Assembly from the Ground Up: x86-64 Edition

An updated Linux edition of *Programming from the Ground Up* by Jonathan Bartlett

Jonathan Bartlett, Israel Roldan

Contents

About This Book 7

1 Introduction 9
1.1 Welcome to Programming 9
1.2 Your Tools 10

2 Computer Architecture 13
2.1 Structure of Computer Memory 13
2.2 The CPU 14
2.3 Some Terms 15
2.4 Interpreting Memory 16
2.5 Data Accessing Methods 16
2.6 Review 17

3 Your First Programs 19
3.1 Entering in the Program 19
3.2 Outline of an Assembly Language Program 21
3.3 Planning the Program 24
3.4 Finding a Maximum Value 25
3.5 Addressing Modes 30
3.6 Review 32

4 All About Functions 35
4.1 Dealing with Complexity 35
4.2 How Functions Work 35
4.3 Assembly-Language Functions using the C Calling Convention 36
4.4 A Function Example 40
4.5 Recursive Functions 43
4.6 Review 48

5 Dealing with Files 51
5.1 The UNIX File Concept 51
5.2 Buffers and `.bss` 51
5.3 Standard and Special Files 52

5.4 Using Files in a Program . . . 53
5.5 Review . . . 61

6 Reading and Writing Simple Records . . . 63
6.1 Writing Records . . . 66
6.2 Reading Records . . . 69
6.3 Modifying the Records . . . 73
6.4 Review . . . 76

7 Developing Robust Programs . . . 77
7.1 Where Does the Time Go? . . . 77
7.2 Some Tips for Developing Robust Programs . . . 77
7.3 Handling Errors Effectively . . . 79
7.4 Making Our Program More Robust . . . 80
7.5 Review . . . 82

8 Sharing Functions with Code Libraries . . . 83
8.1 Using a Dynamic Library . . . 83
8.2 How Dynamic Libraries Work . . . 85
8.3 Finding Information about Libraries . . . 86
8.4 Useful Functions . . . 89
8.5 Building a Dynamic Library . . . 90
8.6 Review . . . 92

9 Intermediate Memory Topics . . . 93
9.1 How a Computer Views Memory . . . 93
9.2 The Memory Layout of a Linux Program . . . 94
9.3 Every Memory Address is a Lie . . . 94
9.4 Virtual Memory . . . 102
9.5 Getting More Memory . . . 103
9.6 A Simple Memory Manager . . . 104
9.7 Using our Allocator . . . 120
9.8 More Information . . . 124
9.9 Review . . . 124

10 Counting Like a Computer . . . 127
10.1 Counting . . . 127
10.2 Truth, Falsehood, and Binary Numbers . . . 130
10.3 The Program Status Register . . . 135
10.4 Other Numbering Systems . . . 135
10.5 Octal and Hexadecimal Numbers . . . 137

10.6 Order of Bytes in a Word . . . 138
10.7 Converting Numbers for Display . . . 140
10.8 Review . . . 144

11 High-Level Languages . . . 147
11.1 Compiled and Interpreted Languages . . . 147
11.2 Your First C Program . . . 148
11.3 Perl . . . 149
11.4 Python . . . 150
11.5 Review . . . 150

12 Optimization . . . 151
12.1 When to Optimize . . . 151
12.2 Where to Optimize . . . 152
12.3 Local Optimizations . . . 152
12.4 Global Optimization . . . 153
12.5 Review . . . 154

13 Moving On from Here . . . 155
13.1 From the Bottom Up . . . 155
13.2 From the Top Down . . . 156
13.3 From the Middle Out . . . 156
13.4 Specialized Topics . . . 156
13.5 Further Resources on Assembly Language . . . 157

Appendices . . . 159

A GUI Programming . . . 161
A.1 Introduction to GUI Programming . . . 161
A.2 The GNOME Libraries . . . 161
A.3 A Simple GNOME Program in Several Languages . . . 161
A.4 GUI Builders . . . 171

B Common x86 Instructions . . . 173
B.1 Reading the Tables . . . 173
B.2 Data Transfer Instructions . . . 173
B.3 Integer Instructions . . . 174
B.4 Logic Instructions . . . 176
B.5 Flow Control Instructions . . . 177
B.6 Assembler Directives . . . 178

B.7 Differences in Other Syntaxes and Terminology . . . 179
B.8 Where to Go for More Information . . . 180

C Important System Calls . . . 181

D Table of ASCII Codes . . . 185

E C Idioms in Assembly Language . . . 187
E.1 If Statement . . . 187
E.2 Function Call . . . 187
E.3 Variables and Assignment . . . 188
E.4 Loops . . . 189
E.5 Structs . . . 190
E.6 Pointers . . . 191
E.7 Getting GCC to Help . . . 192

F Using the GDB Debugger . . . 195
F.1 An Example Debugging Session . . . 195
F.2 Breakpoints and Other GDB Features . . . 198
F.3 GDB Quick-Reference . . . 200

G Document History . . . 205

H GNU Free Documentation License . . . 207

I Personal Dedication . . . 213

J Updated by AirvZxf . . . 215
J.1 Motivations . . . 215

K Solutions to the Review Questions . . . 217
K.1 Chapter 2. Computer Architecture . . . 217
K.2 Chapter 3. Your First Programs . . . 218
K.3 Chapter 4. All About Functions . . . 225
K.4 Chapter 5. Dealing with Files . . . 230
K.5 Chapter 6. Reading and Writing Simple Records . . . 238
K.6 Chapter 7. Developing Robust Programs . . . 251
K.7 Chapter 8. Sharing Functions with Code Libraries . . . 254
K.8 Chapter 9. Intermediate Memory Topics . . . 260
K.9 Chapter 10. Counting Like a Computer . . . 266
K.10 Chapter 11. High-Level Languages . . . 276
K.11 Chapter 12. Optimization . . . 277

About This Book

Assembly from the Ground Up: x86-64 Edition

An updated Linux edition of *Programming from the Ground Up*.

Copyright © 2003 by Jonathan Bartlett

Copyright © 2020–2026 by Israel Roldan (modifications)

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with no Invariant Sections, with no Front-Cover Texts, and with no Back-Cover Texts. A copy of the license is included in Appendix H. GNU Free Documentation License. In addition, you are granted full rights to use the code examples for any purpose without even having to credit the authors.

This book is a Modified Version, as defined by the GNU Free Documentation License, of *Programming from the Ground Up*, Version 1.1, by Jonathan Bartlett, edited by Dominick Bruno, Jr. The changes are listed in Appendix G. Document History. This edition is published by Israel Roldan and is not endorsed by the original author or publisher.

The transparent copy (Markdown source) of this edition, together with the source code of every example, is available at github.com/airvzxf/assembly-from-the-ground-up-x86-64. You can read this edition online, and download it as PDF and ePUB, at asm64.rovisoft.net. The transparent copy of the original book is available at savannah.nongnu.org/projects/pgubook.

All trademarks are property of their respective owners.

The original printed edition: *Programming from the Ground Up*, by Jonathan Bartlett, edited by Dominick Bruno, Jr., published by Bartlett Publishing in Broken Arrow, Oklahoma, 2004. ISBN 0-9752838-4-7. Library of Congress Control Number: 2004091465.

This book is not a reference book, it is an introductory book. It is therefore not suitable by itself to learn how to professionally program in x86 assembly language, as some details have been left out to make the learning process smoother. The point of the book is to help the student understand how assembly language and computer programming works, not to be a reference to the subject. Reference information about a particular processor can be obtained by contacting the company which makes it.

1. Introduction

1.1 Welcome to Programming

I love programming. I enjoy the challenge to not only make a working program, but to do so with style. Programming is like poetry. It conveys a message, not only to the computer, but to those who modify and use your program. With a program, you build your own world with your own rules. You create your world according to your conception of both the problem and the solution. Masterful programmers create worlds with programs that are clear and succinct, much like a poem or essay.

One of the greatest programmers, Donald Knuth, describes programming not as telling a computer how to do something, but telling a person how they would instruct a computer to do something. The point is that programs are meant to be read by people, not just computers. Your programs will be modified and updated by others long after you move on to other projects. Thus, programming is not as much about communicating to a computer as it is communicating to those who come after you. A programmer is a problem-solver, a poet, and an instructor all at once. Your goal is to solve the problem at hand, doing so with balance and taste, and teach your solution to future programmers. I hope that this book can teach at least some of the poetry and magic that makes computing exciting.

Most introductory books on programming frustrate me to no end. At the end of them you can still ask "how does the computer really work?" and not have a good answer. They tend to pass over topics that are difficult even though they are important. I will take you through the difficult issues because that is the only way to move on to masterful programming. My goal is to take you from knowing nothing about programming to understanding how to think, write, and learn like a programmer. You won't know everything, but you will have a background for how everything fits together. At the end of this book, you should be able to do the following:

- Understand how a program works and interacts with other programs.
- Read other people's programs and learn how they work.
- Learn new programming languages quickly.
- Learn advanced concepts in computer science quickly.

I will not teach you everything. Computer science is a massive field, especially when you combine the theory with the practice of computer programming. However, I will attempt to get you started on the foundations so you can easily go wherever you want afterwards.

There is somewhat of a chicken-and-egg problem in teaching programming, especially assembly language. There is a lot to learn - it is almost too much to learn almost at all at once. However, each piece depends on all the others, which makes learning it a piece at a time difficult. Therefore, you must be patient with yourself and the computer while learning to program. If you don't understand something the first time, reread it. If you still don't understand it, it is sometimes best to take it by faith and come back to it later. Often after more exposure to programming the ideas will make more sense. Don't get discouraged. It's a long climb, but very worthwhile.

At the end of each chapter are three sets of review exercises. The first set is more or less regurgitation - they check to see if can you give back what you learned in the chapter. The second set contains application questions - they check to see if you can apply what you learned to solve problems. The final set is to see if you are capable of broadening your horizons. Some of these questions may not be answerable until later in the book, but they give you some things to think about. Other questions require some research into outside sources to discover the answer. Still others require you to simply analyze your options and explain the best solution. Many of the questions don't have right or wrong answers, but that doesn't mean they are unimportant. Learning the issues involved in programming, learning how to research answers, and learning how to look ahead are all a major part of a programmer's work.

If you have problems that you just can't get past, there is a mailing list for this book where readers can discuss and get help with what they are reading. The address is `pgubook-readers@nongnu.org`. This mailing list is open for any type of question or discussion along the lines of this book. You can subscribe to this list by going to https://lists.nongnu.org/mailman/listinfo/pgubook-readers.

If you are thinking of using this book for a class on computer programming but do not have access to Linux computers for your students, I highly suggest you try to find help from the K-12 Linux Project. Their website is at K12 Linux and they have a helpful and responsive mailing list available.

1.2 Your Tools

This book teaches assembly language for x86 processors and the GNU/Linux operating system. Therefore we will be giving all of the examples using the GNU/Linux standard GCC tool set. If you are not familiar with GNU/Linux and the GCC tool set, they will be described shortly. If you are new to Linux, you should check out the guide available at TutorialsPoint.[1] What I intend to show you is more about programming in general than using a specific tool set on a specific platform, but standardizing on one makes the task much easier.

Those new to Linux should also try to get involved in the GNU/Linux Forums.

All of these programs have been tested using *Arch Linux v2020.11.01*, and should work with any other GNU/Linux distribution, too.[2] They will not work with non-Linux operating systems such as BSD or other systems. However, all of the *skills* learned in this book should be easily transferable to any other system.

If you do not have access to a GNU/Linux machine, you can look for a hosting provider who offers a Linux *shell account*, which is a command-line only interface to a Linux machine. There are many low-cost shell account providers, but you have to make sure that they match the requirements above (i.e. - Linux on x86). Shell accounts only require that you already have an Internet connection and a telnet program. If you use Windows®, you already have a telnet client - just click on `start`, then `run`, then type in `telnet`. However, it is usually better to download PuTTY because Windows' telnet has some weird problems. There are a lot of options for the Macintosh, too. *NiftyTelnet* is my favorite.

If you don't have GNU/Linux and can't find a shell account service, then you can download Knoppix. *Knoppix* is a GNU/Linux distribution that boots from CD so that you don't have to actually install it. Once you are done using it, you just reboot and remove the CD and you are back to your regular operating system.

So what is GNU/Linux? GNU/Linux is an operating system modeled after UNIX®. The GNU part comes from the GNU Project,[3] which includes most of the programs you will run, including the GCC tool set that we will use to program with. The GCC tool set contains all of the programs necessary to create programs in various computer languages.

Linux is the name of the *kernel*. The kernel is the core part of an operating system that keeps track of everything. The kernel is both a fence and a gate. As a gate, it allows programs to access hardware in a uniform way. Without the kernel, you would have to write programs to deal with every device model ever made. The kernel handles all device-specific interactions so you don't have to. It also handles file access and interaction between processes. For example, when you type, your typing goes through several programs before it hits your editor. First, the kernel is what handles your hardware, so it is the first to receive notice about the keypress. The keyboard sends in *scancodes* to the kernel, which then converts them to the actual letters, numbers, and symbols they represent. If you are using a windowing system (like Microsoft Windows® or the X Window System), then the windowing system reads the keypress from the kernel, and delivers it to whatever program is currently in focus on the user's display.

Example 1-1. How the computer processes keyboard signals

```
Keyboard -> Kernel -> Windowing system -> Application program
```

The kernel also controls the flow of information between programs. The kernel is a program's gate to the world around it. Every time that data moves between processes, the kernel controls the messaging. In our

[1] This is quite a large document. You certainly don't need to know everything to get started with this book. You simply need to know how to navigate from the command line and how to use an editor like `pico`, `emacs`, or `vi` (or others).

[2] By "GNU/Linux distribution", I mean an x86 GNU/Linux distribution. GNU/Linux distributions for the Power Macintosh, the Alpha processor, or other processors will not work with this book.

[3] The GNU Project is a project by the Free Software Foundation to produce a complete, free operating system.

keyboard example above, the kernel would have to be involved for the windowing system to communicate the keypress to the application program.

As a fence, the kernel prevents programs from accidentally overwriting each other's data and from accessing files and devices that they don't have permission to. It limits the amount of damage a poorly-written program can do to other running programs.

In our case, the kernel is Linux. Now, the kernel all by itself won't do anything. You can't even boot up a computer with just a kernel. Think of the kernel as the water pipes for a house. Without the pipes, the faucets won't work, but the pipes are pretty useless if there are no faucets. Together, the user applications (from the GNU project and other places) and the kernel (Linux) make up the entire operating system, GNU/Linux.

For the most part, this book will be using the computer's low-level assembly language. There are essentially three kinds of languages:

Machine Language:
: This is what the computer actually sees and deals with. Every command the computer sees is given as a number or sequence of numbers.

Assembly Language:
: This is the same as machine language, except the command numbers have been replaced by letter sequences which are easier to memorize. Other small things are done to make it easier as well.

High-Level Languages:
: High-level languages are there to make programming easier. Assembly language requires you to work with the machine itself. High-level languages allow you to describe the program in a more natural language. A single command in a high-level language usually is equivalent to several commands in an assembly language.

In this book we will learn assembly language, although we will cover a bit of high-level languages. Hopefully by learning assembly language, your understanding of how programming and computers work will put you a step ahead.

2. Computer Architecture

Before learning how to program, you need to first understand how a computer interprets programs. You don't need a degree in electrical engineering, but you need to understand some basics.

Modern computer architecture is based off of an architecture called the Von Neumann architecture, named after its creator. The Von Neumann architecture divides the computer up into two main parts - the CPU (for Central Processing Unit) and the memory. This architecture is used in all modern computers, including personal computers, supercomputers, mainframes, and even cell phones.

2.1 Structure of Computer Memory

To understand how the computer views memory, imagine your local post office. They usually have a room filled with PO Boxes. These boxes are similar to computer memory in that each are numbered sequences of fixed-size storage locations. For example, if you have 256 megabytes of computer memory, that means that your computer contains roughly 256 million fixed-size storage locations. Or, to use our analogy, 256 million PO Boxes. Each location has a number, and each location has the same, fixed-length size. The difference between a PO Box and computer memory is that you can store all different kinds of things in a PO Box, but you can only store a single number in a computer memory storage location.

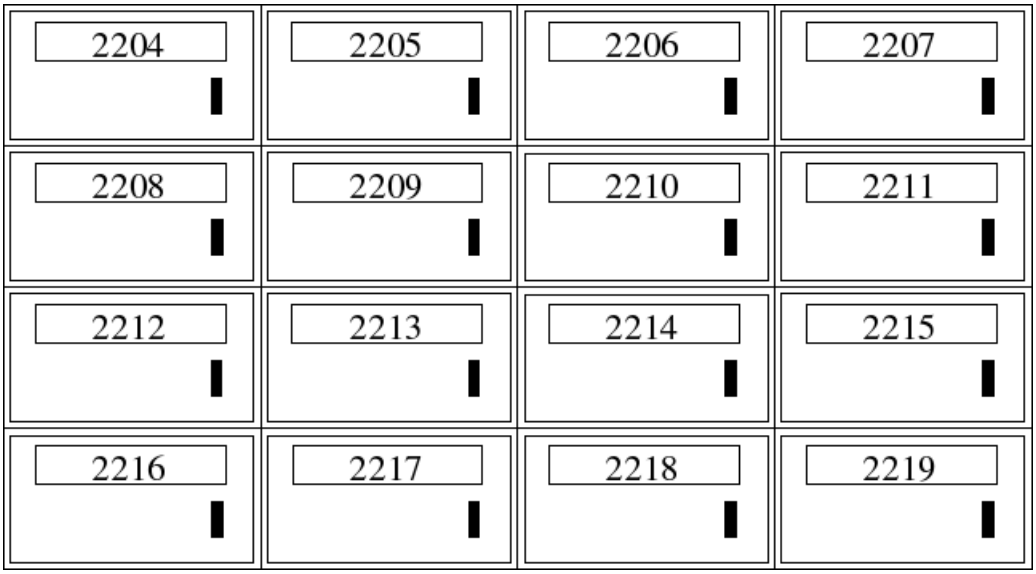

Figure 2.1: *Memory locations are like PO Boxes*

You may wonder why a computer is organized this way. It is because it is simple to implement. If the computer were composed of a lot of differently-sized locations, or if you could store different kinds of data in them, it would be difficult and expensive to implement.

The computer's memory is used for a number of different things. All of the results of any calculations are stored in memory. In fact, everything that is "stored" is stored in memory. Think of your computer at home, and imagine what all is stored in your computer's memory.

- The location of your cursor on the screen.

- The size of each window on the screen.
- The shape of each letter of each font being used.
- The layout of all of the controls on each window.
- The graphics for all of the toolbar icons.
- The text for each error message and dialog box.
- The list goes on and on...

In addition to all of this, the Von Neumann architecture specifies that not only computer data should live in memory, but the programs that control the computer's operation should live there, too. In fact, in a computer, there is no difference between a program and a program's data except how it is used by the computer. They are both stored and accessed the same way.

2.2 The CPU

So how does the computer function? Obviously, simply storing data doesn't do much help - you need to be able to access, manipulate, and move it. That's where the CPU comes in.

The CPU reads in instructions from memory one at a time and executes them. This is known as the *fetch-execute cycle*. The CPU contains the following elements to accomplish this:

- Program Counter.
- Instruction Decoder.
- Data bus.
- General-purpose registers.
- Arithmetic and logic unit.

The *program counter* is used to tell the computer where to fetch the next instruction from. We mentioned earlier that there is no difference between the way data and programs are stored, they are just interpreted differently by the CPU. The program counter holds the memory address of the next instruction to be executed. The CPU begins by looking at the program counter, and fetching whatever number is stored in memory at the location specified. It is then passed on to the *instruction decoder* which figures out what the instruction means. This includes what process needs to take place (addition, subtraction, multiplication, data movement, etc.) and what memory locations are going to be involved in this process. Computer instructions usually consist of both the actual instruction and the list of memory locations that are used to carry it out.

Now the computer uses the *data bus* to fetch the memory locations to be used in the calculation. The data bus is the connection between the CPU and memory. It is the actual wire that connects them. If you look at the motherboard of the computer, the wires that go out from the memory are your data bus.

In addition to the memory on the outside of the processor, the processor itself has some special, high-speed memory locations called registers. There are two kinds of registers - *general registers* and *special-purpose registers*. General-purpose registers are where the main action happens. Addition, subtraction, multiplication, comparisons, and other operations generally use general-purpose registers for processing. However, computers have very few general-purpose registers. Most information is stored in main memory, brought in to the registers for processing, and then put back into memory when the processing is completed. *special-purpose registers* are registers which have very specific purposes. We will discuss these as we come to them.

Now that the CPU has retrieved all of the data it needs, it passes on the data and the decoded instruction to the *arithmetic and logic unit* for further processing. Here the instruction is actually executed. After the results of the computation have been calculated, the results are then placed on the data bus and sent to the appropriate location in memory or in a register, as specified by the instruction.

This is a very simplified explanation. Processors have advanced quite a bit in recent years, and are now much more complex. Although the basic operation is still the same, it is complicated by the use of cache hierarchies, superscalar processors, pipelining, branch prediction, out-of-order execution, microcode translation, coprocessors, and other optimizations. Don't worry if you don't know what those words mean, you can just use them as Internet search terms if you want to learn more about the CPU.

2.3 Some Terms

Computer memory is a numbered sequence of fixed-size storage locations. The number attached to each storage location is called its *address*. The size of a single storage location is called a *byte*. On x86 processors, a byte is a number between 0 and 255.

You may be wondering how computers can display and use text, graphics, and even large numbers when all they can do is store numbers between 0 and 255. First of all, specialized hardware like graphics cards have special interpretations of each number. When displaying to the screen, the computer uses ASCII code tables to translate the numbers you are sending it into letters to display on the screen, with each number translating to exactly one letter or numeral.[4] For example, the capital letter A is represented by the number 65. The numeral 1 is represented by the number 49. So, to print out "HELLO", you would actually give the computer the sequence of numbers 72, 69, 76, 76, 79. To print out the number 100, you would give the computer the sequence of numbers 49, 48, 48. A list of ASCII characters and their numeric codes is found in the Appendix D. Table of ASCII Codes.

In addition to using numbers to represent ASCII characters, you as the programmer get to make the numbers mean anything you want them to, as well. For example, if I am running a store, I would use a number to represent each item I was selling. Each number would be linked to a series of other numbers which would be the ASCII codes for what I wanted to display when the items were scanned in. I would have more numbers for the price, how many I have in inventory, and so on.

So what about if we need numbers larger than 255? We can simply use a combination of bytes to represent larger numbers. Two bytes can be used to represent any number between 0 and 65535. Four bytes can be used to represent any number between 0 and 4294967295. Now, it is quite difficult to write programs to stick bytes together to increase the size of your numbers, and requires a bit of math. Luckily, the computer will do it for us for numbers up to 4 bytes long. In fact, four-byte numbers are what we will work with by default.

We mentioned earlier that in addition to the regular memory that the computer has, it also has special-purpose storage locations called *registers*. Registers are what the computer uses for computation. Think of a register as a place on your desk - it holds things you are currently working on. You may have lots of information tucked away in folders and drawers, but the stuff you are working on right now is on the desk. Registers keep the contents of numbers that you are currently manipulating.

On the computers we are using, registers are each four bytes long. The size of a typical register is called a computer's *word* size. x86 processors have four-byte words. This means that it is most natural on these computers to do computations four bytes at a time.[5] This gives us roughly 4 billion values.

Addresses are also four bytes (1 word) long, and therefore also fit into a register. x86 processors can access up to 4294967296 bytes if enough memory is installed. Notice that this means that we can store addresses the same way we store any other number. In fact, the computer can't tell the difference between a value that is an address, a value that is a number, a value that is an ASCII code, or a value that you have decided to use for another purpose. A number becomes an ASCII code when you attempt to display it. A number becomes an address when you try to look up the byte it points to. Take a moment to think about this, because it is crucial to understanding how computer programs work.

Addresses which are stored in memory are also called *pointers*, because instead of having a regular value in them, they point you to a different location in memory.

As we've mentioned, computer instructions are also stored in memory. In fact, they are stored exactly the same way that other data is stored. The only way the computer knows that a memory location is an instruction is that a special-purpose register called the instruction pointer points to them at one point or another. If the instruction pointer points to a memory word, it is loaded as an instruction. Other than that, the computer has no way of knowing the difference between programs and other types of data.[6]

[4] With the advent of international character sets and Unicode, this is not entirely true anymore. However, for the purposes of keeping this simple for beginners, we will use the assumption that one number translates directly to one character. For more information, see the Appendix D. Table of ASCII Codes.

[5] Previous incarnations of x86 processors only had two-byte words. Therefore, most other literature dealing with x86 processors refers to two-byte entities as words for historical reasons, and therefore refer to four-byte entities as double-words. We are using the term *word* to mean the normal register size of a computer, which in this case is four bytes. More information is available in Appendix B. Common x86 Instructions.

[6] Note that here we are talking about general computer theory. Some processors and operating systems actually mark the regions of memory that can be executed with a special marker that indicates this.

2.4 Interpreting Memory

Computers are very exact. Because they are exact, programmers have to be equally exact. A computer has no idea what your program is supposed to do. Therefore, it will only do exactly what you tell it to do. If you accidentally print out a regular number instead of the ASCII codes that make up the number's digits, the computer will let you - and you will wind up with gibberish on your screen (it will try to look up what your number represents in ASCII and print that). If you tell the computer to start executing instructions at a location containing data instead of program instructions, who knows how the computer will interpret that - but it will certainly try. The computer will execute your instructions in the exact order you specify, even if it doesn't make sense.

The point is, the computer will do exactly what you tell it, no matter how little sense it makes. Therefore, as a programmer, you need to know exactly how you have your data arranged in memory. Remember, computers can only store numbers, so letters, pictures, music, web pages, documents, and anything else are just long sequences of numbers in the computer, which particular programs know how to interpret.

For example, say that you wanted to store customer information in memory. One way to do so would be to set a maximum size for the customer's name and address - say 50 ASCII characters for each, which would be 50 bytes for each. Then, after that, have a number for the customer's age and their customer id. In this case, you would have a block of memory that would look like this:

```
Start of Record:
     Customer's name (50 bytes) - start of record
     Customer's address (50 bytes) - start of record + 50 bytes
     Customer's age (1 word = 4 bytes) - start of record + 100 bytes
     Customer's id number (1 word = 4 bytes) - start of record + 104 bytes
```

This way, given the address of a customer record, you know where the rest of the data lies. However, it does limit the customer's name and address to only 50 ASCII characters each.

What if we didn't want to specify a limit? Another way to do this would be to have in our record pointers to this information. For example, instead of the customer's name, we would have a pointer to their name. In this case, the memory would look like this:

```
Start of Record:
     Customer's name pointer (1 word) - start of record
     Customer's address pointer (1 word) - start of record + 4
     Customer's age (1 word) - start of record + 8
     Customer's id number (1 word) - start of record + 12
```

The actual name and address would be stored elsewhere in memory. This way, it is easy to tell where each part of the data is from the start of the record, without explicitly limiting the size of the name and address. If the length of the fields within our records could change, we would have no idea where the next field started. Because records would be different sizes, it would also be hard to find where the next record began. Therefore, almost all records are of fixed lengths. Variable-length data is usually stored separately from the rest of the record.

2.5 Data Accessing Methods

This is a quick review try to focus in understand the big picture of the accessing methods the next chapter will explain in detail everyone with examples.

Processors have a number of different ways of accessing data, known as addressing modes. The simplest mode is *immediate mode addressing*, in which the data to access is embedded in the instruction itself. For example, if we want to initialize a register to 0, instead of giving the computer an address to read the 0 from, we would specify immediate mode, and give it the number 0.

In the *register addressing mode*, the instruction contains a register to access, rather than a memory location. The rest of the modes will deal with addresses.

In the *direct addressing mode*, the instruction contains the memory address to access. For example, I could say, please load this register with the data at address 2002. The computer would go directly to byte number 2002 and copy the contents into our register.

In the *indexed addressing mode*, the instruction contains a memory address to access, and also specifies an *index register* to offset that address. For example, we could specify address 2002 and an index register. If the index register contains the number 4, the actual address the data is loaded from would be 2006. This way, if you have a set of numbers starting at location 2002, you can cycle between each of them using an index register. On x86 processors, you can also specify a *multiplier* for the index. This allows you to access memory a byte at a time or a word at a time (4 bytes). If you are accessing an entire word, your index will need to be multiplied by 4 to get the exact location of the fourth element from your address. For example, if you wanted to access the fourth byte from location 2002, you would load your index register with 3 (remember, we start counting at 0) and set the multiplier to 1 since you are going a byte at a time. This would get you location 2005. However, if you wanted to access the fourth word from location 2002, you would load your index register with 3 and set the multiplier to 4. This would load from location 2014 - the fourth word. Take the time to calculate these yourself to make sure you understand how it works.

In the *indirect addressing mode*, the instruction contains a register that contains a pointer to where the data should be accessed. For example, if we used indirect addressing mode and specified the *%eax* register, and the *%eax* register contained the value 4, whatever value was at memory location 4 would be used. In direct addressing, we would just load the value 4, but in indirect addressing, we use 4 as the address to use to find the data we want.

Finally, there is the *base pointer addressing mode*. This is similar to indirect addressing, but you also include a number called the *offset* to add to the register's value before using it for lookup. We will use this mode quite a bit in this book.

In Interpreting Memory we discussed having a structure in memory holding customer information. Let's say we wanted to access the customer's age, which was the eighth byte of the data, and we had the address of the start of the structure in a register. We could use base pointer addressing and specify the register as the base pointer, and 8 as our offset. This is a lot like indexed addressing, with the difference that the offset is constant and the pointer is held in a register, and in indexed addressing the offset is in a register and the pointer is constant.

There are other forms of addressing, but these are the most important ones.

2.6 Review

2.6.1 Know the Concepts

- Describe the fetch-execute cycle.
- What is a register? How would computation be more difficult without registers?
- How do you represent numbers larger than 255?
- How big are the registers on the machines we will be using?
- How does a computer know how to interpret a given byte or set of bytes of memory?
- What are the addressing modes and what are they used for?
- What does the instruction pointer do?

2.6.2 Use the Concepts

- What data would you use in an employee record? How would you lay it out in memory?
- If I had the pointer to the beginning of the employee record above, and wanted to access a particular piece of data inside of it, what addressing mode would I use?
- In base pointer addressing mode, if you have a register holding the value 3122, and an offset of 20, what address would you be trying to access?

- In indexed addressing mode, if the base address is 6512, the index register has a 5, and the multiplier is 4, what address would you be trying to access?
- In indexed addressing mode, if the base address is 123472, the index register has a 0, and the multiplier is 4, what address would you be trying to access?
- In indexed addressing mode, if the base address is 9123478, the index register has a 20, and the multiplier is 1, what address would you be trying to access?

2.6.3 Going Further

- What are the minimum number of addressing modes needed for computation?
- Why include addressing modes that aren't strictly needed?
- Research and then describe how pipelining (or one of the other complicating factors) affects the fetch-execute cycle.
- Research and then describe the tradeoffs between fixed-length instructions and variable-length instructions.

3. Your First Programs

In this chapter you will learn the process for writing and building Linux assembly-language programs. In addition, you will learn the structure of assembly-language programs, and a few assembly-language commands. As you go through this chapter, you may want to refer also to Appendix B. Common x86 Instructions and Appendix F. Using the GDB Debugger.

These programs may overwhelm you at first. However, go through them with diligence, read them and their explanations as many times as necessary, and you will have a solid foundation of knowledge to build on. Please tinker around with the programs as much as you can. Even if your tinkering does not work, every failure will help you learn.

3.1 Entering in the Program

Okay, this first program is simple. In fact, it's not going to do anything but exit! It's short, but it shows some basics about assembly language and Linux programming. You need to enter the program in an editor exactly as written, with the filename `003-01-exit.s`. The program follows. Don't worry about not understanding it. This section only deals with typing it in and running it. In Outline of an Assembly Language Program we will describe how it works.

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:    Simple program that exits and returns
4       #             a status code back to the Linux
5       #             kernel.
6       #
7       # INPUT:      None.
8       #
9       # OUTPUT:     Returns a status code.  This can be
10      #             viewed by typing `echo $?` after
11      #             running the program.
12      #
13      # VARIABLES:
14      #             %eax holds the system call number.
15      #             %ebx holds the return status .
16      #
17      .section .data
18
19      .section .text
20          .globl _start
21
22  _start:
23      movl $1, %eax       # This is the Linux kernel
24                          # command number (system call)
25                          # for exiting a program.
26
27      movl $0, %ebx       # This is the status number we
28                          # will return to the operating
29                          # system. Change this around and
30                          # it will return different
```

```
31                          # things to `echo $?`.
32
33      int $0x80           # This wakes up the kernel to
34                          # run the exit command.
```

What you have typed in is called the *source code*. Source code is the human-readable form of a program. In order to transform it into a program that a computer can run, we need to *assemble* and *link* it.

The first step is to *assemble* it. Assembling is the process that transforms what you typed into instructions for the machine. The machine itself only reads sets of numbers, but humans prefer words. An *assembly language* is a more human-readable form of the instructions a computer understands. Assembling transforms the human-readable file into a machine-readable one. To assembly the program type in the command:

```
as -o 003-01-exit.o  --32 \
                     --gstabs+ \
                     003-01-exit.s
```

`as` is the command which runs the assembler, `003-01-exit.s` is the source file, and `-o 003-01-exit.o` tells the assembler to put its output in the file `003-01-exit.o`. `003-01-exit.o` is an *object file*. An object file is code that is in the machine's language, but has not been completely put together. In most large programs, you will have several source files, and you will convert each one into an object file. The `--gstabs+` option, adds debugging information in the executable file, review more information in the Appendix F. Using the GDB Debugger.

The *linker* is the program that is responsible for putting the object files together and adding information to it so that the kernel knows how to load and run it. In our case, we only have one object file, so the linker is only adding the information to enable it to run. To *link* the file, enter the command:

```
ld -o 003-01-exit  -m elf_i386 \
                   003-01-exit.o
```

`ld` is the command to run the linker, `003-01-exit.o` is the object file we want to link, and `-o 003-01-exit` instructs the linker to output the new program into a file called `003-01-exit`.[7] If any of these commands reported errors, you have either mistyped your program or the command. After correcting the program, you have to re-run all the commands. *You must always re-assemble and re-link programs after you modify the source file for the changes to occur in the program.* You can run `003-01-exit` by typing in the command:

```
./003-01-exit
```

The `./` is used to tell the computer that the program isn't in one of the normal program directories, but is the current directory instead[8]. You'll notice when you type this command, the only thing that happens is that you'll go to the next line. That's because this program does nothing but exit. However, immediately after you run the program, if you type in:

```
echo $?
```

It will say `0`. What is happening is that every program when it exits gives Linux an *exit status code*, which tells it if everything went all right. If everything was okay, it returns 0. UNIX programs return numbers other than zero to indicate failure or other errors, warnings, or statuses. The programmer determines what each number means. You can view this code by typing in `echo $?`. In the following section we will look at what each part of the code does. More Information in GNU Automatic variables.

[7] If you are new to Linux and UNIX®, you may not be aware that files don't have to have extensions. In fact, while Windows® uses the `.exe` extension to signify an executable program, UNIX executables usually have no extension.

[8] `.` refers to the current directory in Linux and UNIX systems.

3.2 Outline of an Assembly Language Program

Take a look at the program we just entered. At the beginning there are lots of lines that begin with hashes (#). These are *comments*. Comments are not translated by the assembler. They are used only for the programmer to talk to anyone who looks at the code in the future. Most programs you write will be modified by others. Get into the habit of writing comments in your code that will help them understand both why the program exists and how it works. Always include the following in your comments:

- The purpose of the code.
- An overview of the processing involved.
- Anything strange your program does and why it does it.[9]

After the comments, the next line says:

```
17      .section .data
```

Anything starting with a period isn't directly translated into a machine instruction. Instead, it's an instruction to the assembler itself. These are called *assembler directives* or *pseudo-operations* because they are handled by the assembler and are not actually run by the computer. The `.section` command breaks your program up into sections. This command starts the data section, where you list any memory storage you will need for data. Our program doesn't use any, so we don't need the section. It's just here for completeness. Almost every program you write in the future will have data.

Right after this you have:

```
19      .section .text
```

`.text` which starts the text section. The text section of a program is where the program instructions live.

The next instruction is:

```
20          .globl _start
```

This instructs the assembler that `_start` is important to remember. `_start` is a *symbol*, which means that it is going to be replaced by something else either during assembly or linking. Symbols are generally used to mark locations of programs or data, so you can refer to them by name instead of by their location number. Imagine if you had to refer to every memory location by its address. First of all, it would be very confusing because you would have to memorize or look up the numeric memory address of every piece of code or data. In addition, every time you had to insert a piece of data or code you would have to change all the addresses in your program! Symbols are used so that the assembler and linker can take care of keeping track of addresses, and you can concentrate on writing your program.

`.globl` means that the assembler shouldn't discard this symbol after assembly, because the linker will need it. `_start` is a special symbol that always needs to be marked with `.globl` because it marks the location of the start of the program. *Without marking this location in this way, when the computer loads your program it won't know where to begin running your program.*

The next line:

```
22  _start:
```

defines the value of the `_start` label. A *label* is a symbol followed by a colon. Labels define a symbol's value. When the assembler is assembling the program, it has to assign each data value and instruction an address. Labels tell the assembler to make the symbol's value be wherever the next instruction or data element will be. This way, if the actual physical location of the data or instruction changes, you don't have to rewrite any references to it - the symbol automatically gets the new value.

[9] You'll find that many programs end up doing things strange ways. Usually there is a reason for that, but, unfortunately, programmers never document such things in their comments. So, future programmers either have to learn the reason the hard way by modifying the code and watching it break, or just leaving it alone whether it is still needed or not. You should *always* document any strange behavior your program performs. Unfortunately, figuring out what is strange and what is straightforward comes mostly with experience.

Now we get into actual computer instructions. The first such instruction is this:

```
23      movl $1, %eax      # This is the Linux kernel
24                         # command number (system call)
25                         # for exiting a program.
```

When the program runs, this instruction transfers the number `1` into the *%eax* register. In assembly language, many instructions have *operands*. `movl` has two operands - the *source* and the *destination*. In this case, the source is the literal number `1`, and the destination is the *%eax* register. Operands can be numbers, memory location references, or registers. Different instructions allow different types of operands. See Appendix B. Common x86 Instructions for more information on which instructions take which kinds of operands.

On most instructions which have two operands, the first one is the source operand and the second one is the destination. Note that in these cases, the source operand is not modified at all. Other instructions of this type are, for example, `addl`, `subl`, and `imull`. These add/subtract/multiply the source operand from/to/by the destination operand and save the result in the destination operand. Other instructions may have an operand hardcoded in. `idivl`, for example, requires that the dividend be in *%eax*, and *%edx* be zero, and the quotient is then transferred to *%eax* and the remainder to *%edx*. However, the divisor can be any register or memory location.

On x86 processors, there are several general-purpose registers[10] (all of which can be used with `movl`):

- *%eax*
- *%ebx*
- *%ecx*
- *%edx*
- *%edi*
- *%esi*

In addition to these general-purpose registers, there are also several special-purpose registers, including:

- *%ebp*
- *%esp*
- *%eip*
- *%eflags*

We'll discuss these later, just be aware that they exist.[11] Some of these registers, like *%eip* and *%eflags* can only be accessed through special instructions. The others can be accessed using the same instructions as general-purpose registers, but they have special meanings, special uses, or are simply faster when used in a specific way.

So, the `movl` instruction moves the number `1` into `%eax`. The dollar-sign in front of the one indicates that we want to use immediate mode addressing (refer back to Data Accessing Methods). Without the dollar-sign it would do direct addressing mode, loading whatever number is at address `1`. We want the actual number `1` loaded in, so we have to use immediate mode.

The reason we are moving the number 1 into *%eax* is because we are preparing to call the Linux Kernel. The number `1` is the number of the `exit` *system call*. We will discuss system calls in more depth soon, but basically they are requests for the operating system's help. Normal programs can't do everything. Many operations such as calling other programs, dealing with files, and exiting have to be handled by the operating system

[10] Note that on x86 processors, even the general-purpose registers have some special purposes, or used to before it went 32-bit. However, these are general-purpose registers for most instructions. Each of them has at least one instruction where it is used in a special way. However, for most of them, those instructions aren't covered in this book.

[11] You may be wondering, *why do all of these registers begin with the letter `e`?* The reason is that early generations of x86 processors were 16 bits rather than 32 bits. Therefore, the registers were only half the length they are now. In later generations of x86 processors, the size of the registers doubled. They kept the old names to refer to the first half of the register, and added an `e` to refer to the extended versions of the register. Usually you will only use the extended versions. Newer models also offer a 64-bit mode, which doubles the size of these registers yet again and uses an `r` prefix to indicate the larger registers (i.e. *%rax* is the 64-bit version of *%eax*). However, these processors are not widely used, and are not covered in this book.

through system calls. When you make a system call, which we will do shortly, the system call number has to be loaded into *%eax* (for a complete listing of system calls and their numbers, see Appendix C. Important System Calls). Depending on the system call, other registers may have to have values in them as well. Note that system calls is not the only use or even the main use of registers. It is just the one we are dealing with in this first program. Later programs will use registers for regular computation.

The operating system, however, usually needs more information than just which call to make. For example, when dealing with files, the operating system needs to know which file you are dealing with, what data you want to write, and other details. The extra details, called *parameters* are stored in other registers. In the case of the `exit` system call, the operating system requires a status code be loaded in *%ebx*. This value is then returned to the system. This is the value you retrieved when you typed `echo $?`. So, we load *%ebx* with `0` by typing the following:

```
27      movl $0, %ebx       # This is the status number we
28                          # will return to the operating
29                          # system. Change this around and
30                          # it will return different
31                          # things to `echo $?`.
```

Now, loading registers with these numbers doesn't do anything itself. Registers are used for all sorts of things besides system calls. They are where all program logic such as addition, subtraction, and comparisons take place. Linux simply requires that certain registers be loaded with certain parameter values before making a system call. *%eax* is always required to be loaded with the system call number. For the other registers, however, each system call has different requirements. In the `exit` system call, *%ebx* is required to be loaded with the exit status code. We will discuss different system calls as they are needed. For a list of common system calls and what is required to be in each register, see Appendix C. Important System Calls.

The next instruction is the "magic" one. It looks like this:

```
33      int $0x80           # This wakes up the kernel to
34                          # run the exit command.
```

The `int` stands for *interrupt*. The `0x80` is the interrupt number to use.[12] An *interrupt* interrupts the normal program flow, and transfers control from our program to Linux so that it will do a system call.[13]. You can think of it as like signaling Batman (or Larry-Boy[14], if you prefer). You need something done, you send the signal, and then he comes to the rescue. You don't care how he does his work - it's more or less magic - and when he's done you're back in control. In this case, all we're doing is asking Linux to terminate the program, in which case we won't be back in control. If we didn't signal the interrupt, then no system call would have been performed.

NOTE.

Quick System Call Review: To recap - Operating System features are accessed through system calls. These are invoked by setting up the registers in a special way and issuing the instruction `int $0x80`. Linux knows which system call we want to access by what we stored in the *%eax* register. Each system call has other requirements as to what needs to be stored in the other registers. System call number 1 is the `exit` system call, which requires the status code to be placed in *%ebx*.

Now that you've assembled, linked, run, and examined the program, you should make some basic edits. Do things like change the number that is loaded into `%ebx`, and watch it come out at the end with `echo $?`. Don't

[12] You may be wondering why it's `0x80` instead of just `80`. The reason is that the number is written in hexadecimal. In hexadecimal, a single digit can hold 16 values instead of the normal 10. This is done by utilizing the letters `a` through `f` in addition to the regular digits. `a` represents 10, `b` represents 11, and so on. 0x10 represents the number 16, and so on. This will be discussed more in depth later, but just be aware that numbers starting with `0x` are in hexadecimal. Tacking on an `H` at the end is also sometimes used instead, but we won't do that in this book. For more information about this, see Chapter 10. Counting Like a Computer

[13] Actually, the interrupt transfers control to whoever set up an *interrupt handler* for the interrupt number. In the case of Linux, all of them are set to be handled by the Linux kernel.

[14] If you don't watch Veggie Tales, you should. Start with Dave and the Giant Pickle.

forget to assemble and link it again before running it. Add some comments. Don't worry, the worse thing that would happen is that the program won't assemble or link, or will freeze your screen. That's just part of learning!

3.3 Planning the Program

In our next program we will try to find the maximum of a list of numbers. Computers are very detail-oriented, so in order to write the program we will have to have planned out a number of details. These details include:

- Where will the original list of numbers be stored?
- What procedure will we need to follow to find the maximum number?
- How much storage do we need to carry out that procedure?
- Will all of the storage fit into registers, or do we need to use some memory as well?

You might not think that something as simple as finding the maximum number from a list would take much planning. You can usually tell people to find the maximum number, and they can do so with little trouble. However, our minds are used to putting together complex tasks automatically. Computers need to be instructed through the process. In addition, we can usually hold any number of things in our mind without much trouble. We usually don't even realize we are doing it. For example, if you scan a list of numbers for the maximum, you will probably keep in mind both the highest number you've seen so far, and where you are in the list. While your mind does this automatically, with computers you have to explicitly set up storage for holding the current position on the list and the current maximum number. You also have other problems such as how to know when to stop. When reading a piece of paper, you can stop when you run out of numbers. However, the computer only contains numbers, so it has no idea when it has reached the last of *your* numbers.

In computers, you have to plan every step of the way. So, let's do a little planning. First of all, just for reference, let's name the address where the list of numbers starts as `data_items`. Let's say that the last number in the list will be a zero, so we know where to stop. We also need a value to hold the current position in the list, a value to hold the current list element being examined, and the current highest value on the list. Let's assign each of these a register:

- *%edi* will hold the current position in the list.
- *%ebx* will hold the current highest value in the list.
- *%eax* will hold the current element being examined.

When we begin the program and look at the first item in the list, since we haven't seen any other items, that item will automatically be the current largest element in the list. Also, we will set the current position in the list to be zero - the first element. From then, we will follow the following steps:

1. Check the current list element (*%eax*) to see if it's zero (the terminating element).
2. If it is zero, exit.
3. Increase the current position (*%edi*).
4. Load the next value in the list into the current value register (*%eax*). What addressing mode might we use here? Why?
5. Compare the current value (*%eax*) with the current highest value (*%ebx*).
6. If the current value is greater than the current highest value, replace the current highest value with the current value.
7. Repeat.

That is the procedure. Many times in that procedure I made use of the word "if". These places are where decisions are to be made. You see, the computer doesn't follow the exact same sequence of instructions every time. Depending on which "if"s are correct, the computer may follow a different set of instructions. The second time through, it might not have the highest value. In that case, it will skip step 6, but come back to step 7. In

every case except the last one, it will skip step 2. In more complicated programs, the skipping around increases dramatically.

These "if"s are a class of instructions called *flow control* instructions, because they tell the computer which steps to follow and which paths to take. In the previous program, we did not have any flow control instructions, as there was only one possible path to take - exit. This program is much more dynamic in that it is directed by data. Depending on what data it receives, it will follow different instruction paths.

In this program, this will be accomplished by two different instructions, the conditional jump and the unconditional jump. The conditional jump changes paths based on the results of a previous comparison or calculation. The unconditional jump just goes directly to a different path no matter what. The unconditional jump may seem useless, but it is very necessary since all of the instructions will be laid out on a line. If a path needs to converge back to the main path, it will have to do this by an unconditional jump. We will see more of both of these jumps in the next section.

Another use of flow control is in implementing loops. A loop is a piece of program code that is meant to be repeated. In our example, the first part of the program (setting the current position to 0 and loading the current highest value with the current value) was only done once, so it wasn't a loop. However, the next part is repeated over and over again for every number in the list. It is only left when we have come to the last element, indicated by a zero. This is called a *loop* because it occurs over and over again. It is implemented by doing unconditional jumps to the beginning of the loop at the end of the loop, which causes it to start over. However, you have to always remember to have a conditional jump to exit the loop somewhere, or the loop will continue forever! This condition is called an *infinite loop*. If we accidentally left out step 1, 2, or 3, the loop (and our program) would never end.

In the next section, we will implement this program that we have planned. Program planning sounds complicated - and it is, to some degree. When you first start programming, it's often hard to convert our normal thought process into a procedure that the computer can understand. We often forget the number of "temporary storage locations" that our minds are using to process problems. As you read and write programs, however, this will eventually become very natural to you. Just have patience.

3.4 Finding a Maximum Value

Enter the following program as `003-02-maximum.s`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     This program finds the maximum number of a
5       #     set of data items.
6       #
7       # VARIABLES:
8       #     The registers have the following uses:
9       #       %edi - Holds the index of the data item
10      #       being examined.
11      #       %ebx - Largest data item found.
12      #       %eax - Current data item.
13      #
14      # The following memory locations are used:
15      #     data_items - contains the item data.  A 0 is
16      #                  used to terminate the data.
17      #
18      .section .data
19          data_items:         # These are the data items.
20              .long 3, 67, 34, 222, 45, 22, 11, 125, 0
21
22      .section .text
23          .globl _start
```

```
24
25  _start:
26      movl $0, %edi           # Move 0 into the index
27                              # register.
28      movl data_items(,%edi,4), %eax  # Load the first
29                                      # byte of data.
30      movl %eax, %ebx         # Since this is the first
31                              # item, %eax is the biggest
32
33  _start_loop:                # Start loop.
34      cmpl $0, %eax           # Check to see if we have
35      je _loop_exit           # hit the end.
36      incl %edi               # Increment %edi by 1.
37      movl data_items(,%edi,4), %eax   # Load next value.
38      cmpl %ebx, %eax         # Compare values.
39      jle _start_loop         # Jump to loop beginning if
40                              # the new one is not bigger
41      movl %eax, %ebx         # Move the value as the
42                              # largest.
43      jmp _start_loop         # Jump to loop beginning.
44
45  _loop_exit:
46                              # %ebx is the status code
47                              # for the exit systemcall
48          movl $1, %eax       # and it already has the
49          int  $0x80          # maximum number 1 is the
50                              # exit() syscall.
```

Now, assemble and link it with these commands:

```
as -o 003-02-maximum.o  --32 \
                        --gstabs+ \
                        003-02-maximum.s

ld -o 003-02-maximum    -m elf_i386 \
                        003-02-maximum.o
```

Now run it, and check its status.

```
./003-02-maximum
echo $?
```

You'll notice it returns the value 222. Let's take a look at the program and what it does. If you look in the comments, you'll see that the program finds the maximum of a set of numbers (aren't comments wonderful!). You may also notice that in this program we actually have something in the data section. These lines are the data section:

```
19          data_items:         # These are the data items.
20              .long 3, 67, 34, 222, 45, 22, 11, 125, 0
```

Let's look at this. `data_items` is a label that refers to the location that follows it. Then, there is a directive that starts with `.long`. That causes the assembler to reserve memory for the list of numbers that follow it. `data_items` refers to the location of the first one. Because `data_items` is a label, any time in our program where we need to refer to this address we can use the `data_items` symbol, and the assembler will substitute it with the address where the numbers start during assembly. For example, the instruction `movl data_items, %eax` would move the value 3 into *%eax*. There are several different types of memory locations other than `.long` that can be reserved. The main ones are as follows:

`.byte`:
Bytes take up one storage location for each number. They are limited to numbers between 0 and 255.

`.int`:
Ints (which differ from the `int` instruction) take up two storage locations for each number. These are limited to numbers between 0 and 65535.[15]

`.long`:
Longs take up four storage locations. This is the same amount of space the registers use, which is why they are used in this program. They can hold numbers between 0 and 4294967295.

`.ascii`:
The `.ascii` directive is to enter in characters into memory. Characters each take up one storage location (they are converted into bytes internally). So, if you gave the directive `.ascii "Hello there\0"`, the assembler would reserve 12 storage locations (bytes). The first byte contains the numeric code for `H`, the second byte contains the numeric code for `e`, and so forth. The last character is represented by `\0`, and it is the terminating character (it will never display, it just tells other parts of the program that that's the end of the characters). Letters and numbers that start with a backslash represent characters that are not typeable on the keyboard or easily viewable on the screen. For example, `\n` refers to the "newline" character which causes the computer to start output on the next line and `\t` refers to the "tab" character. All of the letters in an `.ascii` directive should be in quotes.

In our example, the assembler reserves 14 `.long`s, one right after another. Since each long takes up 4 bytes, that means that the whole list takes up 56 bytes. These are the numbers we will be searching through to find the maximum. `data_items` is used by the assembler to refer to the address of the first of these values.

Take note that the last data item in the list is a zero. I decided to use a zero to tell my program that it has hit the end of the list. I could have done this other ways. I could have had the size of the list hard-coded into the program. Also, I could have put the length of the list as the first item, or in a separate location. I also could have made a symbol which marked the last location of the list items. No matter how I do it, I must have some method of determining the end of the list. The computer knows nothing - it can only do what it is told. It's not going to stop processing unless I give it some sort of signal. Otherwise it would continue processing past the end of the list into the data that follows it, and even to locations where we haven't put any data.

