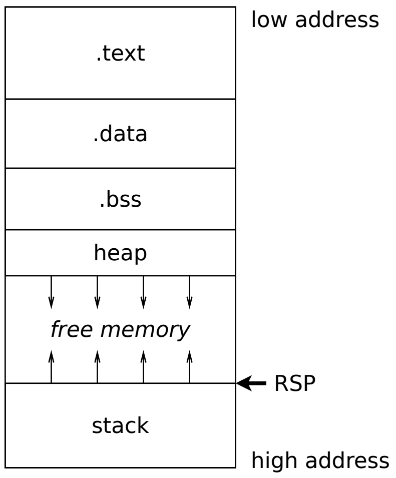
3.4 Registers & Variables

The example program uses a variable to store data. We see in the comments that we are using a variable called "`number`" which corresponds to the one used in the pseudocode. But where do these variables live? Do they exist in the registers, on the stack or somewhere in main memory? The answer is: all of the above. Sometimes, like in the case of `number`, we can simply keep our variables in the registers. The registers are fast and easy to access, so if possible we like to keep our variables there. The number of registers is limited however, so sometimes we may have to temporarily push their values on the stack and later pop it into a register when we need to check the value.

Aside from register shortage, there is one very important reason to store variables on the stack in some cases: on the x86-64 platform, registers are *caller saved* by convention. This means that if you call a subroutine from your program, like `printf` or one of your own subroutines, the subroutine may and will likely overwrite some of your registers. In other words, if you need the data in your registers to be consistent after you call a subroutine, you will need to save it on the stack. We will delve into stack details in one of the exercises.

3.5 The Stack

Here is a visual impression of the memory layout of a running process:



The parts of the memory labeled `.text`, `.data`, and `.bss` contain all program instructions and other data originating from assembler directives. More information on these memory sections can be found in the assembler directive reference (paragraph ??). The *heap* is used to store data allocated using the C functions `malloc` and `calloc`. [9]

3.5.1 The Stack Pointer

We will now explain the stack mechanism. The x86-64 has a special stack pointer register: `RSP`. This register is initialised by the operating system once your program starts. At that point, it contains the address of the first byte *after* your program's memory space. Essentially, this means that the stack is empty at this point in time. The stack can "grow" downward into your program's memory space. When a `push` instruction is executed, the value in the stack pointer register gets decremented by some amount and the pushed value is stored at the new location at which the stack pointer then points.

[9]We will not use the heap in the compulsory part of this lab, but the interested can find more information on how the heap works in C: `https://www.gribblelab.org/CBootCamp/7_Memory_Stack_vs_Heap.html`

3.5.2 Cleaning up the Stack

Of course, if the stack grows too large, it will eventually overwrite your program's code and data. This is called a *stack overflow* and it is usually indicative of a serious design flaw in your program. To avoid this problem, the caller must clean up the stack after every function call by adding the parameter-block size to the stack pointer directly. This is because (as you will read in section 3.6) the stack is at times used to pass parameters to subroutines. Look at the simple example of the print function below. Cleaning the stack should not be more difficult than this:

```
    pushq $42               # Push a magic number, the seventh argument
    movq ..., %...          # Move arguments 2 through 6 to their registers
    movq $formatstr, %rdi   # First argument: the format string
    movq $0, %rax           # no vector arguments for printf
    call printf             # Print the numbers
    addq $8, %rsp           # Clean the stack (pop the magic number)
```

3.5.3 The Base Pointer

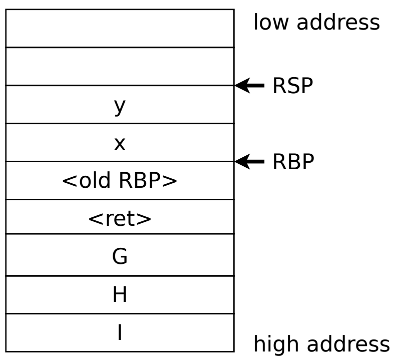
Usually, subroutines push and pop values on and off the stack. With the stack pointer being ever in motion, it may become hard to keep track of things that reside on the stack. To make stack navigation in subroutines easier, the x86-64 offers a special base pointer register: `RBP`. It works like this: upon entry of our subroutine, we immediately push the current value of `RBP` onto the stack. We then copy the current stack pointer value to `RBP`. During the lifetime of our subroutine, `RBP` will not change. That is, it will always point at the "base" of our subroutine's stack area. This way, we can always find our local variables and subroutine arguments relative to `RBP`. At the end of our subroutine we pop the old `RBP` value off the stack again and return from the subroutine.

3.5.4 Subroutine Prologue and Epilogue

At the beginning of the example program, we see that the base pointer is being initialised. The opaque ritual has to be performed at the start of each subroutine, including the `main` subroutine and is explained in the following section.

The process of storing the old base pointer and copying the stack pointer to be a new base pointer is called the *subroutine prologue*. Similarly, restoring the old base and stack pointers is called the *subroutine epilogue*. These two parts of code should be the same for all subroutines you write and can therefore also be seen as part of the calling conventions (paragraph 3.6.1).

To the right is a graphical representation of the stack as it would look during the execution of a typical subroutine. Each "block" in the image represents eight bytes. The calling subroutine has left the values `I`, `H`, and `G` on the stack. On top of that, we find the return address (pushed by the `call` instruction), the base pointer of the calling subroutine (pushed in the *prologue* of the current subroutine), and two values `x` and `y` (which were created on the stack during the current subroutine).



In this same image, you can see the base pointer register pointing to the first memory location that the current subroutine uses. Similarly, the stack pointer points to the first free memory location on the stack. The space between the base pointer and the stack pointer is also called the *stack frame* of the current subroutine.

3.5.5 Accessing arguments passed via the stack

Take another look at the memory layout in the previous image. Now imagine that the current subroutine is one that takes nine arguments. Knowing how the memory is laid out on the "border" between two subroutines, we know that we can find the stack arguments two memory spaces (or, 16 bytes) below the current base pointer. You can use indirect memory addressing (see paragraph 3.3.2) to retrieve these values.

3.6 Subroutines

A subroutine is simply a block of instructions which starts at some memory address (indicated with a *label*). If we want to execute or *call* a subroutine, we simply need to jump[10] to its first instruction. After executing the subroutine we expect control to return to us, i.e. we expect the program to return to the first instruction after our subroutine call. To make this possible, the called subroutine should somehow be aware of the address of the next instruction after the call. By convention, we simply push that address onto the stack right before making the jump. To our ease and comfort, the kind people at Intel provided a single instruction that performs both these steps in one fell swoop: the `call` instruction. Calling a simple subroutine is thus no more difficult than this:

```
call somesub  # call the somesub subroutine
```

The label `somesub` in this example is associated with the starting address of the subroutine that we want to call. The `somesub`-subroutine will now execute all of its instructions and finish off with the `ret` instruction. This instruction will pop the return address (which the `call` instruction had pushed) from the stack and make execution will simply return to the first instruction after the `call` instruction.