Notice that we don't have a `.globl` declaration for `data_items`. This is because we only refer to these locations within the program. No other file or program needs to know where they are located. This is in contrast to the `_start` symbol, which Linux needs to know where it is so that it knows where to begin the program's execution. It's not an error to write `.globl data_items`, it's just not necessary. Anyway, play around with this line and add your own numbers. Even though they are `.long`, the program will produce strange results if any number is greater than 255, because that's the largest allowed exit status code. Also notice that if you move the 0 to earlier in the list, the rest get ignored. *Remember that any time you change the source file, you have to re-assemble and re-link your program. Do this now and see the results.*

All right, we've played with the data a little bit. Now let's look at the code. In the comments you will notice that we've marked some *variables* that we plan to use. A variable is a dedicated storage location used for a specific purpose, usually given a distinct name by the programmer. We talked about these in the previous section, but didn't give them a name. In this program, we have several variables:

- A variable for the current maximum number found.
- A variable for which number of the list we are currently examining, called the index.
- A variable holding the current number being examined.

In this case,we have few enough variables that we can hold them all in registers. In larger programs, you have to put them in memory, and then move them to registers when you are ready to use them. We will discuss how to do that later. When people start out programming, they usually underestimate the number of variables they will need. People are not used to having to think through every detail of a process, and therefore leave out needed variables in their first programming attempts.

In this program, we are using *%ebx* as the location of the largest item we've found. *%edi* is used as the *index* to the current data item we're looking at. Now, let's talk about what an index is. When we read the information from `data_items`, we will start with the first one (data item number 0), then go to the second one (data item

[15]Note that no numbers in assembly language (or any other computer language I've seen) have commas embedded in them. So, always write numbers like `65535`, and never like `65,535`.

number 1), then the third (data item number 2), and so on. The data item number is the *index* of `data_items`. You'll notice that the first instruction we give to the computer is:

```
26      movl $0, %edi           # Move 0 into the index
27                              # register.
```

Since we are using `%edi` as our index, and we want to start looking at the first item, we load `%edi` with 0. Now, the next instruction is tricky, but crucial to what we're doing. It says:

```
28      movl data_items(,%edi,4), %eax  # Load the first
29                                      # byte of data.
```

Now to understand this line, you need to keep several things in mind:

- `data_items` is the location number of the start of our number list.
- Each number is stored across 4 storage locations (because we declared it using `.long`).
- `%edi` is holding 0 at this point.

So, basically what this line does is say, "start at the beginning of data_items, and take the first item number (because `%edi` is 0), and remember that each number takes up four storage locations." Then it stores that number in `%eax`. This is how you write indexed addressing mode instructions in assembly language. The instruction in a general form is this:

```
movl BEGINNINGADDRESS(, %INDEXREGISTER, WORDSIZE)
```

In our case `data_items` was our beginning address, *%edi* was our index register, and 4 was our word size. This topic is discussed further in Addressing Modes.

If you look at the numbers in `data_items`, you will see that the number 3 is now in *%eax*. If *%edi* was set to 1, the number 67 would be in *%eax*, and if it was set to 2, the number 34 would be in *%eax*, and so forth. Very strange things would happen if we used a number other than 4 as the size of our storage locations.[16] The way you write this is very awkward, but if you know what each piece does, it's not too difficult. For more information about this, see Addressing Modes.

Let's look at the next line:

```
30      movl %eax, %ebx         # Since this is the first
31                              # item, %eax is the biggest
```

We have the first item to look at stored in `%eax`. Since it is the first item, we know it's the biggest one we've looked at. We store it in `%ebx`, since that's where we are keeping the largest number found. Also, even though `movl` stands for *move*, it actually copies the value, so `%eax` and `%ebx` both contain the starting value.[17]

Now we move into a *loop*. A loop is a segment of your program that might run more than once. We have marked the starting location of the loop in the symbol `_start_loop`. The reason we are doing a loop is because we don't know how many data items we have to process, but the procedure will be the same no matter how many there are. We don't want to have to rewrite our program for every list length possible. In fact, we don't even want to have to write out code for a comparison for every list item. Therefore, we have a single section of code (a loop) that we execute over and over again for every element in `data_items`.

In the previous section, we outlined what this loop needed to do. Let's review:

- Check to see if the current value being looked at is zero. If so, that means we are at the end of our data and should exit the loop.
- We have to load the next value of our list.
- We have to see if the next value is bigger than our current biggest value.

[16] The instruction doesn't really use 4 for the size of the storage locations, although looking at it that way works for our purposes now. It's actually what's called a *multiplier*. basically, the way it works is that you start at the location specified by `data_items`, then you add `%edi`*4 storage locations, and retrieve the number there. Usually, you use the size of the numbers as your multiplier, but in some circumstances you'll want to do other things.

[17] Also, the `l` in `movl` stands for *move long* since we are moving a value that takes up four storage locations.

- If it is, we have to copy it to the location we are holding the largest value in.
- Now we need to go back to the beginning of the loop.

Okay, so now let's go to the code. We have the beginning of the loop marked with `_start_loop`. That is so we know where to go back to at the end of our loop. Then we have these instructions:

```
34      cmpl $0, %eax           # Check to see if we have
35      je _loop_exit           # hit the end.
```

The `cmpl` instruction compares the two values. Here, we are comparing the number `0` to the number stored in *%eax*. This compare instruction also affects a register not mentioned here, the *%eflags* register. This is also known as the status register, and has many uses which we will discuss later. Just be aware that the result of the comparison is stored in the status register. The next line is a flow control instruction which says to *jump* to the `_loop_exit` location if the values that were just compared are equal (that's what the `e` of `je` means). It uses the status register to hold the value of the last comparison. We used `je`, but there are many jump statements that you can use:

`je`: Jump if the values were equal.

`jg`: Jump if the second value was greater than the first value.[18]

`jge`: Jump if the second value was greater than or equal to the first value.

`jl`: Jump if the second value was less than the first value.

`jle`: Jump if the second value was less than or equal to the first value.

`jmp`: Jump no matter what. This does not need to be preceded by a comparison.

The complete list is documented in Appendix B. Common x86 Instructions. In this case, we are jumping if *%eax* holds the value of zero. If so, we are done and we go to `_loop_exit`.[19]

If the last loaded element was not zero, we go on to the next instructions:

```
36      incl %edi               # Increment %edi by 1.
37      movl data_items(,%edi,4), %eax   # Load next value.
```

If you remember from our previous discussion, *%edi* contains the index to our list of values in `data_items`. `incl` increments the value of *%edi* by one. Then the `movl` is just like the one we did beforehand. However, since we already incremented *%edi*, *%eax* is getting the next value from the list. Now *%eax* has the next value to be tested. So, let's test it!

```
38      cmpl %ebx, %eax         # Compare values.
39      jle _start_loop         # Jump to loop beginning if
40                              # the new one is not bigger
```

Here we compare our current value, stored in *%eax* to our biggest value so far, stored in *%ebx*. If the current value is less or equal to our biggest value so far, we don't care about it, so we just jump back to the beginning of the loop. Otherwise, we need to record that value as the largest one:

```
41      movl %eax, %ebx         # Move the value as the
42                              # largest.
43      jmp _start_loop         # Jump to loop beginning.
```

[18] Notice that the comparison is to see if the *second* value is greater than the first. I would have thought it the other way around. You will find a lot of things like this when learning programming. It occurs because different things make sense to different people. Anyway, you'll just have to memorize such things and go on.

[19] The names of these symbols can be anything you want them to be, as long as they only contain letters and the underscore character(_). The only one that is forced is `_start`, and possibly others that you declare with `.globl`. However, if it is a symbol you define and only you use, feel free to call it anything you want that is adequately descriptive (remember that others will have to modify your code later, and will have to figure out what your symbols mean).

which moves the current value into *%ebx*, which we are using to store the current largest value, and starts the loop over again.

Okay, so the loop executes until it reaches a 0, when it jumps to `_loop_exit`. This part of the program calls the Linux kernel to exit. If you remember from the last program, when you call the operating system (remember it's like signaling Batman), you store the system call number in *%eax* (1 for the `exit` call), and store the other values in the other registers. The exit call requires that we put our exit status code in *%ebx*. We already have the exit status there since we are using *%ebx* as our largest number, so all we have to do is load *%eax* with the number one and call the kernel to exit. Like this:

```
46                              # %ebx is the status code
47                              # for the exit systemcall
48          movl $1, %eax       # and it already has the
49          int  $0x80          # maximum number 1 is the
50                              # exit() syscall.
```

Okay, that was a lot of work and explanation, especially for such a small program. But hey, you're learning a lot! Now, read through the whole program again, paying special attention to the comments. Make sure that you understand what is going on at each line. If you don't understand a line, go back through this section and figure out what the line means.

You might also grab a piece of paper, and go through the program step-by-step, recording every change to every register, so you can see more clearly what is going on.

3.5 Addressing Modes

In Data Accessing Methods we learned the different types of addressing modes available for use in assembly language. This section will deal with how those addressing modes are represented in assembly language instructions.

The general form of memory address references is this:

```
ADDRESS_OR_OFFSET(%BASE_OR_OFFSET,%INDEX,MULTIPLIER)
```

All of the fields are optional. To calculate the address, simply perform the following calculation:

```
FINAL ADDRESS =
    ADDRESS_OR_OFFSET + %BASE_OR_OFFSET +
    MULTIPLIER * %INDEX
```

`ADDRESS_OR_OFFSET` and `MULTIPLIER` must both be constants, while the other two must be registers. If any of the pieces is left out, it is just substituted with zero in the equation.

All of the addressing modes mentioned in Data Accessing Methods except immediate-mode can be represented in this fashion.

Direct addressing mode:

This is done by only using the `ADDRESS_OR_OFFSET` portion. Example:

This loads *%eax* with the value at memory address `ADDRESS`.

```
movl ADDRESS, %eax
```

Indexed addressing mode:

This is done by using the `ADDRESS_OR_OFFSET` and the `%INDEX` portion. You can use any general-purpose register as the index register. You can also have a constant multiplier of 1, 2, or 4 for the index register, to make it easier to index by bytes, double-bytes, and words. For example, let's say that we had a string of bytes as `string_start` and wanted to access the third one (an index of 2 since we start counting the index at zero), and *%ecx* held the value 2. If you wanted to load it into *%eax* you could do the following:

This starts at `string_start`, and adds `1 * %ecx` to that address, and loads the value into *%eax*.

```
movl string_start(,%ecx,1), %eax
```

Indirect addressing mode:
Indirect addressing mode loads a value from the address indicated by a register. For example, if *%eax* held an address, we could move the value at that address to *%ebx* by doing the following:

```
movl (%eax), %ebx
```

Base pointer addressing mode:
Base-pointer addressing is similar to indirect addressing, except that it adds a constant value to the address in the register. For example, if you have a record where the age value is 4 bytes into the record, and you have the address of the record in *%eax*, you can retrieve the age into *%ebx* by issuing the following instruction:

```
movl 4(%eax), %ebx
```

Immediate mode addressing:
Immediate mode is very simple. It does not follow the general form we have been using. Immediate mode is used to load direct values into registers or memory locations. For example, if you wanted to load the number 12 into *%eax*, you would simply do the following:

Notice that to indicate immediate mode, we used a dollar sign in front of the number. If we did not, it would be direct addressing mode, in which case the value located at memory location 12 would be loaded into *%eax* rather than the number 12 itself.

```
movl $12, %eax
```

Register addressing mode:
Register mode simply moves data in or out of a register. In all of our examples, register addressing mode was used for the other operand.

These addressing modes are very important, as every memory access will use one of these. Every mode except immediate mode can be used as either the source or destination operand. Immediate mode can only be a source operand.

In addition to these modes, there are also different instructions for different sizes of values to move. For example, we have been using `movl` to move data a word at a time. in many cases, you will only want to move data a byte at a time. This is accomplished by the instruction `movb`. However, since the registers we have discussed are word-sized and not byte-sized, you cannot use the full register. Instead, you have to use a portion of the register.

Take for instance *%eax*. If you only wanted to work with two bytes at a time, you could just use *%ax*. *%ax* is the least-significant half (i.e. - the last part of the number) of the *%eax* register, and is useful when dealing with two-byte quantities. *%ax* is further divided up into *%al* and *%ah*. *%al* is the least-significant byte of *%ax*, and *%ah* is the most significant byte.[20] Loading a value into *%eax* will wipe out whatever was in *%al* and *%ah* (and also *%ax*, since *%ax* is made up of them). Similarly, loading a value into either *%al* or *%ah* will corrupt any value that was formerly in *%eax*. Basically, it's wise to only use a register for either a byte or a word, but never both at the same time.

```
Layout of the 32-bit registers.
|=======================================|
|----------------%eax-----------------| ===> 32-bit = 4-byte.
|------------------|--------%ax--------| ===> 16-bit = 2-byte.
|------------------|---%ah---|---%al---| ===>  8-bit = 1-byte.
|=======================================|
|----------------%ebx-----------------| ===> 32-bit = 4-byte.
|------------------|--------%bx--------| ===> 16-bit = 2-byte.
|------------------|---%bh---|---%bl---| ===>  8-bit = 1-byte.
|=======================================|
|----------------%ecx-----------------| ===> 32-bit = 4-byte.
```

[20] When we talk about the most or least *significant* byte, it may be a little confusing. Let's take the number 5432. In that number, 54 is the most significant half of that number and 32 is the least significant half. You can't quite divide it like that for registers, since they operate on base 2 rather than base 10 numbers, but that's the basic idea. For more information on this topic, see Chapter 10. Counting Like a Computer.

```
|------------------|--------%cx--------| ===> 16-bit = 2-byte.
|------------------|---%ch---|---%cl---| ===>  8-bit = 1-byte.
|=======================================|
|-----------------%edx------------------| ===> 32-bit = 4-byte.
|------------------|--------%dx--------| ===> 16-bit = 2-byte.
|------------------|---%dh---|---%dl---| ===>  8-bit = 1-byte.
|=======================================|
```

For a more comprehensive list of instructions, see Appendix B. Common x86 Instructions.

3.6 Review

3.6.1 Know the Concepts

- What does it mean if a line in the program starts with the '#' character?
- What is the difference between an assembly language file and an object code file?
- What does the linker do?
- How do you check the result status code of the last program you ran?
- What is the difference between `movl $1, %eax` and `movl 1, %eax`?
- Which register holds the system call number?
- What are indexes used for?
- Why do indexes usually start at 0?
- If I issued the command `movl data_items(,%edi,4), %eax` and data_items was address 3634 and *%edi* held the value 13, what address would you be using to move into *%eax*?
- List the general-purpose registers.
- What is the difference between `movl` and `movb`?
- What is flow control?
- What does a conditional jump do?
- What things do you have to plan for when writing a program?
- Go through every instruction and list what addressing mode is being used for each operand.

3.6.2 Use the Concepts

- Modify the first program to return the value 3.
- Modify the `003-02-maximum` program to find the minimum instead.
- Modify the `003-02-maximum` program to use the number 255 to end the list rather than the number 0.
- Modify the `003-02-maximum` program to use an ending address rather than the number 0 to know when to stop.
- Modify the `003-02-maximum` program to use a length count rather than the number 0 to know when to stop.
- What would the instruction `movl _start, %eax` do? Be specific, based on your knowledge of both addressing modes and the meaning of `_start`. How would this differ from the instruction `movl $_start, %eax`?

3.6.3 Going Further

- Modify the first program to leave off the `int` instruction line. Assemble, link, and execute the new program. What error message do you get. Why do you think this might be?

- So far, we have discussed three approaches to finding the end of the list - using a special number, using the ending address, and using the length count. Which approach do you think is best? Why? Which approach would you use if you knew that the list was sorted? Why?

4. All About Functions

4.1 Dealing with Complexity

In Chapter 3. Your First Programs, the programs we wrote only consisted of one section of code. However, if we wrote real programs like that, it would be impossible to maintain them. It would be really difficult to get multiple people working on the project, as any change in one part might adversely affect another part that another developer is working on.

To assist programmers in working together in groups, it is necessary to break programs apart into separate pieces, which communicate with each other through well-defined interfaces. This way, each piece can be developed and tested independently of the others, making it easier for multiple programmers to work on the project.

Programmers use *functions* to break their programs into pieces which can be independently developed and tested. Functions are units of code that do a defined piece of work on specified types of data. For example, in a word processor program, I may have a function called `handle_typed_character` which is activated whenever a user types in a key. The data the function uses would probably be the keypress itself and the document the user currently has open. The function would then modify the document according to the keypress it was told about.

The data items a function is given to process are called its *parameters*. In the word processing example, the key which was pressed and the document would be considered parameters to the `handle_typed_characters` function. The parameter list and the processing expectations of a function (what it is expected to do with the parameters) are called the function's interface. Much care goes into designing function interfaces, because if they are called from many places within a project, it is difficult to change them if necessary.

A typical program is composed of hundreds or thousands of functions, each with a small, well-defined task to perform. However, ultimately there are things that you cannot write functions for which must be provided by the system. Those are called *primitive functions* (or just *primitives*) - they are the basics which everything else is built off of. For example, imagine a program that draws a graphical user interface. There has to be a function to create the menus. That function probably calls other functions to write text, to write icons, to paint the background, calculate where the mouse pointer is, etc. However, ultimately, they will reach a set of primitives provided by the operating system to do basic line or point drawing. Programming can either be viewed as breaking a large program down into smaller pieces until you get to the primitive functions, or incrementally building functions on top of primitives until you get the large picture in focus. In assembly language, the primitives are usually the same thing as the system calls, even though system calls aren't true functions as we will talk about in this chapter.

4.2 How Functions Work

Functions are composed of several different pieces:

Function name:
A function's name is a symbol that represents the address where the function's code starts. In assembly language, the symbol is defined by typing the function's name as a label before the function's code. This is just like labels you have used for jumping.

Function parameters:
A function's parameters are the data items that are explicitly given to the function for processing. For example, in mathematics, there is a sine function. If you were to ask a computer to find the sine of 2, sine would be the function's name, and 2 would be the parameter. Some functions have many parameters, others have none.[21]

[21] Function parameters can also be used to hold pointers to data that the function wants to send back to the program.

Local variables:
Local variables are data storage that a function uses while processing that is thrown away when it returns. It's kind of like a scratch pad of paper. Functions get a new piece of paper every time they are activated, and they have to throw it away when they are finished processing. Local variables of a function are not accessible to any other function within a program.

Static variables:
Static variables are data storage that a function uses while processing that is not thrown away afterwards, but is reused for every time the function's code is activated. This data is not accessible to any other part of the program. Static variables are generally not used unless absolutely necessary, as they can cause problems later on.

Global variables:
Global variables are data storage that a function uses for processing which are managed outside the function. For example, a simple text editor may put the entire contents of the file it is working on in a global variable so it doesn't have to be passed to every function that operates on it.[22] Configuration values are also often stored in global variables.

Return address:
The return address is an "invisible" parameter in that it isn't directly used during the function. The return address is a parameter which tells the function where to resume executing after the function is completed. This is needed because functions can be called to do processing from many different parts of your program, and the function needs to be able to get back to wherever it was called from. In most programming languages, this parameter is passed automatically when the function is called. In assembly language, the `call` instruction handles passing the return address for you, and `ret` handles using that address to return back to where you called the function from.

Return value:
The return value is the main method of transferring data back to the main program. Most programming languages only allow a single return value for a function.

These pieces are present in most programming languages. How you specify each piece is different in each one, however.

The way that the variables are stored and the parameters and return values are transferred by the computer varies from language to language as well. This variance is known as a language's *calling convention*, because it describes how functions expect to get and receive data when they are called.[23]

Assembly language can use any calling convention it wants to. You can even make one up yourself. However, if you want to interoperate with functions written in other languages, you have to obey their calling conventions. We will use the calling convention of the C programming language for our examples because it is the most widely used, and because it is the standard for Linux platforms.

4.3 Assembly-Language Functions using the C Calling Convention

You cannot write assembly-language functions without understanding how the computer's *stack* works. Each computer program that runs uses a region of memory called the stack to enable functions to work properly. Think of a stack as a pile of papers on your desk which can be added to indefinitely. You generally keep the things that you are working on toward the top, and you take things off as you are finished working with them.

Your computer has a stack, too. The computer's stack lives at the very top addresses of memory. You can push values onto the top of the stack through an instruction called `pushl`, which pushes either a register or memory value onto the top of the stack. Well, we say it's the top, but the "top" of the stack is actually the bottom of the stack's memory. Although this is confusing, the reason for it is that when we think of a stack of anything - dishes, papers, etc. - we think of adding and removing to the top of it. However, in memory the stack starts at the top of memory and grows downward due to architectural considerations. Therefore, when we refer to the "top of the stack" remember it's at the bottom of the stack's memory. You can also pop values

[22] This is generally considered bad practice. Imagine if a program is written this way, and in the next version they decided to allow a single instance of the program edit multiple files. Each function would then have to be modified so that the file that was being manipulated would be passed as a parameter. If you had simply passed it as a parameter to begin with, most of your functions could have survived your upgrade unchanged.

[23] A *convention* is a way of doing things that is standardized, but not forcibly so. For example, it is a convention for people to shake hands when they meet. If I refuse to shake hands with you, you may think I don't like you. Following conventions is important because it makes it easier for others to understand what you are doing, and makes it easier for programs written by multiple independent authors to work together.

off the top using an instruction called `popl`. This removes the top value from the stack and places it into a register or memory location of your choosing.

When we push a value onto the stack, the top of the stack moves to accommodate the additional value. We can actually continually push values onto the stack and it will keep growing further and further down in memory until we hit our code or data. So how do we know where the current "top" of the stack is? The stack register, *%esp*, always contains a pointer to the current top of the stack, wherever it is.

Every time we push something onto the stack with `pushl`, *%esp* gets subtracted by 4 so that it points to the new top of the stack (remember, each word is four bytes long, and the stack grows downward). If we want to remove something from the stack, we simply use the `popl` instruction, which adds 4 to *%esp* and puts the previous top value in whatever register you specified. `pushl` and `popl` each take one operand - the register to push onto the stack for `pushl`, or receive the data that is popped off the stack for `popl`.

If we simply want to access the value on the top of the stack without removing it, we can simply use the *%esp* register in indirect addressing mode. For example, the following code moves whatever is at the top of the stack into *%eax*:

```
movl (%esp), %eax
```

If we were to just do this:

```
movl %esp, %eax
```

then *%eax* would just hold the pointer to the top of the stack rather than the value at the top. Putting *%esp* in parentheses causes the computer to go to indirect addressing mode, and therefore we get the value pointed to by *%esp*. If we want to access the value right below the top of the stack, we can simply issue this instruction:

```
movl 4(%esp), %eax
```

This instruction uses the base pointer addressing mode (see Data Accessing Methods) which simply adds 4 to *%esp* before looking up the value being pointed to.

NOTE:

Please, do a quick review of the tables which explain graphically, how the memory and the stack works: Chapter 9 -> Table of the Physical Memory in the program.

In the C language calling convention, the stack is the key element for implementing a function's local variables, parameters, and return address.

Before executing a function, a program pushes all of the parameters for the function onto the stack in the reverse order that they are documented. Then the program issues a `call` instruction indicating which function it wishes to start. The `call` instruction does two things. First it pushes the address of the next instruction, which is the return address, onto the stack. Then it modifies the instruction pointer (*%eip*) to point to the start of the function. So, at the time the function starts, the stack looks like this (the "top" of the stack is at the bottom on this example):

```
0xffffff50: Parameter #N
...
0xffffff2c: Parameter 2
0xffffff28: Parameter 1
0xffffff24: Return Address <--- (%esp)
```

Each of the parameters of the function have been pushed onto the stack, and finally the return address is there. Now the function itself has some work to do.

The first thing it does is save the current base pointer register, *%ebp*, by doing `pushl %ebp`. The base pointer is a special register used for accessing function parameters and local variables. Next, it copies the stack pointer to *%ebp* by doing `movl %esp, %ebp`. This allows you to be able to access the function parameters as fixed indexes from the base pointer. You may think that you can use the stack pointer for this. However, during your program you may do other things with the stack such as pushing arguments to other functions.

Copying the stack pointer into the base pointer at the beginning of a function allows you to always know where your parameters are (and as we will see, local variables too), even while you may be pushing things on and off the stack. *%ebp* will always be where the stack pointer was at the beginning of the function, so it is more or less a constant reference to the *stack frame* (the stack frame consists of all of the stack variables used within a function, including parameters, local variables, and the return address).

At this point, the stack looks like this:

```
0xffffff50: Parameter #N   <--- N*4+4(%ebp)
...
0xffffff2c: Parameter 2    <--- 12(%ebp)
0xffffff28: Parameter 1    <---  8(%ebp)
0xffffff24: Return Address <---  4(%ebp)
0xffffff20: Old %ebp       <---   (%esp) and (%ebp)
```

As you can see, each parameter can be accessed using base pointer addressing mode using the *%ebp* register.

Next, the function reserves space on the stack for any local variables it needs. This is done by simply moving the stack pointer out of the way. Let's say that we are going to need two words of memory to run a function. We can simply move the stack pointer down two words to reserve the space. This is done like this:

```
subl $8, %esp
```

This subtracts 8 from *%esp* (remember, a word is four bytes long).[24] This way, we can use the stack for variable storage without worrying about clobbering them with pushes that we may make for function calls. Also, since it is allocated on the stack frame for this function call, the variable will only be alive during this function. When we return, the stack frame will go away, and so will these variables. That's why they are called local - they only exist while this function is being called.

Now we have two words for local storage. Our stack now looks like this:

```
0xffffff50: Parameter #N     <--- N*4+4(%ebp)
...
0xffffff2c: Parameter 2      <--- 12(%ebp)
0xffffff28: Parameter 1      <---  8(%ebp)
0xffffff24: Return Address   <---  4(%ebp)
0xffffff20: Old %ebp         <---   (%ebp)
0xffffff1c: Local Variable 1 <--- -4(%ebp)
0xffffff18: Local Variable 2 <--- -8(%ebp) and (%esp)
```

The Rule:

The positive numbers or operations take the old stored values, negative numbers or operations take the new stored values.

Get the values before `%ebp` (old values):

```
0xffffff28: Parameter 1    <--- 8(%ebp)
0xffffff24: Return Address <--- 4(%ebp)
0xffffff20: Old %ebp       <---  (%ebp)
```

Get the values after `%ebp` (new values):

```
0xffffff20: Old %ebp         <---    (%ebp)
0xffffff1c: Local Variable 1 <---  -4(%ebp)
0xffffff18: Local Variable 2 <---  -8(%ebp)
```

Also this rule apply for the %esp, get the values before `%esp` (old values):

[24] Just a reminder - the dollar sign in front of the eight indicates immediate mode addressing, meaning that we subtract the number 8 itself from *%esp* rather than the value at address 8.

```
0xffffff20: Old %ebp         <---    (%ebp)
0xffffff1c: Local Variable 1 <---   8(%esp)
0xffffff18: Local Variable 2 <---   4(%esp)
0xffffff14: New %esp         <---    (%esp)
```

So we can now access all of the data we need for this function by using base pointer addressing mode using different offsets from *%ebp*. *%ebp* was made specifically for this purpose, which is why it is called the base pointer register. You can use other registers in base pointer addressing mode, but the x86 architecture makes using the *%ebp* register a lot faster.

Global variables and static variables are accessed just like the memory we have been accessing memory in previous chapters. The only difference between the global and static variables is that static variables are only used by one function, while global variables are used by many functions. Assembly language treats them exactly the same, although most other languages distinguish them.

When a function is done executing, it does three things:

1. It stores its return value in *%eax*.
2. It resets the stack to what it was when it was called (it gets rid of the current stack frame and puts the stack frame of the calling code back into effect).
3. It returns control back to wherever it was called from. This is done using the `ret` instruction, which pops whatever value is at the top of the stack, and sets the instruction pointer, *%eip*, to that value.

So, before a function returns control to the code that called it, it must restore the previous stack frame. Note also that without doing this, `ret` wouldn't work, because in our current stack frame, the return address is not at the top of the stack. Therefore, before we return, we have to reset the stack pointer *%esp* and base pointer *%ebp* to what they were when the function began.

Therefore to return from the function you have to do the following:

```
movl %ebp, %esp
popl %ebp
ret
```

At this point, you should consider all local variables to be disposed of. The reason is that after you move the stack pointer back, future stack pushes will likely overwrite everything you put there. Therefore, you should never save the address of a local variable past the life of the function it was created in, or else it will be overwritten after the life of its stack frame ends.

Control has now been handed back to the calling code, which can now examine *%eax* for the return value. The calling code also needs to pop off all of the parameters it pushed onto the stack in order to get the stack pointer back where it was (you can also simply add 4 * number of parameters to *%esp* using the `addl` instruction, if you don't need the values of the parameters anymore).[25]

WARNING!

Destruction of Registers:

When you call a function, you should assume that everything currently in your registers will be wiped out. The only register that is guaranteed to be left with the value it started with are *%ebp* and a few others (the Linux C calling convention requires functions to preserve the values of *%ebx*, *%edi*, and *%esi* if they are altered - this is not strictly held during this book because these programs are self-contained and not called by outside functions). *%ebx* also has some other uses in position-independent code, which is not covered in this book. *%eax* is guaranteed to be overwritten with the return value, and the others likely are. If there are registers you want to save before calling a function, you need to save them by pushing them on the stack before pushing the function's parameters. You can then pop them back off in reverse

[25] This is not always strictly needed unless you are saving registers on the stack before a function call. The base pointer keeps the stack frame in a reasonably consistent state. However, it is still a good idea, and is absolutely necessary if you are temporarily saving registers on the stack.

order after popping off the parameters. Even if you know a function does not overwrite a register you should save it, because future versions of that function may.

Other languages' calling convention may be different. For example, other calling conventions may place the burden on the function to save any registers it uses. Be sure to check to make sure the calling conventions of your languages are compatible before trying to mix languages. Or in the case of assembly language, be sure you know how to call the other language's functions.

NOTE.

Extended Specification: Details of the C language calling convention (also known as the ABI, or Application Binary Interface) is available online. We have oversimplified and left out several important pieces to make this simpler for new programmers. For full details, you should check out the documents available at Linux Standard Base (LSB), you should look for the System V Application Binary Interface - Intel386 Architecture Processor Supplement, Fourth Edition.

4.4 A Function Example

Let's take a look at how a function call works in a real program. The function we are going to write is the `_power` function. We will give the power function two parameters - the number and the power we want to raise it to. For example, if we gave it the parameters 2 and 3, it would raise 2 to the power of 3, or 2*2*2, giving 8. In order to make this program simple, we will only allow numbers 1 and greater.

The following is the code for the complete program. As usual, an explanation follows. Name the file `004-01-power.s`.

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Program to illustrate how functions work.
5       #     This program will compute the value of
6       #     2^3 + 5^2
7       #
8       # Everything in the main program is stored in
9       # registers, so the data section does not have
10      # anything.
11      #
12      .section .data
13
14      .section .text
15          .globl _start
16
17  _start:
18      pushl $3                # Push second argument.
19      pushl $2                # Push first argument.
20      call  _power            # Call the function.
21      addl  $8, %esp          # Move the stack pointer
22                              # back.
23
24      pushl %eax              # Save the first answer
25                              # before calling the next
26                              # function.
27
28      pushl $2                # Push second argument.
29      pushl $5                # Push first argument.
```

```
30      call  _power            # Call the function.
31      addl  $8, %esp           # Move the stack pointer
32                               # back.
33
34      popl  %ebx               # The second answer is
35                               # already in %eax.  We
36                               # saved the first answer
37                               # onto the stack, so now we
38                               # can just pop it out into
39                               # %ebx.
40
41      addl  %eax, %ebx         # Add them together
42                               # the result is in %ebx.
43
44      movl  $1, %eax           # Exit (%ebx is returned).
45      int   $0x80
46
47      # PURPOSE:
48      #     This function is used to compute the value of
49      #     a number raised to a power.
50      #
51      # INPUT:
52      #     First argument -  the base number.
53      #     Second argument - the power to raise it to.
54      #
55      # OUTPUT:
56      #     Will give the result as a return value.
57      #
58      # NOTES:
59      #     The power must be 1 or greater.
60      #
61      # VARIABLES:
62      #     %ebx - holds the base number.
63      #     %ecx - holds the power.
64      #     -4(%ebp) - holds the current result.
65      #     %eax is used for temporary storage.
66      #
67          .type  _power,  @function
68
69  _power:
70      pushl %ebp               # Save old base pointer.
71      movl  %esp, %ebp         # Make stack pointer the
72                               # base pointer.
73      subl  $4, %esp           # Get room for our local
74                               # storage.
75
76      movl  8(%ebp), %ebx      # Put first argument in
77                               # %ebx.
78      movl  12(%ebp), %ecx     # Put second argument in
79                               # %ecx.
80
81      movl  %ebx, -4(%ebp)     # Store current result.
82
```

```
83  _power_loop_start:
84      cmpl  $1, %ecx            # If the power is 1, we
85                                # are done.
86      je    _end_power
87      movl  -4(%ebp), %eax      # Move the current result
88                                # into %eax.
89      imull %ebx, %eax          # Multiply the current
90                                # result by the base
91                                # number.
92      movl  %eax, -4(%ebp)      # Store the current
93                                # result.
94
95      decl  %ecx                # Decrease the power.
96      jmp   _power_loop_start   # Run for the next power.
97
98  _end_power:
99      movl -4(%ebp), %eax       # Return value goes in
100                               # %eax.
101     movl %ebp, %esp           # Restore the stack
102                               # pointer.
103     popl %ebp                 # Restore the base
104                               # pointer.
105     ret
```

Type in the program, assemble it, and run it. Try calling power for different values, but remember that the result has to be less than 256 when it is passed back to the operating system. Also try subtracting the results of the two computations. Try adding a third call to the `_power` function, and add its result back in.

The main program code is pretty simple. You push the arguments onto the stack, call the function, and then move the stack pointer back. The result is stored in *%eax*. Note that between the two calls to `_power`, we save the first value onto the stack. This is because the only register that is guaranteed to be saved is *%ebp*. Therefore we push the value onto the stack, and pop the value back off after the second function call is complete.

Let's look at how the function itself is written. Notice that before the function, there is documentation as to what the function does, what its arguments are, and what it gives as a return value. This is useful for programmers who use this function. This is the function's interface. This lets the programmer know what values are needed on the stack, and what will be in *%eax* at the end.

We then have the following line:

```
67          .type  _power,  @function
```

This tells the linker that the symbol `_power` should be treated as a function. Since this program is only in one file, it would work just the same with this left out. However, it is good practice.

After that, we define the value of the `_power` label:

```
69  _power:
```

As mentioned previously, this defines the symbol `_power` to be the address where the instructions following the label begin. This is how `call _power` works. It transfers control to this spot of the program. The difference between `call` and `jmp` is that `call` also pushes the return address onto the stack so that the function can return, while the `jmp` does not.

Next, we have our instructions to set up our function:

```
70      pushl %ebp                # Save old base pointer.
71      movl  %esp, %ebp          # Make stack pointer the
72                                # base pointer.
```

```
73      subl  $4, %esp            # Get room for our local
74                                # storage.
```

At this point, our stack looks like this:

```
Base Number    <--- 12(%ebp)
Power          <--- 8(%ebp)
Return Address <--- 4(%ebp)
Old %ebp       <--- (%ebp)
Current result <--- -4(%ebp) and (%esp)
```

Although we could use a register for temporary storage, this program uses a local variable in order to show how to set it up. Often times there just aren't enough registers to store everything, so you have to offload them into local variables. Other times, your function will need to call another function and send it a pointer to some of your data. You can't have a pointer to a register, so you have to store it in a local variable in order to send a pointer to it.

Basically, what the program does is start with the base number, and store it both as the multiplier (stored in *%ebx*) and the current value (stored in −4(%ebp)). It also has the power stored in *%ecx* It then continually multiplies the current value by the multiplier, decreases the power, and leaves the loop if the power (in *%ecx*) gets down to 1.

By now, you should be able to go through the program without help. The only things you should need to know is that `imull` does integer multiplication and stores the result in the second operand, and `decl` decreases the given register by 1. For more information on these and other instructions, see Appendix B. Common x86 Instructions

A good project to try now is to extend the program so it will return the value of a number if the power is 0 (hint, anything raised to the zero power is 1). Keep trying. If it doesn't work at first, try going through your program by hand with a scrap of paper, keeping track of where *%ebp* and *%esp* are pointing, what is on the stack, and what the values are in each register.

4.5 Recursive Functions

The next program will stretch your brains even more. The program will compute the *factorial* of a number. A factorial is the product of a number and all the numbers between it and one. For example, the factorial of 7 is 7*6*5*4*3*2*1, and the factorial of 4 is 4*3*2*1. Now, one thing you might notice is that the factorial of a number is the same as the product of a number and the factorial just below it. For example, the factorial of 4 is 4 times the factorial of 3. The factorial of 3 is 3 times the factorial of 2. 2 is 2 times the factorial of 1. The factorial of 1 is 1. This type of definition is called a recursive definition. That means, the definition of the factorial function includes the factorial function itself. However, since all functions need to end, a recursive definition must include a *base case*. The base case is the point where recursion will stop. Without a base case, the function would go on forever calling itself until it eventually ran out of stack space. In the case of the factorial, the base case is the number 1. When we hit the number 1, we don't run the factorial again, we just say that the factorial of 1 is 1. So, let's run through what we want the code to look like for our factorial function:

1. Examine the number.
2. Is the number 1?
3. If so, the answer is one.
4. Otherwise, the answer is the number times the factorial of the number minus one.

This would be problematic if we didn't have local variables. In other programs, storing values in global variables worked fine. However, global variables only provide one copy of each variable. In this program, we will have multiple copies of the function running at the same time, all of them needing their own copies of

[26]By "running at the same time" I am talking about the fact that one will not have finished before a new one is activated. I am not implying that their instructions are running at the same time.

the data![26] Since local variables exist on the stack frame, and each function call gets its own stack frame, we are okay.

Let's look at the `004-02-factorial.s` code to see how this works:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Given a number, this program computes the
5       #     factorial.  For example, the factorial of
6       #     3 is 3 * 2 * 1, or 6.  The factorial of
7       #     4 is 4 * 3 * 2 * 1, or 24, and so on.
8       #
9       # This program shows how to call a function
10      # recursively. This program has no global data.
11      #
12      .section .data
13
14      .section .text
15          .globl _start
16          .globl _factorial   # This is unneeded unless
17                              # we want to share this
18                              # function among other
19                              # programs.
20  _start:
21      pushl $4                # The factorial takes one
22                              # argument - the number we
23                              # want a factorial of.  So,
24                              # it gets pushed.
25      call  _factorial        # Run the factorial
26                              # function.
27      addl  $4, %esp          # Scrubs the parameter that
28                              # was pushed on the stack.
29      movl  %eax, %ebx        # Factorial returns the
30                              # answer in %eax, but we
31                              # want it in %ebx to send
32                              # it as our exit status.
33      movl  $1, %eax          # Call the kernel exit
34      int   $0x80             # function.
35
36
37      # This is the actual function definition.
38      #
39      .type  _factorial,  @function
40  _factorial:
41      pushl %ebp              # Atandard function stuff -
42                              # we have to restore %ebp
43                              # to its prior state before
44                              # returning, so we have to
45                              # push it.
46      movl  %esp, %ebp        # This is because we do not
47                              # want to modify the stack
48                              # pointer, so we use %ebp.
49
50      movl  8(%ebp), %eax     # This moves the first
```

```
51                              # argument to %eax 4(%ebp)
52                              # holds the return address,
53                              # and 8(%ebp) holds the
54                              # first parameter.
55      cmpl  $1, %eax          # If the number is 1, that
56                              # is our base case, and we
57                              # simply return (1 is
58                              # already in %eax as the
59                              # return value).
60      je _end_factorial
61      decl  %eax              # Otherwise, decrease the
62                              # value.
63      pushl %eax              # Push it for our call to
64                              # factorial.
65      call  _factorial        # Call factorial.
66      movl  8(%ebp), %ebx     # %eax has the return
67                              # value, so we reload our
68                              # parameter into %ebx.
69      imull %ebx, %eax        # Multiply that by the
70                              # result of the last call
71                              # to factorial (in %eax)
72                              # the answer is stored in
73                              # %eax, which is good since
74                              # that is where return
75                              # values go.
76  _end_factorial:
77      movl  %ebp, %esp        # Standard function return
78      popl  %ebp              # stuff - we have to
79                              # restore %ebp and %esp to
80      ret                     # where they were before
81                              # the function started
82                              # return from the function
83                              # (this pops the return
84                              # value, too).
```

Assemble, link, and run it with these commands:

```
as -o 004-02-factorial.o  --32 \
                          --gstabs+ \
                          004-02-factorial.s

ld -o 004-02-factorial    -m elf_i386 \
                          004-02-factorial.o
./004-02-factorial
echo $?
```

This should give you the value 24. 24 is the factorial of 4, you can test it out yourself with a calculator: 4 * 3 * 2 * 1 = 24.

I'm guessing you didn't understand the whole code listing. Let's go through it a line at a time to see what is happening.

```
20  _start:
21      pushl $4                # The factorial takes one
22                              # argument - the number we
23                              # want a factorial of.  So,
```

```
24                              # it gets pushed.
25      call  _factorial        # Run the factorial
26                              # function.
```

Okay, this program is intended to compute the factorial of the number 4. When programming functions, you are supposed to put the parameters of the function on the top of the stack right before you call it. Remember, a function's *parameters* are the data that you want the function to work with. In this case, the factorial function takes 1 parameter - the number you want the factorial of.

The `pushl` instruction puts the given value at the top of the stack. The `call` instruction then makes the function call.

Next we have these lines:

```
27      addl  $4, %esp          # Scrubs the parameter that
28                              # was pushed on the stack.
29      movl  %eax, %ebx        # Factorial returns the
30                              # answer in %eax, but we
31                              # want it in %ebx to send
32                              # it as our exit status.
33      movl  $1, %eax          # Call the kernel exit
34      int   $0x80             # function.
```

This takes place after `_factorial` has finished and computed the factorial of 4 for us. Now we have to clean up the stack. The `addl` instruction moves the stack pointer back to where it was before we pushed the `$4` onto the stack. You should always clean up your stack parameters after a function call returns.

The next instruction moves *%eax* to *%ebx*. What's in *%eax*? It is `_factorial`'s return value. In our case, it is the value of the factorial function. With 4 as our parameter, 24 should be our return value. Remember, return values are always stored in *%eax*. We want to return this value as the status code to the operating system. However, Linux requires that the program's exit status be stored in *%ebx*, not *%eax*, so we have to move it. Then we do the standard exit system call.

The nice thing about function calls is that:

- Other programmers don't have to know anything about them except its arguments to use them.
- They provide standardized building blocks from which you can form a program.
- They can be called multiple times and from multiple locations and they always know how to get back to where they were since `call` pushes the return address onto the stack.

These are the main advantages of functions. Larger programs also use functions to break down complex pieces of code into smaller, simpler ones. In fact, almost all of programming is writing and calling functions.

Let's now take a look at how the `_factorial` function itself is implemented.

Before the function starts, we have this directive:

```
39      .type  _factorial,  @function
40  _factorial:
```

The `.type` directive tells the linker that `_factorial` is a function. This isn't really needed unless we were using `_factorial` in other programs. We have included it for completeness. The line that says `_factorial:` gives the symbol `_factorial` the storage location of the next instruction. That's how `call` knew where to go when we said `call _factorial`.

The first real instructions of the function are:

```
41      pushl %ebp              # Atandard function stuff -
42                              # we have to restore %ebp
43                              # to its prior state before
44                              # returning, so we have to
45                              # push it.
46      movl  %esp, %ebp        # This is because we do not
```

```
47                              # want to modify the stack
48                              # pointer, so we use %ebp.
```

As shown in the previous program, this creates the stack frame for this function. These two lines will be the way you should start every function.

The next instruction is this:

```
50      movl  8(%ebp), %eax     # This moves the first
51                              # argument to %eax 4(%ebp)
52                              # holds the return address,
53                              # and 8(%ebp) holds the
54                              # first parameter.
```

This uses base pointer addressing mode to move the first parameter of the function into *%eax*. Remember, `(%ebp)` has the old *%ebp*, `4(%ebp)` has the return address, and `8(%ebp)` is the location of the first parameter to the function. If you think back, this will be the value 4 on the first call, since that was what we pushed on the stack before calling the function the first time (with `pushl $4`). As this function calls itself, it will have other values, too.

Next, we check to see if we've hit our base case (a parameter of 1). If so, we jump to the instruction at the label `_end_factorial`, where it will be returned. It's already in *%eax* which we mentioned earlier is where you put return values. That is accomplished by these lines:

```
55      cmpl  $1, %eax          # If the number is 1, that
56                              # is our base case, and we
57                              # simply return (1 is
58                              # already in %eax as the
59                              # return value).
60      je _end_factorial
```

If it's not our base case, what did we say we would do? We would call the `_factorial` function again with our parameter minus one. So, first we decrease *%eax* by one:

```
61      decl  %eax              # Otherwise, decrease the
62                              # value.
```

`decl` stands for decrement. It subtracts 1 from the given register or memory location (*%eax* in our case). `incl` is the inverse - it adds 1. After decrementing *%eax* we push it onto the stack since it's going to be the parameter of the next function call. And then we call `_factorial` again!

```
63      pushl %eax              # Push it for our call to
64                              # factorial.
65      call  _factorial        # Call factorial.
```

Okay, now we've called `_factorial`. One thing to remember is that after a function call, we can never know what the registers are (except `%esp` and `%ebp`). So even though we had the value we were called with in `%eax`, it's not there anymore. Therefore, we need to pull it off the stack from the same place we got it the first time (at `8(%ebp)`). So, we do this:

```
66      movl  8(%ebp), %ebx     # %eax has the return
67                              # value, so we reload our
68                              # parameter into %ebx.
```

Now, we want to multiply that number with the result of the factorial function. If you remember our previous discussion, the result of functions are left in *%eax*. So, we need to multiply *%ebx* with *%eax*. This is done with this instruction:

```
69      imull %ebx, %eax        # Multiply that by the
70                              # result of the last call
71                              # to factorial (in %eax)
72                              # the answer is stored in
73                              # %eax, which is good since
74                              # that is where return
75                              # values go.
```

This also stores the result in *%eax*, which is exactly where we want the return value for the function to be! Since the return value is in place we just need to leave the function. If you remember, at the start of the function we pushed *%ebp*, and moved *%esp* into *%ebp* to create the current stack frame. Now we reverse the operation to destroy the current stack frame and reactivate the last one:

```
76  _end_factorial:
77      movl  %ebp, %esp        # Standard function return
78      popl  %ebp              # stuff - we have to
79                              # restore %ebp and %esp to
```

Now we're already to return, so we issue the following command

```
80      ret                     # where they were before
81                              # the function started
82                              # return from the function
83                              # (this pops the return
84                              # value, too).
```

This pops the top value off of the stack, and then jumps to it. If you remember our discussion about `call`, we said that `call` first pushed the address of the next instruction onto the stack before it jumped to the beginning of the function. So, here we pop it back off so we can return there. The function is done, and we have our answer!

Like our previous program, you should look over the program again, and make sure you know what everything does. Look back through this section and the previous sections for the explanation of anything you don't understand. Then, take a piece of paper, and go through the program step-by-step, keeping track of what the values of the registers are at each step, and what values are on the stack. Doing this should deepen your understanding of what is going on.

4.6 Review

4.6.1 Know the Concepts

- What are primitives?
- What are calling conventions?
- What is the stack?
- How do `pushl` and `popl` affect the stack? What special-purpose register do they affect?
- What are local variables and what are they used for?
- Why are local variables so necessary in recursive functions?
- What are *%ebp* and *%esp* used for?
- What is a stack frame?

4.6.2 Use the Concepts

- Write a function called `square` which receives one argument and returns the square of that argument.

- Write a program to test your `square` function.
- Convert the maximum program given in Finding a Maximum Value so that it is a function which takes a pointer to several values and returns their maximum. Write a program that calls maximum with 3 different lists, and returns the result of the last one as the program's exit status code.
- Explain the problems that would arise without a standard calling convention.

4.6.3 Going Further

- Do you think it's better for a system to have a large set of primitives or a small one, assuming that the larger set can be written in terms of the smaller one?
- The factorial function can be written non-recursively. Do so.
- Find an application on the computer you use regularly. Try to locate a specific feature, and practice breaking that feature out into functions. Define the function interfaces between that feature and the rest of the program.
- Come up with your own calling convention. Rewrite the programs in this chapter using it. An example of a different calling convention would be to pass parameters in registers rather than the stack, to pass them in a different order, to return values in other registers or memory locations. Whatever you pick, be consistent and apply it throughout the whole program.
- Can you build a calling convention without using the stack? What limitations might it have?
- What test cases should we use in our example program to check to see if it is working properly?

5. Dealing with Files

A lot of computer programming deals with files. After all, when we reboot our computers, the only thing that remains from previous sessions are the things that have been put on disk. Data which is stored in files is called *persistent* data, because it persists in files that remain on the disk even when the program isn't running.

5.1 The UNIX File Concept

Each operating system has its own way of dealing with files. However, the UNIX method, which is used on Linux, is the simplest and most universal. UNIX files, no matter what program created them, can all be accessed as a sequential stream of bytes. When you access a file, you start by opening it by name. The operating system then gives you a number, called a *file descriptor*, which you use to refer to the file until you are through with it. You can then read and write to the file using its file descriptor. When you are done reading and writing, you then close the file, which then makes the file descriptor useless.

In our programs we will deal with files in the following ways:

1. Tell Linux the name of the file to open, and in what mode you want it opened (read, write, both read and write, create it if it doesn't exist, etc.). This is handled with the `open` system call, which takes a filename, a number representing the mode, and a permission set as its parameters. *%eax* will hold the system call number, which is 5. The address of the first character of the filename should be stored in *%ebx*. The read/write intentions, represented as a number, should be stored in *%ecx*. For now, use 0 for files you want to read from, and 03101 for files you want to write to (you must include the leading zero).[27] Finally, the permission set should be stored as a number in *%edx*. If you are unfamiliar with UNIX permissions, just use 0666 for the permissions (again, you must include the leading zero).
2. Linux will then return to you a file descriptor in *%eax*. Remember, this is a number that you use to refer to this file throughout your program.
3. Next you will operate on the file doing reads and/or writes, each time giving Linux the file descriptor you want to use. `read` is system call 3, and to call it you need to have the file descriptor in *%ebx*, the address of a buffer for storing the data that is read in *%ecx*, and the size of the buffer in *%edx*. Buffers will be explained in Buffers and `.bss`. `read` will return with either the number of characters read from the file, or an error code. Error codes can be distinguished because they are always negative numbers (more information on negative numbers can be found in Chapter 10. Counting Like a Computer). `write` is system call 4, and it requires the same parameters as the `read` system call, except that the buffer should already be filled with the data to write out. The `write` system call will give back the number of bytes written in *%eax* or an error code.
4. When you are through with your files, you can then tell Linux to close them. Afterwards, your file descriptor is no longer valid. This is done using `close`, system call 6. The only parameter to `close` is the file descriptor, which is placed in *%ebx*.

5.2 Buffers and `.bss`

In the previous section we mentioned buffers without explaining what they were. A buffer is a continuous block of bytes used for bulk data transfer. When you request to read a file, the operating system needs to have a place to store the data it reads. That place is called a buffer. Usually buffers are only used to store data temporarily, and it is then read from the buffers and converted to a form that is easier for the programs to handle. Our programs won't be complicated enough to need that done. For an example, let's say that you want to read in a single line of text from a file but you do not know how long that line is. You would then

[27] This will be explained in more detail in Truth, Falsehood, and Binary Numbers.

simply read a large number of bytes/characters from the file into a buffer, look for the end-of-line character, and copy all of the characters to that end-of-line character to another location. If you didn't find an end-of-line character, you would allocate another buffer and continue reading. You would probably wind up with some characters left over in your buffer in this case, which you would use as the starting point when you next need data from the file.[28]

Another thing to note is that buffers are a fixed size, set by the programmer. So, if you want to read in data 500 bytes at a time, you send the `read` system call the address of a 500-byte unused location, and send it the number 500 so it knows how big it is. You can make it smaller or bigger, depending on your application's needs.

To create a buffer, you need to either reserve static or dynamic storage. Static storage is what we have talked about so far, storage locations declared using `.long` or `.byte` directives. Dynamic storage will be discussed in Getting More Memory. There are problems, though, with declaring buffers using `.byte`. First, it is tedious to type. You would have to type 500 numbers after the `.byte` declaration, and they wouldn't be used for anything but to take up space. Second, it uses up space in the executable. In the examples we've used so far, it doesn't use up too much, but that can change in larger programs. If you want 500 bytes you have to type in 500 numbers and it wastes 500 bytes in the executable. There is a solution to both of these. So far, we have discussed two program sections, the `.text` and the `.data` sections. There is another section called the `.bss`. This section is like the data section, except that it doesn't take up space in the executable. This section can reserve storage, but it can't initialize it. In the `.data` section, you could reserve storage and set it to an initial value. In the `.bss` section, you can't set an initial value. This is useful for buffers because we don't need to initialize them anyway, we just need to reserve storage. In order to do this, we do the following commands:

```
.section .bss
    .lcomm my_buffer, 500
```

This directive, `.lcomm`, will create a symbol, `my_buffer`, that refers to a 500-byte storage location that we can use as a buffer. We can then do the following, assuming we have opened a file for reading and have placed the file descriptor in *%ebx*:

```
movl $my_buffer, %ecx
movl 500, %edx
movl 3, %eax
int  $0x80
```

This will read up to 500 bytes into our buffer. In this example, I placed a dollar sign in front of `my_buffer`. Remember that the reason for this is that without the dollar sign, `my_buffer` is treated as a memory location, and is accessed in direct addressing mode. The dollar sign switches it to immediate mode addressing, which actually loads the number represented by `my_buffer` itself (i.e. - the address of the start of our buffer, which is the address of `my_buffer`) into *%ecx*.

5.3 Standard and Special Files

You might think that programs start without any files open by default. This is not true. Linux programs usually have at least three open file descriptors when they begin. They are:

STDIN:
This is the *standard input*. It is a read-only file, and usually represents your keyboard.[29] This is always file descriptor 0.

STDOUT:
This is the *standard output*. It is a write-only file, and usually represents your screen display. This is always file descriptor 1.

[28] While this sounds complicated, most of the time in programming you will not need to deal directly with buffers and file descriptors. In Sharing Functions with Code Libraries you will learn how to use existing code present in Linux to handle most of the complications of file input/output for you.

[29] As we mentioned earlier, in Linux, almost everything is a "file". Your keyboard input is considered a file, and so is your screen display.

STDERR:
This is your *standard error*. It is a write-only file, and usually represents your screen display. Most regular processing output goes to `STDOUT`, but any error messages that come up in the process go to `STDERR`. This way, if you want to, you can split them up into separate places. This is always file descriptor 2.

Any of these "files" can be redirected from or to a real file, rather than a screen or a keyboard. This is outside the scope of this book, but any good book on the UNIX command-line will describe it in detail. The program itself does not even need to be aware of this indirection - it can just use the standard file descriptors as usual.

Notice that many of the files you write to aren't files at all. UNIX-based operating systems treat all input/output systems as files. Network connections are treated as files, your serial port is treated like a file, even your audio devices are treated as files. Communication between processes is usually done through special files called pipes. Some of these files have different methods of opening and creating them than regular files (i.e. - they don't use the `open` system call), but they can all be read from and written to using the standard `read` and `write` system calls.

5.4 Using Files in a Program

We are going to write a simple program to illustrate these concepts. The program will take two files, and read from one, convert all of its lower-case letters to upper-case, and write to the other file. Before we do so, let's think about what we need to do to get the job done:

- Have a function that takes a block of memory and converts it to upper-case. This function would need an address of a block of memory and its size as parameters.
- Have a section of code that repeatedly reads in to a buffer, calls our conversion function on the buffer, and then writes the buffer back out to the other file.
- Begin the program by opening the necessary files.

Notice that I've specified things in reverse order that they will be done. That's a useful trick in writing complex programs - first decide the meat of what is being done. In this case, it's converting blocks of characters to upper-case. Then, you think about what all needs to be setup and processed to get that to happen. In this case, you have to open files, and continually read and write blocks to disk. One of the keys of programming is continually breaking down problems into smaller and smaller chunks until it's small enough that you can easily solve the problem. Then you can build these chunks back up until you have a working program.[30]

You may have been thinking that you will never remember all of these numbers being thrown at you - the system call numbers, the interrupt number, etc. In this program we will also introduce a new directive, `.equ` which should help out. `.equ` allows you to assign names to numbers. For example, if you did `.equ LINUX_SYSCALL, 0x80`, any time after that you wrote `LINUX_SYSCALL`, the assembler would substitute `0x80` for that. So now, you can write:

```
int $LINUX_SYSCALL
```

Which is much easier to read, and much easier to remember. Coding is complex, but there are a lot of things we can do like this to make it easier.

Here is the `005-01-toupper.s` program. Note that we have more labels than we actually use for jumps, because some of them are just there for clarity. Try to trace through the program and see what happens in various cases. An in-depth explanation of the program will follow.

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     This program converts an input file to an
5       #     output file with all letters converted to
6       #     uppercase.
7       #
```

[30] Maureen Sprankle's *Problem Solving and Programming Concepts* is an excellent book on the problem-solving process applied to computer programming.

```
8       # PROCESSING:
9       #     1) Open the input file.
10      #     2) Open the output file.
11      #     3) While we are not at the end of the input
12      #        file.
13      #        a) Read part of file into our memory
14      #           buffer.
15      #        b) Go through each byte of memory if the
16      #           byte is a lower-case letter, convert it
17      #           to uppercase.
18      #        c) Write the memory buffer to output file.
19      #
20      .section .data
21          # ----- CONSTANTS ----- #
22          #
23          # System call numbers.
24          #
25          .equ SYS_OPEN,   5
26          .equ SYS_WRITE,  4
27          .equ SYS_READ,   3
28          .equ SYS_CLOSE,  6
29          .equ SYS_EXIT,   1
30
31          # Options for open:
32          # Look at /usr/include/asm-generic/fcntl.h or
33          # /usr/include/asm/fcntl.h for various values.
34          # You can combine them by adding them or ORing
35          # them). It is discussed at greater length in
36          # "Counting Like a Computer".
37          #
38          .equ O_RDONLY,              0
39          .equ O_CREAT_WRONLY_TRUNC,  03101
40
41          # Standard file descriptors.
42          #
43          .equ STDIN,   0
44          .equ STDOUT,  1
45          .equ STDERR,  2
46
47          # System call interrupt.
48          #
49          .equ LINUX_SYSCALL,     0x80
50                                  # This is the return value
51                                  # of read which means we
52                                  # have hit the end of the
53                                  # file.
54          .equ END_OF_FILE,       0
55
56
57          .equ NUMBER_ARGUMENTS,  2
58
59      .section .bss
60          # Buffer:
```

```
61          #     This is where the data is loaded into
62          #     from the data file and written from into
63          #     the output file.  This should never
64          #     exceed 16,000 for various reasons.
65          #
66          .equ   BUFFER_SIZE,     500
67          .lcomm BUFFER_DATA,     BUFFER_SIZE
68
69      .section .text
70          .globl _start
71
72          # ----- STACK POSITIONS ----- #
73          #
74          .equ ST_SIZE_RESERVE,   8
75          .equ ST_FD_IN,         -4
76          .equ ST_FD_OUT,        -8
77          .equ ST_ARGC,           0  # Number of args
78          .equ ST_ARGV_0,         4  # Name of program.
79          .equ ST_ARGV_1,         8  # Input file name.
80          .equ ST_ARGV_2,         12 # Output file name.
81
82  _start:
83      # ----- INITIALIZE PROGRAM ----- #
84      #
85      movl  %esp, %ebp        # Save the stack pointer.
86                              # Allocate space for our
87                              # file descriptors on the
88                              # stack.
89      subl  $ST_SIZE_RESERVE, %esp
90
91  __open_files:
92
93  __open_fd_in:
94      # ----- OPEN INPUT FILE ----- #
95      #
96      movl  $SYS_OPEN, %eax   # Open syscall.
97      movl  ST_ARGV_1(%ebp), %ebx     # Input filename
98                                      # into %ebx.
99      movl  $0_RDONLY, %ecx   # Read-only flag.
100     movl  $0666, %edx       # This does not matter for
101                             # reading.
102     int   $LINUX_SYSCALL    # Call Linux.
103
104 __store_fd_in:
105     # ----- STORE INPUT FILE DESCRIPTION ----- #
106     #
107     movl  %eax, ST_FD_IN(%ebp)      # Save the given
108                                     # file descriptor.
109
110 __open_fd_out:
111     # ----- OPEN OUTPUT FILE ----- #
112     #
113     movl  $SYS_OPEN, %eax   # Open the file.
```

```
114                             # Output filename into %ebx
115     movl  ST_ARGV_2(%ebp), %ebx
116                             # Flags for writing to the
117                             # file.
118     movl  $O_CREAT_WRONLY_TRUNC, %ecx
119     movl  $0666, %edx       # Permission set for new
120                             # file (if it is created).
121     int   $LINUX_SYSCALL    # Call Linux.
122
123 __store_fd_out:
124     # ----- STORE OUTPUT FILE DESCRIPTION ----- #
125     #
126                             # Store the file descriptor
127                             # here.
128     movl  %eax, ST_FD_OUT(%ebp)
129
130     # ----- BEGIN MAIN LOOP ----- #
131     #
132 _read_loop_begin:
133     # ----- READ IN A BLOCK FROM THE INPUT FILE ----- #
134     #
135     movl  $SYS_READ, %eax
136                             # Get the input file
137                             # descriptor.
138     movl  ST_FD_IN(%ebp), %ebx
139                             # The location to read into
140     movl  $BUFFER_DATA, %ecx
141                             # The size of the buffer.
142     movl  $BUFFER_SIZE, %edx
143     int   $LINUX_SYSCALL    # Size of buffer read is
144                             # returned in %eax.
145
146     # ----- EXIT IF WE HAVE REACHED THE END ----- #
147     #
148                             # Check for end of file
149                             # marker.
150     cmpl  $END_OF_FILE, %eax
151     jle   _lower_case       # If found or on error, go
152                             # to the end.
153
154 __continue_read_loop:
155     # ----- CONVERT THE BLOCK TO UPPER CASE ----- #
156     #
157     pushl $BUFFER_DATA      # Location of buffer.
158     pushl %eax              # Size of the buffer.
159     call  _convert_to_upper
160     popl  %eax              # Get the size back.
161     addl  $4, %esp          # Restore %esp.
162
163     # --- WRITE THE BLOCK OUT TO THE OUTPUT FILE --- #
164     #
165     movl  %eax, %edx        # Size of the buffer.
166     movl  $SYS_WRITE, %eax
```

```
167                             # File to use.
168     movl  ST_FD_OUT(%ebp), %ebx
169                             # Location of the buffer.
170     movl  $BUFFER_DATA, %ecx
171     int   $LINUX_SYSCALL
172
173     # ----- CONTINUE THE LOOP ----- #
174     #
175     jmp   _read_loop_begin
176
177 _lower_case:
178     # ----- CLOSE THE FILES ----- #
179     # NOTE:
180     #     We do not need to do error checking on
181     #     these, because error conditions do not
182     #     signify anything special here.
183     #
184     movl  $SYS_CLOSE, %eax
185     movl  ST_FD_OUT(%ebp), %ebx
186     int   $LINUX_SYSCALL
187
188     movl  $SYS_CLOSE, %eax
189     movl  ST_FD_IN(%ebp), %ebx
190     int   $LINUX_SYSCALL
191
192     # ----- EXIT ----- #
193     #
194     movl  $SYS_EXIT, %eax
195     movl  $0, %ebx
196     int   $LINUX_SYSCALL
197
198
199     # PURPOSE:
200     #     This function actually does the
201     #     conversion to upper case for a block.
202     #
203     # INPUT:
204     #     The first parameter is the length of
205     #     the block of memory to convert.
206     #
207     #     The second parameter is the starting
208     #     address of that block of memory.
209     #
210     # OUTPUT:
211     #     This function overwrites the current
212     #     buffer with the upper-casified version.
213     #
214     # VARIABLES:
215     #     %eax - beginning of buffer.
216     #     %ebx - length of buffer.
217     #     %edi - current buffer offset.
218     #     %cl -  current byte being examined (first
219     #            part of %ecx).
```

```
220     #
221     # ----- CONSTANTS ----- #
222     #
223                             # The lower boundary of our
224                             # search.
225         .equ  LOWERCASE_A,       'a'
226                             # The upper boundary of our
227                             # search.
228         .equ  LOWERCASE_Z,       'z'
229                             # Conversion between upper
230                             # lower case.
231         .equ  UPPER_CONVERSION,  'A' - 'a'
232
233     # ----- STACK STUFF ----- #
234     #
235         .equ  ST_BUFFER,      12    # Actual buffer.
236         .equ  ST_BUFFER_LEN,  8     # Length of buffer.
237
238 _convert_to_upper:
239     pushl %ebp
240     movl  %esp, %ebp
241
242     # ----- SET UP VARIABLES ----- #
243     #
244     movl  ST_BUFFER(%ebp), %eax
245     movl  ST_BUFFER_LEN(%ebp), %ebx
246     movl  $0, %edi
247
248     cmpl  $0, %ebx          # If a buffer with zero
249                             # length was given to us,
250                             # just leave.
251     je    _end_convert_loop
252
253 _convert_loop:
254                             # Get the current byte.
255     movb  (%eax,%edi,1), %cl
256
257                             # Go to the next byte
258                             # unless it is between 'a'
259                             # and 'z'.
260     cmpb  $LOWERCASE_A, %cl
261
262     jl    _next_byte
263     cmpb  $LOWERCASE_Z, %cl
264     jg    _next_byte
265
266                             # Otherwise convert the
267                             # byte to uppercase and
268                             # store it back.
269     addb  $UPPER_CONVERSION, %cl
270
271     movb  %cl, (%eax,%edi,1)
272
```

```
273 _next_byte:
274     incl  %edi              # Next byte.
275     cmpl  %edi, %ebx        # Continue unless we have
276                             # reached the end.
277     jne   _convert_loop
278
279 _end_convert_loop:
280     movl  %ebp, %esp        # No return value, just
281     popl  %ebp              # leave.
282     ret
```

Type in this program as `005-01-toupper.s`, and then enter in the following commands:

```
as -o 005-01-toupper.o  --32 \
                        --gstabs+ \
                        005-01-toupper.s

ld -o 005-01-toupper    -m elf_i386 \
                        005-01-toupper.o
```

This builds a program called `005-01-toupper`, which converts all of the lowercase characters in a file to uppercase. For example, to convert the file `005-01-toupper.s` to uppercase, type in the following command:

```
./005-01-toupper 005-01-toupper.s 005-01-toupper.uppercase
```

You will now find in the file `005-01-toupper.uppercase` an uppercase version of your original file.

Let's examine how the program works.

The first section of the program is marked `CONSTANTS`. In programming, a constant is a value that is assigned when a program assembles or compiles, and is never changed. I make a habit of placing all of my constants together at the beginning of the program. It's only necessary to declare them before you use them, but putting them all at the beginning makes them easy to find. Making them all upper-case makes it obvious in your program which values are constants and where to find them.[31] In assembly language, we declare constants with the `.equ` directive as mentioned before. Here, we simply give names to all of the standard numbers we've used so far, like system call numbers, the syscall interrupt number, and file open options.

The next section is marked `BUFFERS`. We only use one buffer in this program, which we call `BUFFER_DATA`. We also define a constant, `BUFFER_SIZE`, which holds the size of the buffer. If we always refer to this constant rather than typing out the number 500 whenever we need to use the size of the buffer, if it later changes, we only need to modify this value, rather than having to go through the entire program and changing all of the values individually.

Instead of going on to the `_start` section of the program, go to the end where we define the `_convert_to_upper` function. This is the part that actually does the conversion.

This section begins with a list of constants that we will use The reason these are put here rather than at the top is that they only deal with this one function. We have these definitions:

```
223                             # The lower boundary of our
224                             # search.
225         .equ  LOWERCASE_A,      'a'
226                             # The upper boundary of our
227                             # search.
228         .equ  LOWERCASE_Z,      'z'
229                             # Conversion between upper
230                             # lower case.
231         .equ  UPPER_CONVERSION, 'A' - 'a'
```

[31] This is fairly standard practice among programmers in all languages.

The first two simply define the letters that are the boundaries of what we are searching for. Remember that in the computer, letters are represented as numbers. Therefore, we can use `LOWERCASE_A` in comparisons, additions, subtractions, or anything else we can use numbers in. Also, notice we define the constant `UPPER_CONVERSION`. Since letters are represented as numbers, we can subtract them. Subtracting an upper-case letter from the same lower-case letter gives us how much we need to add to a lower-case letter to make it upper case. If that doesn't make sense, look at the ASCII code tables themselves (see the Appendix D. Table of ASCII Codes). You'll notice that the number for the character `A` is 65 and the character `a` is 97. The conversion factor is then −32. For any lowercase letter if you add −32, you will get its capital equivalent.

After this, we have some constants labelled `STACK POSITIONS`. Remember that function parameters are pushed onto the stack before function calls. These constants (prefixed with `ST` for clarity) define where in the stack we should expect to find each piece of data. The return address is at position 4 + *%esp*, the length of the buffer is at position 8 + *%esp*, and the address of the buffer is at position 12 + *%esp*. Using symbols for these numbers instead of the numbers themselves makes it easier to see what data is being used and moved.

Next comes the label `_convert_to_upper`. This is the entry point of the function. The first two lines are our standard function lines to save the stack pointer. The next two lines:

```
244     movl  ST_BUFFER(%ebp), %eax
245     movl  ST_BUFFER_LEN(%ebp), %ebx
```

Move the function parameters into the appropriate registers for use. Then, we load zero into *%edi*. What we are going to do is iterate through each byte of the buffer by loading from the location *%eax* + *%edi*, incrementing *%edi*, and repeating until *%edi* is equal to the buffer length stored in *%ebx*. The lines:

```
248     cmpl  $0, %ebx          # If a buffer with zero
249                             # length was given to us,
250                             # just leave.
251     je    _end_convert_loop
```

They are just a sanity check to make sure that no one gave us a buffer of zero size. If they did, we just clean up and leave. Guarding against potential user and programming errors is an important task of a programmer. You can always specify that your function should not take a buffer of zero size, but it's even better to have the function check and have a reliable exit plan if it happens.

Now we start our loop. First, it moves a byte into *%cl*. The code for this is:

```
254                             # Get the current byte.
255     movb  (%eax,%edi,1), %cl
```

It is using an indexed indirect addressing mode. It says to start at *%eax* and go *%edi* locations forward, with each location being 1 byte big. It takes the value found there, and put it in *%cl*. After this it checks to see if that value is in the range of lower-case *a* to lower-case *z*. To check the range, it simply checks to see if the letter is smaller than *a*. If it is, it can't be a lower-case letter. Likewise, if it is larger than *z*, it can't be a lower-case letter. So, in each of these cases, it simply moves on. If it is in the proper range, it then adds the uppercase conversion, and stores it back into the buffer.

Either way, it then goes to the next value by incrementing %cl;. Next it checks to see if we are at the end of the buffer. If we are not at the end, we jump back to the beginning of the loop (the `_convert_loop` label). If we are at the end, it simply continues on to the end of the function. Because we are modifying the buffer directly, we don't need to return anything to the calling program - the changes are already in the buffer. The label `_end_convert_loop` is not needed, but it's there so it's easy to see where the parts of the program are.

Now we know how the conversion process works. Now we need to figure out how to get the data in and out of the files.

Before reading and writing the files we must open them. The UNIX `open` system call is what handles this. It takes the following parameters:

- *%eax* contains the system call number as usual - 5 in this case.
- *%ebx* contains a pointer to a string that is the name of the file to open. The string must be terminated with the null character.

- *%ecx* contains the options used for opening the file. These tell Linux how to open the file. They can indicate things such as open for reading, open for writing, open for reading and writing, create if it doesn't exist, delete the file if it already exists, etc. We will not go into how to create the numbers for the options until Truth, Falsehood, and Binary Numbers. For now, just trust the numbers we come up with.
- *%edx* contains the permissions that are used to open the file. This is used in case the file has to be created first, so Linux knows what permissions to create the file with. These are expressed in octal, just like regular UNIX permissions.[32]

After making the system call, the file descriptor of the newly-opened file is stored in *%eax*.

So, what files are we opening? In this example, we will be opening the files specified on the command-line. Fortunately, command-line parameters are already stored by Linux in an easy-to-access location, and are already null-terminated. When a Linux program begins, all pointers to command-line arguments are stored on the stack. The number of arguments is stored at `(%esp)`, the name of the program is stored at `4(%esp)`, and the arguments are stored from `8(%esp)` on. In the C Programming language, this is referred to as the `argv` array, so we will refer to it that way in our program.

The first thing our program does is save the current stack position in *%ebp* and then reserve some space on the stack to store the file descriptors. After this, it starts opening files.

The first file the program opens is the input file, which is the first command-line argument. We do this by setting up the system call. We put the file name into *%ebx*, the read-only mode number into *%ecx*, the default mode of `$0666` into *%edx*, and the system call number into *%eax* After the system call, the file is open and the file descriptor is stored in *%eax*.[33] The file descriptor is then transferred to its appropriate place on the stack.

The same is then done for the output file, except that it is created with a write-only, create-if-doesn't-exist, truncate-if-does-exist mode. Its file descriptor is stored as well.

Now we get to the main part - the read/write loop. Basically, we will read fixed-size chunks of data from the input file, call our conversion function on it, and write it back to the output file. Although we are reading fixed-size chunks, the size of the chunks don't matter for this program - we are just operating on straight sequences of characters. We could read it in with as little or as large of chunks as we want, and it still would work properly.

The first part of the loop is to read the data. This uses the `read` system call. This call just takes a file descriptor to read from, a buffer to write into, and the size of the buffer (i.e. - the maximum number of bytes that could be written). The system call returns the number of bytes actually read, or end-of-file (the number 0).

After reading a block, we check *%eax* for an end-of-file marker. If found, it exits the loop. Otherwise we keep on going.

After the data is read, the `convert_to_upper` function is called with the buffer we just read in and the number of characters read in the previous system call. After this function executes, the buffer should be capitalized and ready to write out. The registers are then restored with what they had before.

Finally, we issue a `write` system call, which is exactly like the `read` system call, except that it moves the data from the buffer out to the file. Now we just go back to the beginning of the loop.

After the loop exits (remember, it exits if, after a read, it detects the end of the file), it simply closes its file descriptors and exits. The close system call just takes the file descriptor to close in *%ebx*.

The program is then finished!

5.5 Review

5.5.1 Know the Concepts

- Describe the lifecycle of a file descriptor.
- What are the standard file descriptors and what are they used for?
- What is a buffer?

[32] If you aren't familiar with UNIX permissions, just put `$0666` here. Don't forget the leading zero, as it means that the number is an octal number.

[33] Notice that we don't do any error checking on this. That is done just to keep the program simple. In normal programs, every system call should normally be checked for success or failure. In failure cases, *%eax* will hold an error code instead of a return value. Error codes are negative, so they can be detected by comparing *%eax* to zero and jumping if it is less than zero.

- What is the difference between the `.data` section and the `.bss` section?
- What are the system calls related to reading and writing files?

5.5.2 Use the Concepts

- Modify the `005-01-toupper` program so that it reads from `STDIN` and writes to `STDOUT` instead of using the files on the command-line.
- Change the size of the buffer.
- Rewrite the program so that it uses storage in the `.bss` section rather than the stack to store the file descriptors.
- Write a program that will create a file called `heynow.txt` and write the words "Hey diddle diddle!" into it.

5.5.3 Going Further

- What difference does the size of the buffer make?
- What error results can be returned by each of these system calls?
- Make the program able to either operate on command-line arguments or use `STDIN` or `STDOUT` based on the number of command-line arguments specified by `ARGC`.
- Modify the program so that it checks the results of each system call, and prints out an error message to `STDOUT` when it occurs.

6. Reading and Writing Simple Records

As mentioned in Chapter 5. Dealing with Files, many applications deal with data that is *persistent* - meaning that the data lives longer than the program by being stored on disk in files. You can shut down the program and open it back up, and you are back where you started. Now, there are two basic kinds of persistent data - structured and unstructured. Unstructured data is like what we dealt with in the `005-01-toupper` program. It just dealt with text files that were entered by a person. The contents of the files weren't usable by a program because a program can't interpret what the user is trying to say in random text.

Structured data, on the other hand, is what computers excel at handling. Structured data is data that is divided up into fields and records. For the most part, the fields and records are fixed-length. Because the data is divided into fixed-length records and fixed-format fields, the computer can interpret the data. Structured data can contain variable-length fields, but at that point you are usually better off with a database.[34]

This chapter deals with reading and writing simple fixed-length records. Let's say we wanted to store some basic information about people we know. We could imagine the following example fixed-length record about people:

- Firstname - 40 bytes.
- Lastname - 40 bytes.
- Address - 240 bytes.
- Age - 4 bytes.

In this, everything is character data except for the age, which is simply a numeric field, using a standard 4-byte word (we could just use a single byte for this, but keeping it at a word makes it easier to process).

In programming, you often have certain definitions that you will use over and over again within the program, or perhaps within several programs. It is good to separate these out into files that are simply included into the assembly language files as needed. For example, in our next programs we will need to access the different parts of the record above. This means we need to know the offsets of each field from the beginning of the record in order to access them using base pointer addressing mode. The following constants describe the offsets to the above structure. Put them in a file named `006-01-record-def.s`:

```
3           .equ RECORD_FIRSTNAME,  0
4           .equ RECORD_LASTNAME,   40
5           .equ RECORD_ADDRESS,    80
6           .equ RECORD_AGE,        320
7           .equ RECORD_SIZE,       324
```

In addition, there are several constants that we have been defining over and over in our programs, and it is useful to put them in a file, so that we don't have to keep entering them. Put the following constants in a file called `006-01-linux.s`:

```
3       # ----- Common Linux Definitions ----- #
4       #
5       # System Call Numbers.
6       #
7           .equ SYS_EXIT,      1
```

[34] A database is a program which handles persistent structured data for you. You don't have to write the programs to read and write the data to disk, to do lookups, or even to do basic processing. It is a very high-level interface to structured data which, although it adds some overhead and additional complexity, is very useful for complex data processing tasks. References for learning how databases work are listed in Chapter 13. Moving On from Here.

```
8           .equ SYS_READ,       3
9           .equ SYS_WRITE,      4
10          .equ SYS_OPEN,       5
11          .equ SYS_CLOSE,      6
12          .equ SYS_BRK,        45
13
14      # System Call Interrupt Number.
15      #
16          .equ LINUX_SYSCALL,  0x80
17
18      # Standard File Descriptors.
19      #
20          .equ STDIN,          0
21          .equ STDOUT,         1
22          .equ STDERR,         2
23
24      # Common Status Codes.
25      #
26          .equ END_OF_FILE,    0
```

We will write three programs in this chapter using the structure defined in `006-01-record-def.s`. The first program will build a file containing several records as defined above. The second program will display the records in the file. The third program will add 1 year to the age of every record.

In addition to the standard constants we will be using throughout the programs, there are also two functions that we will be using in several of the programs - one which reads a record and one which writes a record.

What parameters do these functions need in order to operate? We basically need:

- The location of a buffer that we can read a record into.
- The file descriptor that we want to read from or write to.

Let's look at our reading function first in `006-01-read-record.s`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       .include "006-01-linux.s"      # Linux Definitions.
4       .include "006-01-record-def.s" # Record definitions
5
6       # PURPOSE:
7       #     This function reads a record from the file
8       #     descriptor.
9       #
10      # INPUT:
11      #     The file descriptor and a buffer.
12      #
13      # OUTPUT:
14      #     This function writes the data to the buffer
15      #     and returns a status code.
16      #
17      # ----- STACK LOCAL VARIABLES ----- #
18      #
19          .equ ST_READ_BUFFER,  8
20          .equ ST_FILEDES,      12
21
22      .section .text
23          .globl _read_record
```

```
24          .type  _read_record,  @function
25
26  _read_record:
27      pushl %ebp
28      movl  %esp, %ebp
29
30      pushl %ebx
31      movl  ST_FILEDES(%ebp), %ebx
32      movl  ST_READ_BUFFER(%ebp), %ecx
33      movl  $RECORD_SIZE, %edx
34      movl  $SYS_READ, %eax
35      int   $LINUX_SYSCALL
36
37      popl  %ebx          # NOTE - %eax has the return
38                          # value, which we will give
39                          # back to our calling program.
40
41      movl  %ebp, %esp
42      popl  %ebp
43      ret
```

It's a pretty simple function. It just reads data the size of our structure into an appropriately sized buffer from the given file descriptor. The writing one is similar in `006-01-write-record.s`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       .include "006-01-linux.s"      # Linux Definitions.
4       .include "006-01-record-def.s" # Record definitions
5
6       # PURPOSE:
7       #     This function writes a record to the given
8       #     file descriptor.
9       #
10      # INPUT:
11      #     The file descriptor and a buffer.
12      #
13      # OUTPUT:
14      #     This function produces a status code.
15      #
16      # ----- STACK LOCAL VARIABLES ----- #
17      #
18          .equ ST_WRITE_BUFFER,  8
19          .equ ST_FILEDES,       12
20
21      .section .text
22          .globl _write_record
23          .type  _write_record,  @function
24
25  _write_record:
26      pushl %ebp
27      movl  %esp, %ebp
28
29      pushl %ebx
30      movl  $SYS_WRITE, %eax
```

```
31      movl  ST_FILEDES(%ebp), %ebx
32      movl  ST_WRITE_BUFFER(%ebp), %ecx
33      movl  $RECORD_SIZE, %edx
34      int   $LINUX_SYSCALL
35
36      popl  %ebx      # NOTE - %eax has the return value,
37                      # which we will give back to our
38                      # calling program.
39
40      movl  %ebp, %esp
41      popl  %ebp
42      ret
```

Now that we have our basic definitions down, we are ready to write our programs.

6.1 Writing Records

This program will simply write some hardcoded records to disk. It will:

- Open the file.
- Write three records.
- Close the file.

Type the following code into a file called `006-01-write-records.s`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       .include "006-01-linux.s"      # Linux Definitions.
4       .include "006-01-record-def.s" # Record definitions
5
6       .section .data
7           # ----- CONSTANTS ----- #
8           #
9           # Constant data of the records we want to
10          # write. Each text data item is padded to the
11          # proper length with null (i.e. 0) bytes.
12          #
13          # `.rept` is used to pad each item.  It tells
14          # the assembler to repeat the section between
15          # `.rept` and `.endr` the number of times
16          # specified. This is used in this program to
17          # add extra null characters at the end of each
18          # field to fill it up.
19          #
20          record1:
21              .ascii "Fredrick\0"
22              .rept 31            # Padding to 40 bytes.
23              .byte 0
24              .endr
25
26              .ascii "Bartlett\0"
27              .rept 31            # Padding to 40 bytes.
28              .byte 0
29              .endr
```

```
30
31              .ascii "4242 S Prairie\nTulsa, OK 55555\0"
32              .rept 209           # Padding to 240 bytes.
33              .byte 0
34              .endr
35
36              .long 45
37
38          record2:
39              .ascii "Marilyn\0"
40              .rept 32            # Padding to 40 bytes.
41              .byte 0
42              .endr
43
44              .ascii "Taylor\0"
45              .rept 33            # Padding to 40 bytes.
46              .byte 0
47              .endr
48
49              .ascii "2224 S Johannan St\n"
50              .ascii "Chicago, IL 12345\0"
51              .rept 203           # Padding to 240 bytes.
52              .byte 0
53              .endr
54
55              .long 29
56
57          record3:
58              .ascii "Derrick\0"
59              .rept 32            # Padding to 40 bytes.
60              .byte 0
61              .endr
62
63              .ascii "McIntire\0"
64              .rept 31            # Padding to 40 bytes.
65              .byte 0
66              .endr
67
68              .ascii "500 W Oakland\n"
69              .ascii "San Diego, CA 54321\0"
70              .rept 206           # Padding to 240 bytes.
71              .byte 0
72              .endr
73
74              .long 36
75
76          file_name:
77                              # This is the name of the
78                              # file we will write to.
79              .ascii "test.dat\0"
80
81
82          .equ ST_FILE_DESCRIPTOR,  -4
```

```
83
84          .globl _start
85
86  _start:
87      movl  %esp, %ebp        # Copy the stack pointer to
88                              # %ebp.
89      subl  $4, %esp          # Allocate space to hold
90                              # the file descriptor.
91
92      movl  $SYS_OPEN, %eax   # Open the file.
93      movl  $file_name, %ebx
94      movl  $0101, %ecx       # This says to create if it
95                              # does not exist, and open
96                              # for writing.
97      movl  $0666, %edx
98      int   $LINUX_SYSCALL
99
100                             # Store the file descriptor
101                             # away.
102     movl  %eax, ST_FILE_DESCRIPTOR(%ebp)
103
104                             # Write the first record.
105     pushl ST_FILE_DESCRIPTOR(%ebp)
106     pushl $record1
107     call  _write_record
108     addl  $8, %esp
109
110                             # Write the second record.
111     pushl ST_FILE_DESCRIPTOR(%ebp)
112     pushl $record2
113     call  _write_record
114     addl  $8, %esp
115
116                             # Write the third record.
117     pushl ST_FILE_DESCRIPTOR(%ebp)
118     pushl $record3
119     call  _write_record
120     addl  $8, %esp
121
122                             # Close the file descriptor
123     movl  $SYS_CLOSE, %eax
124     movl  ST_FILE_DESCRIPTOR(%ebp), %ebx
125     int   $LINUX_SYSCALL
126
127                             # Exit the program.
128     movl  $SYS_EXIT, %eax
129     movl  $0, %ebx
130     int   $LINUX_SYSCALL
```

This is a fairly simple program. It merely consists of defining the data we want to write in the `.data` section, and then calling the right system calls and function calls to accomplish it. For a refresher of all of the system calls used, see Appendix C. Important System Calls.

You may have noticed the lines:

```
3       .include "006-01-linux.s"      # Linux Definitions.
4       .include "006-01-record-def.s" # Record definitions
```

These statements cause the given files to basically be pasted right there in the code. You don't need to do this with functions, because the linker can take care of combining functions exported with `.globl`. However, constants defined in another file do need to be imported in this way.

Also, you may have noticed the use of a new assembler directive, `.rept`. This directive repeats the contents of the file between the `.rept` and the `.endr` directives the number of times specified after `.rept`. This is usually used the way we used it - to pad values in the `.data` section. In our case, we are adding null characters to the end of each field until they are their defined lengths.

To build the application, run the commands:

```
as -o 006-01-write-record.o   --32 \
                              --gstabs+ \
                              006-01-write-record.s

as -o 006-01-write-records.o  --32 \
                              --gstabs+ \
                              006-01-write-records.s

ld -o 006-01-write-records    -m elf_i386 \
                              006-01-write-record.o \
                              006-01-write-records.o
```

Here we are assembling two files separately, and then combining them together using the linker. To run the program, just type the following:

```
./006-01-write-records
```

This will cause a file called `test.dat` to be created containing the records. However, since they contain non-printable characters (the null character, specifically), they may not be viewable by a text editor. Therefore we need the next program to read them for us.

6.2 Reading Records

Now we will consider the process of reading records. In this program, we will read each record and display the first name listed with each record.

Since each person's name is a different length, we will need a function to count the number of characters we want to write. Since we pad each field with null characters, we can simply count characters until we reach a null character.[35] Note that this means our records must contain at least one null character each.

Here is the code. Put it in a file called `006-01-count-chars.s`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Count the characters until a null byte is
5       #     reached.
6       #
7       # INPUT:
8       #     The address of the character string.
9       #
10      # OUTPUT:
11      #     Returns the count in %eax.
12      #
```

[35] If you have used C, this is what the `strlen` function does.

```
13      # PROCESS:
14      #     Registers used:
15      #       %ecx - character count.
16      #       %al  - current character.
17      #       %edx - current character address.
18      #
19          .globl _count_chars
20          .type  _count_chars,  @function
21
22                                # The parameter is on the
23                                # stack.
24          .equ ST_STRING_START_ADDRESS,  8
25
26  _count_chars:
27      pushl %ebp
28      movl  %esp, %ebp
29
30      movl  $0, %ecx          # Counter starts at zero.
31
32                              # Starting address of data.
33      movl  ST_STRING_START_ADDRESS(%ebp), %edx
34
35  _count_loop_begin:
36      movb  (%edx), %al       # Grab the current
37                              # character.
38
39      cmpb  $0, %al           # Is it null?
40      je    _count_loop_end   # If yes, we are done.
41
42      incl  %ecx              # Otherwise, increment the
43                              # counter and the pointer.
44      incl  %edx
45      jmp   _count_loop_begin # Go back to the beginning
46                              # of the loop.
47
48  _count_loop_end:
49      movl  %ecx, %eax        # We are done.  Move the
50                              # count into %eax and
51                              # return.
52
53      popl  %ebp
54      ret
```

As you can see, it's a fairly straightforward function. It simply loops through the bytes, counting as it goes, until it hits a null character. Then it returns the count.

Our record-reading program will be fairly straightforward, too. It will do the following:

- Open the file.
- Attempt to read a record.
- If we are at the end of the file, exit.
- Otherwise, count the characters of the first name.
- Write the first name to `STDOUT`.
- Write a newline to `STDOUT`.

- Go back to read another record.

To write this, we need one more simple function - a function to write out a newline to `STDOUT`. Put the following code into `006-01-write-newline.s`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       .include "006-01-linux.s"      # Linux Definitions.
4
5           .globl _write_newline
6           .type  _write_newline,  @function
7
8       .section .data
9           newline:
10              .ascii "\n"
11
12      .section .text
13          .equ ST_FILEDES,  8
14
15  _write_newline:
16      pushl %ebp
17      movl  %esp, %ebp
18
19      movl  $SYS_WRITE, %eax
20      movl  ST_FILEDES(%ebp), %ebx
21      movl  $newline, %ecx
22      movl  $1, %edx
23      int   $LINUX_SYSCALL
24
25      movl  %ebp, %esp
26      popl  %ebp
27      ret
```

Now we are ready to write the main program. Here is the code to `006-01-read-records.s`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       .include "006-01-linux.s"      # Linux Definitions.
4       .include "006-01-record-def.s" # Record definitions
5
6       .section .data
7           file_name:
8               .ascii "test.dat\0"
9
10      .section .bss
11          .lcomm record_buffer,  RECORD_SIZE
12
13      .section .text
14          .globl _start
15
16  _start:
17      # ----- Main Program ----- #
18      #
19      # These are the locations on the stack where we
20      # will store the input and output descriptors
21      # (FYI - we could have used memory addresses in a
```

```
22      # .data section instead).
23      #
24      .equ ST_INPUT_DESCRIPTOR,   -4
25      .equ ST_OUTPUT_DESCRIPTOR,  -8
26
27      movl  %esp, %ebp        # Copy the stack pointer to
28                              # %ebp.
29      subl  $8, %esp          # Allocate space to hold
30                              # the file descriptors.
31
32      movl  $SYS_OPEN, %eax   # Open the file.
33      movl  $file_name, %ebx
34      movl  $0, %ecx          # This says to open
35                              # read-only.
36      movl  $0666, %edx
37      int   $LINUX_SYSCALL
38
39      # ----- Save file descriptor ----- #
40      #
41      movl  %eax, ST_INPUT_DESCRIPTOR(%ebp)
42
43      # Even though it is a constant, we are saving the
44      # output file descriptor in a local variable so
45      # that if we later decide that it is not always
46      # going to be STDOUT, we can change it easily.
47      #
48      movl  $STDOUT, ST_OUTPUT_DESCRIPTOR(%ebp)
49
50  _record_read_loop:
51      pushl ST_INPUT_DESCRIPTOR(%ebp)
52      pushl $record_buffer
53      call  _read_record
54      addl  $8, %esp
55
56      # Returns the number of bytes read. If it is not
57      # the same number we requested, then it is either
58      # an end-of-file, or an error, so we are quitting.
59      #
60      cmpl  $RECORD_SIZE, %eax
61      jne   _finished_reading
62
63      # Otherwise, print out the first name but we must
64      # know the size.
65      #
66      pushl  $RECORD_FIRSTNAME + record_buffer
67      call   _count_chars
68      addl   $4, %esp
69
70      movl   %eax, %edx
71      movl   ST_OUTPUT_DESCRIPTOR(%ebp), %ebx
72      movl   $SYS_WRITE, %eax
73      movl   $RECORD_FIRSTNAME + record_buffer, %ecx
74      int    $LINUX_SYSCALL
```

```
75
76      pushl   ST_OUTPUT_DESCRIPTOR(%ebp)
77      call    _write_newline
78      addl    $4, %esp
79
80      jmp     _record_read_loop
81
82  _finished_reading:
83      movl    $SYS_EXIT, %eax
84      movl    $0, %ebx
85      int     $LINUX_SYSCALL
```

To build this program, we need to assemble all of the parts and link them together:

```
as -o 006-01-count-chars.o    --32 \
                              --gstabs+ \
                              006-01-count-chars.s

as -o 006-01-read-record.o    --32 \
                              --gstabs+ \
                              006-01-read-record.s

as -o 006-01-read-records.o   --32 \
                              --gstabs+ \
                              006-01-read-records.s

as -o 006-01-write-newline.o  --32 \
                              --gstabs+ \
                              006-01-write-newline.s

ld -o 006-01-read-records     -m elf_i386 \
                              006-01-count-chars.o \
                              006-01-read-record.o \
                              006-01-read-records.o \
                              006-01-write-newline.o
```

The backslash in the first line simply means that the command continues on the next line. You can run your program by doing `./006-01-read-records`.

As you can see, this program opens the file and then runs a loop of reading, checking for the end of file, and writing the firstname. The one construct that might be new is the line that says:

```
66      pushl   $RECORD_FIRSTNAME + record_buffer
```

It looks like we are combining and add instruction with a push instruction, but we are not. You see, both `RECORD_FIRSTNAME` and `record_buffer` are constants. The first is a direct constant, created through the use of a `.equ` directive, while the latter is defined automatically by the assembler through its use as a label (it's value being the address that the data that follows it will start at). Since they are both constants that the assembler knows, it is able to add them together while it is assembling your program, so the whole instruction is a single immediate mode addressing push of a single constant.

The `RECORD_FIRSTNAME` constant is the number of bytes after the beginning of a record before we hit the first name. `record_buffer` is the name of our buffer for holding records. Adding them together gets us the address of the first name member of the record stored in `record_buffer`.

6.3 Modifying the Records

In this section, we will write a program that:

- Opens an input and output file.
- Reads records from the input.
- Increments the age.
- Writes the new record to the output file.

Like most programs we've encountered recently, this program `006-01-add-year.s` is pretty straightforward.[36]

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       .include "006-01-linux.s"      # Linux Definitions.
4       .include "006-01-record-def.s" # Record definitions
5
6       .section .data
7           input_file_name:
8               .ascii "test.dat\0"
9
10          output_file_name:
11              .ascii "testout.dat\0"
12
13      .section .bss
14          .lcomm record_buffer,  RECORD_SIZE
15
16          # --- Stack offsets of local variables --- #
17          #
18          .equ ST_INPUT_DESCRIPTOR,  -4
19          .equ ST_OUTPUT_DESCRIPTOR, -8
20
21      .section .text
22          .globl _start
23
24  _start:
25      movl  %esp, %ebp        # Copy stack pointer and
26      subl  $8, %esp          # make room for local
27                              # variables.
28
29      movl  $SYS_OPEN, %eax   # Open file for reading.
30      movl  $input_file_name, %ebx
31      movl  $0, %ecx
32      movl  $0666, %edx
33      int   $LINUX_SYSCALL
34
35      movl  %eax, ST_INPUT_DESCRIPTOR(%ebp)
36
37      movl  $SYS_OPEN, %eax   # Open file for writing.
38      movl  $output_file_name, %ebx
39      movl  $0101, %ecx
40      movl  $0666, %edx
41      int   $LINUX_SYSCALL
42
43      movl  %eax, ST_OUTPUT_DESCRIPTOR(%ebp)
44
```

[36]You will find that after learning the mechanics of programming, most programs are pretty straightforward once you know exactly what it is you want to do. Most of them initialize data, do some processing in a loop, and then clean everything up.

```
45  _loop_begin:
46      pushl ST_INPUT_DESCRIPTOR(%ebp)
47      pushl $record_buffer
48      call  _read_record
49      addl  $8, %esp
50
51      # Returns the number of bytes read. If it is not
52      # the same number we requested, then it is either
53      # an end-of-file, or an error, so we are quitting.
54      #
55      cmpl  $RECORD_SIZE, %eax
56      jne   _loop_end
57
58                              # Increment the age.
59      incl  record_buffer + RECORD_AGE
60
61                              # Write the record out.
62      pushl ST_OUTPUT_DESCRIPTOR(%ebp)
63      pushl $record_buffer
64      call  _write_record
65      addl  $8, %esp
66
67      jmp   _loop_begin
68
69  _loop_end:
70      movl  $SYS_EXIT, %eax
71      movl  $0, %ebx
72      int   $LINUX_SYSCALL
```

You can type it in as `006-01-add-year.s`. To build it, type the following[37]:

```
as -o 006-01-add-year.o  --32 \
                         --gstabs+ \
                         006-01-add-year.s

ld -o 006-01-add-year    -m elf_i386 \
                         006-01-add-year.o \
                         006-01-read-record.o \
                         006-01-write-record.o
```

To run the program, just type in the following[38]:

```
./006-01-add-year
```

This will add a year to every record listed in `test.dat` and write the new records to the file `testout.dat`.

As you can see, writing fixed-length records is pretty simple. You only have to read in blocks of data to a buffer, process them, and write them back out. Unfortunately, this program doesn't write the new ages out to the screen so you can verify your program's effectiveness. This is because we won't get to displaying numbers until Sharing Functions with Code Libraries and Chapter 10. Counting Like a Computer. After reading those you may want to come back and rewrite this program to display the numeric data that we are modifying.

[37] This assumes that you have already built the object files `006-01-read-record.o` and `006-01-write-record.o` in the previous examples. If not, you will have to do so.

[38] This is assuming you created the file in a previous run of `006-01-write-records`. If not, you need to run `006-01-write-records` first before running this program.

6.4 Review

6.4.1 Know the Concepts

- What is a record?
- What is the advantage of fixed-length records over variable-length records?
- How do you include constants in multiple assembly source files?
- Why might you want to split up a project into multiple source files?
- What does the instruction `incl record_buffer + RECORD_AGE` do? What addressing mode is it using? How many operands does the `incl` instructions have in this case? Which parts are being handled by the assembler and which parts are being handled when the program is run?

6.4.2 Use the Concepts

- Add another data member to the person structure defined in this chapter, and rewrite the reading and writing functions and programs to take them into account. Remember to reassemble and relink your files before running your programs.
- Create a program that uses a loop to write 30 identical records to a file.
- Create a program to find the largest age in the file and return that age as the status code of the program.
- Create a program to find the smallest age in the file and return that age as the status code of the program.

6.4.3 Going Further

- Rewrite the programs in this chapter to use command-line arguments to specify the filenames.
- Research the `lseek` system call. Rewrite the `006-01-add-year` program to open the source file for both reading and writing (use $2 for the read/write mode), and write the modified records back to the same file they were read from.
- Research the various error codes that can be returned by the system calls made in these programs. Pick one to rewrite, and add code that checks *%eax* for error conditions, and, if one is found, writes a message about it to `STDERR` and exit.
- Write a program that will add a single record to the file by reading the data from the keyboard. Remember, you will have to make sure that the data has at least one null character at the end, and you need to have a way for the user to indicate they are done typing. Because we have not gotten into characters to numbers conversion, you will not be able to read the age in from the keyboard, so you'll have to have a default age.
- Write a function called `compare-strings` that will compare two strings up to 5 characters. Then write a program that allows the user to enter 5 characters, and have the program return all records whose first name starts with those 5 characters.

7. Developing Robust Programs

This chapter deals with developing programs that are *robust*. Robust programs are able to handle error conditions gracefully. They are programs that do not crash no matter what the user does. Building robust programs is essential to the practice of programming. Writing robust programs takes discipline and work - it usually entails finding every possible problem that can occur, and coming up with an action plan for your program to take.

7.1 Where Does the Time Go?

Programmers schedule poorly. In almost every programming project, programmers will take two, four, or even eight times as long to develop a program or function than they originally estimated. There are many reasons for this problem, including:

- Programmers don't always schedule time for meetings or other non-coding activities that make up every day.
- Programmers often underestimate feedback times (how long it takes to pass change requests and approvals back and forth) for projects.
- Programmers don't always understand the full scope of what they are producing.
- Programmers often have to estimate a schedule on a totally different kind of project than they are used to, and thus are unable to schedule accurately.
- Programmers often underestimate the amount of time it takes to get a program fully robust.

The last item is the one we are interested in here. *It takes a lot of time and effort to develop robust programs.* More so than people usually guess, including experienced programmers. Programmers get so focused on simply solving the problem at hand that they fail to look at the possible side issues.

In the `005-01-toupper` program, we do not have any course of action if the file the user selects does not exist. The program will go ahead and try to work anyway. It doesn't report any error message so the user won't even know that they typed in the name wrong. Let's say that the destination file is on a network drive, and the network temporarily fails. The operating system is returning a status code to us in *%eax*, but we aren't checking it. Therefore, if a failure occurs, the user is totally unaware. This program is definitely not robust. As you can see, even in a simple program there are a lot of things that can go wrong that a programmer must contend with.

In a large program, it gets much more problematic. There are usually many more possible error conditions than possible successful conditions. Therefore, you should always expect to spend the majority of your time checking status codes, writing error handlers, and performing similar tasks to make your program robust. If it takes two weeks to develop a program, it will likely take at least two more to make it robust. Remember that every error message that pops up on your screen had to be programmed in by someone.

7.2 Some Tips for Developing Robust Programs

7.2.1 User Testing

Testing is one of the most essential things a programmer does. If you haven't tested something, you should assume it doesn't work. However, testing isn't just about making sure your program works, it's about making sure your program doesn't break. For example, if I have a program that is only supposed to deal with positive numbers, you need to test what happens if the user enters a negative number. Or a letter. Or the number zero. You must test what happens if they put spaces before their numbers, spaces after their numbers, and other

little possibilities. You need to make sure that you handle the user's data in a way that makes sense to the user, and that you pass on that data in a way that makes sense to the rest of your program. When your program finds input that doesn't make sense, it needs to perform appropriate actions. Depending on your program, this may include ending the program, prompting the user to re-enter values, notifying a central error log, rolling back an operation, or ignoring it and continuing.

Not only should you test your programs, you need to have others test it as well. You should enlist other programmers and users of your program to help you test your program. If something is a problem for your users, even if it seems okay to you, it needs to be fixed. If the user doesn't know how to use your program correctly, that should be treated as a bug that needs to be fixed.

You will find that users find a lot more bugs in your program than you ever could. The reason is that users don't know what the computer expects. You know what kinds of data the computer expects, and therefore are much more likely to enter data that makes sense to the computer. Users enter data that makes sense to them. Allowing non-programmers to use your program for testing purposes usually gives you much more accurate results as to how robust your program truly is.

7.2.2 Data Testing

When designing programs, each of your functions needs to be very specific about the type and range of data that it will or won't accept. You then need to test these functions to make sure that they perform to specification when handed the appropriate data. Most important is testing *corner cases* or *edge cases*. Corner cases are the inputs that are most likely to cause problems or behave unexpectedly.

When testing numeric data, there are several corner cases you always need to test:

- The number 0.
- The number 1.
- A number within the expected range.
- A number outside the expected range.
- The first number in the expected range.
- The last number in the expected range.
- The first number below the expected range.
- The first number above the expected range.

For example, if I have a program that is supposed to accept values between 5 and 200, I should test 0, 1, 4, 5, 153, 200, 201, and 255 at a minimum (153 and 255 were randomly chosen inside and outside the range, respectively). The same goes for any lists of data you have. You need to test that your program behaves as expected for lists of 0 items, 1 item, massive numbers of items, and so on. In addition, you should also test any turning points you have. For example, if you have different code to handle people under and over age 30, for example, you would need to test it on people of ages 29, 30, and 31 at least.

There will be some internal functions that you assume get good data because you have checked for errors before this point. However, while in development you often need to check for errors anyway, as your other code may have errors in it. To verify the consistency and validity of data during development, most languages have a facility to easily check assumptions about data correctness. In the C language there is the `assert` macro. You can simply put in your code `assert(a > b);`, and it will give an error if it reaches that code when the condition is not true. In addition, since such a check is a waste of time after your code is stable, the `assert` macro allows you to turn off asserts at compile-time. This makes sure that your functions are receiving good data without causing unnecessary slowdowns for code released to the public.

7.2.3 Module Testing

Not only should you test your program as a whole, you need to test the individual pieces of your program. As you develop your program, you should test individual functions by providing it with data you create to make sure it responds appropriately.

In order to do this effectively, you have to develop functions whose sole purpose is to call functions for testing. These are called *drivers* (not to be confused with hardware drivers) . They simply load your function, supply it with data, and check the results. This is especially useful if you are working on pieces of an unfinished program. Since you can't test all of the pieces together, you can create a driver program that will test each function individually.

Also, the code you are testing may make calls to functions not developed yet. In order to overcome this problem, you can write a small function called a *stub* which simply returns the values that function needs to proceed. For example, in an e-commerce application, I had a function called `is_ready_to_checkout`. Before I had time to actually write the function I just set it to return true on every call so that the functions which relied on it would have an answer. This allowed me to test functions which relied on `is_ready_to_checkout` without the function being fully implemented.

7.3 Handling Errors Effectively

Not only is it important to know how to test, but it is also important to know what to do when an error is detected.

7.3.1 Have an Error Code for Everything

Truly robust software has a unique error code for every possible contingency. By simply knowing the error code, you should be able to find the location in your code where that error was signalled.

This is important because the error code is usually all the user has to go on when reporting errors. Therefore, it needs to be as useful as possible.

Error codes should also be accompanied by descriptive error messages. However, only in rare circumstances should the error message try to predict *why* the error occurred. It should simply relate what happened. Back in 1995 I worked for an Internet Service Provider. One of the web browsers we supported tried to guess the cause for every network error, rather than just reporting the error. If the computer wasn't connected to the Internet and the user tried to connect to a website, it would say that there was a problem with the Internet Service Provider, that the server was down, and that the user should contact their Internet Service Provider to correct the problem. Nearly a quarter of our calls were from people who had received this message, but merely needed to connect to the Internet before trying to use their browser. As you can see, trying to diagnose what the problem is can lead to a lot more problems than it fixes. It is better to just report error codes and messages, and have separate resources for the user to troubleshooting the application. A troubleshooting guide, not the program itself, is an appropriate place to list possible reasons and courses for action for each error message.

7.3.2 Recovery Points

In order to simplify error handling, it is often useful to break your program apart into distinct units, where each unit fails and is recovered as a whole. For example, you could break your program up so that reading the configuration file was a unit. If reading the configuration file failed at any point (opening the file, reading the file, trying to decode the file, etc.) then the program would simply treat it as a configuration file problem and skip to the *recovery point* for that problem. This way you greatly reduce the number of error-handling mechanism you need for your program, because error recovery is done on a much more general level.