3.6.1 Calling Conventions

The calling of subroutines hinges heavily on a number of conventions. Thanks to these conventions, if you know how to call one subroutine you know how to call them all. Imagine if this was not the case, you would have to check the exact register and stack usage of each subroutine you would want to use. On the flip side, when writing our own subroutines we will have to honour these conventions as well.

Passing Parameters

Usually, we will want to pass some *parameters* to a subroutine. To do this, we need to put them somewhere where the subroutine can find them when it executes. We are more or less free to choose between using the registers, the stack or some part of memory other than the stack to store these parameters, as long as both the writer of the subroutine and the user agree on the location. By convention[11] we will use registers for this purpose. More specifically, we will place the arguments in the following registers:

1. `%RDI`
2. `%RSI`
3. `%RDX`
4. `%RCX`

[10] A "jump" is nothing more than loading a new memory address into the program counter, or `RIP`, as this register is called on the x86-64.

[11] This convention is the so called "C calling convention" and if we adhere to it our subroutines and calls will be fully compatible with the system's standard C library. You can find the full documentation of the calling conventions here: `https://web.archive.org/web/20160801075139/http://www.x86-64.org/documentation/abi.pdf`

5. `%R8`
6. `%R9`

We will clarify this by an example. Let us assume that we have a subroutine called `foo`, that takes three integer arguments, i.e. the signature of the subroutine is `foo(int a, int b, int c)`. Imagine that we want to call `foo` with the parameters 1, 5 and 2, i.e. `foo(1, 5, 2)` in pseudocode. In assembler, we copy the arguments in the registers and execute the `call` instruction to call this subroutine:

```
    movq $2, %rdx # third argument
    movq $5, %rsi # second argument
    movq $1, %rdi # first argument
    call foo      # Call the subroutine
```

If the subroutine that you are calling needs more than six arguments, then the remaining arguments need to be pushed to the stack in reverse order (first argument pushed last). Note that the called subroutine will *not* remove the arguments from the stack, so you should pop them off yourself after the call returns. If you are interested in writing your own subroutine that needs more than six arguments, see paragraph 3.5.5.

Callee-saved vs. Caller-saved

Note that every subroutine is limited to use the same general-purpose registers, so the values in these registers might no longer be the same when the function returns. If you want to preserve these values, you will need to save them somewhere (e.g. the stack).

Some registers are caller-saved: these registers may be modified by subroutines and should thus be saved by the caller of a subroutine if the value needs to be used after the call returns. The list of caller-saved registers is: `%RAX`, `%RCX`, `%RDX`, `%RDI`, `%RSI`, and `%R8` through `%R11`.

Registers can also be callee-saved; these registers may be used by a subroutine, but when the subroutine returns they must have the same value they had when the subroutine started execution. The list of callee saved registers is: `%RBX`, `%RSP`, `%RBP`, and `%R12` through `%R15`.

Stack Alignment

If you are going to use the stack in your code, you need to make sure that the stack remains 16-byte aligned. This means that the `%RSP` register should always be a multiple of 16 when you do a call.[12]

If you are not using the stack inside a subroutine, then this is easy: any `call` instruction pushes an 8 byte return address and in the prologue of your function you push the old `%RBP` value. These two pushes together are exactly 16 bytes, thus ensuring your stack remains aligned. For more information on why you need to push the `%RBP` register to the stack, see paragraphs 3.5.3 and 3.5.4.

Note that the `main` routine will also be called with an aligned stack, but the return address pushed by this call causes the stack to be unaligned again.

The Return Value

The final question that remains regarding the invocation of subroutines is that of the return value. Some subroutines (such as `sqrt()` or `sin()`) return a value after they execute. By convention, subroutines leave their return value in the `RAX` register. If for example our `foo` returned an integer, it would be in the `RAX` register after the `call` instruction returned.

[12]For example, the `scanf` function will crash with a segmentation fault if this is not the case!

3.6.2 Recursive Subroutines

A recursive subroutine is a subroutine that calls itself during its execution. This enables the subroutine to repeat itself for a number of times. Below is the pseudocode of a recursive example function. For a given x less than or equal to 42, the function calculates and returns the sum of all integers from x to 42. Pseudocode:

```
function example(x) {
    if (x == 42)
        return 42;
    else
        return (x + example(x + 1))
}
```

With recursive subroutines there's still an issue: when does the routine need to stop from calling itself? To prevent infinite recursion, you need to determine a recursive case and a base case (or stop condition). With this example it would be logical to stop the recursion when the function receives an input value of 42. This is done by checking for the condition at every invocation of the function. If the condition holds we can return a known correct value. If the condition did not hold the function will call itself with different parameters and use the result of that invocation to compute the correct value.

Recursive functions are often used in computer science because they allow programmers to write a minimal amount of code. It often produces code that is very compact. However, recursion can cause infinite loops when the stop condition is not written properly.

3.7 I/O

If you examine the pseudocode and the resulting assembly code of the example carefully, you see that we have translated the `print(number);` statement into the following lines of assembler code:

```
movq    $formatstr, %rdi    # first argument: formatstr
movq    %rcx, %rsi          # second argument: the number
movq    $0, %rax            # no vector arguments
call    printf              # print the number
```

Doing I/O in an assembler program can be quite tricky. First of all, normal processes do not have permission to access the hardware I/O devices directly, so all input and output has to be handled by the operating system. Since different operating systems have different ways of doing things it isn't very useful to teach you the specifics of one system[13]. Instead, we will use the operating system's standard C library to do I/O for us. Calling functions in the C library is no different from calling subroutines in your own programs. This has many benefits. First of all, there is a standard C library available on most operating systems and second, it will do some nice tricks for us such as ASCII-to-integer conversions and vice versa. In this subsection we will discuss the `printf` and `scanf` subroutines from the standard C library. Both these functions are functions that take a non-fixed amount of arguments, also known as "varargs". These functions take an extra (hidden) argument in `RAX`, defining the number of vector registers used in the call. During this lab we will not be using these registers, so you always load a zero into `RAX`.

3.7.1 Printing to the Terminal

The standard C library contains a subroutine called `printf`. We will use this subroutine for output. The subroutines from the C library can be called directly from your programs, just like normal subroutines. The *linker* will make sure that the actual subroutine is found once your program is built. `printf` takes a variable number of arguments.

[13] If you are curious anyway, check out paragraph .

Basic Example

In its simplest form, `printf` takes only one argument: the memory address of a string of ASCII characters. We will now present a pseudocode example followed by an assembly example.

Pseudocode:

```
printf("Hello world!\n");
```

Assembly:

```
mystring: .asciz "Hello world!\n"

    movq $0, %rax           # no vector registers in use for printf
    movq $mystring, %rdi    # load address of a string
    call printf             # Call the printf routine
```

As you can see there are two strange details in this example. First of all, we include the special '\n'-sequence inside the string. This is translated by the assembler to a single 'newline'-character. Second, we do not actually provide the entire string as an argument, but rather just the memory address of the first character of the string, which is denoted by the `mystring` label[14]. By convention, C functions know where a string ends by looking for a byte with the value `0x00`. That byte indicates the end of the string.