Note that even with recovery points, your error messages need to be specific as to what the problem was. Recovery points are basic units for error recovery, not for error detection. Error detection still needs to be extremely exact, and the error reports need exact error codes and messages.

When using recovery points, you often need to include cleanup code to handle different contingencies. For example, in our configuration file example, the recovery function would need to include code to check and see if the configuration file was still open. Depending on where the error occurred, the file may have been left open. The recovery function needs to check for this condition, and any other condition that might lead to system instability, and return the program to a consistent state.

The simplest way to handle recovery points is to wrap the whole program into a single recovery point. You would just have a simple error-reporting function that you can call with an error code and a message. The function would print them and simply exit the program. This is not usually the best solution for real-world situations, but it is a good fall-back, last resort mechanism.

7.4 Making Our Program More Robust

This section will go through making the `006-01-add-year.s` program from Chapter 6. Reading and Writing Simple Records a little more robust.

Since this is a pretty simple program, we will limit ourselves to a single recovery point that covers the whole program. The only thing we will do to recover is to print the error and exit. The code (`007-01-error-exit.s`) to do that is pretty simple:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       .include "006-01-linux.s"       # Linux Definitions.
4
5           .equ ST_ERROR_CODE,  8
6           .equ ST_ERROR_MSG,   12
7
8           .globl _error_exit
9           .type  _error_exit,   @function
10
11  _error_exit:
12      pushl %ebp
13      movl  %esp, %ebp
14
15                              # Write out error code.
16      movl  ST_ERROR_CODE(%ebp), %ecx
17      pushl %ecx
18      call  _count_chars
19      popl  %ecx
20      movl  %eax, %edx
21      movl  $STDERR, %ebx
22      movl  $SYS_WRITE, %eax
23      int   $LINUX_SYSCALL
24
25                              # Write out error message.
26      movl  ST_ERROR_MSG(%ebp), %ecx
27      pushl %ecx
28      call  _count_chars
29      popl  %ecx
30      movl  %eax, %edx
31      movl  $STDERR, %ebx
32      movl  $SYS_WRITE, %eax
33      int   $LINUX_SYSCALL
34
35      pushl $STDERR
36      call  _write_newline
37
38                              # Exit with status 1.
39      movl  $SYS_EXIT, %eax
40      movl  $1, %ebx
41      int   $LINUX_SYSCALL
```

Enter it in a file called `007-01-error-exit.s`. To call it, you just need to push the address of an error message, and then an error code onto the stack, and call the function.

Now let's look for potential error spots in our `006-01-add-year` program. First of all, we don't check to see if either of our `open` system calls actually complete properly. Linux returns its status code in *%eax*, so we need to check and see if there is an error. This new version is called `007-01-add-year.s`:

```
29      movl  $SYS_OPEN, %eax   # Open file for reading.
30      movl  $input_file_name, %ebx
31      movl  $0, %ecx
32      movl  $0666, %edx
33      int   $LINUX_SYSCALL
34
35      movl  %eax, ST_INPUT_DESCRIPTOR(%ebp)
36
37                    # This will test and see if %eax is
38                    # negative.  If it is not negative,
39                    # it will jump to
40                    # _continue_processing. Otherwise
41                    # it will handle the error
42                    # condition that the negative
43                    # number represents.
44                    #
45      cmpl  $0, %eax
46      jge   _continue_processing
47
48      # ----- SEND THE ERROR ----- #
49      #
50      .section .data
51          no_open_file_code:
52              .ascii "0001: \0"
53          no_open_file_msg:
54              .ascii "Can't Open Input File.\0"
55
56      .section .text
57      pushl $no_open_file_msg
58      pushl $no_open_file_code
59      call  _error_exit
60
61  _continue_processing:
62
63      movl  $SYS_OPEN, %eax   # Open file for writing.
64      movl  $output_file_name, %ebx
65      movl  $0101, %ecx
66      movl  $0666, %edx
67      int   $LINUX_SYSCALL
```

So, after calling the system call, we check and see if we have an error by checking to see if the result of the system call is less than zero. If so, we call our error reporting and exit routine.

After every system call, function call, or instruction which can have erroneous results you should add error checking and handling code.

To assemble and link the files, do:

```
as -o 007-01-add-year.o    --32 \
                           --gstabs+ \
                           007-01-add-year.s

as -o 007-01-error-exit.o  --32 \
                           --gstabs+ \
                           007-01-error-exit.s
```

```
ld -o 007-01-add-year      -m elf_i386 \
                           006-01-count-chars.o \
                           006-01-read-record.o \
                           006-01-write-newline.o \
                           006-01-write-record.o \
                           007-01-add-year.o \
                           007-01-error-exit.o
```

Now try to run it without the necessary files. It now exits cleanly and gracefully!

7.5 Review

7.5.1 Know the Concepts

- What are the reasons programmer's have trouble with scheduling?
- Find your favorite program, and try to use it in a completely wrong manner. Open up files of the wrong type, choose invalid options, close windows that are supposed to be open, etc. Count how many different error scenarios they had to account for.
- What are corner cases? Can you list examples of numeric corner cases?
- Why is user testing so important?
- What are stubs and drivers used for? What's the difference between the two?
- What are recovery points used for?
- How many different error codes should a program have?

7.5.2 Use the Concepts

- Go through the `007-01-add-year.s` program and add error-checking code after every system call.
- Find one other program we have done so far, and add error-checking to that program.
- Add a recovery mechanism for `007-01-add-year.s` that allows it to read from STDIN if it cannot open the standard file.

7.5.3 Going Further

- What, if anything, should you do if your error-reporting function fails? Why?
- Try to find bugs in at least one open-source program. File a bug report for it.
- Try to fix the bug you found in the previous exercise.

8. Sharing Functions with Code Libraries

By now you should realize that the computer has to do a lot of work even for simple tasks. Because of that, you have to do a lot of work to write the code for a computer to even do simple tasks. In addition, programming tasks are usually not very simple. Therefore, we need a way to make this process easier on ourselves. There are several ways to do this, including:

- Write code in a high-level language instead of assembly language.
- Have lots of pre-written code that you can cut and paste into your own programs.
- Have a set of functions on the system that are shared among any program that wishes to use it.

All three of these are usually used to some degree in any given project. The first option will be explored further in Chapter 11. High-Level Languages. The second option is useful but it suffers from some drawbacks, including:

- Code that is copied often has to be majorly modified to fit the surrounding code.
- Every program containing the copied code has the same code in it, thus wasting a lot of space.
- If a bug is found in any of the copied code it has to be fixed in every application program.

Therefore, the second option is usually used sparingly. It is usually only used in cases where you copy and paste skeleton code for a specific type of task, and add in your program-specific details. The third option is the one that is used the most often. The third option includes having a central repository of shared code. Then, instead of each program wasting space storing the same copies of functions, they can simply point to the *dynamic libraries* which contain the functions they need. If a bug is found in one of these functions, it only has to be fixed within the single function library file, and all applications which use it are automatically updated. The main drawback with this approach is that it creates some dependency problems, including:

- If multiple applications are all using the same file, how do we know when it is safe to delete the file? For example, if three applications are sharing a file of functions and 2 of the programs are deleted, how does the system know that there still exists an application that uses that code, and therefore it shouldn't be deleted?
- Some programs inadvertently rely on bugs within shared functions. Therefore, if upgrading the shared functions fixes a bug that a program depended on, it could cause that application to cease functioning.

These problems are what lead to what is known as "DLL hell". However, it is generally assumed that the advantages outweigh the disadvantages.

In programming, these shared code files are referred to as *shared libraries*, *dynamic libraries*, *shared objects*, *dynamic-link libraries*, *DLLs*, or *.so files*.[39] We will refer to all of these as *dynamic libraries*.

8.1 Using a Dynamic Library

The program we will examine here is simple - it writes the characters `hello world` to the screen and exits. The regular program, `008-01-hello-world-nolib.s`, looks like this:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
```

[39]Each of these terms have slightly different meanings, but most people use them interchangeably anyway. Specifically, this chapter will cover dynamic libraries, but not shared libraries. Shared libraries are dynamic libraries which are built using *position-independent code* (often abbreviated PIC) which is outside the scope of this book. However, shared libraries and dynamic libraries are used in the same way by users and programs; the linker just links them differently.

```
3       .include "006-01-linux.s"      # Linux Definitions.
4
5       # PURPOSE:
6       #     This program writes the message
7       #     "hello world" and exits.
8       #
9       .section .data
10          helloworld:
11              .ascii "hello world\n"
12
13          helloworld_end:
14              .equ length, helloworld_end - helloworld
15
16      .section .text
17          .globl _start
18
19  _start:
20      movl  $STDOUT, %ebx
21      movl  $helloworld, %ecx
22      movl  $length, %edx
23      movl  $SYS_WRITE, %eax
24      int   $LINUX_SYSCALL
25
26      movl  $0, %ebx
27      movl  $SYS_EXIT, %eax
28      int   $LINUX_SYSCALL
```

That's not too long. However, take a look at how short `008-01-hello-world-lib` is which uses a library:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     This program writes the message "hello world"
5       #     and exits.
6       #
7       .section .data
8           helloworld:
9               .ascii "hello world\n\0"
10
11      .section .text
12          .globl _start
13
14  _start:
15      pushl $helloworld
16      call  printf
17
18      pushl $0
19      call  exit
```

It's even shorter!

Now, building programs which use dynamic libraries is a little different than normal. You can build the first program normally by doing this:

```
as -o 008-01-hello-world-nolib.o  --32 \
                                  --gstabs+ \
```

```
                                  008-01-hello-world-nolib.s

ld -o 008-01-hello-world-nolib    -m elf_i386 \
                                  008-01-hello-world-nolib.o
```

However, in order to build the second program, you have to do this:

```
as -o 008-01-hello-world-lib.o  --32 \
                                --gstabs+ \
                                008-01-hello-world-lib.s

ld -o 008-01-hello-world-lib    -m elf_i386 \
                                008-01-hello-world-lib.o \
            --library         c \
            --library-path    /usr/lib32/ \
            -dynamic-linker   /usr/lib32/ld-linux.so.2
```

Run both programs and you will get the classic message:

```
./008-01-hello-world-lib
```

```
./008-01-hello-world-nolib
```

Remember, the backslash in the first line simply means that the command continues on the next line. The option `-dynamic-linker /usr/lib32/ld-linux.so.2` allows our program to be linked to libraries. This builds the executable so that before executing, the operating system will load the program `/usr/lib32/ld-linux.so.2` to load in external libraries and link them with the program. This program is known as a *dynamic linker*.

The `-l c` or `--library c` option says to link to the `C` library, named `libc.so` on GNU/Linux systems. Given a library name, `c` in this case (usually library names are longer than a single letter), the GNU/Linux linker prepends the string `lib` to the beginning of the library name and appends `.so` to the end of it to form the library's filename. This library contains many functions to automate all types of tasks. The two we are using are `printf`, which prints strings, and `exit`, which exits the program.

Notice that the symbols `printf` and `exit` are simply referred to by name within the program. In previous chapters, the linker would resolve all of the names to physical memory addresses, and the names would be thrown away. When using dynamic linking, the name itself resides within the executable, and is resolved by the dynamic linker when it is run. When the program is run by the user, the dynamic linker loads the dynamic libraries listed in our link statement, and then finds all of the function and variable names that were named by our program but not found at link time, and matches them up with corresponding entries in the shared libraries it loads. It then replaces all of the names with the addresses which they are loaded at. This sounds time-consuming. It is to a small degree, but it only happens once - at program startup time.

8.2 How Dynamic Libraries Work

In our first programs, all of the code was contained within the source file. Such programs are called *statically-linked executables*, because they contained all of the necessary functionality for the program that wasn't handled by the kernel. In the programs we wrote in Chapter 6. Reading and Writing Simple Records, we used both our main program file and files containing routines used by multiple programs. In these cases, we combined all of the code together using the linker at link-time, so it was still statically-linked. However, in the `008-01-hello-world-lib` program, we started using dynamic libraries. When you use dynamic libraries, your program is then *dynamically-linked*, which means that not all of the code needed to run the program is actually contained within the program file itself, but in external libraries.

When we put the `--library c` on the command to link the `008-01-hello-world-lib` program, it told the linker to use the `C` library (`libc.so`) to look up any symbols that weren't already defined in `008-01-hello-world-lib.o`. However, it doesn't actually add any code to our program, it just notes in the program where to look. When the `008-01-hello-world-lib` program begins, the file `/usr/lib32/ld-linux.so.2` is loaded

first. This is the dynamic linker. This looks at our `008-01-hello-world-lib` program and sees that it needs the `C` library to run. So, it searches for a file called `libc.so` in the standard places (listed in `/etc/ld.so.conf` and in the contents of the `LD_LIBRARY_PATH` environment variable), then looks in it for all the needed symbols (`printf` and `exit` in this case), and then loads the library into the program's virtual memory. Finally, it replaces all instances of `printf` in the program with the actual location of `printf` in the library.

Run the following command:

```
ldd ./008-01-hello-world-nolib
```

It should report back `not a dynamic executable`. This is just like we said - `008-01-hello-world-nolib` is a statically-linked executable. However, try this:

```
ldd ./008-01-hello-world-lib
```

It will report back something like:

```
linux-gate.so.1 (0xf7f17000)
libc.so.6 => /usr/lib32/libc.so.6 (0xf7ce5000)
/usr/lib32/ld-linux.so.2 => /usr/lib/ld-linux.so.2 (0xf7f19000)
```

The numbers in parentheses may be different on your system. This means that the program `008-01-hello-world-lib` is linked to `libc.so.6` (the `.6` is the version number), which is found at `/usr/lib32/`, and `ld-linux.so.2` is found at `/usr/lib32/`. These libraries have to be loaded before the program can be run. If you are interested, run the `ldd` program on various programs that are on your Linux distribution, and see what libraries they rely on.

8.3 Finding Information about Libraries

Okay, so now that you know about libraries, the question is, how do you find out what libraries you have on your system and what they do? Well, let's skip that question for a minute and ask another question: How do programmers describe functions to each other in their documentation? Let's take a look at the function `printf`. Its calling interface (usually referred to as a *prototype*) looks like this:

```
int printf(char *string, ...);
```

In Linux, functions are described in the C programming language. In fact, most Linux programs are written in C. That is why most documentation and binary compatibility is defined using the C language. The interface to the `printf` function above is described using the C programming language.

This definition means that there is a function `printf`. The things inside the parenthesis are the function's parameters or arguments. The first parameter here is `char *string`. This means there is a parameter named `string` (the name isn't important, except to use for talking about it), which has a type `char *`. `char` means that it wants a single-byte character. The `*` after it means that it doesn't actually want a character as an argument, but instead it wants the address of a character or sequence of characters. If you look back at our `008-01-hello-world-lib` program, you will notice that the function call looked like this:

```
15      pushl $helloworld
16      call  printf
```

So, we pushed the address of the `hello` string, rather than the actual characters. You might notice that we didn't push the length of the string. The way that `printf` found the end of the string was because we ended it with a null character (`\0`). Many functions work that way, especially C language functions. The `int` before the function definition tell what type of value the function will return in *%eax* when it returns. `printf` will return an `int` when it's through. Now, after the `char *string`, we have a series of periods, `...`. This means that it can take an indefinite number of additional arguments after the string. Most functions can only take a specified number of arguments. `printf`, however, can take many. It will look into the `string` parameter, and everywhere it sees the characters `%s`, it will look for another string from the stack to insert, and everywhere it sees `%d` it will look for a number from the stack to insert. This is best described using an example `008-02-printf-example.s`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #    This program is to demonstrate how to call
5       #    printf.
6       #
7       .section .data
8           # This string is called the format string.  It
9           # is the first parameter, and printf uses it to
10          # find out how many parameters it was given,
11          # and what kind they are.
12          #
13          first_string:
14              .ascii "Hi! %s is the %s number #%d.\n\0"
15
16          name_string:
17              .ascii "Jonathan\0"
18
19          person_string:
20              .ascii "person\0"
21
22          # This could also have been an .equ, but we
23          # decided to give it a real memory location
24          # just for kicks.
25          #
26          number_loved:
27              .long 3
28
29      .section .text
30          .globl _start
31
32  _start:
33      # Note that the parameters are passed in the
34      # reverse order that they are listed in the
35      # function prototype.
36      #
37      pushl number_loved      # This is the %d.
38      pushl $person_string    # This is the second %s.
39      pushl $name_string      # This is the first %s.
40      pushl $first_string     # This is the format string
41                              # in the prototype.
42      call  printf
43
44      pushl $0
45      call  exit
```

Type it in with the filename `008-02-printf-example.s`, and then do the following commands:

```
as -o 008-02-printf-example.o  --32 \
                               --gstabs+ \
                               008-02-printf-example.s

ld -o 008-02-printf-example    -m elf_i386 \
                               008-02-printf-example.o \
```

```
            --library-path   /usr/lib32/ \
            --library        c \
            -dynamic-linker  /usr/lib32/ld-linux.so.2
```

Then run the program with `./008-02-printf-example`, and it should say this:

```
Hi! Jonathan is the person number #3.
```

Now, if you look at the code, you'll see that we actually push the format string last, even though it's the first parameter listed. You always push a functions parameters in reverse order.[40] You may be wondering how the `printf` function knows how many parameters there are. Well, it searches through your string, and counts how many `%d`s and `%s`s it finds, and then grabs that number of parameters from the stack. If the parameter matches a `%d`, it treats it as a number, and if it matches a `%s`, it treats it as a pointer to a null-terminated string. `printf` has many more features than this, but these are the most-used ones. So, as you can see, `printf` can make output a lot easier, but it also has a lot of overhead, because it has to count the number of characters in the string, look through it for all of the control characters it needs to replace, pull them off the stack, convert them to a suitable representation (numbers have to be converted to strings, etc), and stick them all together appropriately.

We've seen how to use the C programming language prototypes to call library functions. To use them effectively, however, you need to know several more of the possible data types for reading functions. Here are the main ones:

`int`:
An `int` is an integer number. The size of 4 bytes (32 bits ~ 2^32) on x86 processor provide a maximum value of *4,294,967,295*; negative values between *-2,147,483,648* and *2,147,483,647*.

`long`:
A `long` is also an integer number. The size of 4 bytes (32 bits ~ 2^32) on x86 processor provide a maximum value of *4,294,967,295*; negative values between *-2,147,483,648* and *2,147,483,647*.

`long long`:
A `long long` is an integer number that's larger than a `long`. The size of 8 bytes (64 bits ~ 2^64) on x86 processor provide a maximum value of *18,446,744,073,709,551,615*; negative values between *-9,223,372,036,854,775,808* and *9,223,372,036,854,775,807*.

`short`:
A short is an integer number that's shorter than an `int`. The size of 2 bytes (16 bits ~ 2^16) on x86 processor provide a maximum value of *65,535*; negative values between *-32,768* and *32,767*.

`char`:
A `char` is a single-byte integer number. The size of 1 byte (8 bits ~ 2^8) on x86 processor provide a maximum value of *255*; negative values between *-128* and *127*. This is mostly used for storing character data, since ASCII strings usually are represented with one byte per character.

`float`:
A `float` is a floating-point number. (4 bytes on an x86 processor). Floating-point numbers will be explained in more depth in Floating-point Numbers.

`double`:
A `double` is a floating-point number that is larger than a float. (8 bytes on an x86 processor).

`unsigned`:
`unsigned` is a modifier used for any of the above types which keeps them from being used as signed quantities. The difference between signed and unsigned numbers will be discussed in Chapter 10. Counting Like a Computer.

[40] The reason that parameters are pushed in the reverse order is because of functions which take a variable number of parameters like `printf`. The parameters pushed in last will be in a known position relative to the top of the stack. The program can then use these parameters to determine where on the stack the additional arguments are, and what type they are. For example, `printf` uses the format string to determine how many other parameters are being sent. If we pushed the known arguments first, you wouldn't be able to tell where they were on the stack.

***:**
An asterisk (*) is used to denote that the data isn't an actual value, but instead is a pointer to a location holding the given value (4 bytes on an x86 processor). So, let's say in memory location `my_location` you have the number 20 stored. If the prototype said to pass an `int`, you would use direct addressing mode and do `pushl my_location`. However, if the prototype said to pass an `int *`, you would do `pushl $my_location` - an immediate mode addressing push of the address that the value resides in. In addition to indicating the address of a single value, pointers can also be used to pass a sequence of consecutive locations, starting with the one pointed to by the given value. This is called an array.

`struct`:
A `struct` is a set of data items that have been put together under a name. For example you could declare:
And any time you ran into `struct teststruct` you would know that it is actually two words right next to each other, the first being an integer, and the second a pointer to a character or group of characters. You never see structs passed as arguments to functions. Instead, you usually see pointers to structs passed as arguments. This is because passing structs to functions is fairly complicated, since they can take up so many storage locations.

```
struct teststruct {
    int a;
    char *b;
};
```

`typedef`:
A `typedef` basically allows you to rename a type. For example, I can do `typedef int myowntype;` in a C program, and any time I typed `myowntype`, it would be just as if I typed `int`. This can get kind of annoying, because you have to look up what all of the typedefs and structs in a function prototype really mean. However, `typedefs` are useful for giving types more meaningful and descriptive names.

NOTE.
Compatibility: The listed sizes are for intel-compatible (x86) machines. Other machines will have different sizes. Also, even when parameters shorter than a word are passed to functions, they are passed as longs on the stack.

That's how to read function documentation. Now, let's get back to the question of how to find out about libraries. Most of your system libraries are in `/usr/lib` or `/lib`. If you want to just see what symbols they define, just run `objdump -R FILENAME` where `FILENAME` is the full path to the library. The output of that isn't too helpful, though, for finding an interface that you might need. Usually, you have to know what library you want at the beginning, and then just read the documentation. Most libraries have manuals or man pages for their functions. The web is the best source of documentation for libraries. Most libraries from the GNU project also have info pages on them, which are a little more thorough than man pages.
Let's see the `objdump` of the last program:

```
objdump -R  008-02-printf-example-bin
```

It should display something like this:

```
008-02-printf-example-bin:     file format elf32-i386

DYNAMIC RELOCATION RECORDS
OFFSET   TYPE              VALUE
0804b00c R_386_JUMP_SLOT   printf@GLIBC_2.0
0804b010 R_386_JUMP_SLOT   exit@GLIBC_2.0
```

8.4 Useful Functions

Several useful functions you will want to be aware of from the `C` library include:

- `size_t strlen (const char *s)` calculates the size of null-terminated strings.

- `int strcmp (const char *s1, const char *s2)` compares two strings alphabetically.
- `char * strdup (const char *s)` takes the pointer to a string, and creates a new copy in a new location, and returns the new location.
- `FILE * fopen (const char *filename, const char *opentype)` opens a managed, buffered file (allows easier reading and writing than using file descriptors directly).[41][42]
- `int fclose (FILE *stream)` closes a file opened with `fopen`.
- `char * fgets (char *s, int count, FILE *stream)` fetches a line of characters into string `s`.
- `int fputs (const char *s, FILE *stream)` writes a string to the given open file.
- `int fprintf (FILE *stream, const char *template, ...)` is just like `printf`, but it uses an open file rather than defaulting to using standard output.

You can find the complete manual on this library by going to The GNU C Library manual

8.5 Building a Dynamic Library

Let's say that we wanted to take all of our shared code from Chapter 6. Reading and Writing Simple Records and build it into a dynamic library to use in our programs. The first thing we would do is assemble them like normal:

```
as -o 006-01-write-record.o  --32 \
                             --gstabs+ \
                             006-01-write-record.s

as -o 006-01-read-record.o   --32 \
                             --gstabs+ \
                             006-01-read-record.s
```

Now, instead of linking them into a program, we want to link them into a dynamic library. This changes our linker command to this:

```
ld -o librecord.so  -m elf_i386 \
                    -shared \
                    006-01-write-record.o \
                    006-01-read-record.o
```

This links both of these files together into a dynamic library called `librecord.so`. This file can now be used for multiple programs. If we need to update the functions contained within it, we can just update this one file and not have to worry about which programs use it.

Let's look at how we would link against this library. To link the `008-03-write-records` program, we would do the following:

```
as -o 006-01-write-records.o  --32 \
                              --gstabs+ \
                              006-01-write-records.s

ld -o 008-03-write-records    -m elf_i386 \
                              006-01-write-records.o \
                --library        record \
                --library-path   . \
                -dynamic-linker  /lib32/ld-linux.so.2
```

[41] `stdin`, `stdout`, and `stderr` (all lower case) can be used in these programs to refer to the files of their corresponding file descriptors.

[42] `FILE` is a struct. You don't need to know its contents to use it. You only have to store the pointer and pass it to the relevant other functions.

In this command, `-L .` or `--library-path .` told the linker to look for libraries in the current directory (it usually only searches `/lib` directory, `/usr/lib` directory, and a few others). As we've seen, the option `-dynamic-linker /usr/lib32/ld-linux.so.2` specified the dynamic linker. The option `--library record` tells the linker to search for functions in the file named `librecord.so`.

Now the `008-03-write-records` program is built, but it will not run. If we try it, we will get an error like the following:

```
`./008-03-write-records`: error while loading shared libraries:
librecord.so: cannot open shared object file: No such file or directory
```

This is because, by default, the dynamic linker only searches `/lib`, `/usr/lib`, and whatever directories are listed in `/etc/ld.so.conf` for libraries. In order to run the program, you either need to move the library to one of these directories, or execute the following command:

```
LD_LIBRARY_PATH=.  ./008-03-write-records
```

The next solution store the library directory in the session, it keeps alive until the session is done or the terminal/console is closed:

```
LD_LIBRARY_PATH=.
export LD_LIBRARY_PATH
```

Alternatively, if that gives you an error, do this instead:

```
setenv LD_LIBRARY_PATH .
```

Now, you can run `008-03-write-records` normally by typing `./008-03-write-records`. Setting `LD_LIBRARY_PATH` tells the linker to add whatever paths you give it to the library search path for dynamic libraries.

Let's print the shared object dependencies for `./008-03-write-records`. It is a shared library. Try this:

```
LD_LIBRARY_PATH=.  ldd ./008-03-write-records
```

It will report back something like:

```
    linux-gate.so.1 (0xf7fa9000)
    librecord.so => ./librecord.so (0xf7fa0000)
```

And it's the `objdump` result:

```
LD_LIBRARY_PATH=.  objdump -R ./008-03-write-records
```

```
./008-03-write-records-bin:     file format elf32-i386

DYNAMIC RELOCATION RECORDS
OFFSET   TYPE              VALUE
0804b00c R_386_JUMP_SLOT   _write_record
```

For further information about dynamic linking, see the following sources on the Internet:

- The man page for `ld.so` contains a lot of information about how the Linux dynamic linker works, execute in the terminal: `man ld.so`.
- Introduction to the ELF Format: The ELF Header, Understanding Program Headers, The Section Headers, Exploring Section Types and Special Sections, Understanding C start up, The Symbol Table and Relocations: Part I, The Symbol Table and Relocations: Part II, More Relocation tricks: Part III and Dynamic Linking / Loading and the .dynamic section provide a good introduction to the ELF file format.
- Executable and Linkable Format 101: Part 1: Sections and Segments, Part 2: Symbols and Part 3: Relocations contains a great description of how dynamic linking works with ELF files. Part 4: Dynamic Linking is a great presentation on dynamic linking in Linux.

- Program Library HOWTO Shared Libraries contains a good introduction to programming position-independent code for shared libraries under Linux.

8.6 Review

8.6.1 Know the Concepts

- What are the advantages and disadvantages of shared libraries?
- Given a library named 'foo', what would the library's filename be?
- What does the `ldd` command do?
- Let's say we had the files `foo.o` and `bar.o`, and you wanted to link them together, and dynamically link them to the library 'kramer'. What would the linking command be to generate the final executable?
- What is *typedef* for?
- What are *struct*s for?
- What is the difference between a data element of type *int* and *int **? How would you access them differently in your program?
- If you had an object file called `foo.o`, what would be the command to create a shared library called 'bar'?
- What is the purpose of LD_LIBRARY_PATH?

8.6.2 Use the Concepts

- Rewrite one or more of the programs from the previous chapters to print their results to the screen using `printf` rather than returning the result as the exit status code. Also, make the exit status code be 0.
- Use the `_factorial` function you developed in Recursive Functions to make a shared library. Then re-write the main program so that it links with the library dynamically.
- Rewrite the program above so that it also links with the 'C' library. Use the 'C' library's `printf` function to display the result of the `_factorial` call.
- Rewrite the `005-01-toupper` program so that it uses the `C` library functions for files rather than system calls.

8.6.3 Going Further

- Make a list of all the environment variables used by the GNU/Linux dynamic linker.
- Research the different types of executable file formats in use today and in the history of computing. Tell the strengths and weaknesses of each.
- What kinds of programming are you interested in (graphics, databases, science, etc.)? Find a library for working in that area, and write a program that makes some basic use of that library.
- Research the use of `LD_PRELOAD`. What is it used for? Try building a shared library that contained the `exit` function, and have it write a message to STDERR before exiting. Use `LD_PRELOAD` and run various programs with it. What are the results?

9. Intermediate Memory Topics

9.1 How a Computer Views Memory

Let's review how memory within a computer works. You may also want to re-read Chapter 2. Computer Architecture.

A computer looks at memory as a long sequence of numbered storage locations. A sequence of *millions* of numbered storage locations. Everything is stored in these locations. Your programs are stored there, your data is stored there, everything. Each storage location looks like every other one. The locations holding your program are just like the ones holding your data. In fact, the computer has no idea which are which, except that the executable file tells it where to start executing.

These storage locations are called bytes. The computer can combine up to four of them together into a single word. Normally numeric data is operated on a word at a time. As we mentioned, instructions are also stored in this same memory. Each instruction is a different length. Most instructions take up one or two storage locations for the instruction itself, and then storage locations for the instruction's arguments. For example, the instruction:

```
movl data_items(,%edi,4), %ebx
```

Takes up 7 storage locations. The first two hold the instruction, the third one tells which registers to use, and the next four hold the storage location of `data_items`. In memory, instructions look just like all the other numbers, and the instructions themselves can be moved into and out of registers just like numbers, because that's what they are.

This chapter is focused on the details of computer memory. To get started let's review some basic terms that we will be using in this chapter:

Byte:
This is the size of a storage location. On x86 processors, a byte can hold numbers between 0 and 255.

Word:
This is the size of a normal register. On x86 processors, a word is four bytes long. Most computer operations handle a word at a time.

Address:
An address is a number that refers to a byte in memory. For example, the first byte on a computer has an address of 0, the second has an address of 1, and so on.[43] Every piece of data on the computer not in a register has an address. The address of data which spans several bytes is the same as the address of its first byte.

Normally, we don't ever type the numeric address of anything, but we let the assembler do it for us. When we use labels in code, the symbol used in the label will be equivalent to the address it is labelling. The assembler will then replace that symbol with its address wherever you use it in your program. For example, say you have the following code:

Now, any time in the program that `my_data` is used, it will be replaced by the address of the first value of the `.long` directive.

```
.section .data
    my_data:
        .long 2, 3, 4
```

Pointer:
A pointer is a register or memory word whose value is an address. In our programs we use `%ebp` as a pointer to the current stack frame. All base pointer addressing involves pointers. Programming uses a lot of pointers, so it's an important concept to grasp.

[43] You actually never use addresses this low, but it works for discussion.

9.2 The Memory Layout of a Linux Program

When your program is loaded into memory, each `.section` is loaded into its own region of memory. All of the code and data declared in each section is brought together, even if they were separated in your source code.

The actual instructions (the `.text` section) are loaded at the address 0x08048000 (numbers starting with `0x` are in hexadecimal, which will be discussed in Chapter 10. Counting Like a Computer).[44] The `.data` section is loaded immediately after that, followed by the `.bss` section.

The last byte that can be addressed on Linux is location 0xbfffffff. Linux starts the stack here and grows it downward toward the other sections. Between them is a huge gap. The initial layout of the stack is as follows: At the bottom of the stack (the bottom of the stack is the top address of memory - see Chapter 4. All About Functions), there is a word of memory that is zero. After that comes the null-terminated name of the program using ASCII characters. After the program name comes the program's environment variables (these are not important to us in this book). Then come the program's command-line arguments. These are the values that the user typed in on the command line to run this program. When we run `as`, for example, we give it several arguments - `as`, `sourcefile.s`, `-o`, and `objectfile.o`. After these, we have the number of arguments that were used. When the program begins, this is where the stack pointer, *%esp*, is pointing. Further pushes on the stack move *%esp* down in memory. For example, the instruction:

```
pushl %eax
```

is equivalent to

```
movl %eax, (%esp)
subl $4, %esp
```

Likewise, the instruction:

```
popl %eax
```

is the same as

```
movl (%esp), %eax
addl $4, %esp
```

Your program's data region starts at the bottom of memory and goes up. The stack starts at the top of memory, and moves downward with each push. This middle part between the stack and your program's data sections is inaccessible memory - you are not allowed to access it until you tell the kernel that you need it.[45] If you try, you will get an error (the error message is usually "segmentation fault"). The same will happen if you try to access data before the beginning of your program, 0x08048000. The last accessible memory address to your program is called the *system break* (also called the *current break* or just the *break*).

9.3 Every Memory Address is a Lie

So, why does the computer not allow you to access memory in the break area? To answer this question, we will have to delve into the depths of how your computer really handles memory.

You may have wondered, since every program gets loaded into the same place in memory, don't they step on each other, or overwrite each other? It would seem so. However, as a program writer, you only access *virtual memory*.

Physical memory refers to the actual RAM chips inside your computer and what they contain. It's usually between 16 and 512 Megabytes on modern computers. If we talk about a *physical memory address*, we are talking about where exactly on these chips a piece of memory is located. Virtual memory is the way *your program* thinks about memory. Before loading your program, Linux finds an empty physical memory space large enough to fit your program, and then tells the processor to pretend that this memory is actually at the address 0x0804800 to load your program into. Confused yet? Let me explain further.

[44] Addresses mentioned in this chapter are not set in stone and may vary based on kernel version.

[45] The stack can access it as it grows downward, and you can access the stack regions through *%esp*. However, your program's data section doesn't grow that way. The way to grow that will be explained shortly.

Each program gets its own sandbox to play in. Every program running on your computer thinks that it was loaded at memory address 0x0804800, and that its stack starts at 0xbfffffff. When Linux loads a program, it finds a section of unused memory, and then tells the processor to use that section of memory as the address 0x0804800 for this program. The address that a program believes it uses is called the virtual address, while the actual address on the chips that it refers to is called the physical address. The process of assigning virtual addresses to physical addresses is called *mapping*.

Earlier we talked about the inaccessible memory between the `.bss` and the stack, but we didn't talk about why it was there. The reason is that this region of virtual memory addresses hasn't been mapped onto physical memory addresses. The mapping process takes up considerable time and space, so if every possible virtual address of every possible program were mapped, you would not have enough physical memory to even run one program. So, the break is the beginning of the area that contains unmapped memory. With the stack, however, Linux will automatically map in memory that is accessed from stack pushes.

Let's explain these complex concepts using the Linux tools and dynamic practices. The program `009-01-memory-layout.s` helps with this:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       .include "006-01-linux.s"      # Linux Definitions.
4
5       # PURPOSE:
6       #     Represent the memory layout.
7       #
8
9       .section .data
10          name:
11              .ascii "Leo\0"
12          age:
13              .int 31
14          id:
15              .long 89485
16
17      .section .bss
18          .lcomm  comment,  128
19          .lcomm  author,   3
20          .equ    items,    5
21
22      .section .text
23          .globl _start
24
25  _start:
26      movl  $SYS_BRK, %eax
27      movl  $0, %ebx
28      int   $LINUX_SYSCALL    # Find out the break.
29
30      call  _hello
31
32      call  _fine
33
34      jmp   _bye
35
36  _hello:
37      pushl %ebp              # Save old base pointer.
38      movl  %esp, %ebp        # Make ST the BP.
39
```

```
40      pushl %eax
41      movl  $name, %eax
42      popl  %eax
43
44      movl %ebp, %esp         # Restore the ST.
45      popl %ebp               # Restore the BP.
46      ret
47
48  _fine:
49      pushl %ebp              # Save old base pointer.
50      movl  %esp, %ebp        # Make ST the BP.
51
52      subl  $12, %esp         # Add local space for
53                              # variables.
54
55                  # Using %ebp, needs negative numbers.
56      movl  $age, 4(%esp)       # Store at 1st space.
57      movl  $author, -8(%ebp)   # Store at 1rd space.
58
59      movl  $id, 8(%esp)        # Store at 2nd space.
60      movl  $comment, -4(%ebp)  # Store at 2nd space.
61
62                  # Remember the rule: Positive numbers
63                  # or operations take old stored values,
64                  # negative numbers or operations take
65                  # the new stored values.
66
67      pushl age               # Push the age.
68      popl  %eax              # Remove the age.
69
70      addl  $12, %esp         # Remove local variables.
71                  # It is not necessary since the next
72                  # instrucition restore the %esp from
73                  # the %ebp.
74
75      movl %ebp, %esp         # Restore the ST.
76      popl %ebp               # Restore the BP.
77      ret
78
79  _bye:
80      movl   $SYS_EXIT, %eax
81      movl   $0, %ebx
82      int    $LINUX_SYSCALL
```

Time to assemble and link:

```
as -o 009-01-memory-layout.o  --32 \
                              --gstabs+ \
                              009-01-memory-layout.s

ld -o 009-01-memory-layout    -m elf_i386 \
                              009-01-memory-layout
```

How to get the beginning of the memory address (0x08048000)? Search the private headers:

```
objdump  009-01-memory-layout  --private-headers
```

It shows the `LOAD off    0x00000000 vaddr 0x08048000`:

```
Program Header:
    LOAD off    0x00000000 vaddr 0x08048000 paddr 0x08048000 align 2**12
         filesz 0x00000094 memsz 0x00000094 flags r--
    LOAD off    0x00001000 vaddr 0x08049000 paddr 0x08049000 align 2**12
         filesz 0x00000022 memsz 0x00000022 flags r-x
    LOAD off    0x00002000 vaddr 0x0804a000 paddr 0x0804a000 align 2**12
         filesz 0x0000000c memsz 0x0000000c flags rw-
```

The symbols are the sections, variables, constants, labels, functions, and more. These are inside of the binary file:

```
objdump 009-01-memory-layout --syms
```

```
SYMBOL TABLE:
08049000 l    d  .text  00000000 .text
0804a000 l    d  .data  00000000 .data
0804a010 l    d  .bss   00000000 .bss

0804a000 l       .data  00000000 name
0804a004 l       .data  00000000 age
0804a008 l       .data  00000000 id

0804a010 l     O .bss   00000080 comment
0804a090 l     O .bss   00000003 author
00000005 l       *ABS*  00000000 items

08049017 l       .text  00000000 _hello
08049026 l       .text  00000000 _fine
08049039 l       .text  00000000 _bye

08049000 g       .text  00000000 _start
```

Get the overall file header, it contains the `start address`:

```
objdump 009-01-memory-layout --file-headers
```

```
architecture: i386, flags 0x00000112:
EXEC_P,  HAS_SYMS,  D_PAGED
start address 0x08049000
```

In `gdb` we are able to get this information, too:

```
gdb --args ./009-01-memory-layout 123 456
(gdb) info files
```

```
Entry point: 0x8049000
0x08049000 - 0x080490b5 is .text
0x0804a000 - 0x0804a00c is .data
0x0804a010 - 0x0804a094 is .bss
```

Table of the Physical Memory in the program.

As we mentioned in this and other chapters the code is going forward starting at memory 0x08048000 but the dynamic data is pushing backwards from the bottom of the memory 0xffffffff.

```
./009-01-memory-layout 123 456

    +------------------+ ---> 0x08048000
    |   Program Code   |
    |     and Data     |
    |         ↓        |
    +------------------+
    |       .text      | ---> 0x08049000
    |      <_start>    | ---> 0x08049000 movl   $1, %eax
    |     <_start+5>   | ---> 0x08049005 calll  _hello <_hello>
    |    <_start+10>   | ---> 0x0804900a pushl  age <0x804a004>
    |    <_start+16>   | ---> 0x08049010 calll  _fine <_fine>
    |         ↓        |
    +------------------+
    |       .data      | ---> 0x0804a000
    |        name      | ---> 0x0804a000
    |        age       | ---> 0x0804a004
    |        id        | ---> 0x0804a008
    |         ↓        |
    +------------------+
    |       .bss       | ---> 0x0804a010
    |       comment    | ---> 0x0804a010
    |       author     | ---> 0x0804a090
    |         ↓        |
    +------------------+ ---> 0x804b000 *** Break
    |         ↓        |
    |                  |
    |  Unmapped Memory |
    |                  |
    |         ↑        | ---> New pushes (pushl)
    +------------------+
    |  # of arguments  | ---> 0xffffd870
    +------------------+
    |   Program name   | ---> 0xffffd874
    +------------------+
    |      Arg #1      | ---> 0xffffd878
    +------------------+
    |      Arg #2      | ---> 0xffffd87c
    +------------------+
    |     ... ↑ ...    |
    +------------------+
    |         ↑        |
    |    Environment   |
    |     variables    |
    +------------------+ ---> 0xffffffff
```

Try to upside down the previous table to read from the memory stack during the execution of the first function `_hello`. This is the confused part because when we try to take the values from the base pointer (%ebp) or stack pointer (%esp) we need to add or sub in the inverse way that we are thinking, the reason is here:

TIP:

Taking old variables pushed in the stack needs to use positive numbers, the new variables pushed in the stack needs to use the negative numbers. Because the positive numbers are going to the bottom of the memory *0xffffffff*, means it's going backwards.

```
pushl %ebp                # Save old base pointer.
movl  %esp, %ebp          # Make ST the BP.
subl  $12, %ebp           # Reserve 3 new local variables.
movl  %eax, 8(%esp)       # Store in the new 2nd variable.
movl  %eax, -4(%ebp)      # Store in the new 2nd variable.
```

It shows how to the stack memory is decreasing when we `call` or `push` values, and decreasing when use `pop` or `ret`:

```
36  _hello:
37      pushl %ebp              # Save old base pointer.
38      movl  %esp, %ebp        # Make ST the BP.
39
40      pushl %eax
41      movl  $name, %eax
42      popl  %eax
43
44      movl %ebp, %esp         # Restore the ST.
45      popl %ebp               # Restore the BP.
46      ret
```

```
./009-01-memory-layout 123 456
    +------------------+ ---> 0xffffffff
    |    Environment   |
    |     variables    |
    |        ↓         |
    +------------------+
    |   Program name   | ---> 0xffffd874
    +------------------+
    |  # of arguments  | ---> 0xffffd870
    |        ↓         |
    +------------------+ ---> 0xffffd870  -> %esp
    |                  |
    |    _start+17     |    > call _hello
    |        ↓         | ---> 0xffffd86c  -> %esp
    +------------------+
    |       %ebp       |    > pushl %ebp
    |        ↓         | ---> 0xffffd868  -> %esp
    |                  |    > movl  %esp, %ebp
    |                  | ---> 0xffffd868  -> %ebp %esp
    +------------------+
    |       %eax       |    > pushl  %eax
    |        ↓         | ---> 0xffffd864  -> %esp
    +------------------+
    |       %eax       |    > popl   %eax
    |        ↑         | ---> 0xffffd868  -> %ebp %esp
    +------------------+
    |                  |    > movl   %ebp, %esp
    |                  | ---> 0xffffd868  -> %ebp %esp
    |       %ebp       |    > popl   %ebp
    |        ↑         | ---> 0xffffd86c  -> %esp
    +------------------+
    |       ret        |    > ret
    |        ↑         | ---> 0xffffd870  -> %esp
```

```
    |                   |
    +-------------------+ ---> 0x804b000 *** Break
    |         ↓         |
    |  Unmapped Memory  |
    |         ↑         |
    +-------------------+
    |         ↑         |
    |   Code and Data   |
    +-------------------+
```

The memory address is decreasing when `push` and `call` is executed:

```
0xffffd870  -> %esp
0xffffd86c  -> %esp
0xffffd868  -> %ebp %esp
0xffffd864  -> %esp
```

It's increasing when `pop` and `ret` is executed:

```
0xffffd868  -> %ebp %esp
0xffffd86c  -> %esp
0xffffd870  -> %esp
```

Now, checks the next example with the function `_fine`, it adds new local variables. This example also demonstrates that using `%esp` or `%ebp` are the same because at the end it's a mark which indicate the positions, one for the base pointer and other for the stack pointer. Highly recommended to use `%esp` because the program is dynamic and it goes inside of the `calls`. We want to use the recently created spaces for these variables, `%ebp` is recommended when you want to take arguments of the actual function, they always be around the base pointer:

```
48  _fine:
49      pushl %ebp              # Save old base pointer.
50      movl  %esp, %ebp        # Make ST the BP.
51
52      subl  $12, %esp         # Add local space for
53                              # variables.
54
55                  # Using %ebp, needs negative numbers.
56      movl  $age, 4(%esp)       # Store at 1st space.
57      movl  $author, -8(%ebp)   # Store at 1rd space.
58
59      movl  $id, 8(%esp)        # Store at 2nd space.
60      movl  $comment, -4(%ebp)  # Store at 2nd space.
61
62                  # Remember the rule: Positive numbers
63                  # or operations take old stored values,
64                  # negative numbers or operations take
65                  # the new stored values.
66
67      pushl age               # Push the age.
68      popl  %eax              # Remove the age.
69
70      addl  $12, %esp         # Remove local variables.
71                  # It is not necessary since the next
72                  # instrucition restore the %esp from
73                  # the %ebp.
```

```
74
75      movl %ebp, %esp         # Restore the ST.
76      popl %ebp               # Restore the BP.
77      ret
```

```
./009-01-memory-layout 123 456
    +------------------+ ---> 0xffffffff
    |    Environment   |
    |     variables    |
    |        ↓         |
    +------------------+
    |   Program name   | ---> 0xffffd874
    +------------------+
    |  # of arguments  | ---> 0xffffd870
    |        ↓         |
    +------------------+ ---> 0xffffd870  -> %esp
    |                  |
    |     _start+22    |    > call _fine
    |        ↓         | ---> 0xffffd86c  -> %esp
    +------------------+
    |       %ebp       |    > pushl %ebp
    |        ↓         | ---> 0xffffd868  -> %esp
    |                  |    > movl  %esp, %ebp
    |                  | ---> 0xffffd868  -> %ebp %esp
    +------------------+
    |                  |    > subl  $12, %esp
    |                  | ---> 0xffffd868  -> %ebp
    |                  | ---> 0xffffd864
    |                  | ---> 0xffffd860
    |        ↓         | ---> 0xffffd85c  -> %esp
    +------------------+
    |                  |    > movl  $age, 4(%esp)
    |  0x804a004 (age) | ---> 0xffffd860
    +------------------+
    |                  |    > movl  $author, -8(%ebp)
    | 0x804a090 (auth) | ---> 0xffffd860
    +------------------+
    |                  |    > movl  $id, 8(%esp)
    |  0x804a008 (id)  | ---> 0xffffd864
    +------------------+
    |                  |    > movl  $comment, -4(%ebp)
    | 0x804a010 (comm) | ---> 0xffffd864
    +------------------+
    |       %age       |    > pushl  %age
    |        ↓         | ---> 0xffffd858  -> %esp
    +------------------+
    |       %eax       |    > popl   %eax
    |        ↑         | ---> 0xffffd85c  -> %esp
    +------------------+
    |                  |    > addl  $12, %esp
    |                  | ---> 0xffffd868  -> %ebp %esp
    +------------------+
    |                  |    > movl   %ebp, %esp
    |                  | ---> 0xffffd868  -> %ebp %esp
    |       %ebp       |    > popl   %ebp
```

```
    |         ↑         | ---> 0xffffd86c  -> %esp
    +-------------------+
    |        ret        |    > ret
    |         ↑         | ---> 0xffffd870  -> %esp
    |                   |
    +-------------------+ ---> 0x804b000 *** Break
    |         ↓         |
    |  Unmapped Memory  |
    |         ↑         |
    +-------------------+
    |         ↑         |
    |   Code and Data   |
    +-------------------+
```

Flow of the stack pointer:

```
0xffffd870  -> %esp
0xffffd86c  -> %esp
0xffffd868  -> %ebp %esp
0xffffd85c  -> %esp
0xffffd858  -> %esp

0xffffd85c  -> %esp
0xffffd868  -> %ebp %esp
0xffffd86c  -> %esp
0xffffd870  -> %esp
```

9.4 Virtual Memory

Virtual memory can be mapped to more than just physical memory; it can be mapped to disk as well. Swap partitions on Linux allow Linux's virtual memory system to map memory not only to physical RAM, but also to disk blocks as well. For example, let's say you only have 16 Megabytes of physical memory. Let's also say that 8 Megabytes are being used by Linux and some basic applications, and you want to run a program that requires 20 Megabytes of memory. Can you? The answer is yes, but only if you have set up a swap partition. What happens is that after all of your remaining 8 Megabytes of physical memory have been mapped into virtual memory, Linux starts mapping parts of your application's virtual memory to disk blocks. So, if you access a "memory" location in your program, that location may not actually be in memory at all, but on disk. As the programmer you won't know the difference, though, because it is all handled behind the scenes by Linux.

Now, x86 processors cannot run instructions directly from disk, nor can they access data directly from disk. This requires the help of the operating system. When you try to access memory that is mapped to disk, the processor notices that it can't service your memory request directly. It then asks Linux to step in. Linux notices that the memory is actually on disk. Therefore, it moves some data that is currently in memory onto disk to make room, and then moves the memory being accessed from the disk back into physical memory. It then adjusts the processor's virtual-to-physical memory lookup tables so that it can find the memory in the new location. Finally, Linux returns control to the program and restarts it at the instruction which was trying to access the data in the first place. This instruction can now be completed successfully, because the memory is now in physical RAM.[46]

Here is an overview of the way memory accesses are handled under Linux:

- The program tries to load memory from a virtual address.
- The processor, using tables supplied by Linux, transforms the virtual memory address into a physical memory address on the fly.

[46]Note that not only can Linux have a virtual address map to a different physical address, it can also move those mappings around as needed.

- If the processor does not have a physical address listed for the memory address, it sends a request to Linux to load it.
- Linux looks at the address. If it is mapped to a disk location, it continues on to the next step. Otherwise, it terminates the program with a segmentation fault error.
- If there is not enough room to load the memory from disk, Linux will move another part of the program or another program onto disk to make room.
- Linux then moves the data into a free physical memory address.
- Linux updates the processor's virtual-to-physical memory mapping tables to reflect the changes.
- Linux restores control to the program, causing it to re-issue the instruction which caused this process to happen.
- The processor can now handle the instruction using the newly-loaded memory and translation tables.

It's a lot of work for the operating system, but it gives the user and the programmer great flexibility when it comes to memory management.

Now, in order to make the process more efficient, memory is separated out into groups called *pages*. When running Linux on x86 processors, a page is 4096 bytes of memory. All of the memory mappings are done a page at a time. Physical memory assignment, swapping, mapping, etc. are all done to memory pages instead of individual memory addresses. What this means to you as a programmer is that whenever you are programming, you should try to keep most memory accesses within the same basic range of memory, so you will only need a page or two of memory at a time. Otherwise, Linux may have to keep moving pages on and off of disk to satisfy your memory needs. Disk access is slow, so this can really slow down your program.

Sometimes so many programs can be loaded that there is hardly enough physical memory for them. They wind up spending more time just swapping memory on and off of disk than they do actually processing it. This leads to a condition called *swap death* which leads to your system being unresponsive and unproductive. It's usually recoverable if you start terminating your memory-hungry programs, but it's a pain.

NOTE.

Resident Set Size: The amount of memory that your program currently has in physical memory is called its resident set size, and can be viewed by using the program `top`. The resident set size is listed under the column labelled "RSS".

9.5 Getting More Memory

We now know that Linux maps all of our virtual memory into physical memory or swap. If you try to access a piece of virtual memory that hasn't been mapped yet, it triggers an error known as a segmentation fault, which will terminate your program. The program break point, if you remember, is the last valid address you can use. Now, this is all great if you know beforehand how much storage you will need. You can just add all the memory you need to your `.data` or `.bss` sections, and it will all be there. However, let's say you don't know how much memory you will need. For example, with a text editor, you don't know how long the person's file will be. You could try to find a maximum file size, and just tell the user that they can't go beyond that, but that's a waste if the file is small. Therefore Linux has a facility to move the break point to accommodate an application's memory needs.

If you need more memory, you can just tell Linux where you want the new break point to be, and Linux will map all the memory you need between the current and new break point, and then move the break point to the spot you specify. That memory is now available for your program to use. The way we tell Linux to move the break point is through the `brk` system call. The `brk` system call is call number 45 (which will be in *%eax*). *%ebx* should be loaded with the requested breakpoint. Then you call `int $0x80` to signal Linux to do its work. After mapping in your memory, Linux will return the new break point in *%eax*. The new break point might actually be larger than what you asked for, because Linux rounds up to the nearest page. If there is not enough physical memory or swap to fulfill your request, Linux will return a zero in *%eax*. Also, if you call `brk` with a zero in *%ebx*, it will simply return the last usable memory address.

The problem with this method is keeping track of the memory we request. Let's say I need to move the break to have room to load a file, and then need to move a break again to load another file. Let's say I then get rid of the first file. You now have a giant gap in memory that's mapped, but that you aren't using. If you continue to move the break in this way for each file you load, you can easily run out of memory. So, what is needed is a *memory manager*.

A memory manager is a set of routines that takes care of the dirty work of getting your program memory for you. Most memory managers have two basic functions - `allocate` and `deallocate`.[47] Whenever you need a certain amount of memory, you can simply tell `allocate` how much you need, and it will give you back an address to the memory. When you're done with it, you tell `deallocate` that you are through with it. `allocate` will then be able to reuse the memory. This pattern of memory management is called *dynamic memory allocation*. This minimizes the number of "holes" in your memory, making sure that you are making the best use of it you can. The pool of memory used by memory managers is commonly referred to as *the heap*.

The way memory managers work is that they keep track of where the system break is, and where the memory that you have allocated is. They mark each block of memory in the heap as being used or unused. When you request memory, the memory manager checks to see if there are any unused blocks of the appropriate size. If not, it calls the `brk` system call to request more memory. When you free memory it marks the block as unused so that future requests can retrieve it. In the next section we will look at building our own memory manager.

9.6 A Simple Memory Manager

Here I will show you a simple memory manager (`009-02-alloc.s`). It is very primitive but it shows the principles quite well. As usual, I will give you the program first for you to look through. Afterwards will follow an in-depth explanation. It looks long, but it is mostly comments.

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Program to manage memory usage - allocates
5       #     and deallocates memory as requested.
6       #
7       # NOTES:
8       #     The programs using these routines will ask
9       #     for a certain size of memory.  We actually
10      #     use more than that size, but we put it at the
11      #     beginning, before the pointer we hand back.
12      #     We add a size field and an
13      #     AVAILABLE/UNAVAILABLE marker.  So, the memory
14      #     looks like this.
15      #
16      ##################################################
17      # - Available  -#-  Size of  -#-  Actual memory  -#
18      # -  Marker    -#-  memory   -#-   locations     -#
19      ##################################################
20      #                             ^--Returned pointer
21      #                                points here.
22      #
23      # The pointer we return only points to the actual
24      # locations requested to make it easier for the
25      # calling program.  It also allows us to change our
26      # structure without the calling program having to
27      # change at all.
```

[47] The function names usually aren't `_allocate` and `_deallocate`, but the functionality will be the same. In the C programming language, for example, they are named `malloc` and `free`.

```
28      #
29      .section .data
30          # ----- GLOBAL VARIABLES ----- #
31          #
32          heap_begin:         # This points to the
33              .long  0        # beginning of the memory
34                              # we are managing.
35
36          current_break:      # This points to one
37              .long  0        # location past the memory
38                              # we are managing.
39
40          # ----- STRUCTURE INFORMATION ----- #
41          #
42          .equ HEADER_SIZE,      8    # Size of space for
43                                      # memory region
44                                      # header.
45
46          .equ HDR_AVAIL_OFFSET, 0    # Location of the
47                                      # "available" flag
48                                      # in the header.
49
50          .equ HDR_SIZE_OFFSET,  4    # Location of the
51                                      # size field in the
52                                      # header.
53
54          # ----- CONSTANTS ----- #
55          #
56          .equ UNAVAILABLE,    0      # This is the
57                                      # number we will
58                                      # use to mark space
59                                      # that has been
60                                      # given out.
61
62          .equ AVAILABLE,      1      # This is the
63                                      # number we will
64                                      # use to mark space
65                                      # that has been
66                                      # returned, and is
67                                      # available for
68                                      # giving.
69
70          .equ SYS_BRK,        45     # System call
71                                      # number for the
72                                      # break system
73                                      # call.
74
75          .equ LINUX_SYSCALL,  0x80   # Make system calls
76                                      # easier to read.
77
78      .section .text
79      # ----- FUNCTIONS ----- #
80      #
```

```
81      # ----- FUNCTION: _allocate_init ----- #
82      #
83      # PURPOSE:
84      #     Call this function to initialize the
85      #     functions (specifically, this sets heap_begin
86      #     and current_break). This has no parameters
87      #     and no return value.
88      #
89          .globl _allocate_init
90          .type  _allocate_init,  @function
91
92  _allocate_init:
93      pushl %ebp              # Standard function stuff.
94      movl  %esp, %ebp
95
96      # If the brk system call is called with 0 in %ebx,
97      # it returns the last valid usable address.
98      #
99      movl  $SYS_BRK, %eax    # Find out where the
100     movl  $0, %ebx          # break is.
101     int   $LINUX_SYSCALL
102
103     incl  %eax              # %eax now has the last
104                             # valid address, and we
105                             # want the memory location
106                             # after that.
107
108                             # Store the current break.
109     movl  %eax, current_break
110
111     movl  %eax, heap_begin  # Store the current break
112                             # as our first address.
113                             # This will cause the
114                             # allocate function to get
115                             # more memory from Linux
116                             # the first time it is run.
117
118     movl  %ebp, %esp        # Exit the function.
119     popl  %ebp
120     ret
121
122     # ----- END OF FUNCTION: _allocate_init ----- #
123
124     # ----- FUNCTION: allocate ----- #
125     #
126     # PURPOSE:
127     #     This function is used to grab a section of
128     #     memory. It checks to  see if there are any
129     #     free blocks, and, if not, it asks Linux for
130     #     a new one.
131     #
132     # PARAMETERS:
133     #     This function has one parameter - the size
```

```
134     #     of the memory block we want to allocate.
135     #
136     # RETURN VALUE:
137     #     This function returns the address of the
138     #     allocated memory in %eax.  If there is no
139     #     memory available, it will return 0 in %eax.
140     #
141     # PROCESSING:
142     #     Variables used:
143     #       %ecx - hold the size of the requested
144     #       memory (first/only parameter).
145     #       %eax - current memory region being examined
146     #       %ebx - current break position.
147     #       %edx - size of current memory region.
148     #
149     # We scan through each memory region starting with
150     # heap_begin. We look at the size of each one, and
151     # if it has been allocated.  If it is big enough
152     # for the requested size, and its available, it
153     # grabs that one. If it does not find a region
154     # large enough, it asks Linux for more memory.  In
155     # that case, it moves current_break up.
156     #
157         .globl _allocate
158         .type  _allocate,   @function
159
160         .equ ST_MEM_SIZE,  8    # Stack position of the
161                                 # memory size to
162                                 # allocate.
163
164 _allocate:
165     pushl %ebp              # Standard function stuff.
166     movl  %esp, %ebp
167
168                             # %ecx will hold the size
169                             # we are looking for (which
170                             # is the first and only
171                             # parameter).
172                 # ST_MEM_SIZE = 8
173     movl  ST_MEM_SIZE(%ebp), %ecx
174                 # %ecx <- RECORD_SIZE, 324
175
176     movl  heap_begin, %eax  # %eax will hold the
177                             # current search location.
178
179                             # %ebx will hold the
180                             # current break.
181     movl  current_break, %ebx
182
183
184 _alloc_loop_begin:          # Here we iterate through
185                             # each memory region.
186
```

```
187                 # %eax <- heap_begin
188                 # %ebx <- current_break
189     cmpl  %ebx, %eax        # Need more memory if these
190     je    _move_break       # are equal.
191
192                             # Grab the size of this
193                             # memory.
194                 # HDR_SIZE_OFFSET = 4
195                 # %eax <- heap_begin
196     movl  HDR_SIZE_OFFSET(%eax), %edx
197                 # %edx <- HDR_SIZE_OFFSET of heap_begin
198                 #         ~ 324
199
200                             # If the space is
201                             # unavailable, go to the
202                             # next one.
203                 # UNAVAILABLE = 0
204                 # HDR_AVAIL_OFFSET = 0
205                 # %eax <- heap_begin
206     cmpl  $UNAVAILABLE, HDR_AVAIL_OFFSET(%eax)
207     je    _next_location
208
209                 # %ecx <- RECORD_SIZE, 324
210                 # %edx <- HDR_SIZE_OFFSET of heap_begin
211                 #         ~ 324
212     cmpl  %edx, %ecx        # If the space is
213     jle   _allocate_here    # available, compare the
214                             # size to the needed size.
215                             # If its big enough, go to
216                             # _allocate_here.
217
218 _next_location:
219                     # The total size of the memory
220                     # region is the sum of the size
221                     # requested (currently stored in
222                     # %edx), plus another 8 bytes for
223                     # the header (4 for the
224                     # AVAILABLE/UNAVAILABLE flag, and
225                     # 4 for the size of the region).
226                     # So, adding %edx and $8 to %eax
227                     # will get the address of the next
228                     # memory region.
229                     #
230                 # HEADER_SIZE = 8
231                 # %eax <- heap_begin
232     addl  $HEADER_SIZE, %eax
233                 # %eax <- heap_begin + HEADER_SIZE
234
235                 # %eax <- heap_begin + HEADER_SIZE
236                 # %edx <- HDR_SIZE_OFFSET(%eax)
237     addl  %edx, %eax
238                 # %eax <- heap_begin + HEADER_SIZE
239                 #         + HDR_SIZE_OFFSET
```

```
240
241                     # Go look at the next location.
242     jmp   _alloc_loop_begin
243
244 _allocate_here:     # If we have made it here, that
245                     # means that the region header of
246                     # the region to allocate is in
247                     # %eax.
248
249                             # Mark space as unavailable
250                 # UNAVAILABLE = 0
251                 # HDR_AVAIL_OFFSET = 0
252                 # %eax <- heap_begin
253     movl  $UNAVAILABLE, HDR_AVAIL_OFFSET(%eax)
254
255                             # Move %eax past the header
256                             # to the usable memory
257                             # (since that is what we
258                             # return).
259                 # HEADER_SIZE = 8
260                 # %eax <- heap_begin
261     addl  $HEADER_SIZE, %eax
262                 # %eax <- heap_begin + HEADER_SIZE
263
264     movl  %ebp, %esp        # Return from the function.
265     popl  %ebp
266     ret
267
268 _move_break:        # If we have made it here, that
269                     # means that we have exhausted all
270                     # addressable memory, and we need
271                     # to ask for more. %ebx holds the
272                     # current endpoint of the data,
273                     # and %ecx holds its size.
274
275                     # We need to increase %ebx to
276                     # where we want memory to end, so
277                     # we add space for the headers
278                     # structure.
279                 # HEADER_SIZE = 8
280                 # %ebx <- current_break
281     addl  $HEADER_SIZE, %ebx
282                 # %ebx <- current_break + HEADER_SIZE
283
284                 # ST_MEM_SIZE = 8
285                 # HEADER_SIZE = 8
286                 # %ecx <- ST_MEM_SIZE(%ebp) ~ 324
287     addl  %ecx, %ebx        # Add space to the break
288                             # for the data requested.
289                 # %ebx <- current_break + HEADER_SIZE
290                 #         + ST_MEM_SIZE(%ebp) ~ 324
291                 #      == 0x???????? + 8 + 324 = ~342
292
```

```
293                             # Now its time to ask Linux
294                             # for more memory.
295                 # %eax <- heap_begin
296         pushl %eax              # Save needed registers.
297
298         movl  $SYS_BRK, %eax    # Reset the break (%ebx has
299                             # the requested break
300                             # point).
301
302         int   $LINUX_SYSCALL    # Under normal conditions,
303                             # this should return the
304                             # new break in %eax, which
305                             # will be either 0 if it
306                             # fails, or it will be
307                             # equal to or larger than
308                             # we asked for. We do not
309                             # care in this program
310                             # where it actually sets
311                             # the break, so as long as
312                             # %eax is not 0, we do not
313                             # care what it is.
314
315         cmpl  $0, %eax          # Check for error
316         je    _error            # conditions.
317
318                   # %eax <- heap_begin
319         popl  %eax              # Restore saved registers.
320
321                             # Set this memory as
322                             # unavailable, since we are
323                             # about to give it away.
324                   # UNAVAILABLE = 0
325                   # HDR_AVAIL_OFFSET = 0
326                   # %eax <- $heap_begin
327         movl  $UNAVAILABLE, HDR_AVAIL_OFFSET(%eax)
328
329                             # Set the size of the
330                             # memory.
331                   # ST_MEM_SIZE = 8
332                   # HDR_SIZE_OFFSET = 4
333                   # %eax <- $heap_begin
334                   # %ecx <- ST_MEM_SIZE(%ebp) ~ 324
335         movl  %ecx, HDR_SIZE_OFFSET(%eax)
336
337                             # Move %eax to the actual
338                             # start of usable memory.
339                             # %eax now holds the return
340                             # value.
341                   # %eax <- $heap_begin
342                   # HEADER_SIZE = 8
343         addl  $HEADER_SIZE, %eax
344                   # %eax <- $heap_begin + HEADER_SIZE
345
```

```
346                 # %ebx <- current_break + HEADER_SIZE
347                 #         + ST_MEM_SIZE(%ebp) ~ 342
348     movl  %ebx, current_break   # Save the new break.
349
350     movl  %ebp, %esp            # Return the function.
351     popl  %ebp
352     ret
353
354 _error:
355     movl  $0, %eax          # On error, we return zero.
356     movl  %ebp, %esp
357     popl  %ebp
358     ret
359     # ----- END OF FUNCTION: allocate ----- #
360
361
362     # ----- FUNCTION: _deallocate ----- #
363     #
364     # PURPOSE:
365     #     The purpose of this function is to give back
366     #     a region of memory to the pool after we are
367     #     done using it.
368     #
369     # PARAMETERS:
370     #     The only parameter is the address of the
371     #     memory we want to return to the memory pool.
372     #
373     # RETURN VALUE:
374     #     There is no return value
375     #
376     # PROCESSING:
377     #     If you remember, we actually hand the program
378     #     the start of the memory that they can use,
379     #     which is 8 storage locations after the actual
380     #     start of the memory region.  All we have to
381     #     do is go back 8 locations and mark that
382     #     memory as available, so that the allocate
383     #     function knows it can use it.
384     #
385         .globl _deallocate
386         .type  _deallocate,   @function
387
388         .equ ST_MEMORY_SEG,  4  # Stack position of the
389                                 # memory region to free
390
391 _deallocate:        # Since the function is so simple,
392                     # we do not need any of the fancy
393                     # function stuff.
394
395                     # Get the address of the memory to
396                     # free (normally this is 8(%ebp),
397                     # but since we did not push %ebp or
398                     # move %esp to %ebp, we can just
```

```
399                     # do 4(%esp).
400     movl  ST_MEMORY_SEG(%esp), %eax
401
402                             # Get the pointer to the
403                             # real beginning of the
404                             # memory.
405     subl  $HEADER_SIZE, %eax
406
407                             # Mark it as available.
408     movl  $AVAILABLE, HDR_AVAIL_OFFSET(%eax)
409
410     ret
411     # ----- END OF FUNCTION: _deallocate ----- #
```

The first thing to notice is that there is no `_start` symbol. The reason is that this is just a set of functions. A memory manager by itself is not a full program - it doesn't do anything. It is simply a utility to be used by other programs.

To assemble the program, do the following:

```
as -o 009-02-alloc.o  --32 \
                      --gstabs+ \
                      009-02-alloc.s
```

Okay, now let's look at the code.

9.6.1 Variables and Constants

At the beginning of the program, we have two locations set up:

```
32          heap_begin:         # This points to the
33              .long  0        # beginning of the memory
34                              # we are managing.
35
36          current_break:      # This points to one
37              .long  0        # location past the memory
38                              # we are managing.
```

Remember, the section of memory being managed is commonly referred to as the *heap*. When we assemble the program, we have no idea where the beginning of the heap is, nor where the current break is. Therefore, we reserve space for their addresses, but just fill them with a 0 for the time being.

Next we have a set of constants to define the structure of the heap. The way this memory manager works is that before each region of memory allocated, we will have a short record describing the memory. This record has a word reserved for the available flag and a word for the region's size. The actual memory allocated immediately follows this record. The available flag is used to mark whether this region is available for allocations, or if it is currently in use. The size field lets us know both whether or not this region is big enough for an allocation request, as well as the location of the next memory region. The following constants describe this record:

```
42          .equ HEADER_SIZE,      8    # Size of space for
43                                      # memory region
44                                      # header.
45
46          .equ HDR_AVAIL_OFFSET, 0    # Location of the
47                                      # "available" flag
48                                      # in the header.
49
```

```
50          .equ HDR_SIZE_OFFSET,  4    # Location of the
51                                      # size field in the
52                                      # header.
```

This says that the header is 8 bytes total, the available flag is offset 0 bytes from the beginning, and the size field is offset 4 bytes from the beginning. If we are careful to always use these constants, then we protect ourselves from having to do too much work if we later decide to add more information to the header.

The values that we will use for our `available` field are either 0 for unavailable, or 1 for available. To make this easier to read, we have the following definitions:

```
56          .equ UNAVAILABLE,    0      # This is the
57                                      # number we will
58                                      # use to mark space
59                                      # that has been
60                                      # given out.
61
62          .equ AVAILABLE,      1      # This is the
63                                      # number we will
64                                      # use to mark space
65                                      # that has been
66                                      # returned, and is
67                                      # available for
68                                      # giving.
```

Finally, we have our Linux system call definitions:

```
70          .equ SYS_BRK,        45     # System call
71                                      # number for the
72                                      # break system
73                                      # call.
74
75          .equ LINUX_SYSCALL,  0x80   # Make system calls
76                                      # easier to read.
```

9.6.2 The `_allocate_init` function

Okay, this is a simple function. All it does is set up the `heap_begin` and `current_break` variables we discussed earlier. So, if you remember the discussion earlier, the current break can be found using the `brk` system call. So, the function starts like this:

```
92  _allocate_init:
93      pushl %ebp              # Standard function stuff.
94      movl  %esp, %ebp
95
96      # If the brk system call is called with 0 in %ebx,
97      # it returns the last valid usable address.
98      #
99      movl  $SYS_BRK, %eax    # Find out where the
100     movl  $0, %ebx          # break is.
101     int   $LINUX_SYSCALL
```

Anyway, after `int $LINUX_SYSCALL`, `%eax` holds the last valid address. We actually want the first invalid address instead of the last valid address, so we just increment `%eax`. Then we move that value to the `heap_begin` and `current_break` locations. Then we leave the function. The code looks like this:

```
103     incl  %eax              # %eax now has the last
104                             # valid address, and we
105                             # want the memory location
106                             # after that.
107
108                             # Store the current break.
109     movl  %eax, current_break
110
111     movl  %eax, heap_begin  # Store the current break
112                             # as our first address.
113                             # This will cause the
114                             # allocate function to get
115                             # more memory from Linux
116                             # the first time it is run.
117
118     movl  %ebp, %esp        # Exit the function.
119     popl  %ebp
120     ret
```

The heap consists of the memory between `heap_begin` and `current_break`, so this says that we start off with a heap of zero bytes. Our `_allocate` function will then extend the heap as much as it needs to when it is called.

9.6.3 The `_allocate` function

This is the doozy function. Let's start by looking at an outline of the function:

1. Start at the beginning of the heap.
2. Check to see if we're at the end of the heap.
3. If we are at the end of the heap, grab the memory we need from Linux, mark it as "unavailable" and return it. If Linux won't give us any more, return a 0.
4. If the current memory region is marked "unavailable", go to the next one, and go back to step 2.
5. If the current memory region is too small to hold the requested amount of space, go back to step 2.
6. If the memory region is available and large enough, mark it as "unavailable" and return it.

Now, look back through the code with this in mind. Be sure to read the comments so you'll know which register holds which value.

Now that you've looked back through the code, let's examine it one line at a time. We start off like this:

```
164 _allocate:
165     pushl %ebp              # Standard function stuff.
166     movl  %esp, %ebp
167
168                             # %ecx will hold the size
169                             # we are looking for (which
170                             # is the first and only
171                             # parameter).
172                 # ST_MEM_SIZE = 8
173     movl  ST_MEM_SIZE(%ebp), %ecx
174                 # %ecx <- RECORD_SIZE, 324
175
176     movl  heap_begin, %eax  # %eax will hold the
177                             # current search location.
178
```

```
179                             # %ebx will hold the
180                             # current break.
181     movl  current_break, %ebx
```

This part initializes all of our registers. The first two lines are standard function stuff. The next move pulls the size of the memory to allocate off of the stack. This is our only function parameter. After that, it moves the beginning heap address and the end of the heap into registers. I am now ready to do processing.

The next section is marked `_alloc_loop_begin`. In this loop we are going to examine memory regions until we either find an open memory region or determine that we need more memory. Our first instructions check to see if we need more memory:

```
184 _alloc_loop_begin:          # Here we iterate through
185                             # each memory region.
186
187                 # %eax <- heap_begin
188                 # %ebx <- current_break
189     cmpl  %ebx, %eax        # Need more memory if these
190     je    _move_break       # are equal.
```

%eax holds the current memory region being examined and *%ebx* holds the location past the end of the heap. Therefore if the next region to be examined is past the end of the heap, it means we need more memory to allocate a region of this size. Let's skip down to `_move_break` and see what happens there:

```
268 _move_break:        # If we have made it here, that
269                     # means that we have exhausted all
270                     # addressable memory, and we need
271                     # to ask for more. %ebx holds the
272                     # current endpoint of the data,
273                     # and %ecx holds its size.
274
275                     # We need to increase %ebx to
276                     # where we want memory to end, so
277                     # we add space for the headers
278                     # structure.
279                 # HEADER_SIZE = 8
280                 # %ebx <- current_break
281     addl  $HEADER_SIZE, %ebx
282                 # %ebx <- current_break + HEADER_SIZE
283
284                 # ST_MEM_SIZE = 8
285                 # HEADER_SIZE = 8
286                 # %ecx <- ST_MEM_SIZE(%ebp) ~ 324
287     addl  %ecx, %ebx        # Add space to the break
288                             # for the data requested.
289                 # %ebx <- current_break + HEADER_SIZE
290                 #         + ST_MEM_SIZE(%ebp) ~ 324
291                 #      == 0x???????? + 8 + 324 = ~342
292
293                             # Now its time to ask Linux
294                             # for more memory.
295                 # %eax <- heap_begin
296     pushl %eax              # Save needed registers.
297
298     movl  $SYS_BRK, %eax    # Reset the break (%ebx has
299                             # the requested break
```

```
300                             # point).
301
302     int   $LINUX_SYSCALL    # Under normal conditions,
303                             # this should return the
304                             # new break in %eax, which
305                             # will be either 0 if it
306                             # fails, or it will be
307                             # equal to or larger than
308                             # we asked for. We do not
309                             # care in this program
310                             # where it actually sets
311                             # the break, so as long as
312                             # %eax is not 0, we do not
313                             # care what it is.
```

When we reach this point in the code, *%ebx* holds where we want the next region of memory to be. So, we add our header size and region size to *%ebx*, and that's where we want the system break to be. We then push all the registers we want to save on the stack, and call the `brk` system call. After that we check for errors:

```
315     cmpl  $0, %eax          # Check for error
316     je    _error            # conditions.
```

If there were no errors we pop the registers back off the stack, mark the memory as unavailable, record the size of the memory, and make sure *%eax* points to the start of usable memory (which is *after* the header).

```
318                 # %eax <- heap_begin
319     popl  %eax              # Restore saved registers.
320
321                             # Set this memory as
322                             # unavailable, since we are
323                             # about to give it away.
324                 # UNAVAILABLE = 0
325                 # HDR_AVAIL_OFFSET = 0
326                 # %eax <- $heap_begin
327     movl  $UNAVAILABLE, HDR_AVAIL_OFFSET(%eax)
328
329                             # Set the size of the
330                             # memory.
331                 # ST_MEM_SIZE = 8
332                 # HDR_SIZE_OFFSET = 4
333                 # %eax <- $heap_begin
334                 # %ecx <- ST_MEM_SIZE(%ebp) ~ 324
335     movl  %ecx, HDR_SIZE_OFFSET(%eax)
336
337                             # Move %eax to the actual
338                             # start of usable memory.
339                             # %eax now holds the return
340                             # value.
341                 # %eax <- $heap_begin
342                 # HEADER_SIZE = 8
343     addl  $HEADER_SIZE, %eax
344                 # %eax <- $heap_begin + HEADER_SIZE
```

Then we store the new program break and return the pointer to the allocated memory.

```
346                 # %ebx <- current_break + HEADER_SIZE
347                 #         + ST_MEM_SIZE(%ebp) ~ 342
348     movl  %ebx, current_break   # Save the new break.
349
350     movl  %ebp, %esp            # Return the function.
351     popl  %ebp
352     ret
```

The `_error` code just returns 0 in *%eax*, so we won't discuss it.

Let's go back look at the rest of the loop. What happens if the current memory being looked at isn't past the end of the heap? Well, let's look.

```
192                           # Grab the size of this
193                           # memory.
194                 # HDR_SIZE_OFFSET = 4
195                 # %eax <- heap_begin
196     movl  HDR_SIZE_OFFSET(%eax), %edx
197                 # %edx <- HDR_SIZE_OFFSET of heap_begin
198                 #         ~ 324
199
200                           # If the space is
201                           # unavailable, go to the
202                           # next one.
203                 # UNAVAILABLE = 0
204                 # HDR_AVAIL_OFFSET = 0
205                 # %eax <- heap_begin
206     cmpl  $UNAVAILABLE, HDR_AVAIL_OFFSET(%eax)
207     je    _next_location
```

This first grabs the size of the memory region and puts it in *%edx*. Then it looks at the available flag to see if it is set to `UNAVAILABLE`. If so, that means that memory region is in use, so we'll have to skip over it. So, if the available flag is set to `UNAVAILABLE`, you go to the code labeled `_next_location`. If the available flag is set to `AVAILABLE`, then we keep on going.

Let's say that the space was available, and so we keep going. Then we check to see if this space is big enough to hold the requested amount of memory. The size of this region is being held in *%edx*, so we do this:

```
209                 # %ecx <- RECORD_SIZE, 324
210                 # %edx <- HDR_SIZE_OFFSET of heap_begin
211                 #         ~ 324
212     cmpl  %edx, %ecx        # If the space is
213     jle   _allocate_here    # available, compare the
214                             # size to the needed size.
215                             # If its big enough, go to
216                             # _allocate_here.
```

If the requested size is less than or equal to the current region's size, we can use this block. It doesn't matter if the current region is larger than requested, because the extra space will just be unused. So, let's jump down to `_allocate_here` and see what happens:

```
244 _allocate_here:     # If we have made it here, that
245                     # means that the region header of
246                     # the region to allocate is in
247                     # %eax.
248
249                             # Mark space as unavailable
```

```
250                 # UNAVAILABLE = 0
251                 # HDR_AVAIL_OFFSET = 0
252                 # %eax <- heap_begin
253     movl  $UNAVAILABLE, HDR_AVAIL_OFFSET(%eax)
254
255                             # Move %eax past the header
256                             # to the usable memory
257                             # (since that is what we
258                             # return).
259                 # HEADER_SIZE = 8
260                 # %eax <- heap_begin
261     addl  $HEADER_SIZE, %eax
262                 # %eax <- heap_begin + HEADER_SIZE
263
264     movl  %ebp, %esp        # Return from the function.
265     popl  %ebp
266     ret
```

It marks the memory as being unavailable. Then it moves the pointer *%eax* past the header, and uses it as the return value for the function. Remember, the person using this function doesn't need to even know about our memory header record. They just need a pointer to usable memory.

Okay, so let's say the region wasn't big enough. What then? Well, we would then be at the code labeled `_next_location`. This section of code is used any time that we figure out that the current memory region won't work for allocating memory. All it does is advance *%eax* to the next possible memory region, and goes back to the beginning of the loop. Remember that *%edx* is holding the size of the current memory region, and `HEADER_SIZE` is the symbol for the size of the memory region's header. So this code will move us to the next memory region:

```
218 _next_location:
219                     # The total size of the memory
220                     # region is the sum of the size
221                     # requested (currently stored in
222                     # %edx), plus another 8 bytes for
223                     # the header (4 for the
224                     # AVAILABLE/UNAVAILABLE flag, and
225                     # 4 for the size of the region).
226                     # So, adding %edx and $8 to %eax
227                     # will get the address of the next
228                     # memory region.
229                     #
230                 # HEADER_SIZE = 8
231                 # %eax <- heap_begin
232     addl  $HEADER_SIZE, %eax
233                 # %eax <- heap_begin + HEADER_SIZE
234
235                 # %eax <- heap_begin + HEADER_SIZE
236                 # %edx <- HDR_SIZE_OFFSET(%eax)
237     addl  %edx, %eax
238                 # %eax <- heap_begin + HEADER_SIZE
239                 #         + HDR_SIZE_OFFSET
240
241                     # Go look at the next location.
242     jmp   _alloc_loop_begin
```

And now the function runs another loop.

Whenever you have a loop, you must make sure that it will *always* end. The best way to do that is to examine all of the possibilities, and make sure that all of them eventually lead to the loop ending. In our case, we have the following possibilities:

- We will reach the end of the heap.
- We will find a memory region that's available and large enough.
- We will go to the next location.

The first two items are conditions that will cause the loop to end. The third one will keep it going. However, even if we never find an open region, we will eventually reach the end of the heap, because it is a finite size. Therefore, we know that no matter which condition is true, the loop has to eventually hit a terminating condition.

9.6.4 The `_deallocate` function

The `_deallocate` function is much easier than the `_allocate` one. That's because it doesn't have to do any searching at all. It can just mark the current memory region as `AVAILABLE`, and `_allocate` will find it next time it is called. So we have:

```
391  _deallocate:        # Since the function is so simple,
392                      # we do not need any of the fancy
393                      # function stuff.
394
395                      # Get the address of the memory to
396                      # free (normally this is 8(%ebp),
397                      # but since we did not push %ebp or
398                      # move %esp to %ebp, we can just
399                      # do 4(%esp).
400      movl  ST_MEMORY_SEG(%esp), %eax
401
402                              # Get the pointer to the
403                              # real beginning of the
404                              # memory.
405      subl  $HEADER_SIZE, %eax
406
407                              # Mark it as available.
408      movl  $AVAILABLE, HDR_AVAIL_OFFSET(%eax)
409
410      ret
```

In this function, we don't have to save *%ebp* or *%esp* since we're not changing them, nor do we have to restore them at the end. All we're doing is reading the address of the memory region from the stack, backing up to the beginning of the header, and marking the region as available. This function has no return value, so we don't care what we leave in *%eax*.

9.6.5 Performance Issues and Other Problems

Our simplistic memory manager is not really useful for anything more than an academic exercise. This section looks at the problems with such a simplistic allocator.

The biggest problem here is speed. Now, if there are only a few allocations made, then speed won't be a big issue. But think about what happens if you make a thousand allocations. On allocation number 1000, you have to search through 999 memory regions to find that you have to request more memory. As you can see, that's getting pretty slow. In addition, remember that Linux can keep pages of memory on disk instead of in memory. So, since you have to go through every piece of memory your program's memory, that means that Linux has to load every part of memory that's currently on disk to check to see if it is available. You can see how this could

get really, really slow.[48] This method is said to run in *linear* time, which means that every element you have to manage makes your program take longer. A program that runs in *constant* time takes the same amount of time no matter how many elements you are managing. Take the `_deallocate` function, for instance. It only runs 4 instructions, no matter how many elements we are managing, or where they are in memory. In fact, although our `_allocate` function is one of the slowest of all memory managers, the `_deallocate` function is one of the fastest.

Another performance problem is the number of times we're calling the `brk` system call. System calls take a long time. They aren't like functions, because the processor has to switch modes. Your program isn't allowed to map itself memory, but the Linux kernel is. So, the processor has to switch into *kernel mode*, then Linux maps the memory, and then switches back to *user mode* for your application to continue running. This is also called a *context switch*. Context switches are relatively slow on x86 processors. Generally, you should avoid calling the kernel unless you really need to.

Another problem that we have is that we aren't recording where Linux actually sets the break. Previously we mentioned that Linux might actually set the break past where we requested it. In this program, we don't even look at where Linux actually sets the break - we just assume it sets it where we requested. That's not really a bug, but it will lead to unnecessary `brk` system calls when we already have the memory mapped in.

Another problem we have is that if we are looking for a 5-byte region of memory, and the first open one we come to is 1000 bytes, we will simply mark the whole thing as allocated and return it. This leaves 995 bytes of unused, but allocated, memory. It would be nice in such situations to break it apart so the other 995 bytes can be used later. It would also be nice to combine consecutive free spaces when looking for large allocations.

9.7 Using our Allocator

The programs we do in this book aren't complicated enough to necessitate a memory manager. Therefore, we will just use our memory manager to allocate a buffer for one of our file reading/writing programs instead of assigning it in the `.bss`.

The program we will demonstrate this on is `009-02-read-records.s` from Chapter 6. Reading and Writing Simple Records. This program uses a buffer named `_record_buffer` to handle its input/output needs. We will simply change this from being a buffer defined in `.bss` to being a pointer to a dynamically-allocated buffer using our memory manager. You will need to have the code from that program handy as we will only be discussing the changes in this section.

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       .include "006-01-linux.s"      # Linux Definitions.
4       .include "006-01-record-def.s" # Record definitions
5
6       .section .data
7           file_name:
8               .ascii "test.dat\0"
9
10          record_buffer_ptr:
11              .long 0
12
13      .section .bss
14          .lcomm record_buffer,  RECORD_SIZE
15
16      .section .text
17          .globl _start
18
19  _start:
20      # ----- Main Program ----- #
```

[48] This is why adding more memory to your computer makes it run faster. The more memory your computer has, the less it puts on disk, so it doesn't have to always be interrupting your programs to retrieve pages off the disk.

```
21      #
22      # These are the locations on the stack where we
23      # will store the input and output descriptors
24      # (FYI - we could have used memory addresses in a
25      # .data section instead).
26      #
27      .equ ST_INPUT_DESCRIPTOR,   -4
28      .equ ST_OUTPUT_DESCRIPTOR,  -8
29
30      call _allocate_init
31
32      pushl $RECORD_SIZE
33      call  _allocate
34      movl  %eax, record_buffer_ptr
35
36      movl  %esp, %ebp        # Copy the stack pointer to
37                              # %ebp.
38      subl  $8, %esp          # Allocate space to hold
39                              # the file descriptors.
40
41      movl  $SYS_OPEN, %eax   # Open the file.
42      movl  $file_name, %ebx
43      movl  $0, %ecx          # This says to open
44                              # read-only.
45      movl  $0666, %edx
46      int   $LINUX_SYSCALL
47
48      # ----- Save file descriptor ----- #
49      #
50      movl  %eax, ST_INPUT_DESCRIPTOR(%ebp)
51
52      # Even though it is a constant, we are saving the
53      # output file descriptor in a local variable so
54      # that if we later decide that it is not always
55      # going to be STDOUT, we can change it easily.
56      #
57      movl  $STDOUT, ST_OUTPUT_DESCRIPTOR(%ebp)
58
59  _record_read_loop:
60      pushl ST_INPUT_DESCRIPTOR(%ebp)
61      pushl record_buffer_ptr
62      call  _read_record
63      addl  $8, %esp
64
65      # Returns the number of bytes read. If it is not
66      # the same number we requested, then it is either
67      # an end-of-file, or an error, so we are quitting.
68      #
69      cmpl  $RECORD_SIZE, %eax
70      jne   _finished_reading
71
72      # Otherwise, print out the first name but we must
73      # know the size.
```

```
74      #
75      movl  record_buffer_ptr, %eax
76      addl  $RECORD_FIRSTNAME, %eax
77      pushl %eax
78      call   _count_chars
79      addl   $4, %esp
80
81      movl   %eax, %edx
82      movl   ST_OUTPUT_DESCRIPTOR(%ebp), %ebx
83      movl   $SYS_WRITE, %eax
84      movl  record_buffer_ptr, %ecx
85      addl  $RECORD_FIRSTNAME, %ecx
86      int    $LINUX_SYSCALL
87
88      pushl  ST_OUTPUT_DESCRIPTOR(%ebp)
89      call   _write_newline
90      addl   $4, %esp
91
92      jmp    _record_read_loop
93
94  _finished_reading:
95      pushl record_buffer_ptr
96      call  _deallocate
97
98      movl   $SYS_EXIT, %eax
99      movl   $0, %ebx
100     int    $LINUX_SYSCALL
```

The first change we need to make is in the declaration. Currently it looks like this:

```
6       .section .data
7           file_name:
8               .ascii "test.dat\0"
9
10      .section .bss
11          .lcomm record_buffer,  RECORD_SIZE
```

It would be a misnomer to keep the same name, since we are switching it from being an actual buffer to being a pointer to a buffer. In addition, it now only needs to be one word big (enough to hold a pointer). The new declaration will stay in the `.data` section and look like this:

```
6       .section .data
7           file_name:
8               .ascii "test.dat\0"
9
10          record_buffer_ptr:
11              .long 0
12
13      .section .bss
14          .lcomm record_buffer,  RECORD_SIZE
```

Our next change is we need to initialize our memory manager immediately after we start our program. Therefore, right after the stack is set up, the following call needs to be added:

```
30      call _allocate_init
```

After that, the memory manager is ready to start servicing memory allocation requests. We need to allocate enough memory to hold these records that we are reading. Therefore, we will call `_allocate` to allocate this memory, and then save the pointer it returns into `record_buffer_ptr`. Like this:

```
32      pushl $RECORD_SIZE
33      call  _allocate
34      movl  %eax, record_buffer_ptr
```

Now, when we make the call to `_read_record`, it is expecting a pointer. In the old code, the pointer was the immediate-mode reference to `_record_buffer`. Now, `record_buffer_ptr` just holds the pointer rather than the buffer itself. Therefore, we must do a direct mode load to get the value in `record_buffer_ptr`. We need to remove this line:

```
52      pushl $record_buffer
```

And put this line in its place:

```
61      pushl record_buffer_ptr
```

The next change comes when we are trying to find the address of the firstname field of our record. In the old code, it was `$RECORD_FIRSTNAME + record_buffer`. However, that only works because it is a constant offset from a constant address. In the new code, it is the offset of an address stored in `record_buffer_ptr`. To get that value, we will need to move the pointer into a register, and then add `$RECORD_FIRSTNAME` to it to get the pointer. So where we have the following code:

```
66      pushl  $RECORD_FIRSTNAME + record_buffer
```

We need to replace it with this:

```
75      movl  record_buffer_ptr, %eax
76      addl  $RECORD_FIRSTNAME, %eax
77      pushl %eax
```

Similarly, we need to change the line that says

```
73      movl   $RECORD_FIRSTNAME + record_buffer, %ecx
```

so that it reads like this:

```
84      movl  record_buffer_ptr, %ecx
85      addl  $RECORD_FIRSTNAME, %ecx
```

Finally, one change that we need to make is to deallocate the memory once we are done with it (in this program it's not necessary, but it's a good practice anyway). To do that, we just send `record_buffer_ptr` to the `_deallocate` function right before exiting:

```
95      pushl record_buffer_ptr
96      call  _deallocate
```

Now you can build your program with the following commands:

```
as -o 009-02-read-records.o  --32 \
                             --gstabs+ \
                             009-02-read-records.s

ld -o 009-02-read-records    -m elf_i386 \
                             006-01-count-chars.o \
                             006-01-read-record.o \
                             006-01-write-newline.o \
```

```
                                009-02-alloc.o \
                                009-02-read-records.o
```

You can then run your program by doing `./009-02-read-records`.

The uses of dynamic memory allocation may not be apparent to you at this point, but as you go from academic exercises to real-life programs you will use it continually.

9.8 More Information

More information on memory handling in Linux and other operating systems can be found at the following locations:

- More information about the memory layout of Linux programs can be found in Konstantin Boldyshev's document, Startup state of a Linux/i386 ELF binary.
- A good overview of virtual memory in many different systems is available at Virtual Memory - Operating System Concepts.
- Several in-depth articles on Linux's virtual memory subsystem is available at Linux Kernel Documentation Project.
- Doug Lea has written up a description of his popular memory allocator at A Memory Allocator by Doug Lea.
- A paper on the 4.4 BSD memory allocator is available at Malloc(3) in modern Virtual Memory environments.

9.9 Review

9.9.1 Know the Concepts

- Describe the layout of memory when a Linux program starts.
- What is the heap?
- What is the current break?
- Which direction does the stack grow in?
- Which direction does the heap grow in?
- What happens when you access unmapped memory?
- How does the operating system prevent processes from writing over each other's memory?
- Describe the process that occurs if a piece of memory you are using is currently residing on disk?
- Why do you need an allocator?

9.9.2 Use the Concepts

- Modify the memory manager so that it calls `_allocate_init` automatically if it hasn't been initialized.
- Modify the memory manager so that if the requested size of memory is smaller than the region chosen, it will break up the region into multiple parts. Be sure to take into account the size of the new header record when you do this.
- Modify one of your programs that uses buffers to use the memory manager to get buffer memory rather than using the `.bss`.

9.9.3 Going Further

- Research *garbage collection*. What advantages and disadvantages does this have over the style of memory management used here?

- Research *reference counting*. What advantages and disadvantages does this have over the style of memory management used here?
- Change the name of the functions to `malloc` and `free`, and build them into a shared library. Use `LD_PRELOAD` to force them to be used as your memory manager instead of the default one. Add some `write` system calls to STDOUT to verify that your memory manager is being used instead of the default one.

10. Counting Like a Computer

10.1 Counting

10.1.1 Counting Like a Human

In many ways, computers count just like humans. So, before we start learning how computers count, let's take a deeper look at how we count.

How many fingers do you have? No, it's not a trick question. Humans (normally) have ten fingers. Why is that significant? Look at our numbering system. At what point does a one-digit number become a two-digit number? That's right, at ten. Humans count and do math using a base ten numbering system. Base ten means that we group everything in tens. Let's say we're counting sheep. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. Why did we all of a sudden now have two digits, and re-use the 1? That's because we're grouping our numbers by ten, and we have 1 group of ten sheep. Okay, let's go to the next number 11. That means we have 1 group of ten sheep, and 1 sheep left ungrouped. So we continue - 12, 13, 14, 15, 16, 17, 18, 19, 20. Now we have 2 groups of ten. 21 - 2 groups of ten, and 1 sheep ungrouped. 22 - 2 groups of ten, and 2 sheep ungrouped. So, let's say we keep counting, and get to 97, 98, 99, and 100. Look, it happened again! What happens at 100? We now have ten groups of ten. At 101 we have ten groups of ten, and 1 ungrouped sheep. So we can look at any number like this. If we counted 60879 sheep, that would mean that we had 6 groups of ten groups of ten groups of ten groups of ten, 0 groups of ten groups of ten groups of ten, 8 groups of ten groups of ten, 7 groups of ten, and 9 sheep left ungrouped.

So, is there anything significant about grouping things by ten? No! It's just that grouping by ten is how we've always done it, because we have ten fingers. We could have grouped at nine or at eleven (in which case we would have had to make up a new symbol). The only difference between the different groupings of numbers is that we have to re-learn our multiplication, addition, subtraction, and division tables for each grouping. The rules haven't changed, just the way we represent them. Also, some of our tricks that we learned don't always apply, either. For example, let's say we grouped by nine instead of ten. Moving the decimal point one digit to the right no longer multiplies by ten, it now multiplies by nine. In base nine, 500 is only nine times as large as 50.

10.1.2 Counting Like a Computer

The question is, how many fingers does the computer have to count with? The computer only has two fingers. So that means all of the groups are groups of two. So, let's count in binary - 0 (zero), 1 (one), 10 (two - one group of two), 11 (three - one group of two and one left over), 100 (four - two groups of two), 101 (five - two groups of two and one left over), 110 (six - two groups of two and one group of two), and so on. In base two, moving the decimal one digit to the right multiplies by two, and moving it to the left divides by two. Base two is also referred to as binary.

The nice thing about base two is that the basic math tables are very short. In base ten, the multiplication tables are ten columns wide, and ten columns tall. In base two, it is very simple:

Table of binary addition

+	0	1
0	0	1
1	1	10

Table of binary multiplication

```
+----------------+
| * ||  0  |  1  |
|================|
| 0 ||  0  |  0  |
|----+-----+-----|
| 1 ||  0  |  1  |
+----------------+
```

So, let's add the numbers 10010101 with 1100101:

```
   10010101
+   1100101
-----------
   11111010
```

Now, let's multiply them:

```
       10010101
    *   1100101
    -----------
       10010101
      00000000
     10010101
    00000000
   00000000
  10010101
 10010101
---------------
 11101011001001
```

10.1.3 Conversions Between Binary and Decimal

Let's learn how to convert numbers from binary (base two) to decimal (base ten). This is actually a rather simple process. If you remember, each digit stands for some grouping of two. So, we just need to add up what each digit represents, and we will have a decimal number. Take the binary number 10010101. To find out what it is in decimal, we take it apart like this:

```
 1    0    0    1    0    1    0    1
 |    |    |    |    |    |    |    |
 |    |    |    |    |    |    |    Individual units (2^0)
 |    |    |    |    |    |    0 groups of 2 (2^1)
 |    |    |    |    |    1 group of 4 (2^2)
 |    |    |    |    0 groups of 8 (2^3)
 |    |    |    1 group of 16 (2^4)
 |    |    0 groups of 32 (2^5)
 |    0 groups of 64 (2^6)
 1 group of 128 (2^7)
```

And then we add all of the pieces together, like this:

```
1*128 + 0*64 + 0*32 + 1*16 + 0*8 + 1*4 + 0*2 + 1*1
128 + 16 + 4 + 1 = 149
```

So 10010101 in binary is 149 in decimal. Let's look at 1100101. It can be written as:

```
1*64 + 1*32 + 0 * 16 + 0*8 + 1*4 + 0*2 + 1*1
64 + 32 + 4 + 1 = 101
```

So we see that 1100101 in binary is 101 in decimal. Let's look at one more number, 11101011001001. You can convert it to decimal by doing:

```
1*8192 + 1*4096 + 1*2048 + 0*1024 + 1*512 + 0*256
       + 1*128 + 1*64 + 0*32 + 0*16 + 1*8 + 0*4
       + 0*2 + 1*1

8192 + 4096 + 2048 + 512 + 128 + 64 + 8 + 1 = 15049
```

Now, if you've been paying attention, you have noticed that the numbers we just converted are the same ones we used to multiply with earlier. So, let's check our results: 101 * 149 = 15049. It worked!

Now let's look at going from decimal back to binary. In order to do the conversion, you have to *divide* the number into groups of two. So, let's say you had the number 17. If you divide it by two, you get 8 with 1 left over. So that means there are 8 groups of two, and 1 ungrouped. That means that the rightmost digit will be 1. Now, we have the rightmost digit figured out, and 8 groups of 2 left over. Now, let's see how many groups of two groups of two we have, by dividing 8 by 2. We get 4, with nothing left over. That means that all groups two can be further divided into more groups of two. So, we have 0 groups of only two. So the next digit to the left is 0. So, we divide 4 by 2 and get two, with 0 left over, so the next digit is 0. Then, we divide 2 by 2 and get 1, with 0 left over. So the next digit is 0. Finally, we divide 1 by 2 and get 0 with 1 left over, so the next digit to the left is 1. Now, there's nothing left, so we're done. So, the number we wound up with is 10001.

Previously, we converted to binary 11101011001001 to decimal 15049. Let's do the reverse to make sure that we did it right:

```
15049 / 2 = 7524    Remaining 1
7524 / 2 = 3762     Remaining 0
3762 / 2 = 1881     Remaining 0
1881 / 2 = 940      Remaining 1
940 / 2 = 470       Remaining 0
470 / 2 = 235       Remaining 0
235 / 2 = 117       Remaining 1
117 / 2 = 58        Remaining 1
58 / 2 = 29         Remaining 0
29 / 2 = 14         Remaining 1
14 / 2 = 7          Remaining 0
7 / 2 = 3           Remaining 1
3 / 2 = 1           Remaining 1
1 / 2 = 0           Remaining 1
```

Then, we put the remaining numbers back together, and we have the original number! Remember the first division remainder goes to the far right, so from the bottom up you have 11101011001001.

Each digit in a binary number is called a *bit*, which stands for *binary digit*. Remember, computers divide up their memory into storage locations called bytes. Each storage location on an x86 processor (and most others) is 8 bits long. Earlier we said that a byte can hold any number between 0 and 255. The reason for this is that the largest number you can fit into 8 bits is 255. You can see this for yourself if you convert binary 11111111 into decimal:

```
11111111 = (1 * 2^7) + (1 * 2^6) + (1 * 2^5) + (1 * 2^4)
          + (1 * 2^3)+ (1 * 2^2) + (1 * 2^1) + (1 * 2^0)

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255
```

The largest number that you can hold in 16 bits is 65,535. The largest number you can hold in 32 bits is 4,294,967,295 (4 billion). The largest number you can hold in 64 bits is 18,446,744,073,709,551,615. The largest number you can hold in 128 bits is 340,282,366,920,938,463,463,374,607,431,768,211,456. Anyway, you see the

picture. For x86 processors, most of the time you will deal with 4-byte numbers (32 bits), because that's the size of the registers.

10.2 Truth, Falsehood, and Binary Numbers

Now we've seen that the computer stores everything as sequences of 1's and 0's. Let's look at some other uses of this. What if, instead of looking at a sequence of bits as a number, we instead looked at it as a set of switches. For example, let's say there are four switches that control lighting in the house. We have a switch for outside lights, a switch for the hallway lights, a switch for the living room lights, and a switch for the bedroom lights. We could make a little table showing which of these were on and off, like so:

```
Outside  Hallway  Living Room  Bedroom
  On       Off        On         On
```

It's obvious from looking at this that all of the lights are on except the hallway ones. Now, instead of using the words "On" and "Off", let's use the numbers 1 and 0. 1 will represent on, and 0 will represent off. So, we could represent the same information as:

```
Outside  Hallway  Living Room  Bedroom
   1        0           1         1
```

Now, instead of having labels on the light switches, let's say we just memorized which position went with which switch. Then, the same information could be represented as:

```
   1        0           1         1
```

Or as:

```
1011
```

This is just one of many ways you can use the computers storage locations to represent more than just numbers. The computer's memory just sees numbers, but programmers can use these numbers to represent anything their imaginations can come up with. They just sometimes have to be creative when figuring out the best representation.

Not only can you do regular arithmetic with binary numbers, they also have a few operations of their own, called binary operations or logical operations. The standard binary operations are:

- AND.
- OR.
- NOT.
- XOR.

Before we look at examples, I'll describe them for you. AND takes two bits and returns one bit. AND will return a 1 only if both bits are 1, and a 0 otherwise. For example, 1 AND 1 is 1, but 1 AND 0 is 0, 0 AND 1 is 0, and 0 AND 0 is 0.

OR takes two bits and returns one bit. It will return 1 if either of the original bits is 1. For example, 1 OR 1 is 1, 1 OR 0 is one, 0 OR 1 is 1, but 0 OR 0 is 0.

NOT only takes one bit and returns its opposite. NOT 1 is 0 and NOT 0 is 1.

Finally, XOR is like OR, except it returns 0 if both bits are 1.

Computers can do these operations on whole registers at a time. For example, if a register has 10100010101010010101101100101010 and another one has 10001000010101010101010101111010, you can run any of these operations on the whole registers. For example, if we were to AND them, the computer will run from the first bit to the 32nd and run the AND operation on that bit in both registers. In this case:

```
10100010101010010101101100101010 AND
10001000010101010101010101111010
```

```
--------------------------------
10000000000000010101000100101010
```

You'll see that the resulting set of bits only has a one where *both* numbers had a one, and in every other position it has a zero. Let's look at what an OR looks like:

```
10100010101010010101101100101010 OR
10001000010101010101010101111010
--------------------------------
10101010111111010101111101111010
```

In this case, the resulting number has a 1 where either number has a 1 in the given position. Let's look at the NOT operation:

```
10100010101010010101101100101010 NOT
----------------------------------
01011101010101101010010011010101
```

This just reverses each digit. Finally, we have XOR, which is like an OR, except if *both* digits are 1, it returns 0.