Printing Variables

In addition to simple printing, we can also use `printf` to print variables and other calculated output to the terminal. We do this by embedding special character sequences in our string and by passing extra values to `printf`. Note that these character sequences have no special meaning for the assembler like '\n', instead they are understood by the `printf` function (and related functions).

We give another example.

Pseudocode:

```
printf("I am %ld years old\n", 25);
```

Assembly:

```
mystring: .asciz "I am %ld years old\n"

    movq $0, %rax           # no vector registers in use for printf
    movq $25, %rsi          # load the value
    movq $mystring, %rdi    # load the string address
    call printf             # Call the printf routine
```

The `printf` function will automatically convert the integer value 25 to a ASCII representation of the decimal number 25 and it will substitute the value into the string at the point where the '%ld' sequence is encountered. The '%ld' sequence simply tells `printf` that it may expect an extra argument and that the argument must be interpreted as a long decimal number (64 bits) for printing.

Other Format Specifiers

There are many other format specifiers, but you will probably not need to use them for the compulsory assignments. For the interested, here are some of the most commonly used format specifiers[15]:

[14] Remember that a label is just a memory address?
[15] Other format specifiers are neatly listed at `http://www.cplusplus.com/reference/cstdio/printf/`

Specifier	Usage
`%d`	decimal number (32 bits)
`%lx`	hexadecimal number (64 bits, using lowercase `a-f`)
`%lX`	hexadecimal number (64 bits, using uppercase `A-F`)
`%lu`	unsigned decimal number (64 bits)
`%c`	character
`%s`	string of characters (passed as a memory address)
`%%`	the literal character '%'

3.7.2 Reading from the Terminal

To gather input from the user, we use another routine from the system C library called `scanf`. This routine also has powerful number conversion facilities which work in a similar fashion as the `printf` subroutine we saw in the last paragraph. We supply at least two arguments to `scanf`, the first one being a *format string* containing a number of special character sequences and the subsequent ones being memory addresses at which `scanf` may put the read values. In the following pseudocode we use the '&' operator to denote "address of", e.g. `&number` is the memory address of the variable `number`:

```
int number;
scanf("%ld", &number);
```

In assembly, the address of a variable depends on its location. If you want to store a value into a global address you can simply use its label as the address. If you want to put a value in a stack variable you could calculate the address using the base pointer. Fortunately, x86-64 offers a `lea` instruction ("load effective address") which makes this rather simple. We provide a complete example of a `scanf` call which reads a decimal number from the keyboard and stores it in some local stack variable:

```
formatstr: .asciz "%ld"
      ...
      subq $8, %rsp              # Reserve stack space for variable
      leaq -8(%rbp), %rsi        # Load address of stack var in rsi
      movq $formatstr, %rdi      # load first argument of scanf
      movq $0, %rax              # no vector registers for scanf
      call scanf                 # Call scanf
```

3.8 The End of the Program

At the end of the example program, we see another call to a function in the C system library. In most operating systems, programs need to return an *error code* which tells the operating system whether your program encountered any internal errors while running. By convention, programs return zero if no errors were encountered. Furthermore, the operating system may want to do some cleaning up after a program runs. To facilitate this, we call the `exit` function with our error code (zero) in the same way we used the `printf` function earlier.

3.9 Programming Constructs

In your pseudocode specifications you will often use common, high-level programming constructs such as `if`-statements, `while`-loops and `switch`-statements. In this subsection we show you how to transcribe these constructs into assembly language by means of a series of examples. Fundamental to all the conditional examples is the general concept of *Conditional branching* which is discussed in paragraph 3.9.1. In paragraphs 3.9.2 through 3.9.3 we provide examples of actual programming constructs and Chapter 4 provides some higher-level ones which are not necessary for the mandatory lab.

3.9.1 Conditional Branching

There are many so-called "jump" or "branch" instructions in the x86-64 instruction set which load a new value into the program counter. These instructions come in two flavors. First, there are the regular branch instructions such as `jmp` or `call` which cause program execution to continue at a different memory address. Second are the *conditional* branch instructions, which will only jump to the new target address if some condition holds. We can use these conditional jump instructions to implement conditional constructs, such as `if`-statements and `while`-loops:

Pseudocode:

```
    if (RAX > 1) {
        //IF-code
    } else {
        //ELSE-code
    }
```

Implementation:

```
        cmpq $1, %rax   # compare RAX to 1
        jg  ifcode      # jump to IF-code if RAX > 1
        jmp elsecode    # jump to ELSE-code otherwise

    ifcode:
        ...             # IF-code
        jmp end

    elsecode:
        ...             # ELSE-code
    end:
```

The `cmp` instruction on the first line compares the contents of `RAX` to the number 1. It stores the results of this comparison (e.g. whether the contents of `RAX` were greater than-, equal to or less than 1) in the special `RFLAGS` register. The `jg` instruction ("jump if greater-than") is a conditional branch instruction. It tests the contents of the `RFLAGS` register and jumps to the `ifcode` label *if* the flags indicate that the second operand of the `cmp` instruction was greater than the first. For an overview of the various conditional branch instructions, see the instruction set reference in paragraph 3.3.3. The subsequent paragraphs will demonstrate other programming constructs based on the conditional branch instructions. Paragraph 3.9.2 will give a more compact implementation of the `if`-statement.

3.9.2 `if-then-else` Statements

In the previous paragraph we have seen an example implementation of the familiar `if`-statement. In this paragraph we change the sequence of the if- and else-blocks to come to a shorter implementation.

Pseudocode:

```
    if (RAX > 1) {
        //IF-code
    } else {
        //ELSE-code
    }
```

Implementation:

```
        cmpq $1, %rax # compare RAX to 1
        jg  ifcode    # jump to IF-code if RAX > 1

    elsecode:
        ...           # ELSE-code
        jmp end

    ifcode:
        ...                # IF—code
    end:
```

3.9.3 Loops

The `do-while`-loop Pseudocode:

```
    do {
        //loop code
    } while(RAX > 1);
```

In this example we jump back to the beginning of the loop as long as the condition holds. Implementation-wise, this is the simplest type of loop:

```
    loop:
        ...             # loop code

        cmpq $1, %rax   # repeat the loop
        jg   loop       # if RAX > 1
```

The `while`-loop Pseudocode:

```
    while(RAX > 1) {
        //loop code
    }
```

In this example we will break the loop if the condition does *not* hold, i.e. we jump to the end if `RAX` is lesser or equal to 1:

```
    loop:
        cmpq $1, %rax   # if RAX <= 1 jump to
        jle  end        # the end of the loop

        ...             # loop code

        jmp loop        # repeat the loop
    end:
```

The `for`-loop Pseudocode:

```
    for(RAX = 0; RAX < 100; RAX++) {
        //loop code
    }
```

A `for` loop is really nothing more than a glorified `while`-loop:

```
    RAX = 0;
    while(RAX < 100) {
        //loop code

        RAX++;
    }
```

You should be able to implement this one yourself.

3.10 ASSIGNMENT 1: Powers

This first assignment consists of two parts. Part A will get you started with assembly and how to build and run your own assembly programs. In part B, you will write your first *subroutine* with I/O and some basic programming constructs. You will only need to hand in part B, but you can ask an assistant (not make a submission!) whether you are on the right track after finishing part A.

3.10.1 Part A: Getting Started

In this assignment you will be asked to write your first assembly program. You will have to use the knowledge you acquired from the example program in order to complete this task, so make sure you have a thorough understanding of it. Remember that you can always ask the lab course assistants for help. For this program, you will not have to write any specifications, since there is no significant algorithmic complexity involved. However, you are of course required to write proper comments.

In order to complete this assignment you will need to call the `printf` subroutine. Paragraph 3.6.1 of the reference section explains the details of calling subroutines and paragraph 3.7.1 explain how to use the `printf` subroutine. Paragraph 2.3.1 explains the commands that you will need to enter on your shell in order to build and run your program.

Exercises:

1. Create a new text file, called "power.s".
2. Implement a simple `main` routine that exits the program immediately with the proper exit code and without crashing.
3. Build your program and run it.
4. Alter your `main` routine in such a way that it prints a message containing your names, netIDs and the name of the assignment on the terminal.

You should not need more than one call to `printf` to display your message. After completing the rest of the exercises in part B, you will need to have the source code of this program checked by the teaching assistants, so make sure you keep all your files in order.

3.10.2 Part B: Your First Assembly Algorithm

Now that you have successfully run your first assembly program, it is time to write a more complex program. In this assignment you will write a subroutine that takes several input parameters and returns a computed value.

From the reference part of this manual, you might find section 3.9 useful for this assignment. Remember that subroutines should always have proper stack frames and you should use the official calling conventions, as discussed in paragraphs 3.6 and 3.5.4.

Exercises:

1. The following partial specification of the `pow` subroutine is given:

```
/**
 * The pow subroutine calculates powers
 * of non-negative bases and exponents.
 *
 * Arguments:
 *
 *     base - the exponential base
 *     exp  - the exponent
 *
 * Return value: 'base' raised to the power of 'exp'.
 */
int pow(int base, int exp) {
        int total = 1;

        //...

        return total;
}
```

Complete the specification of the `pow` subroutine. You should only use looping constructs and simple arithmetic operations to compute the total.
It is not required to sign-off this specification, but you can ask a teaching assistant to check that it is correct. Also when you have questions about this assignment, the teaching assistant will ask for your specification.

2. Create a new subroutine called `pow`, which will be the implementation of your `pow` subroutine.

3. Alter your `main` routine in such a way that it asks the user for a non-negative base and exponent.

4. Alter your `main` routine in such a way that it calls `pow` with the numbers it reads and prints the result of `pow` on the terminal.

3.11 ASSIGNMENT 2: Recursion

By now, you should have a fairly thorough understanding of the stack mechanism and of its uses (e.g., storing local subroutine variables). In this assignment you are going to write a recursive subroutine (see paragraph 3.6.2) that calculates the factorial of a number ("n!"). This subroutine will be about 14 instructions in length when it is finished, but writing it will be fairly difficult. Do not be discouraged if it takes you a few hours to get it working.

Exercises:

1. Copy your "power" program to a new file called "factorial.s". Create a new subroutine called `factorial`. This new subroutine should take one parameter, n, and for now it should simply do nothing and return n in the RAX register. Alter your `main` routine in such a way that it calls `factorial` with the number it reads, instead of calling power. `main` should print the result of `factorial` on the terminal.

2. Write a pseudocode specification of your `factorial` subroutine. The subroutine accepts a non-negative parameter n and it should return n!. Make sure your algorithm is **recursive**. It should not need to be more than a few lines of pseudocode.
It is not required to sign-off this specification, but you can ask a teaching assistant to check that it is correct. Also when you have questions about this assignment, the teaching assistant will ask for your specification.

3. Implement your `factorial` routine. Test your program thoroughly.

3.12 Memory

3.13 Bit Shifting

One of the powerful things about the assembly language is that you can very easily manage your values on the bitwise level. Bit shifting is a common advantage of this property.

The following is an example of a bit shift:

```
        movq     $0, %rax           # 00000000 ... 00000000 00000000
        movb     $142, %al          # 00000000 ... 00000000 10001110
        shr      $3, %rax           # 00000000 ... 00000000 00010001
```

It shifts the bits in memory by the number and in the direction you specify (`shl` is left-shift, `shr` is right-shift).

3.14 ASSIGNMENT 3: Memory

Hundreds of years ago, archeologists discovered a treasure chest full of ancient scripts and drawings. Sadly, the puny minds of the current civilisation could not comprehend the contents of these precious documents and after decades of searching for a way to unlock their mysteries, people were forced to admit defeat and locked them away until someone worthy came along and could decode them.

Then, a few days ago, a strange machine was discovered. Our knowledge of technology is yet too limited to be able to get it working, but the group of scientists working on it managed to glean how the machine decodes these artifacts.

Now, they have tasked you with recreating it in the primitive ways of our technology. They have found that the artifacts are encoded in 8-byte memory blocks. The bytes in a memory block signify the following (from highest to lowest):

Byte 1 - 2	Unknown - this is still being worked on but they have already determined that it is not crucial knowledge for decoding the messages.
Byte 3 - 6	The next memory block to visit.
Byte 7	The amount of times that character should be printed.
Byte 8	The ASCII[16]character which should be printed.

So executed on the following memory blocks (where B = 00000000):

0	`B B`	`B B B 00001000`	`00000001`	`01001000`	`?`	`8`	`1`	`H`
1	`B B`	`B B B 00001010`	`00000001`	`01010111`	`?`	`10`	`1`	`W`
2	`B B`	`B B B 00000111`	`00000001`	`01101100`	`?`	`7`	`1`	`l`
3	`B B`	`B B B 00000001`	`00000001`	`00100000`	`?`	`1`	`1`	`␣`
4	`B B`	`B B B 00000101`	`00000010`	`01101100`	`?`	`5`	`2`	`l`
5	`B B`	`B B B 00000011`	`00000001`	`01101111`	`?`	`3`	`1`	`o`
6	`B B`	`B B B 00000000`	`00000001`	`00100001`	`?`	`0`	`1`	`!`
7	`B B`	`B B B 00000110`	`00000001`	`01100100`	`?`	`6`	`1`	`d`
8	`B B`	`B B B 00000100`	`00000001`	`01100101`	`?`	`4`	`1`	`e`
9	`B B`	`B B B 00000010`	`00000001`	`01110010`	`?`	`2`	`1`	`r`
10	`B B`	`B B B 00001001`	`00000001`	`01101111`	`?`	`9`	`1`	`o`

your program should do the following:

1. Start at memory block `0`.
2. Print the character `H` once and jump to memory block 8.
3. Print the character `e` once and jump to memory block 4.
4. Print the character `l` **twice**, and jump to memory block 5.
5. ...
6. Print the character `!` and terminate.