```
10100010101010010101101100101010 XOR
10001000010101010101010101111010
--------------------------------
00101010111111000000111001010000
```

This is the same two numbers used in the OR operation, so you can compare how they work. Also, if you XOR a number with itself, you will always get 0, like this:

```
10100010101010010101101100101010 XOR
10100010101010010101101100101010
--------------------------------
00000000000000000000000000000000
```

These operations are useful for two reasons:

- The computer can do them extremely fast.
- You can use them to compare many truth values at the same time.

You may not have known that different instructions execute at different speeds. It's true, they do. And these operations are the fastest on most processors. For example, you saw that XORing a number with itself produces 0. Well, the XOR operation is faster than the loading operation, so many programmers use it to load a register with zero. For example, the code:

```
1    movl  $0, %eax
```

Is often replaced by:

```
1    xorl  %eax, %eax
```

We'll discuss speed more in Chapter 12. Optimization, but I want you to see how programmers often do tricky things, especially with these binary operators, to make things fast. Now let's look at how we can use these operators to manipulate true/false values. Earlier we discussed how binary numbers can be used to represent any number of things. Let's use binary numbers to represent what things my Dad and I like. First, let's look at the things I like:

```
Food: Yes
Heavy Metal Music: Yes
Wearing Dressy Clothes: No
Football: Yes
```

Now, let's look at what my Dad likes:

```
Food: Yes
Heavy Metal Music: No
Wearing Dressy Clothes: Yes
Football: Yes
```

Now, let's use a 1 to say yes we like something, and a 0 to say no we don't. Now we have:

```
Me
Food: 1
Heavy Metal Music: 1
Wearing Dressy Clothes: 0
Football: 1

Dad
Food: 1
Heavy Metal Music: 0
Wearing Dressy Clothes: 1
Football: 1
```

Now, if we just memorize which position each of these are in, we have:

```
Me
1101

Dad
1011
```

Now, let's see we want to get a list of things both my Dad and I like. You would use the AND operation. So:

```
1101 AND
1011
--------
1001
```

Which translates to:

```
Things we both like
Food: Yes
Heavy Metal Music: No
Wearing Dressy Clothes: No
Football: Yes
```

Remember, the computer has no idea what the ones and zeroes represent. That's your job and your program's job. If you wrote a program around this representation your program would at some point examine each bit and have code to tell the user what it's for (if you asked a computer what two people agreed on and it answered 1001, it wouldn't be very useful). Anyway, let's say we want to know the things that we disagree on. For that we would use XOR, because it will return 1 only if one or the other is 1, but not both. So:

```
1101 XOR
1011
--------
0110
```

And I'll let you translate that back out.

The previous operations: AND, OR, NOT, and XOR are called *boolean operators* because they were first studied by George Boole. So, if someone mentions boolean operators or boolean algebra, you now know what they are talking about.

In addition to the boolean operations, there are also two binary operators that aren't boolean, shift and rotate. Shifts and rotates each do what their name implies, and can do so to the right or the left. A left shift moves each digit of a binary number one space to the left, puts a zero in the ones spot, and chops off the furthest digit to the left. A left rotate does the same thing, but takes the furthest digit to the left and puts it in the ones spot. For example:

Shift left:

```
# Logic and Arithmetic
Binary:       1 0 0 1 0 1 1 1       = 151 | -105 | 0x97
               / / / / / / /
Result:       0 0 1 0 1 1 1 0 <- 0  =  46 |   46 | 0x2e
```

Shift right:

```
# Logic
Binary:       1 0 0 1 0 1 1 1       = 151 | -105 | 0x97
               \ \ \ \ \ \ \
Result:  0 -> 0 1 0 0 1 0 1 1       =  75 |   75 | 0x4b

# Arithmetic
Binary:       1 0 0 1 0 1 1 1       = 151 | -105 | 0x97
              |\ \ \ \ \ \ \
Result:       1 1 0 0 1 0 1 1       = 203 |  -53 | 0xcb
```

Rotate left:

```
Binary:     ->1 0 0 1 0 1 1 1       = 151 | -105 | 0x97
               / / / / / / /
Result:       0 0 1 0 1 1 1 1<-     =  47 |   47 | 0x2f
```

Rotate right:

```
Binary:       1 0 0 1 0 1 1 1<-     = 151 | -105 | 0x97
               \ \ \ \ \ \ \
Result:     ->1 1 0 0 1 0 1 1       = 203 |  -53 | 0xcb
```

Notice that if you rotate a number for every digit it has (i.e. - rotating a 32-bit number 32 times), you wind up with the same number you started with. However, if you *shift* a number for every digit you have, you wind up with 0. So, what are these shifts useful for? Well, if you have binary numbers representing things, you use shifts to peek at each individual value. Let's say, for instance, that we had my Dad's likes stored in a register (32 bits). It would look like this:

```
00000000000000000000000000001011
```

Now, as we said previously, this doesn't work as program output. So, in order to do output, we would need to do shifting and *masking*. Masking is the process of eliminating everything you don't want. In this case, for every value we are looking for, we will shift the number so that value is in the ones place, and then mask that digit so that it is all we see. Masking is accomplished by doing an AND with a number that has the bits we are interested in set to 1. For example, let's say we wanted to print out whether my Dad likes dressy clothes or not. That data is the second value from the right. So, we have to shift the number right 1 digit so it looks like this:

```
00000000000000000000000000000101
```

And then, we just want to look at that digit, so we mask it by ANDing it with `00000000000000000000000000000001`.

```
00000000000000000000000000000101 AND
00000000000000000000000000000001
```

```
----------------------------------
00000000000000000000000000000001
```

This will make the value of the register 1 if my Dad likes dressy clothes, and 0 if he doesn't. Then we can do a comparison to 1 and print the results. The code would look like this:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       .include "006-01-linux.s"      # Linux Definitions.
4
5       .section .text
6           .globl _start
7
8   _start:
9       movl   $0b00000000000000000000000000001011, %ebx
10
11                  # This is the shift operator. It stands
12                  # for Shift Right Long. This first
13                  # number is the number of positions to
14                  # shift, and the second is the register
15                  # to shift.
16      shrl  $1, %ebx
17
18                  # This does the masking.
19      andl  $0b00000000000000000000000000000001, %ebx
20
21                  # Check to see if the result is 1 or 0.
22      cmpl  $0b00000000000000000000000000000001, %ebx
23      je    _yes_he_likes_dressy_clothes
24      jmp   _no_he_doesnt_like_dressy_clothes
25
26  _yes_he_likes_dressy_clothes:
27  _no_he_doesnt_like_dressy_clothes:
28      movl   $SYS_EXIT, %eax
29      movl   $0, %ebx
30      int    $LINUX_SYSCALL
```

And then we would have two labels which printed something about whether or not he likes dressy clothes and then exits. The `0b` notation means that what follows is a binary number. In this case it wasn't needed, because 1 is the same in any numbering system, but I put it there for clarity. We also didn't need the 31 zeroes, but I put them in to make a point that the number you are using is 32 bits.

When a number represents a set of options for a function or system call, the individual true/false elements are called *flags*. Many system calls have numerous options that are all set in the same register using a mechanism like we've described. The `open` system call, for example, has as its second parameter a list of flags to tell the operating system how to open the file. Some of the flags include:

`O_WRONLY`: This flag is `0b00000000000000000000000000000001` in binary, or `01` in octal (or any number system for that matter). This says to open the file in write-only mode.

`O_RDWR`: This flag is `0b00000000000000000000000000000010` in binary, or `02` in octal. This says to open the file for both reading and writing.

`O_CREAT`: This flag is `0b00000000000000000000000001000000` in binary, or `0100` in octal. It means to create the file if it doesn't already exist.

`O_TRUNC`: This flag is `0b00000000000000000000001000000000` in binary, or `01000` in octal. It means to erase the contents of the file if the file already exists.

O_APPEND:
This flag is `0b00000000000000000000010000000000` in binary, or `02000` in octal. It means to start writing at the end of the file rather than at the beginning.

To use these flags, you simply OR them together in the combination that you want. For example, to open a file in write-only mode, and have it create the file if it doesn't exist, I would use `O_WRONLY` (01) and `O_CREAT` (0100). OR'd together, I would have 0101.

Note that if you don't set either `O_WRONLY` or `O_RDWR`, then the file is automatically opened in read-only mode (`O_RDONLY`, except that it isn't really a flag since it's zero).

Many functions and system calls use flags for options, as it allows a single word to hold up to 32 possible options if each option is represented by a single bit.

10.3 The Program Status Register

We've seen how bits on a register can be used to give the answers of yes/no and true/false statements. On your computer, there is a register called the *program status register*. This register holds a lot of information about what happens in a computation. For example, have you ever wondered what would happen if you added two numbers and the result was larger than would fit in a register? The program status register has a flag called the carry flag. You can test it to see if the last computation overflowed the register. There are flags for a number of different statuses. In fact, when you do a compare (`cmpl`) instruction, the result is stored in this register. The conditional jump instructions (`jge`, `jne`, etc) use these results to tell whether or not they should jump. `jmp`, the unconditional jump, doesn't care what is in the status register, since it is unconditional.

Let's say you needed to store a number larger than 32 bits. So, let's say the number is 2 registers wide, or 64 bits. How could you handle this? If you wanted to add two 64-bit numbers, you would add the least significant registers first. Then, if you detected a carry, you could add 1 to the most significant register. In fact, this is probably the way you learned to do decimal addition. If the result in one column is more than 9, you simply carried the number to the next most significant column. If you added 65 and 37, first you add 7 and 4 to get 12. You keep the 2 in the right column, and carry the one to the next column. There you add 6, 3, and the 1 you carried. This results in 10. So, you keep the zero in that column and carry the one to the next most significant column, which is empty, so you just put the one there. Luckily, 32 bits is usually big enough to hold the numbers we use regularly.

Additional program status register flags are examined in Appendix B. Common x86 Instructions.

10.4 Other Numbering Systems

What we have studied so far only applies to positive integers. However, real-world numbers are not always positive integers. Negative numbers and numbers with decimals are also used.

10.4.1 Floating-point Numbers

So far, the only numbers we've dealt with are integers - numbers with no decimal point. Computers have a general problem with numbers with decimal points, because computers can only store fixed-size, finite values. Decimal numbers can be any length, including infinite length (think of a repeating decimal, like the result of 1 / 3).

The way a computer handles decimals is by storing them at a fixed precision (number of significant bits). A computer stores decimal numbers in two parts - the *exponent* and the *mantissa*. The mantissa contains the actual digits that will be used, and the exponent is what magnitude the number is. For example, 12345.2 can be represented as 1.23452 * 10^4. The mantissa is 1.23452 and the exponent is 4 with a base of 10. Computers, however, use a base of 2. All numbers are stored as X.XXXXX * 2^XXXX. The number 1, for example, is stored as 1.00000 * 2^0. Separating the mantissa and the exponent into two different values is called a *floating point* representation, because the position of the significant digits with respect to the decimal point can vary based on the exponent.

Now, the mantissa and the exponent are only so long, which leads to some interesting problems. For example, when a computer stores an integer, if you add 1 to it, the resulting number is one larger. This does not necessarily happen with floating point numbers. If the number is sufficiently big, adding 1 to it might not even register in the mantissa (remember, both parts are only so long). This affects several things, especially order

of operations. If you add 1.0 to a given floating point number, it might not even affect the number if it is large enough. For example, on x86 platforms, a four-byte floating-point number, although it can represent very large numbers, cannot have 1.0 added to it past 16777216.0, because it is no longer significant. The number no longer changes when 1.0 is added to it. So, if there is a multiplication followed by an addition it may give a different result than if the addition is performed first.

You should note that it takes most computers a lot longer to do floating-point arithmetic than it does integer arithmetic. So, for programs that really need speed, integers are mostly used.

Short floating-point:

- The first bit is the sign bit: 0 for positive and 1 for negative.
- The next 8 bits are the exponent. Follow this formula `2^(x - 127) = exponent`.
- The last 23 bits are the fraction of the mantissa. For normal numbers, the mantissa is `1.fraction` in binary: the leading 1 is always there, so it is not stored.

Example:

```
0xC3478100
Binary:      1 10000110 10001111000000100000000
Sign bit:    1 -> -1
Exponent:    10000110 -> 134 -> 2^(134 - 127) -> 128
Mantissa:    1.10001111000000100000000 -> 1.558624267578125
Value:       -1 * 128 * 1.558624267578125
             = -199.50390625

0x43478100
Binary:      0 10000110 10001111000000100000000
Sign bit:    0 -> 1
Exponent:    10000110 -> 134 -> 2^(134 - 127) -> 128
Mantissa:    1.10001111000000100000000 -> 1.558624267578125
Value:       1 * 128 * 1.558624267578125
             = 199.50390625
```

References to understand in deep how the computer handle the floating points.

- Fixed Point and Floating Point.
- Floating Point Tutorial.
- IEEE Standard for Floating-Point Arithmetic (IEEE 754).
- Single-precision floating-point format.

For more information on using floating point numbers in assembly language, see:

- Floating Point Assembly Language.
- Floating-Point Instruction Set.

10.4.2 Negative Numbers

How would you think that negative numbers on a computer might be represented? One thought might be to use the first digit of a number as the sign, so `00000000000000000000000000000001` would represent the number 1, and `10000000000000000000000000000001` would represent −1. This makes a lot of sense, and in fact some old processors work this way. However, it has some problems. First of all, it takes a lot more circuitry to add and subtract signed numbers represented this way. Even more problematic, this representation has a problem with the number 0. In this system, you could have both a negative and a positive 0. This leads to a lot of questions, like "should negative zero be equal to positive zero?", and "What should the sign of zero be in various circumstances?".

These problems were overcome by using a representation of negative numbers called *two's complement* representation. To get the negative representation of a number in two's complement form, you must perform the following steps:

1. Perform a NOT operation on the number.
2. Add one to the resulting number.

So, to get the negative of `00000000000000000000000000000001`, you would first do a NOT operation, which gives `11111111111111111111111111111110`, and then add one, giving `11111111111111111111111111111111`. To get negative two, first take `00000000000000000000000000000010`. The NOT of that number is `11111111111111111111111111111101`. Adding one gives `11111111111111111111111111111110`. With this representation, you can add numbers just as if they were positive, and come out with the right answers. For example, if you add one plus negative one in binary, you will notice that all of the numbers flip to zero. Also, the first digit still carries the sign bit, making it simple to determine whether or not the number is positive or negative. Negative numbers will always have a `1` in the leftmost bit. This also changes which numbers are valid for a given number of bits. With signed numbers, the possible magnitude of the values is split to allow for both positive and negative numbers. For example, a byte can normally have values up to 255. A signed byte, however, can store values from −128 to 127.

One thing to note about the two's complement representation of signed numbers is that, unlike unsigned quantities, if you increase the number of bits, you can't just add zeroes to the left of the number. For example, let's say we are dealing with four-bit quantities and we had the number −3, `1101`. If we were to extend this into an eight-bit register, we could not represent it as `00001101` as this would represent 13, not −3. When you increase the size of a signed quantity in two's complement representation, you have to perform *sign extension*. Sign extension means that you have to pad the left-hand side of the quantity with whatever digit is in the sign digit when you add bits. So, if we extend a negative number by 4 digits, we should fill the new digits with a 1. If we extend a positive number by 4 digits, we should fill the new digits with a 0. So, the extension of −3 from four to eight bits will yield `11111101`.

The x86 processor has different forms of several instructions depending on whether they expect the quantities they operate on to be signed or unsigned. These are listed in Appendix B. Common x86 Instructions. For example, the x86 processor has both a sign-preserving shift-right, `sarl`, and a shift-right which does not preserve the sign bit, `shrl`.

10.5 Octal and Hexadecimal Numbers

The numbering systems discussed so far have been decimal and binary. However, two others are used common in computing - octal and hexadecimal. In fact, they are probably written more often than binary. Octal is a representation that only uses the numbers 0 through 7. So the octal number 10 is actually 8 in decimal because it is one group of eight. Octal 121 is decimal 81 (one group of 64 (8^2), two groups of 8, and one left over). What makes octal nice is that every 3 binary digits make one octal digit (there is no such grouping of binary digits into decimal). So 0 is 000, 1 is 001, 2 is 010, 3 is 011, 4 is 100, 5 is 101, 6 is 110, and 7 is 111.

Permissions in Linux are done using octal. This is because Linux permissions are based on the ability to read, write and execute. The first bit is the read permission, the second bit is the write permission, and the third bit is the execute permission. So, 0 (000) gives no permissions, 6 (110) gives read and write permission, and 5 (101) gives read and execute permissions. These numbers are then used for the three different sets of permissions - the owner, the group, and everyone else. The number 0644 means read and write for the first permission set, and read-only for the second and third set. The first permission set is for the owner of the file. The third permission set is for the group owner of the file. The last permission set is for everyone else. So, `0751` means that the owner of the file can read, write, and execute the file, the group members can read and execute the file, and everyone else can only execute the file.

Anyway, as you can see, octal is used to group bits (binary digits) into threes. The way the assembler knows that a number is octal is because octal numbers are prefixed with a zero. For example 010 means 10 in octal, which is 8 in decimal. If you just write 10 that means 10 in decimal. The beginning zero is what differentiates the two. So, *be careful not to put any leading zeroes in front of decimal numbers, or they will be interpreted as octal numbers*!

Hexadecimal numbers (also called just "hex") use the numbers 1-15 for each digit. however, since 10-15 don't have their own numbers, hexadecimal uses the letters `a` through `f` to represent them. For example, the letter `a` represents 10, the letter `b` represents 11, and so on. 10 in hexadecimal is 16 in decimal. In octal, each digit represented three bits. In hexadecimal, each digit represents four bits. Every two digits is a full byte, and eight digits is a 32-bit word. So you see, it is considerably easier to write a hexadecimal number than it is to write a binary number, because it's only a quarter as many digits. The most important number to remember in hexadecimal is `f`, which means that all bits are set. So, if I want to set all of the bits of a register to 1, I can just do:

```
movl  $0xFFFFFFFF, %eax
```

Which is considerably easier and less error-prone than writing:

```
movl  $0b11111111111111111111111111111111, %eax
```

Note also that hexadecimal numbers are prefixed with `0x`. So, when we do

```
int   $0x80
```

We are calling interrupt number 128 (8 groups of 16), or interrupt number `0b00000000000000000000000010000000`.

Hexadecimal and octal numbers take some getting used to, but they are heavily used in computer programming. It might be worthwhile to make up some numbers in hex and try to convert them back and forth to binary, decimal, and octal.

10.6 Order of Bytes in a Word

One thing that confuses many people when dealing with bits and bytes on a low level is that, when bytes are written from registers to memory, their bytes are written out least-significant-portion-first.[49] What most people expect is that if they have a word in a register, say `0x5d 23 ef ee` (the spacing is so you can see where the bytes are), the bytes will be written to memory in that order. However, on x86 processors, the bytes are actually written in reverse order. In memory the bytes would be `0xee ef 23 5d` on x86 processors. The bytes are written in reverse order from what they would appear conceptually, but the bits within the bytes are ordered normally.

Not all processors behave this way. The x86 processor is a *little-endian* processor, which means that it stores the "little end", or least-significant byte of its words first.

[49] *Significance* in this context is referring to which digit they represent. For example, in the number 294, the digit 2 is the most significant because it represents the hundreds place, 9 is the next most significant, and 4 is the least significant.

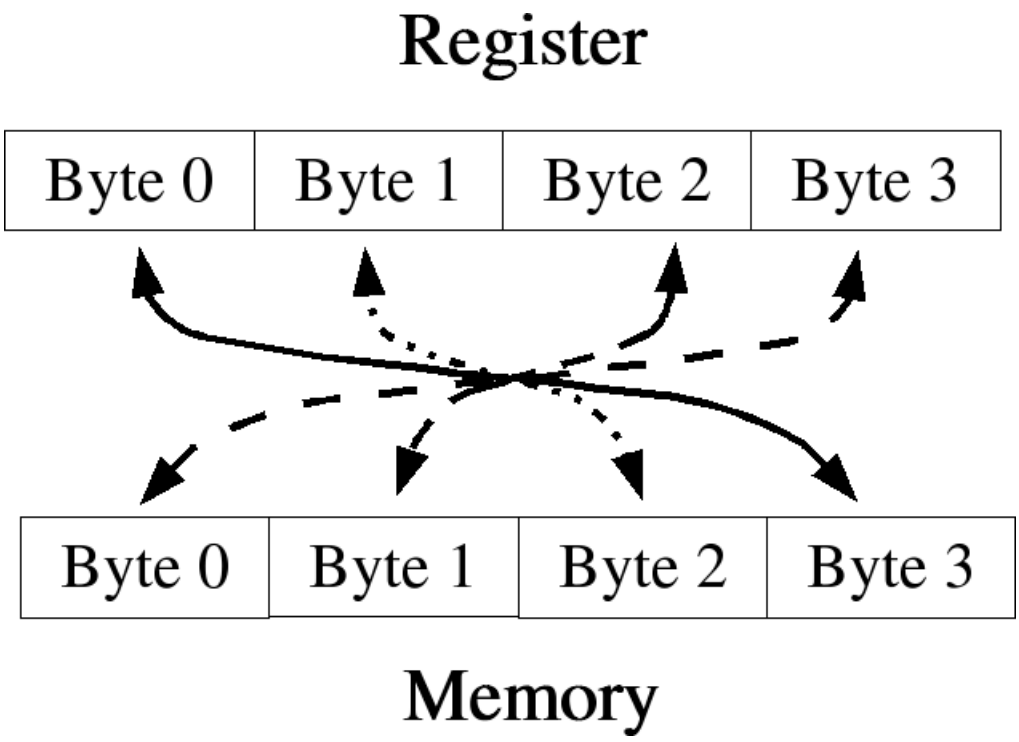

Figure 10.1: *Register-to-memory transfers on little-endian systems*

Other processors are *big-endian* processors, which means that they store the "big end", or most significant byte, of their words first, the way we would naturally read a number.

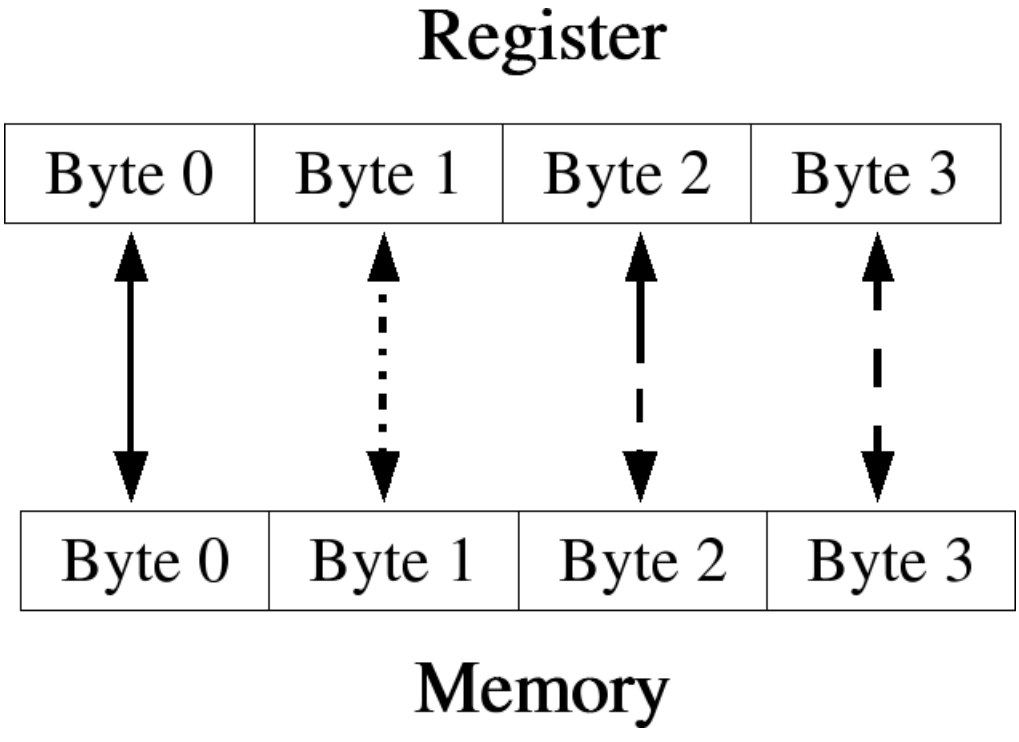

Figure 10.2: *Register-to-memory transfers on big-endian systems*

This difference is not normally a problem (although it has sparked many technical controversies throughout the years). Because the bytes are reversed again (or not, if it is a big-endian processor) when being read back into a register, the programmer usually never notices what order the bytes are in. The byte-switching magic happens automatically behind the scenes during register-to-memory transfers. However, the byte order can cause problems in several instances:

- If you try to read in several bytes at a time using `movl` but deal with them on a byte-by-byte basis using the least significant byte (i.e. - by using *%al* and/or shifting of the register), this will be in a different order than they appear in memory.
- If you read or write files written for different architectures, you may have to account for whatever order they write their bytes in.
- If you read or write to network sockets, you may have to account for a different byte order in the protocol.

As long as you are aware of the issue, it usually isn't a big deal. For more in-depth look at byte order issues, you should read DAV's Endian FAQ, especially the article "On Holy Wars and a Plea for Peace" by Daniel Cohen.

10.7 Converting Numbers for Display

So far, we have been unable to display any number stored to the user, except by the extremely limited means of passing it through exit codes. In this section, we will discuss converting positive numbers into strings for display.

The function will be called `_integer2string`, and it will take two parameters - an integer to convert and a string buffer filled with null characters (zeroes). The buffer will be assumed to be big enough to store the entire number as a string (at least 11 characters long, to include a trailing null character).

Remember that the way that we see numbers is in base 10. Therefore, to access the individual decimal digits of a number, we need to be dividing by 10 and displaying the remainder for each digit. Therefore, the process will look like this:

- Divide the number by ten.
- The remainder is the current digit. Convert it to a character and store it.
- We are finished if the quotient is zero.
- Otherwise, take the quotient and the next location in the buffer and repeat the process.

The only problem is that since this process deals with the one's place first, it will leave the number backwards. Therefore, we will have to finish by reversing the characters. We will do this by storing the characters on the stack as we compute them. This way, as we pop them back off to fill in the buffer, it will be in the reverse order that we pushed them on.

The code for the function should be put in a file called `010-02-integer-to-string.s` and should be entered as follows:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Convert an integer number to a decimal string
5       #     for display.
6       #
7       # INPUT:
8       #     A buffer large enough to hold the largest
9       #     possible number an integer to convert.
10      #
11      # OUTPUT:
12      #     The buffer will be overwritten with the
13      #     decimal string.
```

```
14      #
15      # Variables:
16      #     %ecx will hold the count of characters
17      #     processed.
18      #     %eax will hold the current value.
19      #     %edi will hold the base (10).
20      #
21          .equ ST_VALUE,   8
22          .equ ST_BUFFER,  12
23
24          .globl _integer2string
25          .type  _integer2string,  @function
26
27  _integer2string:
28      pushl %ebp              # Normal function beginning
29      movl  %esp, %ebp
30
31      movl  $0, %ecx          # Current character count.
32
33                              # Move the value into
34                              # position.
35      movl  ST_VALUE(%ebp), %eax
36
37      movl  $10, %edi         # When we divide by 10, the
38                              # 10 must be in a register
39                              # or memory location.
40
41  _conversion_loop:
42      # Division is actually performed on the combined
43      # %edx:%eax register, so first clear out %edx.
44      #
45      movl  $0, %edx
46
47      # Divide %edx:%eax (which are implied) by 10. Store
48      # the quotient in %eax and the remainder in %edx
49      # (both of which are implied).
50      #
51      divl  %edi
52
53      # Quotient is in the right place.  %edx has the
54      # remainder, which now needs to be converted into a
55      # number.  So, %edx has a number that is 0 through
56      # 9.  You could also interpret this as an index on
57      # the ASCII table starting from the character '0'.
58      # The ascii code for '0' plus zero is still the
59      # ascii code for '0'.  The ascii code for '0' plus
60      # 1 is the ascii code for the character '1'.
61      # Therefore, the following instruction will give us
62      # the character for the number stored in %edx.
63      #
64      addl  $'0', %edx
65
66      # Now we will take this value and push it on the
```

```
67      # stack.  This way, when we are done, we can just
68      # pop off the characters one-by-one and they will
69      # be in the right order.  Note that we are pushing
70      # the whole register, but we only need the byte in
71      # %dl (the last byte of the %edx register) for the
72      # character.
73      #
74      pushl %edx
75
76      incl  %ecx              # Increment the digit count
77
78      cmpl  $0, %eax          # Check to see if %eax is
79                              # zero yet,
80      je    _end_conversion_loop  # go to next step if so
81                              # %eax already has its new
82                              # value.
83
84      jmp _conversion_loop
85
86  _end_conversion_loop:
87      # The string is now on the stack, if we pop it off
88      # a character at a time we can copy it into the
89      # buffer and be done.
90      #
91      movl  ST_BUFFER(%ebp), %edx     # Get the pointer
92                                      # to the buffer in
93                                      # %edx.
94
95  _copy_reversing_loop:
96      # We pushed a whole register, but we only need the
97      # last byte.  So we are going to pop off to the
98      # entire %eax register, but then only move the
99      # small part (%al) into the character string.
100     #
101     popl  %eax
102     movb  %al, (%edx)
103
104     decl  %ecx              # Decreasing %ecx so we
105                             # know when we are finished
106
107     incl  %edx              # Increasing %edx so that
108                             # it will be pointing to
109                             # the next byte.
110
111     cmpl  $0, %ecx          # Check to see if we are
112                             # finished.
113     je    _end_copy_reversing_loop  # If so, jump to
114                                     # the end of the
115                                     # function.
116     jmp   _copy_reversing_loop      # Otherwise, repeat
117                                     # the loop.
118
119 _end_copy_reversing_loop:
```

```
120     movb  $0, (%edx)        # Done copying.  Now write
121                             # a null byte and return.
122
123     movl  %ebp, %esp
124     popl  %ebp
125     ret
```

To show this used in a full program, use the following code, along with the `_count_chars` and `_write_newline` functions written about in previous chapters. The code should be in a file called `010-02-conversion-program.s`.

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       .include "006-01-linux.s"      # Linux Definitions.
4
5       .section .data          # This is where it will be
6           tmp_buffer:         # stored.
7               .ascii "\0\0\0\0\0\0\0\0\0\0\0"
8
9       .section .text
10          .globl _start
11
12  _start:
13      movl  %esp, %ebp
14
15      pushl $tmp_buffer       # Storage for the result.
16      pushl $824              # Number to convert.
17      call  _integer2string
18      addl  $8, %esp
19
20      pushl $tmp_buffer       # Get the character count
21                              # for our system call.
22      call  _count_chars
23      addl  $4, %esp
24
25      movl  %eax, %edx        # The count goes in %edx
26                              # for SYS_WRITE.
27
28      movl  $SYS_WRITE, %eax  # Make the system call.
29      movl  $STDOUT, %ebx
30      movl  $tmp_buffer, %ecx
31
32      int   $LINUX_SYSCALL
33
34      pushl $STDOUT           # Write a carriage return.
35      call  _write_newline
36
37      movl  $SYS_EXIT, %eax   # Exit.
38      movl  $0, %ebx
39      int   $LINUX_SYSCALL
```

To build the program, issue the following commands:

```
as -o 010-02-integer-to-number.o   --32 \
                                   --gstabs+ \
```

```
                                  010-02-integer-to-string.s

as -o 006-01-count-chars.o        --32 \
                                  --gstabs+ \
                                  006-01-count-chars.s

as -o 006-01-write-newline.o      --32 \
                                  --gstabs+ \
                                  006-01-write-newline.s

as -o 010-02-conversion-program.o --32 \
                                  --gstabs+ \
                                  010-02-conversion-program.s

ld -o 010-02-conversion-program   -m elf_i386 \
                                  006-01-count-chars.o \
                                  006-01-write-newline.o \
                                  010-02-conversion-program.o \
                                  010-02-integer-to-number.o
```

To run just type `./010-02-conversion-program` and the output should say `824`.

10.8 Review

10.8.1 Know the Concepts

- Convert the decimal number 5,294 to binary.
- What number does 0x0234aeff represent? Specify in binary, octal, and decimal.
- Add the binary numbers 10111001 and 101011.
- Multiply the binary numbers 1100 1010110.
- Convert the results of the previous two problems into decimal.
- Describe how AND, OR, NOT, and XOR work.
- What is masking for?
- What number would you use for the flags of the `open` system call if you wanted to open the file for writing, and create the file if it doesn't exist?
- How would you represent −55 in a 32-bit register?
- Sign-extend the previous quantity into a 64-bit register.
- Describe the difference between little-endian and big-endian storage of words in memory.

10.8.2 Use the Concepts

- Go back to previous programs that returned numeric results through the exit status code, and rewrite them to print out the results instead using our integer to string conversion function.
- Modify the `_integer2string` code to return results in octal rather than decimal.
- Modify the `_integer2string` code so that the conversion base is a parameter rather than hardcoded.
- Write a function called `_is_negative` that takes a single integer as a parameter and returns 1 if the parameter is negative, and 0 if the parameter is positive.

10.8.3 Going Further

- Modify the `_integer2string` code so that the conversion base can be greater than 10 (this requires you to use letters for numbers past 9).
- Create a function that does the reverse of `_integer2string` called `_number2integer` which takes a character string and converts it to a register-sized integer. Test it by running that integer back through the `_integer2string` function and displaying the results.
- Write a program that stores likes and dislikes into a single machine word, and then compares two sets of likes and dislikes for commonalities.
- Write a program that reads a string of characters from STDIN and converts them to a number.

11. High-Level Languages

In this chapter we will begin to look at our first "real-world" programming language. Assembly language is the language used at the machine's level, but most people find coding in assembly language too cumbersome for everyday use. Many computer languages have been invented to make the programming task easier. Knowing a wide variety of languages is useful for many reasons, including:

- Different languages are based on different concepts, which will help you to learn different and better programming methods and ideas.
- Different languages are good for different types of projects.
- Different companies have different standard languages, so knowing more languages makes your skills more marketable.
- The more languages you know, the easier it is to pick up new ones.

As a programmer, you will often have to pick up new languages. Professional programmers can usually pick up a new language with about a weeks worth of study and practice. Languages are simply tools, and learning to use a new tool should not be something a programmer flinches at. In fact, if you do computer consulting you will often have to learn new languages on the spot in order to keep yourself employed. It will often be your customer, not you, who decides what language is used. This chapter will introduce you to a few of the languages available to you. I encourage you to explore as many languages as you are interested in. I personally try to learn a new language every few months.

11.1 Compiled and Interpreted Languages

Many languages are *compiled* languages. When you write assembly language, each instruction you write is translated into exactly one machine instruction for processing. With compilers, a statement can translate into one or hundreds of machine instructions. In fact, depending on how advanced your compiler is, it might even restructure parts of your code to make it faster. In assembly language what you write is what you get.

There are also languages that are *interpreted* languages. These languages require that the user run a program called an *interpreter* that in turn runs the given program. These are usually slower than compiled programs, since the interpreter has to read and interpret the code as it goes along. However, in well-made interpreters, this time can be fairly negligible. There is also a class of hybrid languages which partially compile a program before execution into byte-codes. This is done because the interpreter can read the byte-codes much faster than it can read the regular language.

There are many reasons to choose one or the other. Compiled programs are nice, because you don't have to already have an interpreter installed in the user's machine. You have to have a compiler for the language, but the users of your program don't. In an interpreted language, you have to be sure that the user has an interpreter installed for your program, and that the computer knows which interpreter to run your program with. However, interpreted languages tend to be more flexible, while compiled languages are more rigid.

Language choice is usually driven by available tools and support for programming methods rather than by whether a language is compiled or interpreted. In fact many languages have options for either one.

High-level languages, whether compiled or interpreted, are oriented around you, the programmer, instead of around the machine. This opens them up to a wide variety of features, which can include the following:

- Being able to group multiple operations into a single expression.
- Being able to use "big values" - values that are much more conceptual than the 4-byte words that computers normally deal with (for example, being able to view text strings as a single value rather than as a string of bytes).

- Having access to better flow control constructs than just jumps.
- Having a compiler to check types of value assignments and other assertions.
- Having memory handled automatically.
- Being able to work in a language that resembles the problem domain rather than the computer hardware.

So why does one choose one language over another? For example, many choose Perl because it has a vast library of functions for handling just about every protocol or type of data on the planet. Python, however, has a cleaner syntax and often lends itself to more straightforward solutions. Its cross-platform GUI tools are also excellent. PHP makes writing web applications simple. Common LISP has more power and features than any other environment for those willing to learn it. Scheme is the model of simplicity and power combined together. C is easy to interface with other languages.

Each language is different, and the more languages you know the better programmer you will be. Knowing the concepts of different languages will help you in all programming, because you can match the programming language to the problem better, and you have a larger set of tools to work with. Even if certain features aren't directly supported in the language you are using, often they can be simulated. However, if you don't have a broad experience with languages, you won't know of all the possibilities you have to choose from.

11.2 Your First C Program

Here is your first C program, which prints "Hello world" to the screen and exits. Type it in, and give it the name `011-01-hello-world.c`:

```
1   #include <stdio.h>
2
3   /* PURPOSE:
4    *     This program is mean to show a basic C program.
5    *     All it does is print "Hello World!" to the
6    *     screen and exit.
7    * /
8
9   /* Main Program */
10  int main(int argc, char **argv)
11  {
12      /* Print our string to standard output */
13      puts("Hello World!\n");
14
15      /* Exit with status 0 */
16      return 0;
17  }
```

As you can see, it's a pretty simple program. To compile it, run the command:

```
gcc -o 011-01-hello-world-c  011-01-hello-world.c
```

To run the program, do:

```
./011-01-hello-world-c
```

Let's look at how this program was put together.

Comments in C are started with `/*` and ended with `*/`. Comments can span multiple lines, but many people prefer to start and end comments on the same line so they don't get confused.

`#include <stdio.h>` is the first part of the program. This is a *preprocessor directive*. C compiling is split into two stages - the preprocessor and the main compiler. This directive tells the preprocessor to look for the file `stdio.h` and paste it into your program. The preprocessor is responsible for putting together the text of the program. This includes sticking different files together, running macros on your program text, etc. After the text is put together, the preprocessor is done and the main compiler goes to work.

Now, everything in `stdio.h` is now in your program just as if you typed it there yourself. The angle brackets around the filename tell the compiler to look in its standard paths for the file (`/usr/include` and `/usr/local/include`, usually). If it was in quotes, like `#include "stdio.h"` it would look in the current directory for the file. Anyway, `stdio.h` contains the declarations for the standard input and output functions and variables. These declarations tell the compiler what functions are available for input and output. The next few lines are simply comments about the program.

Then there is the line `int main(int argc, char **argv)`. This is the start of a function. C Functions are declared with their name, arguments and return type. This declaration says that the function's name is `main`, it returns an `int` (integer - 4 bytes long on the x86 platform), and has two arguments - an `int` called `argc` and a `char **` called `argv`. You don't have to worry about where the arguments are positioned on the stack - the C compiler takes care of that for you. You also don't have to worry about loading values into and out of registers because the compiler takes care of that, too.

The `main` function is a special function in the C language - it is the start of all C programs (much like `_start` in our assembly-language programs). It always takes two parameters. The first parameter is the number of arguments given to this command, and the second parameter is a list of the arguments that were given.

The next line is a function call. In assembly language, you had to push the arguments of a function onto the stack, and then call the function. C takes care of this complexity for you. You simply have to call the function with the parameters in parentheses. In this case, we call the function `puts`, with a single parameter. This parameter is the character string we want to print. We just have to type in the string in quotations, and the compiler takes care of defining storage and moving the pointers to that storage onto the stack before calling the function. As you can see, it's a lot less work.

Finally our function returns the number `0`. In assembly language, we stored our return value in *%eax*, but in C we just use the `return` command and it takes care of that for us. The return value of the `main` function is what is used as the exit code for the program.

As you can see, using high-level languages makes life much easier. It also allows our programs to run on multiple platforms more easily. In assembly language, your program is tied to both the operating system and the hardware platform, while in compiled and interpreted languages the same code can usually run on multiple operating systems and hardware platforms. For example, this program can be built and executed on x86 hardware running Linux®, Windows®, UNIX®, or most other operating systems. In addition, it can also run on Macintosh hardware running a number of operating systems.

Additional information on the C programming language can be found in Appendix E. C Idioms in Assembly Language.

11.3 Perl

Perl is an interpreted language, existing mostly on Linux and UNIX-based platforms. It actually runs on almost all platforms, but you find it most often on Linux and UNIX-based ones. Anyway, here is the Perl version of the program, which should be typed into a file named `011-01-hello-world.pl`:

```
1    #!/usr/bin/perl
2
3    print("Hello world!\n");
```

Since Perl is interpreted, you don't need to compile or link it. Just run in with the following command:

```
perl 011-01-hello-world.pl
```

As you can see, the Perl version is even shorter than the C version. With Perl you don't have to declare any functions or program entry points. You can just start typing commands and the interpreter will run them as it comes to them. In fact this program only has two lines of code, one of which is optional.

The first, optional line is used for UNIX machines to tell which interpreter to use to run the program. The `#!` tells the computer that this is an interpreted program, and the `/usr/bin/perl` tells the computer to use the program `/usr/bin/perl` to interpret the program. However, since we ran the program by typing in `perl 011-01-hello-world.pl`, we had already specified that we were using the perl interpreter.

The next line calls a Perl builtin function, print. This has one parameter, the string to print. The program doesn't have an explicit return statement - it knows to return simply because it runs off the end of the file.

It also knows to return 0 because there were no errors while it ran. You can see that interpreted languages are often focused on letting you get working code as quickly as possible, without having to do a lot of extra legwork.

One thing about Perl that isn't so evident from this example is that Perl treats strings as a single value. In assembly language, we had to program according to the computer's memory architecture, which meant that strings had to be treated as a sequence of multiple values, with a pointer to the first letter. Perl pretends that strings can be stored directly as values, and thus hides the complication of manipulating them for you. In fact, one of Perl's main strengths is its ability and speed at manipulating text.

11.4 Python

The Python version of the program looks almost exactly like the Perl one. However, Python is really a very different language than Perl, even if it doesn't seem so from this trivial example. Type the program into a file named `011-01-hello-world.py`. The program follows:

```
1    #!/usr/bin/python
2
3    print ("Hello World")
```

Since Python is interpreted, you don't need to compile or link it. Just run in with the following command:

```
python 011-01-hello-world.py
```

You should be able to tell what the different lines of the program do.

11.5 Review

11.5.1 Know the Concepts

- What is the difference between an interpreted language and a compiled language?
- What reasons might cause you to need to learn a new programming language?

11.5.2 Use the Concepts

- Learn the basic syntax of a new programming language. Re-code one of the programs in this book in that language.
- In the program you wrote in the question above, what specific things were automated in the programming language you chose?
- Modify your program so that it runs 10,000 times in a row, both in assembly language and in your new language. Then run the `time` command to see which is faster. Which does come out ahead? Why do you think that is?
- How does the programming language's input/output methods differ from that of the Linux system calls?

11.5.3 Going Further

- Having seen languages which have such brevity as Perl, why do you think this book started you with a language as verbose as assembly language?
- How do you think high level languages have affected the process of programming?
- Why do you think so many languages exist?
- Learn two new high level languages. How do they differ from each other? How are they similar? What approach to problem-solving does each take?

12. Optimization

Optimization is the process of making your application run more effectively. You can optimize for many things - speed, memory space usage, disk space usage, etc. This chapter, however, focuses on speed optimization.

12.1 When to Optimize

It is better to not optimize at all than to optimize too soon. When you optimize, your code generally becomes less clear, because it becomes more complex. Readers of your code will have more trouble discovering why you did what you did which will increase the cost of maintenance of your project. Even when you know how and why your program runs the way it does, optimized code is harder to debug and extend. It slows the development process down considerably, both because of the time it takes to optimize the code, and the time it takes to modify your optimized code.

Compounding this problem is that you don't even know beforehand where the speed issues in your program will be. Even experienced programmers have trouble predicting which parts of the program will be the bottlenecks which need optimization, so you will probably end up wasting your time optimizing the wrong parts. Where to Optimize will discuss how to find the parts of your program that need optimization.

While you develop your program, you need to have the following priorities:

- Everything is documented.
- Everything works as documented.
- The code is written in a modular, easily modifiable form.

Documentation is essential, especially when working in groups. The proper functioning of the program is essential. You'll notice application speed was not anywhere on that list. Optimization is not necessary during early development for the following reasons:

- Minor speed problems can be usually solved through hardware, which is often much cheaper than a programmer's time.
- Your application will change dramatically as you revise it, therefore wasting most of your efforts to optimize it.[50]
- Speed problems are usually localized in a few places in your code - finding these is difficult before you have most of the program finished.

Therefore, the time to optimize is toward the end of development, when you have determined that your correct code actually has performance problems.

In a web-based e-commerce project I was involved in, I focused entirely on correctness. This was much to the dismay of my colleagues, who were worried about the fact that each page took twelve seconds to process before it ever started loading (most web pages process in under a second). However, I was determined to make it the right way first, and put optimization as a last priority. When the code was finally correct after 3 months of work, it took only three days to find and eliminate the bottlenecks, bringing the average processing time under a quarter of a second. By focusing on the correct order, I was able to finish a project that was both correct and efficient.

[50] Many new projects often have a first code base which is completely rewritten as developers learn more about the problem they are trying to solve. Any optimization done on the first codebase is completely wasted.

12.2 Where to Optimize

Once you have determined that you have a performance issue you need to determine where in the code the problems occur. You can do this by running a *profiler*. A profiler is a program that will let you run your program, and it will tell you how much time is spent in each function, and how many times they are run. `gprof` is the standard GNU/Linux profiling tool, but a discussion of using profilers is outside the scope of this text. After running a profiler, you can determine which functions are called the most or have the most time spent in them. These are the ones you should focus your optimization efforts on.

If a program only spends 1% of its time in a given function, then no matter how much you speed it up you will only achieve a *maximum* of a 1% overall speed improvement. However, if a program spends 20% of its time in a given function, then even minor improvements to that functions speed will be noticeable. Therefore, profiling gives you the information you need to make good choices about where to spend your programming time.

In order to optimize functions, you need to understand in what ways they are being called and used. The more you know about how and when a function is called, the better position you will be in to optimize it appropriately.

There are two main categories of optimization - local optimizations and global optimization. Local optimizations consist of optimizations that are either hardware specific - such as the fastest way to perform a given computation - or program-specific - such as making a specific piece of code perform the best for the most often-occurring case. Global optimization consist of optimizations which are structural. For example, if you were trying to find the best way for three people in different cities to meet in St. Louis, a local optimization would be finding a better road to get there, while a global optimization would be to decide to teleconference instead of meeting in person. Global optimization often involves restructuring code to avoid performance problems, rather than trying to find the best way through them.

12.3 Local Optimizations

The following are some well-known methods of optimizing pieces of code. When using high level languages, some of these may be done automatically by your compiler's optimizer.

Precomputing Calculations:
Sometimes a function has a limited number of possible inputs and outputs. In fact, it may be so few that you can actually precompute all of the possible answers beforehand, and simply look up the answer when the function is called. This takes up some space since you have to store all of the answers, but for small sets of data this works out really well, especially if the computation normally takes a long time.

Remembering Calculation Results:
This is similar to the previous method, but instead of computing results beforehand, the result of each calculation requested is stored. This way when the function starts, if the result has been computed before it will simply return the previous answer, otherwise it will do the full computation and store the result for later lookup. This has the advantage of requiring less storage space because you aren't precomputing all results. This is sometimes termed *caching* or *memoizing*.

Locality of Reference:
Locality of reference is a term for where in memory the data items you are accessing are. With virtual memory, you may access pages of memory which are stored on disk. In such a case, the operating system has to load that memory page from disk, and unload others to disk. Let's say, for instance, that the operating system will allow you to have 20k of memory in physical memory and forces the rest of it to be on disk, and your application uses 60k of memory. Let's say your program has to do 5 operations on each piece of data. If it does one operation on every piece of data, and then goes through and does the next operation on each piece of data, eventually every page of data will be loaded and unloaded from the disk 5 times. Instead, if you did all 5 operations on a given data item, you only have to load each page from disk once. When you bundle as many operations on data that is physically close to each other in memory, then you are taking advantage of locality of reference. In addition, processors usually store some data on-chip in a cache. If you keep all of your operations within a small area of physical memory, your program may bypass even main memory and only use the chip's ultra-fast cache memory. This is all done for you - all you have to do is to try to operate on small sections of memory at a time, rather than bouncing all over the place.

Register Usage:
Registers are the fastest memory locations on the computer. When you access memory, the processor has to wait while it is loaded from the memory bus. However, registers are located on the processor itself, so access is extremely fast. Therefore making wise usage of registers is extremely important. If you have few enough data items you are working with, try to store them all in registers. In high level languages, you do not always have this option - the compiler decides what goes in registers and what doesn't.

Inline Functions:
Functions are great from the point of view of program management - they make it easy to break up your program into independent, understandable, and reusable parts. However, function calls do involve the overhead of pushing arguments onto the stack and doing the jumps (remember locality of reference - your code may be swapped out on disk instead of in memory). For high level languages, it's often impossible for compilers to do optimizations across function-call boundaries. However, some languages support inline functions or function macros. These functions look, smell, taste, and act like real functions, except the compiler has the option to simply plug the code in exactly where it was called. This makes the program faster, but it also increases the size of the code. There are also many functions, like recursive functions, which cannot be inlined because they call themselves either directly or indirectly.

Optimized Instructions:
Often times there are multiple assembly language instructions which accomplish the same purpose. A skilled assembly language programmer knows which instructions are the fastest. However, this can change from processor to processor. For more information on this topic, you need to see the user's manual that is provided for the specific chip you are using. As an example, let's look at the process of loading the number 0 into a register. On most processors, doing a `movl $0, %eax` is not the quickest way. The quickest way is to exclusive-or the register with itself, `xorl %eax, %eax`. This is because it only has to access the register, and doesn't have to transfer any data. For users of high-level languages, the compiler handles this kind of optimizations for you. For assembly-language programmers, you need to know your processor well.

Addressing Modes:
Different addressing modes work at different speeds. The fastest are the immediate mode addressing and register addressing modes. Direct addressing mode is the next fastest, indirect is next, and base pointer addressing mode and indexed indirect addressing mode are the slowest. Try to use the faster addressing modes, when possible. One interesting consequence of this is that when you have a structured piece of memory that you are accessing using base pointer addressing, the first element can be accessed the quickest. Since its offset is 0, you can access it using indirect addressing instead of base pointer addressing, which makes it faster.

Data Alignment:
Some processors can access data on word-aligned memory boundaries (i.e. - addresses divisible by the word size) faster than non-aligned data. So, when setting up structures in memory, it is best to keep it word-aligned. Some non-x86 processors, in fact, cannot access non-aligned data in some modes.

These are just a smattering of examples of the kinds of local optimizations possible. However, remember that the maintainability and readability of code is much more important except under extreme circumstances.

12.4 Global Optimization

Global optimization has two goals. The first one is to put your code in a form where it is easy to do local optimizations. For example, if you have a large procedure that performs several slow, complex calculations, you might see if you can break parts of that procedure into their own functions where the values can be precomputed or memoized.

Stateless functions (functions that only operate on the parameters that were passed to them - i.e. no globals or system calls) are the easiest type of functions to optimize in a computer. The more stateless parts of your program you have, the more opportunities you have to optimize. In the e-commerce situation I wrote about above, the computer had to find all of the associated parts for specific inventory items. This required about 12 database calls, and in the worst case took about 20 seconds. However, the goal of this program was to be interactive, and a long wait would destroy that goal. However, I knew that these inventory configurations do not change. Therefore, I converted the database calls into their own functions, which were stateless. I was then able to memoize the functions. At the beginning of each day, the function results were cleared in case anyone had changed them, and several inventory items were automatically preloaded. From then on during

the day, the first time someone accessed an inventory item, it would take the 20 seconds it did beforehand, but afterwards it would take less than a second, because the database results had been memoized.

Global optimization usually often involves achieving the following properties in your functions:

Parallelization:
Parallelization means that your algorithm can effectively be split among multiple processes. For example, pregnancy is not very parallelizable because no matter how many women you have, it still takes nine months. However, building a car is parallelizable because you can have one worker working on the engine while another one is working on the interior. Usually, applications have a limit to how parallelizable they are. The more parallelizable your application is, the better it can take advantage of multiprocessor and clustered computer configurations.

Statelessness:
As we've discussed, stateless functions and programs are those that rely entirely on the data explicitly passed to them for functioning. Most processes are not entirely stateless, but they can be within limits. In my e-commerce example, the function wasn't entirely stateless, but it was within the confines of a single day. Therefore, I optimized it as if it were a stateless function, but made allowances for changes at night. Two great benefits resulting from statelessness is that most stateless functions are parallelizable and often benefit from memoization.

Global optimization takes quite a bit of practice to know what works and what doesn't. Deciding how to tackle optimization problems in code involves looking at all the issues, and knowing that fixing some issues may cause others.

12.5 Review

12.5.1 Know the Concepts

- At what level of importance is optimization compared to the other priorities in programming?
- What is the difference between local and global optimizations?
- Name some types of local optimizations.
- How do you determine what parts of your program need optimization?
- At what level of importance is optimization compared to the other priorities in programming? Why do you think I repeated that question?

12.5.2 Use the Concepts

- Go back through each program in this book and try to make optimizations according to the procedures outlined in this chapter.
- Pick a program from the previous exercise and try to calculate the performance impact on your code under specific inputs.[51]

12.5.3 Going Further

- Find an open-source program that you find particularly fast. Contact one of the developers and ask about what kinds of optimizations they performed to improve the speed.
- Find an open-source program that you find particularly slow, and try to imagine the reasons for the slowness. Then, download the code and try to profile it using `gprof` or similar tool. Find where the code is spending the majority of the time and try to optimize it. Was the reason for the slowness different than you imagined?
- Has the compiler eliminated the need for local optimizations? Why or why not?
- What kind of problems might a compiler run in to if it tried to optimize code across function call boundaries?

[51] Since these programs are usually short enough not to have noticeable performance problems, looping through the program thousands of times will exaggerate the time it takes to run enough to make calculations.

13. Moving On from Here

Congratulations on getting this far. You should now have a basis for understanding the issues involved in many areas of programming. Even if you never use assembly language again, you have gained a valuable perspective and mental framework for understanding the rest of computer science.

There are essentially three methods to learn to program:

- From the Bottom Up - This is how this book teaches. It starts with low-level programming, and works toward more generalized teaching.
- From the Top Down - This is the opposite direction. This focuses on what you want to do with the computer, and teaches you how to break it down more and more until you get to the low levels.
- From the Middle - This is characterized by books which teach a specific programming language or API. These are not as concerned with concepts as they are with specifics.

Different people like different approaches, but a good programmer takes all of them into account. The bottom-up approaches help you understand the machine aspects, the top-down approaches help you understand the problem-area aspects, and the middle approaches help you with practical questions and answers. To leave any of these aspects out would be a mistake.

Computer Programming is a vast subject. As a programmer, you will need to be prepared to be constantly learning and pushing your limits. These books will help you do that. They not only teach their subjects, but also teach various ways and methods of *thinking*. As Alan Perlis said, "A language that doesn't affect the way you think about programming is not worth knowing". If you are constantly looking for new and better ways of doing and thinking, you will make a successful programmer. If you do not seek to enhance yourself, "A little sleep, a little slumber, a little folding of the hands to rest - and poverty will come on you like a bandit and scarcity like an armed man." (Proverbs 24:33-34 NIV). Perhaps not quite that severe, but still, it is best to always be learning.