Which would result in the famous `Hello World!`

Exercises:

1. Download the files for this assignment from Brightspace.
   The file you will be writing your code in is "decoder.s". It currently includes the message from "helloWorld.s" (the `.include ''helloWorld.s''` line does this). If you want to change the input message, simply change this line to include the file you want.

[16]`http://www.asciitable.com/`

2. Write a pseudocode specification of your `decode` subroutine. The subroutine accepts the address of the message as its first parameter and has no return value. The following is an outline for you specification:

   ```
   /**
    * The decode subroutine decodes the messages.
    *
    * Arguments:
    *
    *    address — the address of the message
    *              in memory
    *
    * Return value: none
    */
   void decode(int adress) {
           // ...
   }
   ```

   You may also write helper subroutines which will be called from `decode`.
   It is not required to sign-off this specification but you can ask a teaching assistant to check that it is correct. Also, when you have questions about this assignment, the teaching assistant will ask for your specification.

3. Implement your `decode` subroutine. Test your program thoroughly. Provided are test files “abc_sorted.s”, “helloWorld.s”, and “final.s”. We recommend starting with “abc_sorted.s”. This should print two lines: 0 through 9 on the first line and a through z on the second line. The memory is sorted, so this should work by each time just taking the next memory block. For Hello World you will need to extract the index of the next memory block. As for the contents of Final: the archeologists have not been able to figure this out yet. Can you?

This exercise wraps up the basic assembler programming assignments. You should go and have your code checked by a lab course assistant. Well done!

Chapter 4

Bonus Content

This chapter contains only bonus content and assignments. For each assignment, you can receive extra points towards your final grade (the amount is always listed with the assignment).

4.1 ANSI Escape Codes

ANSI escape codes (also known as ANSI sequences) were invented in the 70s to control the text terminals. This way they could do things like setting the cursor position, clear the screen, change the colours, etc in a standardised manner. For the terminal to understand that such a sequence needs to be treated differently from the normal text it starts with the escape character (ASCII character 27) followed by '['. Once the terminal detects these 2 characters the next few characters are interpreted as an ANSI code. As an example: Escape, '[', 4, A moves the cursor 4 lines up. A complete list of all codes can be found online [1]. Although the standard is already quite old, all terminal programs today support this standardised way of manipulating the text on the terminal.

4.2 ASSIGNMENT 4: A Colourful Discovery (max 500 points)

Good news!

The team of scientists has figured out the last two bytes of our mysterious messages from the previous assignment: colours. So simple! The first byte is supposedly the colour of the background and the second one is the colour the character should be (foreground). Both of them are in the format of the ANSI 8-bit escape codes.

So returning to our example from section 3.14, the complete table would look as follows:

0	`00000000`	`00000010`	`B B B 00001000`	`00000001`	`01001000`	`0`	`2`	`8`	`1`	`H`
1	`00000010`	`00000000`	`B B B 00001010`	`00000001`	`01010111`	`2`	`0`	`10`	`1`	`W`
2	`00000010`	`00000000`	`B B B 00000111`	`00000001`	`01101100`	`2`	`0`	`7`	`1`	`l`
3	`00000000`	`00000000`	`B B B 00000001`	`00000001`	`00100000`	`0`	`0`	`1`	`1`	`␣`
4	`00000000`	`00000010`	`B B B 00000101`	`00000010`	`01101100`	`0`	`2`	`5`	`2`	`l`
5	`00000000`	`00000010`	`B B B 00000011`	`00000001`	`01101111`	`0`	`2`	`3`	`1`	`o`
6	`00000000`	`00000010`	`B B B 00000000`	`00000001`	`00100001`	`0`	`2`	`0`	`1`	`!`
7	`00000010`	`00000000`	`B B B 00000110`	`00000001`	`01100100`	`2`	`0`	`6`	`1`	`d`
8	`00000000`	`00000010`	`B B B 00000100`	`00000001`	`01100101`	`0`	`2`	`4`	`1`	`e`
9	`00000010`	`00000000`	`B B B 00000010`	`00000001`	`01110010`	`2`	`0`	`3`	`1`	`r`
10	`00000010`	`00000000`	`B B B 00001001`	`00000001`	`01101111`	`2`	`0`	`9`	`1`	`o`

Here is the what the colours used here stand for:

[1] `https://en.wikipedia.org/wiki/ANSI_escape_code#8-bit`

0	BLACK
2	GREEN

And so, here is what the message is actually supposed to look like:

```
Hello World !
```

If foreground and background colour are the same you would end up with unreadable text. The scientists have not figured what to do when this happens, so for now you should ignore the colours if the foreground and background colours are the same.

Exercise 4.1: +200 points

1. Copy over your solution from “decode.s”.
2. Write a pseudocode specification of your new `decode` subroutine which now also prints the message in its correct colour scheme.
   It is not required to sign-off this specification but you can ask a teaching assistant to check that it is correct. Also, when you have questions about this assignment, the teaching assistant will ask for your specification.
3. Implement your new `decode` subroutine. Test your program thoroughly.

Science is advancing rapidly here! The scientist figured out what to do with memory blocks where the foreground and background colour are the same. These are apparently used for special effects. The scientists have not figured them all out yet, but we already know of the following:

0	reset to normal
37	stop blinking
42	bold
66	faint
105	conceal
153	reveal
182	blink

Note for WSL users: Support for these special effects depends on the terminal you are using. To get them to work properly, we recommend using ”Windows Terminal”, which is available in the Microsoft Store: `https://www.microsoft.com/en-us/p/windows-terminal-preview/9n8g5rfz9xk3`. You will need the latest preview version for it to work.

Exercise 4.2: +300 points

1. Copy over your solution from “4.1”.
2. Implement the features in your `decode` subroutine. Test your program thoroughly.
3. Implement the special effect codes. Keep in mind that a special effect code should not change the colours. Now let’s see what that final message actually should look like!

4.3 Advanced Programming Constructs

4.3.1 Switch-Case Statements

Pseudocode:

```
switch(RAX) {
    case 0:
            // case 0 code
            break;

    case 1:
            // case 1 code
            break;

    case 2:
            // case 2 code
            break;
}
```

To implement the `switch`-statement we have to create one small subroutine for each of the cases. We then create a table containing the starting addresses of these subroutines and we use the value of `RAX` to look up the proper subroutine address in the table. A table like this is called a *jump table*:

```
# The jumptable:
jumptable:
    .quad case0sub
    .quad case1sub
    .quad case2sub

# The case subroutines:
case0sub:
    ... # case 0 code
    ret

case1sub:
    ... # case 1 code
    ret

case2sub:
    ... # case 2 code
    ret

# The actual switch statement:
    shlq $3, %rax               # multiply RAX by 8
    movq jumptable(%rax), %rax  # load the address from the table
    call *%rax                  # call the subroutine
```

There is some trickery going on in the last three instructions that deserves some attention: first of all, we have to remember that the subroutine addresses in the jumptable are eight bytes long, so we will have to multiply our `RAX` register by eight before we can use it as a table index. We can of course accomplish this by shifting the operand left by three bits. Second, we have to use the '`*`' when calling a subroutine whose address is located in a register.

4.3.2 Lookup Tables

Very often, programs need to perform time consuming computations inside tight loops. If a small number of values are computed over and over again, we can simply precompute them at compile-time, put them in a table and replace the actual computation with a table lookup. Such a construct is called a *lookup table* and it can be used to simplify and speed up programs considerably. We demonstrate the lookup table through an example:

```
// Print various Fibonacci numbers
for(int i = 0; i < 100000; i++) {
    print(fibonacci(30 + (i % 10)));
}
```

Computing the n-th Fibonacci number is a very computationally intensive task and the `fibonacci` subroutine can be tricky to implement in assembler. By studying the example carefully, we observe that the only values which are actually calculated are `fibonacci(30)` through `fibonacci(39)`. Of course, we can simply precompute these values at compile time without having to implement the `fibonacci()` routine at all. The resulting program is both faster and easier to implement:

```
// A table containing the Fibonacci numbers from 30 to 39
int fibtable[] = {
                832040,
                1346269,
                2178309,
                3524578,
                5702887,
                9227465,
                14930352,
                24157817,
                39088169,
                63245986
    };

// Print various Fibonacci numbers
for(int i = 0; i < 100000; i++) {
        print(fibtable[i % 10]);
}
```

In assembly, we can use the `.byte`, `.word`, `.long` and `.quad` directives to construct the lookup table:

```
fibtable:
        .long 832040
        .long 1346269
        .long 2178309
        .long 3524578
        .long 5702887
        .long 9227465
        .long 14930352
        .long 24157817
        .long 39088169
        .long 63245986
```

4.4 Doing I/O without the C library

During the lab course we have used the system's standard C library to perform input and output operations. Of course, it is also possible to do I/O without the C library. The benefit of this approach is that our programs will be as short and small as possible, as we save ourselves the trouble of executing an extra subroutine call. The drawback, as explained earlier, is that the details of the procedure differ from one operating system to another. As an example, we demonstrate how to print a line of text on the terminal without using `printf`.

The procedure is fairly simple, but as with all topics in this advanced section, it requires some prior knowledge that is slightly outside of the scope of this lab course. During the Operating Systems course, you will learn that programs communicate with the kernel by performing a "system call". In a system call, a program transfers control to the kernel, much like a subroutine call transfers control to a subroutine. In fact, it is possible to pass parameters to a system call in much the same way.

The difference with an ordinary subroutine call is, as always, in the details. In 32 bit, the actual control transfer was achieved by causing a software interrupt, which is sometimes called a *trap*. This is done by executing an `int` instruction. On Linux, the interrupt number for a system call is always `0x80`. In 64 bit mode, things are not that different from what you are used to. The arguments still go in the same registers as before, but now you will have to provide a magic number in %RAX defining what system call you want. For instance, doing an exit is done by setting %RAX to 60, putting the error code in %RDI (normally 0) and then use the syscall instruction.

```
# Perform the 'sys_exit' system call:
    movq    $60, %rax       # system call 60 is sys_exit
    movq    $0, %rdi        # normal exit: 0
    syscall
```

A complete list of available Linux system calls can be found in the kernel source code [2]. The complete call looks a bit less friendly than printf:

```
# define the string and its length:
hello:
    .asciz  "Hello!\n"
helloend:
    .equ    length, helloend - hello

# Perform the 'sys_write' system call:
    movq    $1, %rax        # system call 1 is sys_write
    movq    $1, %rdi        # first argument is where to write; stdout is 1
    movq    $hello, %rsi    # next argument: what to write
    movq    $length, %rdx   # last argument: how many bytes to write
    syscall
```

The code we see here is actually very similar to the code that we find inside the printf function itself. Many functions in the C library, including printf, use inline assembly code to perform their actual function (see 4.8). Since compilers are not operating system specific, the authors of printf have to resort to this technique.
Now that your code does not depend on the C library anymore, you can even assemble and link it yourself, without the gcc magic:

```
as -o hello.o hello.s
ld --entry main -o hello hello.o
```

Compare the size of your final program to the size of its C equivalent. Now that's efficiency!

4.5 ASSIGNMENT 5 (500 points)

Choose **only one** of the following three options (you will not receive points for more than one).

4.5.1 Option A: Implement "diff" in Assembly

For this exercise you will implement the Unix "diff" program in assembly. The purpose of the diff program is to compare two files line by line and show all the differences between them. As a sample output, consider the following two files:

```
Hi, this is a testfile.             Hi, this is a testfile.
Testfile 1 to be precise.           Testfile 2 to be precise.
```

The resulting output of diff is then:

```
$ diff testfile1 testfile2
2c2
< Testfile 1 to be precise.
---
> Testfile 2 to be precise.
```

[2] Or in lookup tables like this one: https://filippo.io/linux-syscall-table/

As you can see it tells us that the second line is different (2c2 means that line 2 in the original has been **c**hanged to become line 2 in the new file). For more information on how the diff command works, please check the diff manuals (type `man diff` in a terminal) and check Wikipedia at `http://en.wikipedia.org/wiki/Diff`.

For this assignment your program will have to be able to do the following:

- Implement a line-by-line comparison version of diff. This means it is not required to have the `a` and `d` outputs that the real diff offers. Only the changes will suffice, though we encourage you to also try the detection of addition and deletion of lines.
- Implement at least the -i and -B options that diff offers (see the diff manual to learn what these options do).

Note : It is not required that you read text from a file or the standard input. It is allowed for you to hardcode the texts you are comparing in your source. If you do this however, the student assistants will change this hardcoded text to confirm that your program works for different texts as well.

Note : The -i and -B options should be read from the command line arguments; not hardcoded. By convention you get your command line arguments the following way: first an integer that tells you how many arguments were provided (always at least 1; the name of your own program) and then the actual parameters. More information can be found online.

4.5.2 Option B: Implement a Simplified `printf` Function

As mentioned before, the `printf` subroutine is just a subroutine like any other. To prove this, you will write your own simplified version of `printf` in this assignment.

Write a simplified `printf` subroutine that takes a variable amount of arguments. The first argument for your subroutine is the format string. The rest of the arguments are printed instead of the placeholders (also called format specifiers) in the format string. How those arguments are printed depends on the corresponding format specifiers. Your `printf` function has to support any number of format specifiers in the format string. Note that any number means that you need to support more than 6 arguments.

Unlike the real `printf`, your version only has to understand the format specifiers listed below. If a format specifier is not recognized, it should be printed without modification. Give your `printf` function a different name (e.g. `my_printf`) to avoid confusion with the real `printf` function in the C library. Please note that for this exercise you are not allowed to use the `printf` function or any other C library function. This means you will have to use system calls for the actual printing. Your function must follow the proper x86-64 calling conventions.