These books were selected because of their content and the amount of respect they have in the computer science world. Each of them brings something unique. There are many books here. The best way to start would be to look through online reviews of several of the books, and find a starting point that interests you.

13.1 From the Bottom Up

This list is in the best reading order I could find. It's not necessarily easiest to hardest, but based on subject matter.

- Programming from the Ground Up by Jonathan Bartlett.
- Introduction to Algorithms by Thomas H. Cormen, Charles E. Leiserson, and Ronald L. Rivest.
- The Art of Computer Programming by Donald Knuth (3 volume set - volume 1 is the most important).
- Programming Languages by Samuel N. Kamin.
- Modern Operating Systems by Andrew Tanenbaum.
- Linkers and Loaders by John Levine.
- Computer Organization and Design: The Hardware/Software Interface by David Patterson and John Hennessy.

13.2 From the Top Down

These books are arranged from the simplest to the hardest. However, they can be read in any order you feel comfortable with.

- How to Design Programs by Matthias Felleisen, Robert Bruce Findler, Matthew Flatt, and Shiram Krishnamurthi.
- Simply Scheme: An Introduction to Computer Science by Brian Harvey and Matthew Wright.
- How to Think Like a Computer Scientist: Learning with Python by Allen Downey, Jeff Elkner, and Chris Meyers.
- Structure and Interpretation of Computer Programs by Harold Abelson and Gerald Jay Sussman with Julie Sussman.
- Design Patterns: Elements of Reusable Object-Oriented Software by Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides.
- What not How: The Rules Approach to Application Development by Chris Date.
- The Algorithm Design Manual by Steve Skiena.
- Programming Language Pragmatics by Michael Scott.
- Essentials of Programming Languages by Daniel P. Friedman, Mitchell Wand, and Christopher T. Haynes.

13.3 From the Middle Out

Each of these is the best book on its subject. If you need to know these languages, these will tell you all you need to know.

- Programming Perl by Larry Wall, Tom Christiansen, and Jon Orwant.
- Common LISP: The Language by Guy R. Steele.
- ANSI Common LISP by Paul Graham.
- The C Programming Language by Brian W. Kernighan and Dennis M. Ritchie.
- The Waite Group's C Primer Plus by Stephen Prata.
- The C++ Programming Language by Bjarne Stroustrup.
- Thinking in Java by Bruce Eckel.
- The Scheme Programming Language by Kent Dybvig.
- Linux Assembly Language Programming by Bob Neveln.

13.4 Specialized Topics

These books are the best books that cover their topic. They are thorough and authoritative. To get a broad base of knowledge, you should read several outside of the areas you normally program in.

- Practical Programming - Programming Pearls and More Programming Pearls by Jon Louis Bentley.
- Databases - Understanding Relational Databases by Fabian Pascal.
- Project Management - The Mythical Man-Month by Fred P. Brooks.
- UNIX Programming - The Art of UNIX Programming by Eric S. Raymond.
- UNIX Programming - Advanced Programming in the UNIX Environment by W. Richard Stevens.
- Network Programming - UNIX Network Programming (2 volumes) by W. Richard Stevens.
- Generic Programming - Modern C++ Design by Andrei Alexandrescu.

- Compilers - The Art of Compiler Design: Theory and Practice by Thomas Pittman and James Peters.
- Compilers - Advanced Compiler Design and Implementation by Steven Muchnick.
- Development Process - Refactoring: Improving the Design of Existing Code by Martin Fowler, Kent Beck, John Brant, William Opdyke, and Don Roberts.
- Typesetting - Computers and Typesetting (5 volumes) by Donald Knuth.
- Cryptography - Applied Cryptography by Bruce Schneier.
- Linux - Professional Linux Programming by Neil Matthew, Richard Stones, and 14 other people.
- Linux Kernel - Linux Device Drivers by Alessandro Rubini and Jonathan Corbet.
- Open Source Programming - The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary by Eric S. Raymond.
- Computer Architecture - Computer Architecture: A Quantitative Approach by David Patterson and John Hennessy.

13.5 Further Resources on Assembly Language

In assembly language, your best resources are on the web.

- Sandpile - A repository of reference material on x86, x86-64, and compatible processors.
- Dr. Dobb's - Journal Microprocessor Resources.
- Dr. Paul Carter's PC Assembly Language Page.
- The Art of Assembly Home Page.
- Intel's manuals for their processors.
- Jan Wagemaker's Linux assembly language examples.
- Paul Hsieh's x86 Assembly Page.

Appendices

A. GUI Programming

A.1 Introduction to GUI Programming

The purpose of this appendix is not to teach you how to do Graphical User Interfaces. It is simply meant to show how writing graphical applications is the same as writing other applications, just using an additional library to handle the graphical parts. As a programmer you need to get used to learning new libraries. Most of your time will be spent passing data from one library to another.

A.2 The GNOME Libraries

The GNOME projects is one of several projects to provide a complete desktop to Linux users. The GNOME project includes a panel to hold application launchers and mini-applications called applets, several standard applications to do things such as file management, session management, and configuration, and an API for creating applications which fit in with the way the rest of the system works.

One thing to notice about the GNOME libraries is that they constantly create and give you pointers to large data structures, but you never need to know how they are laid out in memory. All manipulation of the GUI data structures are done entirely through function calls. This is a characteristic of good library design. Libraries change from version to version, and so does the data that each data structure holds. If you had to access and manipulate that data yourself, then when the library is updated you would have to modify your programs to work with the new library, or at least recompile them. When you access the data through functions, the functions take care of knowing where in the structure each piece of data is. The pointers you receive from the library are *opaque* - you don't need to know specifically what the structure they are pointing to looks like, you only need to know the functions that will properly manipulate it. When designing libraries, even for use within only one program, this is a good practice to keep in mind.

This chapter will not go into details about how GNOME works. If you would like to know more, visit the GNOME developer web site. This site contains tutorials, mailing lists, API documentation, and everything else you need to start programming in the GNOME environment.

A.3 A Simple GNOME Program in Several Languages

This program will simply show a Window that has a button to quit the application. When that button is clicked it will ask you if you are sure, and if you click yes it will close the application. To run this program, type in the following as `0AA-01-gnome-example.s`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     This program is meant to be an example of
5       #     what GUI programs look like written with the
6       #     GNOME libraries.
7       #
8       # INPUT:
9       #     The user can only click on the "Quit" button
10      #     or close the window.
11      #
12      # OUTPUT:
13      #     The application will close.
```

```
14      #
15      # PROCESS:
16      #     If the user clicks on the "Quit" button, the
17      #     program will display a dialog asking if they
18      #     are sure.  If they click Yes, it will close
19      #     the application.  Otherwise it will continue
20      #     running.
21      #
22      .section .data
23          # GNOME definitions:
24          #     These were found in the GNOME header
25          #     files for the C language and converted
26          #     into their assembly equivalents.
27          #
28          GNOME_STOCK_BUTTON_YES:   # GNOME Button Names.
29              .ascii "Button_Yes\0"
30
31          GNOME_STOCK_BUTTON_NO:
32              .ascii "Button_No\0"
33
34                              # Gnome MessageBox Types.
35          GNOME_MESSAGE_BOX_QUESTION:
36              .ascii "question\0"
37
38          .equ NULL, 0        # Standard definition of
39                              # NULL.
40
41          signal_destroy:     # GNOME signal definitions.
42              .ascii "destroy\0"
43
44          signal_delete_event:
45              .ascii "delete_event\0"
46
47          signal_clicked:
48              .ascii "clicked\0"
49
50          # --- Application-specific definitions --- #
51          #
52          app_id:             # Application information.
53              .ascii "gnome-example\0"
54
55          app_version:
56              .ascii "1.000\0"
57
58          app_title:
59              .ascii "Gnome Example Program\0"
60
61                              # Text for Buttons and
62          button_quit_text:   # windows.
63              .ascii "I Want to Quit the GNOME Example\0"
64
65          quit_question:
66              .ascii "Are you sure you want to quit?\0"
```

```
67
68      .section .bss
69          .equ   WORD_SIZE,  4            # Variables to
70          .lcomm appPtr,     WORD_SIZE    # save the
71          .lcomm btnQuit,    WORD_SIZE    # created
72                                          # widgets in.
73
74      .section .text
75          .globl main
76          .type  main,  @function
77
78  main:
79      pushl %ebp
80      movl  %esp, %ebp
81
82      # Initialize GNOME libraries.
83      #
84      pushl 12(%ebp)          # Argv.
85      pushl 8(%ebp)           # Argc.
86      pushl $app_version
87      pushl $app_id
88      call  gnome_init
89      addl  $16, %esp         # Recover the stack.
90
91      # Create new application window.
92      #
93      pushl $app_title        # Window title.
94      pushl $app_id           # Application ID.
95      call  gnome_app_new
96      addl  $8, %esp          # Recover the stack.
97      movl  %eax, appPtr      # Save the window pointer.
98
99      # Create new button.
100     #
101     pushl $button_quit_text     # Button text.
102     call  gtk_button_new_with_label
103     addl  $4, %esp              # Recover the stack.
104     movl  %eax, btnQuit         # Save the button
105                                 # pointer.
106
107     # Make the button show up inside the application
108     # window.
109     #
110     pushl btnQuit
111     pushl appPtr
112     call  gnome_app_set_contents
113     addl  $8, %esp
114
115     # Makes the button show up (only after it is window
116     # shows up, though).
117     #
118     pushl btnQuit
119     call  gtk_widget_show
```

```
120     addl  $4, %esp
121
122     # Makes the application window show up.
123     #
124     pushl appPtr
125     call  gtk_widget_show
126     addl  $4, %esp
127
128     # Have GNOME call our delete_handler function
129     # whenever a "delete" event occurs.
130     #
131     pushl $NULL             # Extra data to pass to our
132                             # function (we do not use
133                             # any).
134     pushl $_delete_handler  # Function address to call.
135     pushl $signal_delete_event  # Name of the signal.
136     pushl appPtr                # Widget to listen for
137     call  gtk_signal_connect    # events on.
138     addl  $16, %esp             # Recover stack.
139
140     # Have GNOME call our destroy_handler function
141     # whenever a "destroy" event occurs.
142     #
143     pushl $NULL             # Extra data to pass to our
144                             # function (we do not use
145                             # any).
146     pushl $_destroy_handler # Function address to call.
147     pushl $signal_destroy   # Name of the signal.
148     pushl appPtr            # Widget to listen for
149                             # events on.
150     call  gtk_signal_connect
151     addl  $16, %esp         # Recover stack.
152
153     # Have GNOME call our click_handler function
154     # whenever a "click" event occurs.  Note that the
155     # previous signals were listening on the
156     # application window, while this one is only
157     # listening on the button.
158     #
159     pushl $NULL
160     pushl $_click_handler
161     pushl $signal_clicked
162     pushl btnQuit
163     call  gtk_signal_connect
164     addl  $16, %esp
165
166     # Transfer control to GNOME.  Everything that
167     # happens from here out is in reaction to user
168     # events, which call signal handlers.  This main
169     # function just sets up the main window and
170     # connects signal handlers, and the signal handlers
171     # take care of the rest.
172     #
```

```
    call  gtk_main

    # After the program is finished, leave.
    #
    movl  $0, %eax
    leave
    ret

_destroy_handler:
    # A "destroy" event happens when the widget is
    # being removed.  In this case, when the
    # application window is being removed, we simply
    # want the event loop to quit.
    #
    pushl %ebp
    movl  %esp, %ebp

    # This causes gtk to exit it is event loop as soon
    # as it can.
    #
    call  gtk_main_quit

    movl  $0, %eax
    leave
    ret

    # A "delete" event happens when the application
    # window gets clicked in the "x" that you normally
    # use to close a window.
    #
_delete_handler:
    movl  $1, %eax
    ret

_click_handler:
    # A "click" event happens when the widget gets
    # clicked.
    #
    pushl %ebp
    movl  %esp, %ebp

    # Create the "Are you sure" dialog.
    #
    pushl $NULL                     # End of buttons.
    pushl $GNOME_STOCK_BUTTON_NO    # Button 1.
    pushl $GNOME_STOCK_BUTTON_YES   # Button 0.
    pushl $GNOME_MESSAGE_BOX_QUESTION   # Dialog type.
    pushl $quit_question            # Dialog mesasge.
    call  gnome_message_box_new
    addl  $16, %esp                 # Recover stack.

    # %eax now holds the pointer to the dialog window.

```

```
226      # Setting Modal to 1 prevents any other user
227      # interaction while the dialog is being shown.
228      #
229      pushl $1
230      pushl %eax
231      call  gtk_window_set_modal
232      popl  %eax
233      addl  $4, %esp
234
235      # Now we show the dialog.
236      #
237      pushl %eax
238      call  gtk_widget_show
239      popl  %eax
240
241      # This sets up all the necessary signal handlers in
242      # order to just show the dialog, close it when one
243      # of the buttons is clicked, and return the number
244      # of the button that the user clicked on.  The
245      # button number is based on the order the buttons
246      # were pushed on in the gnome_message_box_new
247      # function.
248      #
249      pushl %eax
250      call  gnome_dialog_run_and_close
251      addl  $4, %esp
252
253      # Button 0 is the Yes button.  If this is the
254      # button they clicked on, tell GNOME to quit it is
255      # event loop.  Otherwise, do nothing.
256      #
257      cmpl  $0, %eax
258      jne   _click_handler_end
259
260      call  gtk_main_quit
261
262  _click_handler_end:
263      leave
264      ret
```

To build this application, execute the following commands:

```
as -o 0AA-01-gnome-example.o   --32 \
                               --gstabs+ \
                               0AA-01-gnome-example.s

gcc -o 0AA-01-gnome-example    `gnome-config --libs gnomeui` \
                               0AA-01-gnome-example.o
```

Then type in `./0AA-01-gnome-example` to run it.

This program, like most GUI programs, makes heavy use of passing pointers to functions as parameters. In this program you create widgets with the GNOME functions and then you set up functions to be called when certain events happen. These functions are called *callback* functions. All of the event processing is handled by the function `gtk_main`, so you don't have to worry about how the events are being processed. All you have to do is have callbacks set up to wait for them.

Here is a short description of all of the GNOME functions that were used in this program:

gnome_init:
Takes the command-line arguments, argument count, application id, and application version and initializes the GNOME libraries.

gnome_app_new:
Creates a new application window, and returns a pointer to it. Takes the application id and the window title as arguments.

gtk_button_new_with_label:
Creates a new button and returns a pointer to it. Takes one argument - the text that is in the button.

gnome_app_set_contents:
This takes a pointer to the gnome application window and whatever widget you want (a button in this case) and makes the widget be the contents of the application window

gtk_widget_show:
This must be called on every widget created (application window, buttons, text entry boxes, etc) in order for them to be visible. However, in order for a given widget to be visible, all of its parents must be visible as well.

gtk_signal_connect:
This is the function that connects widgets and their signal handling callback functions. This function takes the widget pointer, the name of the signal, the callback function, and an extra data pointer. After this function is called, any time the given event is triggered, the callback will be called with the widget that produced the signal and the extra data pointer. In this application, we don't use the extra data pointer, so we just set it to NULL, which is 0.

gtk_main:
This function causes GNOME to enter into its main loop. To make application programming easier, GNOME handles the main loop of the program for us. GNOME will check for events and call the appropriate callback functions when they occur. This function will continue to process events until `gtk_main_quit` is called by a signal handler.

gtk_main_quit:
This function causes GNOME to exit its main loop at the earliest opportunity.

gnome_message_box_new:
This function creates a dialog window containing a question and response buttons. It takes as parameters the message to display, the type of message it is (warning, question, etc), and a list of buttons to display. The final parameter should be NULL to indicate that there are no more buttons to display.

gtk_window_set_modal:
This function makes the given window a modal window. In GUI programming, a modal window is one that prevents event processing in other windows until that window is closed. This is often used with Dialog windows.

gnome_dialog_run_and_close:
This function takes a dialog pointer (the pointer returned by `gnome_message_box_new` can be used here) and will set up all of the appropriate signal handlers so that it will run until a button is pressed. At that time it will close the dialog and return to you which button was pressed. The button number refers to the order in which the buttons were set up in `gnome_message_box_new`.

The following is the same program written in the C language. Type it in as `0AA-01-gnome-example-c.c`:

```
1   /* PURPOSE:
2    *     This program is meant to be an example of what
3    *     GUI programs look like written with the GNOME
4    *     libraries.
5    */
6
7   #include <gnome.h>;
8
9   /* Program definitions. */
10  #define MY_APP_TITLE "Gnome Example Program"
11  #define MY_APP_ID "gnome-example"
12  #define MY_APP_VERSION "1.000"
13  #define MY_BUTTON_TEXT "I Want to Quit this Program"
14  #define MY_QUIT_QUESTION "Are you sure? Quit?"
```

```
15
16  /* Must declare functions before they are used. */
17  int destroy_handler(gpointer window,
18          GdkEventAny *e,
19          gpointer data);
20  int delete_handler(gpointer window,
21          GdkEventAny *e,
22          gpointer data);
23  int click_handler(gpointer window,
24          GdkEventAny *e,
25          gpointer data);
26
27  int main(int argc, char **argv)
28  {
29      gpointer appPtr;  /* Application window. */
30      gpointer btnQuit; /* Quit button. */
31
32      /* Initialize GNOME libraries. */
33      gnome_init(MY_APP_ID, MY_APP_VERSION, argc, argv);
34
35      /* Create new application window. */
36      appPtr = gnome_app_new(MY_APP_ID, MY_APP_TITLE);
37
38      /* Create new button. */
39      btnQuit = gtk_button_new_with_label(
40                                      MY_BUTTON_TEXT);
41
42      /* Make the button show up inside the */
43      /* application window. */
44      gnome_app_set_contents(appPtr, btnQuit);
45
46      /* Makes the button show up. */
47      gtk_widget_show(btnQuit);
48
49      /* Makes the application window show up. */
50      gtk_widget_show(appPtr);
51
52      /* Connect the signal handlers. */
53      gtk_signal_connect(appPtr, "delete_event",
54              GTK_SIGNAL_FUNC(delete_handler), NULL);
55      gtk_signal_connect(appPtr, "destroy",
56              GTK_SIGNAL_FUNC(destroy_handler), NULL);
57      gtk_signal_connect(btnQuit, "clicked",
58              GTK_SIGNAL_FUNC(click_handler), NULL);
59
60      /* Transfer control to GNOME. */
61      gtk_main();
62
63      return 0;
64  }
65
66
67  /* Function to receive the "destroy" signal. */
```

```
int destroy_handler(gpointer window,
        GdkEventAny *e,
        gpointer data)
{
    /* Leave GNOME event loop. */
    gtk_main_quit();
    return 0;
}

/* Function to receive the "delete_event" signal. */
int delete_handler(gpointer window,
        GdkEventAny *e,
        gpointer data)
{
    return 0;
}

/* Function to receive the "clicked" signal. */
int click_handler(gpointer window,
        GdkEventAny *e,
        gpointer data)
{
    gpointer msgbox;
    int buttonClicked;

    /* Create the "Are you sure" dialog. */
    msgbox = gnome_message_box_new(
        MY_QUIT_QUESTION,
        GNOME_MESSAGE_BOX_QUESTION,
        GNOME_STOCK_BUTTON_YES,
        GNOME_STOCK_BUTTON_NO,
        NULL);
    gtk_window_set_modal(msgbox, 1);
    gtk_widget_show(msgbox);

    /* Run dialog box. */
    buttonClicked = gnome_dialog_run_and_close(msgbox);

    /* Button 0 is the Yes button.  If this is the
     * button they clicked
     * on, tell GNOME to quit it's event loop.
     * Otherwise, do nothing. */
    if(buttonClicked == 0)
    {
        gtk_main_quit();
    }

    return 0;
}
```

To compile it, type

```
gcc -o 0AA-01-gnome-example-c  \
           `gnome-config --cflags --libs gnomeui` \
           0AA-01-gnome-example-c.c
```

Run it by typing `./0AA-01-gnome-example-c`.

Finally, we have a version in Python. Type it in as `0AA-01-gnome-example.py`:

```
1   # PURPOSE:
2   #     This program is meant to be an example of what
3   #     GUI programs look like written with the GNOME
4   #     libraries.
5   #
6
7   # Import GNOME libraries.
8   #
9   import gtk
10  import gnome.ui
11
12  #### DEFINE CALLBACK FUNCTIONS FIRST ####
13
14  # In Python, functions have to be defined before they
15  # are used, so we have to define our callback
16  # functions first.
17  #
18  def destroy_handler(event):
19      gtk.mainquit()
20      return 0
21
22  def delete_handler(window, event):
23      return 0
24
25  def click_handler(event):
26      # Create the "Are you sure" dialog.
27      #
28      msgbox = gnome.ui.GnomeMessageBox(
29          "Are you sure you want to quit?",
30          gnome.ui.MESSAGE_BOX_QUESTION,
31          gnome.ui.STOCK_BUTTON_YES,
32          gnome.ui.STOCK_BUTTON_NO)
33      msgbox.set_modal(1)
34      msgbox.show()
35
36      result = msgbox.run_and_close()
37
38      # Button 0 is the Yes button.  If this is the
39      # button they clicked on, tell GNOME to quit it's
40      # event loop.  Otherwise, do nothing.
41      #
42      if (result == 0):
43          gtk.mainquit()
44
45      return 0
46
47  #### MAIN PROGRAM ####
```

```
48
49  # Create new application window.
50  #
51  myapp = gnome.ui.GnomeApp(
52      "gnome-example", "Gnome Example Program")
53
54  # Create new button.
55  #
56  mybutton = gtk.GtkButton(
57      "I Want to Quit the GNOME Example program")
58  myapp.set_contents(mybutton)
59
60  # Makes the button show up.
61  #
62  mybutton.show()
63
64  # Makes the application window show up.
65  #
66  myapp.show()
67
68  # Connect signal handlers.
69  #
70  myapp.connect("delete_event", delete_handler)
71  myapp.connect("destroy", destroy_handler)
72  mybutton.connect("clicked", click_handler)
73
74  # Transfer control to GNOME.
75  #
76  gtk.mainloop()
```

To run it type `python 0AA-01-gnome-example.py`.

A.4 GUI Builders

In the previous example, you have created the user-interface for the application by calling the create functions for each widget and placing it where you wanted it. However, this can be quite burdensome for more complex applications. Many programming environments, including GNOME, have programs called GUI builders that can be used to automatically create your GUI for you. You just have to write the code for the signal handlers and for initializing your program. The main GUI builder for GNOME applications is called GLADE. GLADE ships with most Linux distributions.

There are GUI builders for most programming environments. Borland has a range of tools that will build GUIs quickly and easily on Linux and Win32 systems. The KDE environment has a tool called QT Designer which helps you automatically develop the GUI for their system.

There is a broad range of choices for developing graphical applications, but hopefully this appendix gave you a taste of what GUI programming is like.

B. Common x86 Instructions

B.1 Reading the Tables

The tables of instructions presented in this appendix include:

- The instruction code.
- The operands used.
- The flags used.
- A brief description of what the instruction does.

In the operands section, it will list the type of operands it takes. If it takes more than one operand, each operand will be separated by a comma. Each operand will have a list of codes which tell whether the operand can be an immediate-mode value (I), a register (R), or a memory address (M). For example, the `movl` instruction is listed as `I/R/M, R/M`. This means that the first operand can be any kind of value, while the second operand must be a register or memory location. Note, however, that in x86 assembly language you cannot have more than one operand be a memory location.

In the flags section, it lists the flags in the *%eflags* register affected by the instruction. The following flags are mentioned:

O: Overflow flag. This is set to true if the destination operand was not large enough to hold the result of the instruction.

S: Sign flag. This is set to the sign of the last result.

Z: Zero flag. This flag is set to true if the result of the instruction is zero.

A: Auxiliary carry flag. This flag is set for carries and borrows between the third and fourth bit. It is not often used.

P: Parity flag. This flag is set to true if the low byte of the last result had an even number of 1 bits.

C: Carry flag. Used in arithmetic to say whether or not the result should be carried over to an additional byte. If the carry flag is set, that usually means that the destination register could not hold the full result. It is up to the programmer to decide on what action to take (i.e. - propagate the result to another byte, signal an error, or ignore it entirely).

Other flags exist, but they are much less important.

B.2 Data Transfer Instructions

These instructions perform little, if any computation. Instead they are mostly used for moving data from one place to another.

An example of this table is the `movl` instruction which could read like this:

```
movl   I/R/M,  I/R/M      # eFlags affected: O/S/Z/A/C
movl   $5,     eax        # I, R -> eFlags that may affect: O/S/Z/A/C
movl   edx,    (%ebp)     # R, M -> eFlags that may affect: O/S/Z/A/C
```

Table B-1. Data Transfer Instructions.

Instruction *Operands* —–> Affected Flags (eFlags).

movl *I/R/M, I/R/M* —–> O/S/Z/A/C:

This copies a word of data from one location to another. `movl %eax, %ebx` copies the contents of *%eax* to *%ebx*.

movb *I/R/M*, *I/R/M* —–> O/S/Z/A/C:

Same as `movl`, but operates on individual bytes.

leal *M*, *I/R/M* —–> O/S/Z/A/C:

This takes a memory location given in the standard format, and, instead of loading the contents of the memory location, loads the computed address. For example, `leal 5(%ebp,%ecx,1), %eax` loads the address computed by `5 + %ebp + 1*%ecx` and stores that in *%eax*.

popl *R/M* —–> O/S/Z/A/C:

Pops the top of the stack into the given location. This is equivalent to performing `movl (%esp), R/M` followed by `addl $4, %esp`. `popfl` is a variant which pops the top of the stack into the *%eflags* register.

pushl *I/R/M* —–> O/S/Z/A/C:

Pushes the given value onto the stack. This is the equivalent to performing `subl $4, %esp` followed by `movl I/R/M, (%esp)`. `pushfl` is a variant which pushes the current contents of the *%eflags* register onto the top of the stack.

xchgl *R/M*, *R/M* —–> O/S/Z/A/C:

Exchange the values of the given operands.

B.3 Integer Instructions

These are basic calculating instructions that operate on signed or unsigned integers.

Table B-2. Integer Instructions.

Instruction *Operands* —–> Affected Flags (eFlags).

adcl *I/R/M*, *R/M* —–> O/S/Z/A/P/C:

Add with carry. Adds the carry bit and the first operand to the second, and, if there is an overflow, sets overflow and carry to true. This is usually used for operations larger than a machine word. The addition on the least-significant word would take place using `addl`, while additions to the other words would use the `adcl` instruction to take the carry from the previous add into account. For the usual case, this is not used, and `addl` is used instead.

addl *I/R/M*, *R/M* —–> O/S/Z/A/P/C:

Addition. Adds the first operand to the second, storing the result in the second. If the result is larger than the destination register, the overflow and carry bits are set to true. This instruction operates on both signed and unsigned integers.

cdq *Not Applicable* —–> O/S/Z/A/P/C:

Converts the *%eax* word into the double-word consisting of *%edx*:*%eax* with sign extension. The `q` signifies that it is a *quad-word*. It's actually a double-word, but it's called a quad-word because of the terminology used in the 16-bit days. This is usually used before issuing an `idivl` instruction.

cmpl *I/R/M*, *R/M* —–> O/S/Z/A/P/C:

Compares two integers. It does this by subtracting the first operand from the second. It discards the results, but sets the flags accordingly. Usually used before a conditional jump.

decl *R/M* —–> O/S/Z/A/P:

Decrements the register or memory location. Use `decb` to decrement a byte instead of a word.

divl *R/M* —–> O/S/Z/A/P:

Performs unsigned division. Divides the contents of the double-word contained in the combined *%edx*:*%eax* registers by the value in the register or memory location specified. The *%eax* register contains the resulting quotient, and the *%edx* register contains the resulting remainder. If the quotient is too large to fit in *%eax*, it triggers a type 0 interrupt.

idivl *R/M* —–> O/S/Z/A/P:

Performs signed division. Operates just like `divl` above.

imull *R/M/I*, *R* —–> O/S/Z/A/P/C:

Performs signed multiplication and stores the result in the second operand. If the second operand is left out, it is assumed to be *%eax*, and the full result is stored in the double-word *%edx*:*%eax*.

incl *R/M* —–> O/S/Z/A/P:

Increments the given register or memory location. Use `incb` to increment a byte instead of a word.

mull *R/M/I*, *R* —–> O/S/Z/A/P/C:

Perform unsigned multiplication. Same rules as apply to `imull`.

negl *R/M* —–> O/S/Z/A/P/C:

Negates (gives the two's complement inversion of) the given register or memory location.

sbbl *I/R/M*, *R/M* —–> O/S/Z/A/P/C:

Subtract with borrowing. This is used in the same way that `adc` is, except for subtraction. Normally only `subl` is used.

subl *I/R/M*, *R/M* —–> O/S/Z/A/P/C:

Subtract the two operands. This subtracts the first operand from the second, and stores the result in the second operand. This instruction can be used on both signed and unsigned numbers.

B.4 Logic Instructions

These instructions operate on memory as bits instead of words.

Table B-3. Logic Instructions.

Instruction *Operands* —–> Affected Flags (eFlags).

andl *I/R/M*, *R/M* —–> O/S/Z/P/C:

Performs a logical and of the contents of the two operands, and stores the result in the second operand. Sets the overflow and carry flags to false.

notl *R/M* —–> Not Applicable:

Performs a logical not on each bit in the operand. Also known as a one's complement.

orl *I/R/M*, *R/M* —–> O/S/Z/A/P/C:

Performs a logical or between the two operands, and stores the result in the second operand. Sets the overflow and carry flags to false.

rcll *I/cl*, *R/M* —–> O/C:

Rotates the given location's bits to the left the number of times in the first operand, which is either an immediate-mode value or the register *%cl*. The carry flag is included in the rotation, making it use 33 bits instead of 32. Also sets the overflow flag.

rcrl *I/cl*, *R/M* —–> O/C:

Same as above, but rotates right.

roll *I/cl*, *R/M* —–> O/C:

Rotate bits to the left. It sets the overflow and carry flags, but does not count the carry flag as part of the rotation. The number of bits to roll is either specified in immediate mode or is contained in the *%cl* register.

rorl *I/cl*, *R/M* —–> O/C:

Same as above, but rotates right.

sall *I/cl*, *R/M* —–> C:

Arithmetic shift left. The sign bit is shifted out to the carry flag, and a zero bit is placed in the least significant bit. Other bits are simply shifted to the left. This is the same as the regular shift left. The number of bits to shift is either specified in immediate mode or is contained in the *%cl* register.

sarl *I/cl, R/M* —–> C:

Arithmetic shift right. The least significant bit is shifted out to the carry flag. The sign bit is shifted in, and kept as the sign bit. Other bits are simply shifted to the right. The number of bits to shift is either specified in immediate mode or is contained in the *%cl* register.

shll *I/cl, R/M* —–> C:

Logical shift left. This shifts all bits to the left (sign bit is not treated specially). The leftmost bit is pushed to the carry flag. The number of bits to shift is either specified in immediate mode or is contained in the *%cl* register.

shrl *I/cl, R/M* —–> C:

Logical shift right. This shifts all bits in the register to the right (sign bit is not treated specially). The rightmost bit is pushed to the carry flag. The number of bits to shift is either specified in immediate mode or is contained in the *%cl* register.

testl *I/R/M, R/M* —–> O/S/Z/A/P/C:

Does a logical and of both operands and discards the results, but sets the flags accordingly.

xorl *I/R/M, R/M* —–> O/S/Z/A/P/C:

Does an exclusive or on the two operands, and stores the result in the second operand. Sets the overflow and carry flags to false.

B.5 Flow Control Instructions

These instructions may alter the flow of the program.

Table B-4. Flow Control Instructions.

Instruction *Operands* —–> Affected Flags (eFlags).

call *Destination address* —–> O/S/Z/A/C:

This pushes what would be the next value for *%eip* onto the stack, and jumps to the destination address. Used for function calls. Alternatively, the destination address can be an asterisk followed by a register for an indirect function call. For example, `call *%eax` will call the function at the address in *%eax*.

int *I* —–> O/S/Z/A/C:

Causes an interrupt of the given number. This is usually used for system calls and other kernel interfaces.

Jcc *Destination address* —–> O/S/Z/A/C:

Conditional branch. `cc` is the *condition code*. Jumps to the given address if the condition code is true (set from the previous instruction, probably a comparison). Otherwise, goes to the next instruction. The condition codes are:

- `[n]a[e]` - above(unsigned greater than). An `n` can be added for "not" and an `e` can be added for "or equal to".
- `[n]b[e]` - below (unsigned less than).
- `[n]e` - equal to.
- `[n]z` - zero.
- `[n]g[e]` - greater than (signed comparison).
- `[n]l[e]` - less than (signed comparison).
- `[n]c` - carry flag set.
- `[n]o` - overflow flag set.
- `[p]p` - parity flag set.
- `[n]s` - sign flag set.
- `ecxz` - *%ecx* is zero.

jmp *Destination address* —–> O/S/Z/A/C:

An unconditional jump. This simply sets *%eip* to the destination address. Alternatively, the destination address can be an asterisk followed by a register for an indirect jump. For example, `jmp *%eax` will jump to the address in *%eax*.

ret *Not Applicable* —–> O/S/Z/A/C:

Pops a value off of the stack and then sets *%eip* to that value. Used to return from function calls.

B.6 Assembler Directives

These are instructions to the assembler and linker, instead of instructions to the processor. These are used to help the assembler put your code together properly, and make it easier to use.

Table B-5. Assembler Directives.

Directive *Operands*.

.ascii *Quoted String*:

Takes the given quoted string and converts it into byte data.

.byte *Values*:

Takes a comma-separated list of values and inserts them right there in the program as data.

.endr *Not Applicable*:

Ends a repeating section defined with `.rept`.

.equ *Label, Value*:

Sets the given label equivalent to the given value. The value can be a number, a character, or a constant expression that evaluates to a number or character. From that point on, use of the label will be substituted for the given value.

.globl *Label*:

Sets the given label as global, meaning that it can be used from separately-compiled object files.

.include *File*:

Includes the given file just as if it were typed in right there.

.lcomm *Symbol*, *Size*:

This is used in the `.bss` section to specify storage that should be allocated when the program is executed. Defines the symbol with the address where the storage will be located, and makes sure that it is the given number of bytes long.

.long *Values*:

Takes a sequence of numbers separated by commas, and inserts those numbers as 4-byte words right where they are in the program.

.rept *Count*:

Repeats everything between this directive and the `.endr` directives the number of times specified.

.section *Section Name*:

Switches the section that is being worked on. Common sections include `.text` (for code), `.data` (for data embedded in the program itself), and `.bss` (for uninitialized global data).

.type *Symbol*, *@function*:

Tells the linker that the given symbol is a function.

B.7 Differences in Other Syntaxes and Terminology

The syntax for assembly language used in this book is known at the *AT&T* syntax. It is the one supported by the GNU tool chain that comes standard with every Linux distribution. However, the official syntax for x86 assembly language (known as the Intel® syntax) is different. It is the same assembly language for the same platform, but it looks different. Some of the differences include:

- In Intel syntax, the operands of instructions are often reversed. The destination operand is listed before the source operand.
- In Intel syntax, registers are not prefixed with the percent sign (`%`).

- In Intel syntax, a dollar-sign (`$`) is not required to do immediate-mode addressing. Instead, non-immediate addressing is accomplished by surrounding the address with brackets (`[ ]`).
- In Intel syntax, the instruction name does not include the size of data being moved. If that is ambiguous, it is explicitly stated as `BYTE`, `WORD`, or `DWORD` immediately after the instruction name.
- The way that memory addresses are represented in Intel assembly language is much different (shown below).
- Because the x86 processor line originally started out as a 16-bit processor, most literature about x86 processors refer to words as 16-bit values, and call 32-bit values double words. However, we use the term "word" to refer to the standard register size on a processor, which is 32 bits on an x86 processor. The syntax also keeps this naming convention - `DWORD` stands for "double word" in Intel syntax and is used for standard-sized registers, which we would call simply a "word".
- Intel assembly language has the ability to address memory as a segment/offset pair. We do not mention this because Linux does not support segmented memory, and is therefore irrelevant to normal Linux programming.

Other differences exist, but they are small in comparison. To show some of the differences, consider the following instruction:

```
1    movl $5, %eax
2    movl 12(%ebx), %eax
3    movl (%ebx,%edi), %ecx
4    movl 8(%ebx,%edi), %eax
5    movl (%ebx,%edi,4), %eax
6    movl 8(%ebx,%edi,4), %eax
```

In Intel syntax, this would be written as:

```
1    mov  eax, 5
2    mov  eax, [ebx+12]
3    mov  ecx, [ebx+edi]
4    mov  eax, [ebx+edi+8]
5    mov  eax, [ebx+edi*4]
6    mov  eax, [ebx+edi*4+8]
```

The memory reference is a bit easier to read than its AT&T counterpart because it spells out exactly how the address will be computed. However, but the order of operands in Intel syntax can be confusing.

The tool intel2gas is a small text parser that can convert assembler source written in NASM syntax (Intel) to gas syntax (AT&T). And nowadays more often also the other way.

B.8 Where to Go for More Information

Intel has a set of comprehensive guides to their processors. These are available at Intel, Resource & Design Center Note that all of these use the Intel syntax, not the AT&T syntax. The most important one is the Intel® 64 and IA-32 Architectures Software Developer's Manual Combined Volumes: 1, 2A, 2B, 2C, 2D, 3A, 3B, 3C, 3D, and 4.

In addition, you can find a lot of information in the manual for the GNU assembler. Similarly, the manual for the GNU linker.

C. Important System Calls

These are some of the more important system calls to use when dealing with Linux. For most cases, however, it is best to use library functions rather than direct system calls, because the system calls were designed to be minimalistic while the library functions were designed to be easy to program with. For information about the GNU C Library.

Remember that *%eax* holds the system call numbers, and that the return values and error codes are also stored in *%eax*.

Table C-1. Important Linux System Calls.

System Call: *%eax*.

---

exit: *1*.

- **%ebx**: Return value (int).
- Exits the program.

read: *3*.

- **%ebx**: File descriptor.
- **%ecx**: Buffer start.
- **%edx**: Buffer size (int).
- Reads into the given buffer.

write: *4*.

- **%ebx**: File descriptor.
- **%ecx**: Buffer start.
- **%edx**: Buffer size (int).
- Writes the buffer to the file descriptor.

open: *5*.

- **%ebx**: Null-terminated file name.
- **%ecx**: Option list.
- **%edx**: Permission mode.
- Opens the given file. Returns the file descriptor or an error number.

close: *6*.

- **%ebx**: File descriptor.
- Closes the give file descriptor.

chdir: *12*.

- **%ebx**: Null-terminated directory name.

- Changes the current directory of your program.

lseek: *19*.

- **%ebx**: File descriptor.
- **%ecx**: Offset.
- **%edx**: Mode.
- Repositions where you are in the given file. The mode (called the "whence") should be 0 for absolute positioning, and 1 for relative positioning.

getpid: *20*.

- Returns the process ID of the current process.

mkdir: *39*.

- **%ebx**: Null-terminated directory name.
- **%ecx**: Permission mode.
- Creates the given directory. Assumes all directories leading up to it already exist.

rmdir: *40*.

- **%ebx**: Null-terminated directory name.
- Removes the given directory.

dup: *41*.

- **%ebx**: File descriptor.
- Returns a new file descriptor that works just like the existing file descriptor.

pipe: *42*.

- **%ebx**: Pipe array.
- Creates two file descriptors, where writing on one produces data to read on the other and vice-versa. %ebx is a pointer to two words of storage to hold the file descriptors.

brk: *45*.

- **%ebx**: New system break.
- Sets the system break If the system break is 0, it simply returns the current system break. I.E. - The end of the data section.

ioctl: *54*.

- **%ebx**: File descriptor.
- **%ecx**: Request.
- **%edx**: Arguments.
- This is used to set parameters on device files. Its actual usage varies based on the type of file or device your descriptor references.

A more complete listing of system calls is in this web site Call convention by architecture, along with additional information is available at System Calls for Assembly Level Access You can also get more information about a system call by typing in `man 2 syscalls` which will return you the information about the system call from section 2 of the UNIX manual. However, this refers to the usage of the system call from the C programming language, and may or may not be directly helpful.

For information on how system calls are implemented on Linux, see the Linux Kernel 2.4 Internals section on how system calls are implemented.

D. Table of ASCII Codes

To use this table, simply find the character or escape that you want the code for, and add the number on the left and the top.

Table D-1. Table of ASCII codes in decimal.

Num	+0	+1	+2	+3	+4	+5	+6	+7
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL
8	BS	HT	LF	VT	FF	CR	SO	SI
16	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB
24	CAN	EM	SUB	ESC	FS	GS	RS	US
32		!	"	#	$	%	&	'
40	(	)	*	+	,	-	.	/
48	0	1	2	3	4	5	6	7
56	8	9	:	;	<	=	>	?
64	@	A	B	C	D	E	F	G
72	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W
88	X	Y	Z	[	\	]	^	_
96	`	a	b	c	d	e	f	g
104	h	i	j	k	l	m	n	o
112	p	q	r	s	t	u	v	w
120	x	y	z	{	|	}	~	DEL

ASCII is actually being phased out in favor of an international standard known as Unicode, which allows you to display any character from any known writing system in the world. As you may have noticed, ASCII only has support for English characters. Unicode is much more complicated, however, because it requires more than one byte to encode a single character. There are several different methods for encoding Unicode characters. The most common is UTF-8 and UTF-32. UTF-8 is somewhat backwards-compatible with ASCII (it is stored the same for English characters, but expands into multiple byte for international characters). UTF-32 simply requires four bytes for each character rather than one. Windows® uses UTF-16, which is a variable-length encoding which requires at least 2 bytes per character, so it is not backwards-compatible with ASCII.

A good tutorial on internationalization issues, fonts, and Unicode is available in a great Article by Joe Spolsky, called "The Absolute Minimum Every Software Developer Absolutely, Positively Must Know About Unicode and Character Sets (No Excuses!)".

E. C Idioms in Assembly Language

This appendix is for C programmers learning assembly language. It is meant to give a general idea about how C constructs can be implemented in assembly language.

E.1 If Statement

In C, an if statement consists of three parts - the condition, the true branch, and the false branch. However, since assembly language is not a block structured language, you have to work a little to implement the block-like nature of C. For example, look at the following C code:

```
if(a == b)
{
    /* True Branch Code Here */
}
else
{
    /* False Branch Code Here */
}

/* At This Point, Reconverge */
```

In assembly language, this can be rendered as:

```
    movl a, %eax        # Move a and b into registers
    movl b, %ebx        # for comparison.

    cmpl %eax, %ebx     # Compare.

    je true_branch      # If True, go to true branch.

false_branch:           # This label is unnecessary,
                        # only here for documentation.
                        # False branch code here.

    jmp reconverge      # Jump to recovergence point.

true_branch:            # True branch code here.

reconverge:             # Both branches recoverge to
                        # this point.
```

As you can see, since assembly language is linear, the blocks have to jump around each other. Reconvergence is handled by the programmer, not the system.

A case statement is written just like a sequence of if statements.

E.2 Function Call

A function call in assembly language simply requires pushing the arguments to the function onto the stack in *reverse* order, and issuing a `call` instruction. After calling, the arguments are then popped back off of the stack. For example, consider the C code:

```
printf("The number is %d", 88);
```

In assembly language, this would be rendered as:

```
.section .data
    text_string:
        .ascii "The number is %d\0"

.section .text
    pushl $88
    pushl $text_string
    call  printf
    popl  %eax
    popl  %eax      # %eax is just a dummy variable,
                    # nothing is actually being done
                    # with the value.  You can also
                    # directly re-adjust %esp to the
                    # proper location.
```

E.3 Variables and Assignment

Global and static variables are declared using `.data` or `.bss` entries. Local variables are declared by reserving space on the stack at the beginning of the function. This space is given back at the end of the function.

Interestingly, global variables are accessed differently than local variables in assembly language. Global variables are accessed using direct addressing mode, while local variables are accessed using base pointer addressing mode. For example, consider the following C code:

```
int my_global_var;

int foo()
{
    int my_local_var;

    my_local_var = 1;
    my_global_var = 2;

    return 0;
}
```

This would be rendered in assembly language as:

```
    .section .data
        .lcomm my_global_var, 4

    .type  foo,  @function

foo:
    pushl %ebp              # Save old base pointer.
    movl  %esp, $ebp        # Make stack pointer base
                            # pointer.
    subl  $4, %esp          # Make room for
                            # my_local_var.
    .equ my_local_var, -4   # Can now use my_local_var
                            # to find the local
                            # variable.
```

```
    movl  $1, my_local_var(%ebp)
    movl  $2, my_global_var

    movl  %ebp, %esp        # Clean up function and
    popl  %ebp              # return.
    ret
```

What may not be obvious is that accessing the global variable takes fewer machine cycles than accessing the local variable. However, that may not matter because the stack is more likely to be in physical memory (instead of swap) than the global variable is.

Also note that in the C programming language, after the compiler loads a value into a register, that value will likely stay in that register until that register is needed for something else. It may also move registers. For example, if you have a variable `foo`, it may start on the stack, but the compiler will eventually move it into registers for processing. If there aren't many variables in use, the value may simply stay in the register until it is needed again. Otherwise, when that register is needed for something else, the value, if it's changed, is copied back to its corresponding memory location. In C, you can use the keyword `volatile` to make sure all modifications and references to the variable are done to the memory location itself, rather than a register copy of it, in case other processes, threads, or hardware may be modifying the value while your function is running.

E.4 Loops

Loops work a lot like if statements in assembly language - the blocks are formed by jumping around. In C, a while loop consists of a loop body, and a test to determine whether or not it is time to exit the loop. A for loop is exactly the same, with optional initialization and counter-increment sections. These can simply be moved around to make a while loop.

In C, a while loop looks like this:

```
while(a < b)
{
    /* Do stuff here */
}

/* Finished Looping */
```

This can be rendered in assembly language like this:

```
loop_begin:
    movl  a, %eax
    movl  b, %ebx
    cmpl  %eax, %ebx
    jge   loop_end

loop_body:                  # Do stuff here.

    jmp loop_begin

loop_end:                   # Finished looping.
```

The x86 assembly language has some direct support for looping as well. The *%ecx* register can be used as a counter that *ends* with zero. The `loop` instruction will decrement *%ecx* and jump to a specified address unless *%ecx* is zero. For example, if you wanted to execute a statement 100 times, you would do this in C:

```
for(i=0; i < 100; i++)
{
```

```
    /* Do process here */
}
```

In assembly language it would be written like this:

```
loop_initialize:
    movl $100, %ecx

loop_begin:                 # Do Process Here.
    loop loop_begin         # Decrement %ecx and loops
                            # if not zero.

rest_of_program:            # Continues on to here.
```

One thing to notice is that the `loop` instruction *requires you to be counting backwards to zero*. If you need to count forwards or use another ending number, you should use the loop form which does not include the `loop` instruction.

For really tight loops of character string operations, there is also the `rep` instruction, but we will leave learning about that as an exercise to the reader.

E.5 Structs

Structs are simply descriptions of memory blocks. For example, in C you can say:

```
struct person {
    char firstname[40];
    char lastname[40];
    int age;
};
```

This doesn't do anything by itself, except give you ways of intelligently using 84 bytes of data. You can do basically the same thing using `.equ` directives in assembly language. Like this:

```
.equ PERSON_FIRSTNAME_OFFSET,  0
.equ PERSON_LASTNAME_OFFSET,   40
.equ PERSON_AGE_OFFSET,        80
.equ PERSON_SIZE,              84
```

When you declare a variable of this type, all you are doing is reserving 84 bytes of space. So, if you have this in C:

```
void foo()
{
    struct person p;

    /* Do stuff here */
}
```

In assembly language you would have:

```
foo:                        # Standard header beginning
    pushl %ebp
    movl %esp, %ebp

    subl $PERSON_SIZE, %esp     # Reserve our local
                                # variable.
    .equ P_VAR, 0 - PERSON_SIZE # This is the
                                # variable's offset
```

```
                                # from %ebp.