Supported format specifiers:

%d Print a signed integer in decimal. The corresponding parameter is a 64 bit signed integer.

%u Print an unsigned integer in decimal. The corresponding parameter is a 64 bit unsigned integer.

%s Print a null terminated string. No format specifiers should be parsed in this string. The corresponding parameter is the address of first character of the string.

%% Print a percent sign. This format specifier takes no argument.

Example:

Suppose you have the following format string:

My name is %s. I think I'll get a %u for my exam. What does %r do? And %%?

Also suppose you have the additional arguments “Piet” and 10. Then your subroutine should output:

> My name is Piet. I think I’ll get a 10 for my exam. What does %r do? And %?

Hints

To get started you may divide the work in a number of steps. Note that these are just hints, you do not have to follow these steps to finish this assignment.

1. Write a subroutine that prints a string using system calls.
2. Write a new subroutine to recognize format specifiers in the format string. Initially, you can discard the format specifiers rather than process them. The rest of the string can be printed using the subroutine from the previous hint.
3. Implement the various format specifiers. It may help to implement %u before %d. Again, you may use the print function from the first hint if you implemented it.
4. It may help to store all input argument registers on the stack at the start of your function, even if you don’t end up using them.

4.5.3 Option C: Implement a Hashing Function

For this assignment, implement a program to calculate a hash such as SHA-1, SHA-256, MD4, MD5, or any other hash you like, of the input given to the program. If you do not know what a hash function is, Google a bit first.

Choose a well known hashing algorithm, and write a program that calculates and prints the hash of the input given to the program. (From standard input or from a file.)

Optional help from our side for SHA-1:

Read the Wikipedia page about SHA-1[3] (especially the pseudo code). As you will see, the algorithm has to split up the data up in 512-bit chunks, and then process each chunk separately. In this simplified exercise, you will only implement the function to process a chunk. The rest of the code is provided by us. After you finish this exercise, you can implement the rest of the code too, but that is not required.

Our part of the code can be downloaded from Brightspace. You can combine this with your own code by adding “`./sha1_test64.so`”[4] as another parameter to `gcc`. Our code does everything until and including the line “break chunk into sixteen ...” in the pseudo code on Wikipedia. The command used to compile your code could like something like this:

```
gcc -o test my_sha1_chunk.s ./sha1_test64.so
```

Your part of the code should not have a `main` function, but instead have a `sha1_chunk` function, which will be called by our part of the code. This `sha1_chunk` function takes two parameters: First, the address of `h0` (`h1`, `h2`, etc. are stored directly after `h0`). (See Wikipedia’s pseudo code for SHA-1 for these names.) Second, the address of the first 32-bit word of an array of 80 32-bit words. The first sixteen of this array are set to the sixteen 32-bit words the chunk contains (which are called `w[0]` till `w[15]` on Wikipedia). Your function should modify `h0` till `h4` as described in the pseudo code.

When you execute the combined program, our part of the code prints a lot of information on what is happening, and when your function is called. It displays the result of your function, and whether that is correct or not. You can of course print more debugging information from your own function using `printf`.

[3] `http://en.wikipedia.org/wiki/Sha1`

[4] there is also a sha1_test32.so for 32 bit compilation available

4.6 ASSIGNMENT 6: Hide Data in a Bitmap (750 points)

The scientists from Assignment 3 (3.14) suggested that our generation should also leave a message for future generations. Frustrated at how long it took them to implement a decoder, the decision was made that this new effort should also be an "interesting" puzzle.

You are tasked by the scientists to encrypt messages using assembly, into everyday barcodes. This assembly code will then later be hacked into a popular barcode software package. In detail:

1. Make sure you understand the message, including the "lead" and "trail".
2. Compress the message using the Run-Length Encoding (RLE) technique.
3. Prepare the barcode.
4. Use XOR to encrypt the message into the barcode.
5. Save the results as image bitmaps, in BMP format.
6. Test that you can decrypt the message, using again the XOR encryption technique.

Data: The Message

Complexity: Easy
To demonstrate that your assembly code works, encrypt and decrypt the message `The answer for exam question 42 is not F.`, including the final dot ('.'). Save the message as an assembly data chunk before you continue.

Each message, before encryption, must be preceded and followed by the following pattern:

$$8 \times C, 4 \times S, 2 \times E, 4 \times 1, 4 \times 4, 8 \times 0$$

Here, `<number>` × `<character>` means that *character* is repeated *number* times, e.g., $8 \times C$ means `CCCCCCCC`. The added parts are called the "lead" and the "trail" of the message.

Data Compression: Run-Length Encoding (RLE)

Complexity: Moderate
Run-Length Encoding (RLE) is one of the simplest data encoding techniques. RLE is based on the notion of runs, which are sequences of specified length of the same item.

For this assignment, you will use RLE-8, which encodes, in turn, the size of the sequence and each item on 8 bits each. For example, the RLE-8-encoded sequence of two bytes with values `8` and `67` (the ASCII value of `C`) means that the sequence length is 8 and the item is `C`, for the fully decrypted text `CCCCCCCC`.

You have to devise your own algorithms for RLE-8-encoding and RLE-8-decoding the message described in the previous paragraph.

Data: Barcodes

Complexity: Easy
The message will be encoded in the first part of a barcode. For simplicity you can assume that the barcode looks like this:

```
W W W W W W W W B B B B B B B B W W W W B B B B W W B B B W W
```

This pattern is 31 pixels long. In this pattern, `W` stands for a white pixel and `B` stands for black.

Create a sequence by repeating this pattern, followed by a red pixel, 32 times. This will form a 32×32 image, where each pixel is either white, black, or red. Note that this key represents an RGB image, where each pixel is represented using three bytes.

Input		Output
x	y	XOR(x,y)
0	0	0
0	1	1
1	0	1
1	1	0

Table 4.1: XOR truth table.

Data Encryption: XOR

Complexity: Moderate
One of the common logical operations is the eXclusive OR (XOR, $\oplus$), equivalent to the Boolean logic concept of "TRUE if only one of the two operands, but not both, is TRUE". Table 4.1 summarises the truth table of XOR.
Two properties of XOR are of interest:

$$x \oplus 0 = x \tag{4.1a}$$
$$x \oplus x = 0 \tag{4.1b}$$

From Equations 4.1a and 4.1b (non-idempotency), it is trivial to observe that:

$$\begin{aligned}(x \oplus y) \oplus y &= x \oplus (y \oplus y)\\ &= x \oplus 0\\ &= x\end{aligned} \tag{4.2}$$

Equation 4.2 means that we can use XOR to first encrypt ($x \oplus y$) and then decrypt ($(x \oplus y) \oplus y$) a one-bit message x with the encryption/decryption key y. It turns out that these two one-bit operations can be extended to n-bit operations, that is, for an n-bit message M and an n-bit key K:

$$(M \oplus K) \oplus K = M \tag{4.3}$$

For example, if the message is `TEST` in ASCII (`M = 01010100 01000101 01010011 01010100` in binary) and the key is `TRY!` in ASCII (`K = 01010100 01010010 01011001 00100001`), the encrypted text is:

$$\begin{aligned}M \oplus K &= \texttt{01010100 01000101 01010011 01010100}\\ &\oplus \texttt{01010100 01010010 01011001 00100001}\\ &= \texttt{00000000 00010111 00001010 01110101}\end{aligned} \tag{4.4}$$

The decrypted text is:

$$\begin{aligned}(M \oplus K) \oplus K &= \texttt{00000000 00010111 00001010 01110101}\\ &\oplus \texttt{01010100 01010010 01011001 00100001}\\ &= \texttt{01010100 01000101 01010011 01010100}\\ &= M\end{aligned} \tag{4.5}$$

Last, a good example of implementing the XOR encryption technique in C is the "C Tutorial - XOR Encryption" by Shaden Smith, June 2009[5].

Your task is to encrypt the RLE-encoded message using the barcode image as key. Note that the key consists of $32 \times 32 \times 3$ bytes, while the message is much shorter. This means that only a small part of the image will change.

[5] [Online] Available: `http://forum.codecall.net/topic/48889-c-tutorial-xor-encryption/`.

Data Representation: the BMP Format (Simplified)

Complexity: Difficult
Storing data as images requires complex data formats. One of the simplest is the bitmap (BMP) format, which you must use. BMP files encode raster images, that is, images whose unit of information is a pixel; raster images can be directly displayed on computer screens, as their pixel information can be mapped one-to-one to the pixels displayed on the screen.

The BMP file format consists of a header, followed by a meta-description of the encoding used for pixel data, followed sometimes by more details about the colours used in the image (look-up table, see also the paragraph on barcodes). The BMP file format is versatile, that is, it can accommodate a large variety of colour encodings, image sizes, etc. It is beyond the purpose of this manual to provide a full description of the BMP format, which is provided elsewhere[6].

Luckily for you, of the many flavors of encodings, we opted to only accept one type. Thus, you must use the following BMP format for this assignment:

1. File Header, encoded as signature (two bytes, `BM` in ASCII); file size (integer, four bytes); reserved field (four bytes, `00 00 00 00` in hexadecimal encoding); offset of pixel data inside the image (integer, four bytes). The file size is the sum between the file header size, the size of the bitmap info header, and the size of the pixel data. The file header size is 14 (two bytes for signature and four bytes each for file size, reserved field, and offset of pixel data). The file size is the sum of 14 (the file header size), 40 (the size of the bitmap header), and the size of the pixel data.

2. Bitmap Header, encoded as[7]: header size (integer, four bytes, must have a value of 40); width of image in pixels (integer, four bytes, set to 32–see see paragraph on barcodes); height of image in pixels (integer, four bytes, set to 32–see paragraph on barcodes); reserved field (two bytes, integer, must be 1); the number of bits per pixel (two bytes, integer, set here to 24); the compression method (four bytes, integer, set here to 0–no compression); size of pixel data (four bytes, integer); horizontal resolution of the image, in pixels per meter (four bytes, integer, set to 2835); vertical resolution of the image, in pixels per meter (four bytes, integer, set to 2835); colour palette information (four bytes, integer, set to 0); number of important colours (four bytes, integer, set to 0).

3. Pixel Data, encoded as `B G R` triplets for each pixel, where `B`, `G`, and `R` are intensities of the blue, green, and red channels, respectively, with values stored as one-byte unsigned integers (0–255). It is important that the number of bytes per row must be a multiple of 4; use 0 to 3 bytes of padding, that is, having a value of zero (0) to achieve this for each row of pixels. The total size of the pixel data is $N_{rows} \times S_{row} \times 3$, where N_{rows} is the number of rows in the image (32–see paragraph on barcodes); S_{row} is the size of the row, equal to the smallest multiple of 4 that is larger than the number of pixels per row (here, 32–see paragraph on barcodes); and the constant 3 is the number of bytes per pixel (24 bits per pixel, as specified in the field "number of bits per pixel", see the Bitmap header description).

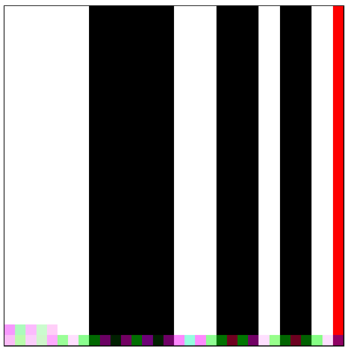
Note: the message will be quite more visible in this example than what one would do in reality. As an example, the following image contains the message `The quick brown fox jumps over the lazy dog` encrypted in the barcode pattern:

Last But Not Least

Make sure that you are also able to decrypt the message. After this, you should go and have your code checked by a lab course assistant. You have now officially proved mastery in the basics of

[6]BMP file format, Wikipedia article. [Online] Available: `http://en.wikipedia.org/wiki/BMP_file_format`. Note: Although Wikipedia is not a universally trustworthy source of information, many of its articles on technical aspects, such as the "BMP file format" have been checked by tens to hundreds of domain experts.

[7]This encoding is `BITMAPINFOHEADER`, which is a typical encoding for Windows and Linux machines. Older encodings, such as `BITMAPCOREHEADER` for OS/2, are obsolete. Newer versions, such as `BITMAPV5HEADER` exist, but they are too complex for our scientists.



assembly programming. Not bad!

4.7 ASSIGNMENT 7: Implement an Interpreter for Brainfuck (500–800 points)

For this assignment, you will implement an interpreter for the very simple “programming language” called Brainfuck. [8] In Brainfuck, every character of the source code is a command, and there are only eight very simple commands. The interesting thing about this language is that even though it might not seem like it, it is still Turing complete. (This basically means that you can write every possible program in it, but not necessarily in an efficient way.)

Exercise:

You can find a tarball containing assembly code and instructions for reading a file specified as a command line argument on Brightspace. You should write a `brainfuck` subroutine that takes a pointer to the Brainfuck code as argument and executes this program.

Examples:

- `hello.b`:

  ```
  >+++++++++[<++++++++>-]<.>+++++++[<++++>-]<+.+++++++..+++.>>>++++++++
  [<++++>-]<.>>>++++++++++[<+++++++++>-]<---.<<<<.+++.------.--------.>>+.
  ```

  Now, executing your program as follows

  ```
  ./brainfuck hello.b
  ```

  should make it give

  ```
  Hello World!
  ```

  as output.

- `cat.b`:

  ```
  ,[.,]
  ```

  This program is the equivalent of the Linux command `cat`; running this program will copy whatever you enter in the console. By sending the null character to the console, the loop halts (this is done by pressing `Ctrl+2` in the terminal).

- More complex programs to test your interpreter with can be found all over the internet. (For example: `http://esoteric.sange.fi/brainfuck/utils/mandelbrot/mandelbrot.b`.)

[8] `https://esolangs.org/wiki/Brainfuck`