                            # Do stuff here.

    movl %ebp, %esp         # Standard function ending.
    popl %ebp
    ret
```

To access structure members, you just have to use base pointer addressing mode with the offsets defined above. For example, in C you could set the person's age like this:

```
p.age = 30;
```

In assembly language it would look like this:

```
movl $30, P_VAR + PERSON_AGE_OFFSET(%ebp)
```

E.6 Pointers

Pointers are very easy. Remember, pointers are simply the address that a value resides at. Let's start by taking a look at global variables. For example:

```
int global_data = 30;
```

In assembly language, this would be:

```
.section .data
    global_data:
        .long 30
```

Taking the address of this data in C:

```
a = &global_data;
```

Taking the address of this data in assembly language:

```
movl $global_data, %eax
```

You see, with assembly language, you are almost always accessing memory through pointers. That's what direct addressing is. To get the pointer itself, you just have to go with immediate mode addressing.

Local variables are a little more difficult, but not much. Here is how you take the address of a local variable in C:

```
void foo()
{
    int a;
    int *b;

    a = 30;

    b = &a;

    *b = 44;
}
```

The same code in assembly language:

```
foo:
    pushl %ebp              # Standard opening.
    movl  %esp, %ebp

    subl  $8, $esp          # Reserve two words of
    .equ A_VAR, -4          # memory.
    .equ B_VAR, -8

    movl $30, A_VAR(%ebp)           # a = 30.

    movl $A_VAR, B_VAR(%ebp)        # b = &a.
    addl %ebp, B_VAR(%ebp)

    movl B_VAR(%ebp), %eax          # *b = 30.
    movl $30, (%eax)

    movl %ebp, %esp         # Standard closing.
    popl %ebp
    ret
```

As you can see, to take the address of a local variable, the address has to be computed the same way the computer computes the addresses in base pointer addressing. There is an easier way - the processor provides the instruction `leal`, which stands for "load effective address". This lets the computer compute the address, and then load it wherever you want. So, we could just say:

```
leal A_VAR(%ebp), %eax              # b = &a.
movl %eax, B_VAR(%ebp)
```

It's the same number of lines, but a little cleaner. Then, to use this value, you simply have to move it to a general-purpose register and use indirect addressing mode, as shown in the example above.

E.7 Getting GCC to Help

One of the nice things about GCC is its ability to spit out assembly language code. To convert a C language file to assembly, you can simply do:

```
gcc -S file.c
```

The output will be in `file.s`. It's not the most readable output - most of the variable names have been removed and replaced either with numeric stack locations or references to automatically-generated labels. To start with, you probably want to turn off optimizations with `-O0` so that the assembly language output will follow your source code better.

Something else you might notice is that GCC reserves more stack space for local variables than we do, and then AND's *%esp*[52] This is to increase memory and cache efficiency by double-word aligning variables.

Finally, at the end of functions, we usually do the following instructions to clean up the stack before issuing a `ret` instruction:

```
movl %ebp, %esp
popl %ebp
```

However, GCC output will usually just include the instruction `leave`. This instruction is simply the combination of the above two instructions. We do not use `leave` in this text because we want to be clear about exactly what is happening at the processor level.

[52]Note that different versions of GCC do this differently.

I encourage you to take a C program you have written and compile it to assembly language and trace the logic. Then, add in optimizations and try again. See how the compiler chose to rearrange your program to be more optimized, and try to figure out why it chose the arrangement and instructions it did.

F. Using the GDB Debugger

By the time you read this appendix, you will likely have written at least one program with an error in it. In assembly language, even minor errors usually have results such as the whole program crashing with a segmentation fault error. In most programming languages, you can simply print out the values in your variables as you go along, and use that output to find out where you went wrong. In assembly language, calling output functions is not so easy. Therefore, to aid in determining the source of errors, you must use a *source debugger*.

A debugger is a program that helps you find bugs by stepping through the program one step at a time, letting you examine memory and register contents along the way. A *source debugger* is a debugger that allows you to tie the debugging operation directly to the source code of a program. This means that the debugger allows you to look at the source code as you typed it in - complete with symbols, labels, and comments.

The debugger we will be looking at is GDB - the GNU Debugger. This application is present on almost all GNU/Linux distributions. It can debug programs in multiple programming languages, including assembly language.

F.1 An Example Debugging Session

The best way to explain how a debugger works is by using it. The program we will be using the debugger on is the `003-02-maximum` program used in Chapter 3. Your First Programs. Let's say that you entered the program perfectly, except that you left out the line:

```
incl %edi
```

When you run the program, it just goes in an infinite loop - it never exits. To determine the cause, you need to run the program under GDB. However, to do this, you need to have the assembler include debugging information in the executable. All you need to do to enable this is to add the `--gstabs+` option to the `as` command. So, you would assemble it like this:

```
as -o 003-02-maximum.o  --32 \
                        --gstabs+ \
                        003-02-maximum.s

ld -o 003-02-maximum    -m elf_i386 \
                        003-02-maximum.o
```

Linking would be the same as normal. "stabs" is the debugging format used by GDB. The `plus(+)` means that it provides the GNU extension which is the location of the current working directory. Now, to run the program under the debugger, you would type in `gdb ./003-02-maximum`. Be sure that the source files are in the current directory. The output should look similar to this:

```
GNU gdb (GDB) 10.1
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later.
This GDB was configured as "x86_64-pc-linux-gnu".
Type "show configuration" for configuration details.
For help, type "help".
Type "apropos word" to search for commands related to "word".
Debugger response to a program call of fork or vfork is "parent".
Whether gdb will detach the child of a fork is off.
```

```
Reading symbols from `./003-02-maximum`...
(gdb)
```

Depending on which version of GDB you are running, this output may vary slightly. At this point, the program is loaded, but is not running yet. The debugger is waiting your command. To run your program, just type in `run`. This will not return, because the program is running in an infinite loop. To stop the program, hit `control-c`. The screen will then say this:

```
Starting program: /home/johnnyb/003-02-maximum
^C
Program received signal SIGINT, Interrupt.
_start_loop () at 003-02-maximum.s:31
31          cmpl %ebx, %eax
(gdb)
```

This tells you that the program was interrupted by the SIGINT signal (from your `control-c`), and was within the section labelled `_start_loop`, and was executing on line 31 when it stopped. It gives you the code that it is about to execute. Depending on exactly when you hit `control-c`, it may have stopped on a different line or a different instruction than the example.

One of the best ways to find bugs in a program is to follow the flow of the program to see where it is branching incorrectly. To follow the flow of this program, keep on entering `stepi` (for "step instruction"), which will cause the computer to execute one instruction at a time. If you do this several times, your output will look something like this:

```
27          cmpl $0, %eax

(gdb) stepi
28          je _loop_exit

(gdb) stepi
29          incl %edi

(gdb) stepi
30          movl data_items(,%edi,4), %eax

(gdb) stepi
31          cmpl %ebx, %eax

(gdb) stepi
32          jle _start_loop

(gdb) stepi
27          cmpl $0, %eax

(gdb)
```

As you can tell, it has looped. In general, this is good, since we wrote it to loop. However, the problem is that it is *never stopping*. Therefore, to find out what the problem is, let's look at the point in our code where we should be exiting the loop:

```
cmpl  $0, %eax
je    _loop_exit
```

Basically, it is checking to see if *%eax* hits zero. If so, it should exit the loop. There are several things to check here. First of all, you may have left this piece out altogether. It is not uncommon for a programmer to forget to include a way to exit a loop. However, this is not the case here. Second, you should make sure that `_loop_exit` actually is outside the loop. If we put the label in the wrong place, strange things would happen. However, again, this is not the case.

Neither of those potential problems are the culprit. So, the next option is that perhaps *%eax* has the wrong value. There are two ways to check the contents of register in GDB. The first one is the command `info register`. This will display the contents of all registers in hexadecimal. However, we are only interested in *%eax* at this point. To just display *%eax* we can do `print $eax` to print it in hexadecimal, or do `print/d $eax` to print it in decimal. Notice that in GDB, registers are prefixed with dollar signs rather than percent signs. Your screen should have this on it:

```
(gdb) print $eax        # Default print.
$1 = 3
(gdb) print/d $eax      # Print as a decimal.
$2 = 3
(gdb) print/t $eax      # Print as a binary.
$3 = 11
(gdb) print/o $eax      # Print as a octal
$4 = 03
(gdb) print/x $eax      # Print as a hexadecimal.
$5 = 0x3
(gdb) print/f $eax      # Print as a floating.
$6 = 4.20389539e-45
(gdb) print/s $eax      # Print as a string.
$7 = 3
(gdb) print/c $eax      # Print as a character.
$8 = 3 '\003'
(gdb) print/a $eax      # Print as an address.
$9 = 0x3
```

This means that the result of your first inquiry is 3. Every inquiry you make will be assigned a number prefixed with a dollar sign. Now, if you look back into the code, you will find that 3 is the first number in the list of numbers to search through. If you step through the loop a few more times, you will find that in every loop iteration *%eax* has the number 3. This is not what should be happening. *%eax* should go to the next value in the list in every iteration.

Okay, now we know that *%eax* is being loaded with the same value over and over again. Let's search to see where *%eax* is being loaded from. The line of code is this:

```
movl data_items(,%edi,4), %eax
```

So, step until this line of code is ready to execute. Now, this code depends on two values - `data_items` and *%edi*. `data_items` is a symbol, and therefore constant. It's a good idea to check your source code to make sure the label is in front of the right data, but in our case it is. Therefore, we need to look at *%edi*. So, we need to print it out. It will look like this:

```
(gdb) print $edi
$1 = 0
```

This indicates that *%edi* is set to zero, which is why it keeps on loading the first element of the array. This should cause you to ask yourself two questions - what is the purpose of *%edi*, and how should its value be changed? To answer the first question, we just need to look in the comments. *%edi* is holding the current index of `data_items`. Since our search is a sequential search through the list of numbers in `data_items`, it would make sense that *%edi* should be incremented with every loop iteration.

Scanning the code, there is no code which alters *%edi* at all. Therefore, we should add a line to increment *%edi* at the beginning of every loop iteration. This happens to be exactly the line we tossed out at the beginning. Assembling, linking, and running the program again will show that it now works correctly.

Let's finish the execution typing `quit`, it will show a warning about kill the process because it is an infinite loop and the program never exit properly, type `y` to kill and exit from GDB:

```
(gdb) quit
A debugging session is active.
```

```
        Inferior 1 [process 682240] will be killed.
Quit anyway? (y or n) y
```

Hopefully this exercise provided some insight into using GDB to help you find errors in your programs.

F.2 Breakpoints and Other GDB Features

The program we entered in the last section had an infinite loop, and could be easily stopped using `control-c`. Other programs may simply abort or finish with errors. In these cases, `control-c` doesn't help, because by the time you press `control-c`, the program is already finished. To fix this, you need to set *breakpoints*. A breakpoint is a place in the source code that you have marked to indicate to the debugger that it should stop the program when it hits that point.

To set breakpoints you have to set them up before you run the program. Before issuing the `run` command, you can set up breakpoints using the `break` command. For example, to break on line 25, issue the command `break 25`. Then, when the program crosses line 25, it will stop running, and print out the current line and instruction. You can then step through the program from that point and examine registers and memory. To look at the lines and line numbers of your program, you can simply use the command `l`. This will print out your program with line numbers a screen at a time.

```
GNU gdb (GDB) 10.1
For help, type "help".
Reading symbols from ./003-02-maximum...

(gdb) break 25
Breakpoint 1 at 0x401005: file 003-02-maximum.s, line 25.

(gdb) run
Starting program: /home/johnnyb/003-02-maximum
Breakpoint 1, _start () at 003-02-maximum.s:25
warning: Source file is more recent than executable.
25          movl data_items(,%edi,4), %eax   # Load the first byte of data.

(gdb) l
20          .section .text
21              .globl _start
22
23      _start:
24          movl $0, %edi       # Move 0 into the index register.
25          movl data_items(,%edi,4), %eax  # Load first byte of data.
26          movl %eax, %ebx     # Since this is the first item,
27                              # %eax is the biggest.
28      _start_loop:            # Start loop.
29          cmpl $0, %eax       # Check to see if we've hit the end.
```

When dealing with functions, you can also break on the function names. For example, in the factorial program in Chapter 4. All About Functions, we could set a breakpoint for the factorial function by typing in `break factorial`. This will cause the debugger to break immediately after the function call and the function setup (it skips the pushing of *%ebp* and the copying of *%esp*). To send arguments through the GDB is necessary to type `set args` and the arguments same as we usually do in the command line.

```
as -o 004-02-factorial.o  --32 \
                          --gstabs+ \
                          004-02-factorial.s

ld -o 004-02-factorial    -m elf_i386 \
                          004-02-factorial.o
```

```
$ gdb ./004-02-factorial
GNU gdb (GDB) 10.1
For help, type "help".

(gdb) set args 55

(gdb) break factorial
Breakpoint 1 at 0x401013: file 004-02-factorial.s, line 34.
```

When stepping through code, you often don't want to have to step through every instruction of every function. Well-tested functions are usually a waste of time to step through except on rare occasion. Therefore, if you use the `nexti` command instead of the `stepi` command, GDB will wait until completion of the function before going on. Otherwise, with `stepi`, GDB would step you through every instruction within every called function.

```
(gdb) run
Starting program: /home/johnnyb/004-02-factorial
Breakpoint 1, factorial () at 004-02-factorial.s:34
34          pushl %ebp

(gdb) nexti
37          movl  %esp, %ebp

(gdb) nexti
40          movl  8(%ebp), %eax

(gdb) nexti
Program received signal SIGSEGV, Segmentation fault.
factorial () at 004-02-factorial.s:40
40          movl  8(%ebp), %eax

(gdb) nexti
Program terminated with signal SIGSEGV, Segmentation fault.
The program no longer exists.
```

Warning!

One problem that GDB has is with handling interrupts. Often times GDB will miss the instruction that immediately follows an interrupt. The instruction is actually executed, but GDB doesn't step through it. This should not be a problem - just be aware that it may happen.

Let's see the differences between `step`, `next` and `until`. The intention is not to show every output from the GDB. It shows the executed functions:

```
gdb ./004-02-factorial
```

`next`:

```
Breakpoint 1, _start () at 004-02-factorial.s:21
_factorial () at 004-02-factorial.s:50
_end_factorial () at 004-02-factorial.s:77
_end_factorial () at 004-02-factorial.s:78
_end_factorial () at 004-02-factorial.s:80
_start () at 004-02-factorial.s:27
[Inferior 1 (process 7536) exited with code 030]
# Instructions executed: 18
```

`until`:

```
Breakpoint 1, _start () at 004-02-factorial.s:21
_factorial () at 004-02-factorial.s:50
_end_factorial () at 004-02-factorial.s:77
_end_factorial () at 004-02-factorial.s:80
_factorial () at 004-02-factorial.s:66
_end_factorial () at 004-02-factorial.s:77
_end_factorial () at 004-02-factorial.s:78
_end_factorial () at 004-02-factorial.s:80
_factorial () at 004-02-factorial.s:66
_end_factorial () at 004-02-factorial.s:77
_end_factorial () at 004-02-factorial.s:78
_end_factorial () at 004-02-factorial.s:80
_factorial () at 004-02-factorial.s:66
_end_factorial () at 004-02-factorial.s:77
_end_factorial () at 004-02-factorial.s:78
_end_factorial () at 004-02-factorial.s:80
_start () at 004-02-factorial.s:27
[Inferior 1 (process 7660) exited with code 030]
# Instructions executed: 31
```

`step`:

```
Breakpoint 1, _start () at 004-02-factorial.s:21
_factorial () at 004-02-factorial.s:50
_factorial () at 004-02-factorial.s:41
_factorial () at 004-02-factorial.s:41
_factorial () at 004-02-factorial.s:41
_end_factorial () at 004-02-factorial.s:77
_end_factorial () at 004-02-factorial.s:80
_factorial () at 004-02-factorial.s:66
_end_factorial () at 004-02-factorial.s:77
_end_factorial () at 004-02-factorial.s:78
_end_factorial () at 004-02-factorial.s:80
_factorial () at 004-02-factorial.s:66
_end_factorial () at 004-02-factorial.s:77
_end_factorial () at 004-02-factorial.s:78
_end_factorial () at 004-02-factorial.s:80
_factorial () at 004-02-factorial.s:66
_end_factorial () at 004-02-factorial.s:77
_end_factorial () at 004-02-factorial.s:78
_end_factorial () at 004-02-factorial.s:80
_start () at 004-02-factorial.s:27
[Inferior 1 (process 8304) exited with code 030]
# Instructions executed: 52
```

The command `next` goes inside of the `_factorial` function only one time then it never goes inside, the total number of executed instructions was 18. The command `until` and `step` goes inside of every `_factorial` function, the difference is that `until` step program until past the current line or past a location, and the `step` until it reaches a different source line. The differences about instructions executed are 31 versus 52 respectively.

F.3 GDB Quick-Reference

This quick-reference table is copyright 2002 Robert M. Dondero, Jr., and is used by permission in this book. Parameters listed in brackets are optional. Here is another GDB quick reference created by Free Software Foundation.

Table F-1. Common GDB Debugging Commands

F.3.1 Miscellaneous

quit

Exit GDB.

help [cmd]

Print description of debugger command `cmd`. Without `cmd`, prints a list of topics.

directory [dir1] [dir2]...

Add directories `dir1`, `dir2`, etc. to the list of directories searched for source files.

F.3.2 Running the Program

run [arg1] [arg2]...

Run the program with command line arguments `arg1`, `arg2`, etc.

set args arg1 [arg2]...

Set the program's command-line arguments to `arg1`, `arg2`, etc.

show args

Print the program's command-line arguments.

F.3.3 Using Breakpoints

info breakpoints

Print a list of all breakpoints and their numbers (breakpoint numbers are used for other breakpoint commands).

break *linenum*

Set a breakpoint at line number *linenum*.

break **addr*

Set a breakpoint at memory address *addr*.

break *fn*

Set a breakpoint at the beginning of function *fn*.

condition *bpnum expr*

Break at breakpoint *bpnum* only if expression *expr* is non-zero.

command [*bpnum*] *cmd1* [*cmd2*]...

Execute commands `cmd1`, `cmd2`, etc. whenever breakpoint *bpnum* (or the current breakpoint) is hit.

continue

Continue executing the program.

kill

Stop executing the program.

delete [*bpnum1*] [*bpnum2*]...

Delete breakpoints *bpnum1*, *bpnum2*, etc., or all breakpoints if none specified.

clear **addr*

Clear the breakpoint at memory address *addr*.

clear [*fn*]

Clear the breakpoint at function *fn*, or the current breakpoint.

clear *linenum*

Clear the breakpoint at line number *linenum*.

disable [*bpnum1*] [*bpnum2*]...

Disable breakpoints *bpnum1*, *bpnum2*, etc., or all breakpoints if none specified.

enable [*bpnum1*] [*bpnum2*]...

Enable breakpoints *bpnum1*, *bpnum2*, etc., or all breakpoints if none specified.

F.3.4 Stepping through the Program

nexti

"Step over" the next instruction (doesn't follow function calls).

stepi

"Step into" the next instruction (follows function calls).

finish

"Step out" of the current function.

F.3.5 Examining Registers and Memory

info registers

Print the contents of all registers.

print/*f* *$reg*

Print the contents of register *$reg* using format *f*.The format can be *x* (hexadecimal), *u* (unsigned decimal), *o* (octal), *a* (address), *c* (character), *s* (string), or *f* (floating point).

x/*rsf* *addr*

Print the contents of memory address *addr* using repeat count *r*, size *s*, and format *f*. Repeat count defaults to 1 if not specified. Size can be *b* (byte), *h* (halfword), *w* (word), or *g* (double word). Size defaults to word if not specified. Format is the same as for print, with the additions of *s* (string) and *i* (instruction). For example `x/5i $eip` should display 5 instructions or `x/4bs 0x56559004` it will be display four bits in this specific memory address.

info display

Shows a numbered list of expressions set up to display automatically at each break.

display/*f* *$reg*

At each break, print the contents of register *reg* using format *f*.

display/*si* *addr*

At each break, print the contents of memory address *addr* using size *s* (same options as for the x command).

display/*ss* *addr*

At each break, print the string of size *s* that begins in memory address *addr*.

undisplay *displaynum*

Remove *displaynum* from the display list.

F.3.6 Examining the Call Stack

where

Print the call stack.

backtrace

Print the call stack.

frame

Print the top of the call stack.

up

Move the context toward the bottom of the call stack.

down

Move the context toward the top of the call stack.

G. Document History

- 11/24/2026 - Version 4.0 - Israel Roldan (AirvZxf). Started the x86-64 edition from Version 3.0 of the x86 32-bit edition: renamed the Modified Version to *Assembly from the Ground Up: x86-64 Edition*, as required by the GNU Free Documentation License, and pointed the copyright page, the links and the website to this edition. The text and the examples are being ported to 64-bit Linux programs: AT&T syntax with the GNU Assembler, the `syscall` instruction and the System V AMD64 calling convention.
- 11/23/2026 - Version 3.0 - Israel Roldan (AirvZxf). Renamed the Modified Version to *Assembly from the Ground Up: x86 32-bit Edition*, as required by the GNU Free Documentation License, and rewrote the copyright page to credit the original edition and point to the transparent copy of this edition. Replaced the links to unauthorized copies of other books in Chapter 13 with links to the books' catalog pages. Fixed spelling mistakes and duplicated words across the book and the examples. Added Appendix K with solutions to the review questions of Chapters 2 to 12, with tested example programs. Fixed two bugs in the examples: the memory manager jumped to the wrong label when a region was in use, and two records of `006-01-write-records` had the wrong size. Corrected the description of the bits of a floating-point number in Chapter 10, and grammar mistakes found with LanguageTool. The PDF edition is now typeset with Typst instead of LaTeX, and the book is built with Quarto: the website has one page per chapter, with search and download links for the PDF, ePUB and example source code.
- 12/15/2020 - Version 2.1 - Israel Roldan (AirvZxf) convert the DocBook to a Pandoc's Markdown then it will export to ePUB, PDF, HTML and GitHub Markdown, could be extended to other types of documents. This version fixed some minimal details, convert graphical tables to ASCII tables, update the links from some broken web sites, minor updates was done also extended sub-topics to clarify.
- 04/18/2004 - Version 1.1 - Lots of minor updates based on reader comments. Made cleared distinction between dynamic and shared libraries.
- 01/31/2004 - Version 1.0 - Rewrote chapter 9. Added full index. Lots of minor corrections.
- 01/29/2004 - Version 0.9 - Lots of editing of all chapters. Made code more consistent and made explanations clearer. Added some illustrations.
- 01/22/2004 - Version 0.8 - Finished GDB appendix, mostly finished w/ appendix of x86 instructions, added section on planning programs, added lots of review questions, and got everything to a completed, initial draft state.
- 01/11/2004 - Version 0.7 - Added C translation appendix, added the beginnings of an appendix of x86 instructions, added the beginnings of a GDB appendix, finished out the files chapter, finished out the counting chapter, added a records chapter, created a source file of common Linux definitions, corrected several errors, and lots of other fixes
- 07/18/2003 - Version 0.6 - Added ASCII appendix, finished the discussion of the CPU in the Memory chapter, reworked exercises into a new format, corrected several errors. Thanks to Harald Korneliussen for the many suggestions and the ASCII table.
- 12/17/2002 - Version 0.5 - Initial posting of book under GNU FDL

H. GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other written document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. The “Document”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “you”.

A “Modified Version” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “Secondary Section” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (For example, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “Invariant Sections” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, whose contents can be viewed and edited directly and straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup has been designed to thwart or discourage subsequent modification by readers is not Transparent. A copy that is not “Transparent” is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML designed for human modification. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies of the Document numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a publicly-accessible computer-network location containing a complete Transparent copy of the Document, free of added material, which the general network-using public has access to download anonymously at no charge using public-standard network protocols. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- **A.**

  Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

- **B.**

  List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has less than five).

- **C.**

  State on the Title Page the name of the publisher of the Modified Version, as the publisher.

- **D.**

  Preserve all the copyright notices of the Document.

- **E.**

  Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

- **F.**

  Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

- **G.**

  Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

- **H.**

  Include an unaltered copy of this License.

- **I.**

  Preserve the section entitled “History”, and its title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section entitled “History” in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

- **J.**

  Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the “History” section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

- **K.**

  In any section entitled “Acknowledgements” or “Dedications”, preserve the section's title, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

- **L.**

  Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

- **M.**

  Delete any section entitled “Endorsements”. Such a section may not be included in the Modified Version.

- **N.**

  Do not retitle any existing section as “Endorsements” or to conflict in title with any Invariant Section.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section entitled “Endorsements”, provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version .

`5. COMBINING DOCUMENTS`

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections entitled "History" in the various original documents, forming one section entitled "History"; likewise combine any sections entitled "Acknowledgements", and any sections entitled "Dedications". You must delete all sections entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, does not as a whole count as a Modified Version of the Document, provided no compilation copyright is claimed for the compilation. Such a compilation is called an "aggregate", and this License does not apply to the other self-contained works thus compiled with the Document , on account of their being thus compiled, if they are not themselves derivative works of the Document. If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one quarter of the entire aggregate, the Document's Cover Texts may be placed on covers that surround only the Document within the aggregate. Otherwise they must appear on covers around the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License provided that you also include the original English version of this License. In case of a disagreement between the translation and the original English version of this License, the original English version will prevail.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

Addendum

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright © YEAR YOUR NAME.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have no Invariant Sections, write "with no Invariant Sections" instead of saying which ones are invariant. If you have no Front-Cover Texts, write "no Front-Cover Texts" instead of "Front-Cover Texts being LIST"; likewise for Back-Cover Texts.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

I. Personal Dedication

There are so many people I could thank. I will name here but a few of the people who have brought me to where I am today. The many family members, Sunday School teachers, youth pastors, school teachers, friends, and other relationships that God has brought into my life to lead me, help me, and teach me are too many to count. This book is dedicated to you all.

There are some people, however, that I would like to thank specifically.

First of all, I want to thank the members of the Vineyard Christian Fellowship Church in Champaign, Illinois for everything that you have done to help me and my family in our times of crisis. It's been a long time since I've seen or heard from any of you, but I think about you always. You have been such a blessing to me, my wife, and Daniel, and I could never thank you enough for showing us Christ's love when we needed it most. I thank God every time I think of you - I thank Him for bringing you all to us in our deepest times of need. Even out in the middle of Illinois with no friends of family, God showed that He was still watching after us. Thank you for being His hands on Earth. Specifically, I'd like to thank Joe and Rhonda, Pam and Dell, and Herschel and Vicki. There were many, many others, too - so many people helped us that it would be impossible to list them all.

I also want to thank my parents, who gave me the example of perseverance and strength in hard times. Your example has helped me be a good father to my children, and a good husband to my wife.

I also want to thank my wife, who even from when we first started dating encouraged me to seek God in everything. Thank you for your support in writing this book, and more importantly, for your support in being obedient to God.

I also want to thank the Little Light House school. My entire family is continually blessed by the help you give to our son.

I also want to thank Joe and D.A. Thank you for taking a chance on me in ministry. Being able to be a part of God's ministry again has helped me in so many ways.

You all have given me the strength I needed to write this book over the last few years. Without your support, I would have been too overwhelmed by personal crises to even think about anything more than getting through a day, much less putting this book together. You have all been a great blessing to me, and I will keep you in my prayers always.

J. Updated by AirvZxf

I'm Israel Roldan and I try to learn the GNU Assembler (`as` or `gas`) and I didn't find many resources but this book is great.

This is the x86-64 edition of the book, for 64-bit programs. It is based on the x86 32-bit edition, which is maintained in its own repository.

All the information is in my GitHub repository. To check the advance on this project and the pending reviews go to the TO-DO's list. I added some script to compile the source files, emulating to i386/x86.

J.1 Motivations

- I believe that Linux is the future, I dream with a world when everyone is using Linux in our laptops, desktop computers, and all the video game companies make perfect games for Linux.
- I was researching about GNU Assembler ("as" or "gas") but unfortunately, there are not many resources, these resources talk about the most popular as "NASM" and "FASM".
- Why NOT focus on "NASM" or "FASM"? I started with "NASM" then I saw a few years ago the active development stopped. I researched about "FASM" and looks like it's awesome but then I discovered some curious detail. These assemblers can compile in many architectures and it is powerful but trying to be very compatible they spend a lot of effort to create the most generic binary source possible ([53]). At this moment I start to consider the possibility to use the pure Linux assembler because for me the idea to use a multi-architectural assembler is only marketing. I have been software developer over 14 years and I never created a multi-architecture system neither in my personal projects. Why am I living in a utopia? Wanted a tool to convert to other architectures, if I always create programs for Linux and very rarely for Windows. In these cases I usually use Python or Java. Note: This is my personal point of view, haters please hate more.
- Why use Assembler rather other languages programs? The benchmarks that I did demonstrate that Assembler is the most powerful even tan C which is the top language. My benchmarks and the C benchmarks.
- Why update this book? This book is one of the best that I found but it has many areas of opportunity. I read until the chapter 3 and I had three doubts in the final exercises but there are no answers. The book said that we saw this subject and I reviewed all the chapters and it didn't.
- Deep thanks to the men and companies who inspired me to be better and thanks to the Open Source: Linus Torvalds, Richard Stallman, Linux, GNU, GitHub.

[53] FASM: Design Principles, or Why FASM Is Different sections "4) Resolving The Code" and "5) Complex Solutions With Simple Features". In general this document provides an overview of the complexity behind trying to do an assembler multi-architecture.

K. Solutions to the Review Questions

This appendix was added in this edition. It answers the review questions at the end of each chapter (Chapter 13 has none). Every program in it is included with the examples, in the `resource/asm/` directory: `make.bash` assembles and links all of them, and `test.bash` runs each one and checks its exit status, its output or the files it creates, so the results shown here are the real ones.

Some questions ask you to research a topic, to use a program of your own choice, or to contact other people. For those, this appendix gives a short answer and a way to start, but the exercise is yours.

To run the programs that read or write `test.dat`, create the file first with `006-01-write-records`. The programs that use the C library or a shared library are linked as shown in `make.bash`.

K.1 Chapter 2. Computer Architecture

K.1.1 Know the Concepts

- **Describe the fetch-execute cycle.** The CPU reads the instruction stored at the address held by the instruction pointer, decodes it to find out what it must do and which operands it needs, fetches those operands from registers or memory, executes the operation (usually in the arithmetic and logic unit), and stores the result. Then the instruction pointer moves to the next instruction, unless the instruction was a jump, and the cycle starts again.
- **What is a register? How would computation be more difficult without registers?** A register is a small storage location inside the CPU itself. The CPU works on registers much faster than on memory. Without registers, every intermediate value would have to be written to and read back from memory, which is slower, and every instruction would need to carry full memory addresses for all of its operands, which makes instructions larger.
- **How do you represent numbers larger than 255?** By using several bytes together. On x86, four bytes form a word, which can hold unsigned values up to 4294967295. Larger numbers use several words.
- **How big are the registers on the machines we will be using?** Four bytes (32 bits).
- **How does a computer know how to interpret a given byte or set of bytes of memory?** It doesn't. Memory only holds numbers. Whether they are an instruction, a number, an address or a character depends entirely on how the program uses them. If the instruction pointer points to them, they are executed as instructions.
- **What are the addressing modes and what are they used for?** Addressing modes are the ways an instruction can find its data: *immediate* (the value is inside the instruction), *register* (the value is in a register), *direct* (the instruction contains the memory address), *indexed* (a base address plus an index register multiplied by the element size, used for lists), *indirect* (a register holds the address) and *base pointer* (a register holds an address and the instruction adds a fixed offset, used for records and for the stack).
- **What does the instruction pointer do?** It holds the address of the next instruction to execute.

K.1.2 Use the Concepts

- **What data would you use in an employee record? How would you lay it out in memory?** For example, an identifier, a name, a department number, a salary and a hire date, stored one after the other with fixed sizes, so that each field is always at the same offset from the start of the record:

```
Offset  Size  Field
0       4     Employee ID
4       40    Name (padded with zeros)
44      4     Department number
48      4     Salary
52      4     Hire date (days since 1970-01-01)
56            Total size of the record
```

- **If I had the pointer to the beginning of the employee record above, and wanted to access a particular piece of data inside of it, what addressing mode would I use?** Base pointer addressing: the register holds the address of the record and the instruction adds the offset of the field. For example, `movl 48(%ebx), %eax` loads the salary.
- **Base pointer addressing, register 3122, offset 20:** 3122 + 20 = **3142**.
- **Indexed addressing, base 6512, index 5, multiplier 4:** 6512 + 5 × 4 = **6532**.
- **Indexed addressing, base 123472, index 0, multiplier 4:** 123472 + 0 × 4 = **123472**.
- **Indexed addressing, base 9123478, index 20, multiplier 1:** 9123478 + 20 × 1 = **9123498**.

K.1.3 Going Further

- **What are the minimum number of addressing modes needed for computation?** In theory, very few: a way to put constants into registers (immediate) and a way to reach memory through an address held in a register (indirect). Every other mode can be emulated by computing the address with arithmetic instructions first and then using indirect addressing. Many RISC processors work this way, with only a handful of addressing modes.
- **Why include addressing modes that aren't strictly needed?** Because they make programs shorter and faster. Indexed addressing, for example, does in one instruction what would otherwise take a multiplication, an addition and a load, and it doesn't use an extra register to hold the computed address.
- **How does pipelining affect the fetch-execute cycle?** With pipelining, the CPU doesn't wait for one instruction to finish before starting the next one. While one instruction executes, the next one is being decoded and the one after it is being fetched, like an assembly line. This multiplies throughput, but it causes problems when an instruction needs the result of one that hasn't finished yet, or when a jump changes the instruction pointer and the instructions already in the pipeline must be thrown away. Processors use branch prediction and out-of-order execution to reduce these costs.
- **Tradeoffs between fixed-length and variable-length instructions.** Fixed-length instructions (for example 4 bytes in most ARM and RISC-V code) are easy and fast to decode, and several can be decoded in parallel, but simple instructions waste space. Variable-length instructions (1 to 15 bytes on x86) make programs smaller and leave room to add new instructions over time, but the decoder is much more complex, because the CPU doesn't know where the next instruction starts until it has decoded the current one.

K.2 Chapter 3. Your First Programs

K.2.1 Know the Concepts

- **What does it mean if a line in the program starts with the '#' character?** It is a comment. The assembler ignores everything from the # to the end of the line.
- **What is the difference between an assembly language file and an object code file?** The assembly language file (`.s`) is text that a person writes. The object file (`.o`) is the machine code that the assembler generates from it. It can't run yet, because it still has to be linked.
- **What does the linker do?** It joins one or more object files, resolves the symbols that one file uses and another defines, assigns the final memory addresses, and writes an executable file that the operating system can load.

- **How do you check the result status code of the last program you ran?** With `echo $?`.
- **What is the difference between `movl $1, %eax` and `movl 1, %eax`?** The first uses immediate addressing and loads the number 1 into *%eax*. The second uses direct addressing and loads the four bytes stored at memory address 1. That address isn't mapped, so the program would crash with a segmentation fault.
- **Which register holds the system call number?** *%eax*.
- **What are indexes used for?** To select one element of a list by its position, counting from the start of the list.
- **Why do indexes usually start at 0?** Because the index is really the distance from the start of the list. The first element is zero elements away from the start, so its address is the base address plus 0 × the size of an element.
- **If I issued the command `movl data_items(,%edi,4), %eax` and data_items was address 3634 and *%edi* held the value 13, what address would you be using to move into *%eax*?** 3634 + 13 × 4 = **3686**.
- **List the general-purpose registers.** *%eax*, *%ebx*, *%ecx*, *%edx*, *%edi* and *%esi*.
- **What is the difference between `movl` and `movb`?** `movl` moves a long, which is four bytes (a word); `movb` moves a single byte.
- **What is flow control?** Deciding which instruction runs next. Instead of always running the next instruction in memory, a program uses jumps to repeat code (loops) or to skip code (conditions).
- **What does a conditional jump do?** It looks at the result of a previous comparison, stored in the *%eflags* register. If the condition is true, it jumps to the given label; otherwise the program continues with the next instruction.
- **What things do you have to plan for when writing a program?** Where the data is stored, what each register holds, the initial values, how a loop knows when to stop, special cases (such as an empty list or the first element), and how the program returns its result.
- **Go through every instruction and list what addressing mode is being used for each operand.** In `003-01-exit`:

```
movl $1, %eax     immediate, register
movl $0, %ebx     immediate, register
int  $0x80        immediate
```

In `003-02-maximum`:

```
movl $0, %edi                   immediate, register
movl data_items(,%edi,4), %eax  indexed, register
movl %eax, %ebx                 register, register
cmpl $0, %eax                   immediate, register
je   _loop_exit                 jump target (label)
incl %edi                       register
movl data_items(,%edi,4), %eax  indexed, register
cmpl %ebx, %eax                 register, register
jle  _start_loop                jump target (label)
movl %eax, %ebx                 register, register
jmp  _start_loop                jump target (label)
movl $1, %eax                   immediate, register
int  $0x80                      immediate
```

K.2.2 Use the Concepts

Modify the first program to return the value 3. Only the status code in *%ebx* changes:

```
        # Assemble with `as --32` and `ld -m elf_i386`.
        #
        # PURPOSE:
        #     Solution to Chapter 3, "Use the Concepts":
        #     the first program, returning 3 instead of 0.
        #
        # OUTPUT:
        #     Exit status code 3. Check it with `echo $?`.
        #
        .section .data

        .section .text
            .globl _start

    _start:
        movl $1, %eax      # exit() system call number.
        movl $3, %ebx      # Status code returned to the
                           # shell.
        int  $0x80         # Call the kernel.
```

```
as -o 0AK-03-01-exit-3.o --32 0AK-03-01-exit-3.s
ld -o 0AK-03-01-exit-3 -m elf_i386 0AK-03-01-exit-3.o
./0AK-03-01-exit-3
echo $?
```

It prints 3.

Modify the `003-02-maximum` program to find the minimum instead. Changing `jle` to `jge` is not enough. The original loop compares each item before checking whether it is the terminating 0. For the maximum that doesn't matter, because 0 is never bigger than the maximum, but for the minimum the 0 would always win. The solution checks for the end of the list right after loading each item:

```
        # Assemble with `as --32` and `ld -m elf_i386`.
        #
        # PURPOSE:
        #     Solution to Chapter 3, "Use the Concepts":
        #     find the minimum number of a set of data
        #     items. A 0 terminates the data.
        #
        # VARIABLES:
        #     %edi - Index of the data item being examined.
        #     %ebx - Smallest data item found.
        #     %eax - Current data item.
        #
        # NOTE:
        #     The terminator must be checked BEFORE the
        #     comparison. Otherwise the final 0 would be
        #     taken as the smallest number of the list.
        #
        .section .data
            data_items:
                .long 3, 67, 34, 222, 45, 22, 11, 125, 0

        .section .text
            .globl _start
```

```
24
25  _start:
26      movl $0, %edi            # Start at index 0.
27      movl data_items(,%edi,4), %eax
28      movl %eax, %ebx          # The first item is the
29                               # smallest so far.
30
31  _start_loop:
32      incl %edi                # Load the next item.
33      movl data_items(,%edi,4), %eax
34      cmpl $0, %eax            # End of the list?
35      je   _loop_exit
36      cmpl %ebx, %eax          # Compare with the
37      jge  _start_loop         # smallest; skip it if
38                               # it is not smaller.
39      movl %eax, %ebx          # New smallest value.
40      jmp  _start_loop
41
42  _loop_exit:
43      movl $1, %eax            # exit(); %ebx holds
44      int  $0x80               # the minimum.
```

It returns 3.

Modify the `003-02-maximum` program to use the number 255 to end the list rather than the number 0. The same issue appears here: 255 is bigger than every item, so the end of the list has to be checked before the comparison. As a bonus, 0 is now a valid item:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 3, "Use the Concepts":
5       #     find the maximum number of a set of data
6       #     items. A 255 terminates the data, so 0 is
7       #     now a valid item.
8       #
9       # VARIABLES:
10      #     %edi - Index of the data item being examined.
11      #     %ebx - Largest data item found.
12      #     %eax - Current data item.
13      #
14      .section .data
15          data_items:
16              .long 3, 67, 34, 0, 45, 22, 11, 125, 255
17
18      .section .text
19          .globl _start
20
21  _start:
22      movl $0, %edi            # Start at index 0.
23      movl data_items(,%edi,4), %eax
24      movl %eax, %ebx          # The first item is the
25                               # largest so far.
26
27  _start_loop:
```

```
    incl %edi               # Load the next item.
    movl data_items(,%edi,4), %eax
    cmpl $255, %eax         # End of the list?
    je   _loop_exit         # (Checked first, or
                            # 255 would win.)
    cmpl %ebx, %eax
    jle  _start_loop
    movl %eax, %ebx         # New largest value.
    jmp  _start_loop

_loop_exit:
    movl $1, %eax           # exit(); %ebx holds
    int  $0x80              # the maximum.
```

It returns 125.

Modify the `003-02-maximum` program to use an ending address rather than the number 0 to know when to stop. The label `data_end` marks the first address after the list. The program walks the list with a pointer in *%ecx* (indirect addressing) and stops when it reaches `data_end`:

```
    # Assemble with `as --32` and `ld -m elf_i386`.
    #
    # PURPOSE:
    #     Solution to Chapter 3, "Use the Concepts":
    #     find the maximum number of a set of data
    #     items, stopping at an ending address
    #     instead of a terminating number.
    #
    # VARIABLES:
    #     %ecx - Address of the data item examined.
    #     %ebx - Largest data item found.
    #     %eax - Current data item.
    #
    .section .data
        data_items:
            .long 3, 67, 34, 222, 45, 22, 11, 125
        data_end:           # First address AFTER
                            # the last item.

    .section .text
        .globl _start

_start:
    movl $data_items, %ecx  # Address of item 0.
    movl (%ecx), %ebx       # The first item is the
                            # largest so far.

_start_loop:
    addl $4, %ecx           # Next item (4 bytes).
    cmpl $data_end, %ecx    # Past the last item?
    je   _loop_exit
    movl (%ecx), %eax       # Indirect addressing.
    cmpl %ebx, %eax
    jle  _start_loop
    movl %eax, %ebx         # New largest value.
```

```
36      jmp  _start_loop
37
38  _loop_exit:
39      movl $1, %eax            # exit(); %ebx holds
40      int  $0x80               # the maximum.
```

It returns 222.

Modify the `003-02-maximum` program to use a length count rather than the number 0 to know when to stop. The number of items is stored in `data_length`, and the loop stops when the index reaches it:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 3, "Use the Concepts":
5       #     find the maximum number of a set of data
6       #     items, using a length count instead of a
7       #     terminating number.
8       #
9       # VARIABLES:
10      #     %edi - Index of the data item being examined.
11      #     %ebx - Largest data item found.
12      #     %eax - Current data item.
13      #
14      .section .data
15          data_length:         # Number of items.
16              .long 8
17          data_items:
18              .long 3, 67, 34, 222, 45, 22, 11, 125
19
20      .section .text
21          .globl _start
22
23  _start:
24      movl $0, %edi            # Start at index 0.
25      movl data_items(,%edi,4), %ebx
26                               # The first item is the
27                               # largest so far.
28
29  _start_loop:
30      incl %edi                # Next index.
31      cmpl data_length, %edi   # index == length?
32      je   _loop_exit
33      movl data_items(,%edi,4), %eax
34      cmpl %ebx, %eax
35      jle  _start_loop
36      movl %eax, %ebx          # New largest value.
37      jmp  _start_loop
38
39  _loop_exit:
40      movl $1, %eax            # exit(); %ebx holds
41      int  $0x80               # the maximum.
```

It returns 222.

What would the instruction `movl _start, %eax` do? How would this differ from `movl $_start, %eax`? `movl _start, %eax` uses direct addressing: it loads the four bytes stored *at* the address `_start`, which are

the machine code of the first instruction. In `003-02-maximum`, the first instruction `movl $0, %edi` is encoded as the bytes `bf 00 00 00 00`, so *%eax* would get `0x000000bf` (191). `movl $_start, %eax` uses immediate addressing: it loads the address `_start` itself, which is `0x08049000` in that program.

K.2.3 Going Further

Modify the first program to leave off the `int` instruction line. What error message do you get? Why?

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 3, "Going Further":
5       #     the first program without the `int`
6       #     instruction. It crashes on purpose.
7       #
8       .section .data
9
10      .section .text
11          .globl _start
12
13  _start:
14      movl $1, %eax      # exit() system call number.
15      movl $0, %ebx      # Status code.
16                         # No `int $0x80`: the kernel
17                         # is never called, so the CPU
18                         # keeps executing whatever
19                         # bytes follow in memory.
```

```
as -o 0AK-03-06-exit-without-int.o --32 0AK-03-06-exit-without-int.s
ld -o 0AK-03-06-exit-without-int -m elf_i386 0AK-03-06-exit-without-int.o
./0AK-03-06-exit-without-int
echo $?
```

The shell prints `Segmentation fault (core dumped)` and `echo $?` prints `139` (128 + 11, where 11 is the number of the `SIGSEGV` signal). Without `int $0x80`, the kernel is never asked to end the program. The CPU doesn't know that the program is over, so it keeps executing whatever bytes come after the last instruction. Those bytes are not valid code for this program, and sooner or later one of them accesses memory the program isn't allowed to touch, so the kernel stops it.

Which approach to finding the end of the list is best? Which would you use if you knew that the list was sorted? It depends on the data:

- A special terminating number is simple, but that number can never be a real item, and the program must read the whole list to know its length.
- An ending address or a length count allow any value in the list, and they make an empty list easy to detect. A length count is the easiest to work with, because it also tells you how many items there are without reading them.
- If the list is sorted, you don't need a loop at all. In ascending order, the maximum is the last item and the minimum is the first. With a length count (or an ending address) you can jump straight to the last item: `data_items + (length - 1) × 4`. With a terminating number you would still have to walk the whole list to find the end.

K.3 Chapter 4. All About Functions

K.3.1 Know the Concepts

- **What are primitives?** The basic operations that a language or a system provides directly, from which everything else is built. In assembly language, the primitives are the processor instructions and the system calls.
- **What are calling conventions?** The rules that a function and its caller agree on: how parameters are passed (on the stack, in reverse order), where the return value goes (*%eax*), which registers the function may change, and who removes the parameters from the stack (the caller).
- **What is the stack?** A region at the top of memory that grows down, used to store data in last-in, first-out order: return addresses, parameters, saved registers and local variables. *%esp* always points to its top.
- **How do `pushl` and `popl` affect the stack? What special-purpose register do they affect?** `pushl` subtracts 4 from *%esp* and stores the value at the new top; `popl` reads the value at the top and adds 4 to *%esp*. Both change the stack pointer, *%esp*.
- **What are local variables and what are they used for?** Variables that exist only while a function runs, stored in the function's stack frame below *%ebp*. They hold the function's intermediate results without touching the data of the rest of the program.
- **Why are local variables so necessary in recursive functions?** Because each call needs its own copy of its data. If a recursive function used global variables, each new call would overwrite the values of the calls still waiting for it to return.
- **What are *%ebp* and *%esp* used for?** *%esp* points to the top of the stack. *%ebp* (the base pointer) is set to the value of *%esp* when a function starts, and stays fixed while the function runs, so parameters (`8(%ebp)`, `12(%ebp)`, ...) and local variables (`-4(%ebp)`, ...) are always at the same offsets.
- **What is a stack frame?** The part of the stack that belongs to one function call: its parameters, the return address, the saved *%ebp* of the caller and its local variables.

K.3.2 Use the Concepts

Write a function called `square` and a program to test it. The function multiplies its argument by itself with `imull`:

```
1        # Assemble with `as --32` and `ld -m elf_i386`.
2        #
3        # PURPOSE:
4        #     Solution to Chapter 4, "Use the Concepts":
5        #     a `_square` function and a program that
6        #     tests it with the number 12.
7        #
8        # OUTPUT:
9        #     Exit status code 144 (12 * 12).
10       #
11       .section .data
12
13       .section .text
14           .globl _start
15
16   _start:
17       pushl $12               # Argument.
18       call  _square
19       addl  $4, %esp          # Remove the argument.
20
```

```
21      movl  %eax, %ebx         # Result as the status.
22      movl  $1, %eax           # exit()
23      int   $0x80
24
25      # PURPOSE:
26      #     Return the square of a number.
27      #
28      # INPUT:
29      #     First argument - The number.
30      #
31      # OUTPUT:
32      #     %eax - The number multiplied by itself.
33      #
34          .type _square, @function
35  _square:
36      pushl %ebp               # Standard function
37      movl  %esp, %ebp         # prologue.
38
39      movl  8(%ebp), %eax      # %eax = argument.
40      imull %eax, %eax         # %eax = %eax * %eax.
41
42      movl  %ebp, %esp         # Standard function
43      popl  %ebp               # epilogue.
44      ret
```

It returns 144.

Convert the maximum program into a function, and call it with 3 different lists. The function receives the address of the list in its parameter, and walks the list with indirect addressing:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 4, "Use the Concepts":
5       #     the maximum program as a function that
6       #     receives a pointer to a list of numbers
7       #     ended by 0, called with 3 different lists.
8       #
9       # OUTPUT:
10      #     The maximum of the last list (99) as the
11      #     exit status code.
12      #
13      .section .data
14          list_1:
15              .long 3, 67, 34, 222, 45, 0
16          list_2:
17              .long 5, 4, 3, 2, 1, 0
18          list_3:
19              .long 10, 99, 18, 50, 0
20
21      .section .text
22          .globl _start
23
24  _start:
25      pushl $list_1
```

```
26      call  _maximum           # %eax = 222
27      addl  $4, %esp
28
29      pushl $list_2
30      call  _maximum           # %eax = 5
31      addl  $4, %esp
32
33      pushl $list_3
34      call  _maximum           # %eax = 99
35      addl  $4, %esp
36
37      movl  %eax, %ebx         # Last result as the
38      movl  $1, %eax           # status code.
39      int   $0x80
40
41      # PURPOSE:
42      #     Find the largest number of a list.
43      #
44      # INPUT:
45      #     First argument - Address of the list. The
46      #     list ends with a 0.
47      #
48      # OUTPUT:
49      #     %eax - The largest number (0 if the list
50      #     is empty).
51      #
52      # VARIABLES:
53      #     %edx - Address of the current item.
54      #     %ecx - Current item.
55      #
56          .type _maximum, @function
57  _maximum:
58      pushl %ebp
59      movl  %esp, %ebp
60
61      movl  8(%ebp), %edx      # Address of item 0.
62      movl  (%edx), %eax       # Largest so far.
63
64  _maximum_loop:
65      movl  (%edx), %ecx       # Current item.
66      cmpl  $0, %ecx           # End of the list?
67      je    _maximum_end
68      cmpl  %eax, %ecx
69      jle   _maximum_next
70      movl  %ecx, %eax         # New largest value.
71  _maximum_next:
72      addl  $4, %edx           # Next item.
73      jmp   _maximum_loop
74
75  _maximum_end:
76      movl  %ebp, %esp
77      popl  %ebp
78      ret
```

It returns 99, the maximum of the third list.

Explain the problems that would arise without a standard calling convention. Every function could expect its parameters in different places, return its result in a different register and destroy different registers. You would have to read the code of every function before calling it, functions written by different people (or in different languages, or in libraries) couldn't call each other, and any change in one function could break all its callers.

K.3.3 Going Further

- **Is it better to have a large set of primitives or a small one?** A small set is easier to learn, to implement and to make correct and fast; a large set makes programs shorter and lets each operation be optimized on its own. Most systems choose a small set of primitives plus libraries built on top of them, which gives most of the benefits of both.
- **Write the factorial function non-recursively.** A loop multiplies the result by `n`, `n - 1`, ..., 2:

```
1        # Assemble with `as --32` and `ld -m elf_i386`.
2        #
3        # PURPOSE:
4        #     Solution to Chapter 4, "Going Further":
5        #     the factorial function without recursion.
6        #     It returns the factorial of 5.
7        #
8        # OUTPUT:
9        #     Exit status code 120.
10       #
11       .section .data
12
13       .section .text
14           .globl _start
15
16   _start:
17       pushl $5
18       call  _factorial
19       addl  $4, %esp
20
21       movl  %eax, %ebx
22       movl  $1, %eax
23       int   $0x80
24
25       # PURPOSE:
26       #     Compute n! with a loop:
27       #     result = 1; while (n > 1) result *= n--;
28       #
29       # INPUT:
30       #     First argument - n.
31       #
32       # OUTPUT:
33       #     %eax - n! (1 for n = 0 or 1).
34       #
35           .type _factorial, @function
36   _factorial:
37       pushl %ebp
38       movl  %esp, %ebp
39
```

```
40      movl  $1, %eax          # Result.
41      movl  8(%ebp), %ecx     # Counter = n.
42
43  _factorial_loop:
44      cmpl  $1, %ecx          # Done when n <= 1.
45      jle   _factorial_end
46      imull %ecx, %eax        # result *= n
47      decl  %ecx              # n--
48      jmp   _factorial_loop
49
50  _factorial_end:
51      movl  %ebp, %esp
52      popl  %ebp
53      ret
```

It returns `120`. It uses no stack space per step, so it can't run out of stack for large numbers (although the result overflows 32 bits after 12!).

- **Break a feature of an application into functions.** This exercise is yours. As an example, the "save file" feature of a text editor could be: `choose_file_name(suggested) -> name`, `serialize(document) -> bytes`, `write_file(name, bytes) -> status` and `report_error(status)`.
- **Come up with your own calling convention.** This program passes the parameters in registers instead of the stack:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 4, "Going Further":
5       #     the power program (2^3 + 5^2) with a custom
6       #     calling convention that uses registers
7       #     instead of the stack.
8       #
9       # CALLING CONVENTION:
10      #     %ebx - Base (first parameter).
11      #     %ecx - Power (second parameter).
12      #     %eax - Return value.
13      #     The function may change %ecx and %edx; it
14      #     preserves %ebx and every other register.
15      #
16      # OUTPUT:
17      #     Exit status code 33.
18      #
19      .section .data
20
21      .section .text
22          .globl _start
23
24  _start:
25      movl  $2, %ebx          # 2^3
26      movl  $3, %ecx
27      call  _power
28      movl  %eax, %edi        # Save the result.
29
```

```
30      movl  $5, %ebx          # 5^2
31      movl  $2, %ecx
32      call  _power
33
34      addl  %edi, %eax        # 8 + 25
35      movl  %eax, %ebx
36      movl  $1, %eax
37      int   $0x80
38
39          .type _power, @function
40  _power:
41      movl  $1, %eax          # Result.
42  _power_loop:
43      cmpl  $0, %ecx          # Done when power = 0.
44      je    _power_end
45      imull %ebx, %eax
46      decl  %ecx
47      jmp   _power_loop
48  _power_end:
49      ret                     # No stack frame needed.
```

It returns `33`, the same as `004-01-power`.

- **Can you build a calling convention without using the stack?** Yes, for example with registers (as above) or with a fixed memory area for each function. The limitations: there are only a few registers, so the number of parameters is limited; the caller must save any register it still needs; and, above all, recursion doesn't work without extra work, because a function can only store one return address and one set of parameters at a time.
- **What test cases should we use for the example program?** The simplest cases (`power(2, 0)` = 1, `power(0, 3)` = 0, `power(1, 5)` = 1), normal cases with known answers (`power(2, 3)` = 8), and the limits: results that don't fit in 32 bits, or in the 8 bits of the exit status (`power(2, 8)` = 256 returns 0). Also check what happens with a negative power, which this function doesn't support.

  These tests find a real bug: `_power` stops when the power reaches 1, so with a power of 0 it counts down past 0, wraps around and loops about four billion times. Changing the program to compute `power(2, 0) + power(5, 0)` takes several seconds and returns 1 instead of 2. The register version above checks for 0 at the start of the loop, so it returns 1 for any number to the power 0.

K.4 Chapter 5. Dealing with Files

K.4.1 Know the Concepts

- **Describe the lifecycle of a file descriptor.** The program asks Linux to open a file with the `open` system call, and Linux returns a file descriptor, a small number that identifies the open file. The program uses that number with `read` and `write` as many times as it needs, and finally gives it back with `close`. After that, the number is no longer valid and may be reused by the next `open`.
- **What are the standard file descriptors and what are they used for?** Every program starts with three open file descriptors: `STDIN` (0) for input, usually the keyboard; `STDOUT` (1) for normal output, usually the screen; and `STDERR` (2) for error messages, also the screen by default. The shell can redirect any of them to files or pipes.
- **What is a buffer?** A block of memory used to hold data temporarily, for example the data read from a file before it is processed.

- **What is the difference between the `.data` section and the `.bss` section?** Both hold data, but `.data` stores initial values in the executable file, while `.bss` only reserves space, which is filled with zeros when the program starts. Large buffers go in `.bss`, so they don't make the executable bigger.
- **What are the system calls related to reading and writing files?** `open` (5), `read` (3), `write` (4) and `close` (6).

K.4.2 Use the Concepts

All these programs use the `_convert_to_upper` function of `005-01-toupper`, moved to its own file, `0AK-05-00-convert-to-upper.s`, so each one can link it:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     The `_convert_to_upper` function of
5       #     `005-01-toupper`, in its own file so the
6       #     Chapter 5 solutions can link it.
7       #
8       # INPUT:
9       #     First argument  - Length of the buffer.
10      #     Second argument - Address of the buffer.
11      #
12      # OUTPUT:
13      #     The buffer is converted in place.
14      #
15          .equ LOWERCASE_A,       'a'
16          .equ LOWERCASE_Z,       'z'
17          .equ UPPER_CONVERSION,  'A' - 'a'
18          .equ ST_BUFFER_LEN,     8
19          .equ ST_BUFFER,         12
20
21      .section .text
22          .globl _convert_to_upper
23          .type  _convert_to_upper, @function
24  _convert_to_upper:
25      pushl %ebp
26      movl  %esp, %ebp
27      pushl %ebx              # Preserve %ebx and
28      pushl %edi              # %edi for the caller.
29
30      movl  ST_BUFFER(%ebp), %eax
31      movl  ST_BUFFER_LEN(%ebp), %ebx
32      movl  $0, %edi
33      cmpl  $0, %ebx          # Empty buffer?
34      je    _end_convert_loop
35
36  _convert_loop:
37      movb  (%eax,%edi,1), %cl
38      cmpb  $LOWERCASE_A, %cl  # Only 'a' to 'z'.
39      jl    _next_byte
40      cmpb  $LOWERCASE_Z, %cl
41      jg    _next_byte
42      addb  $UPPER_CONVERSION, %cl
43      movb  %cl, (%eax,%edi,1)
```

```
_next_byte:
    incl  %edi
    cmpl  %edi, %ebx
    jne   _convert_loop

_end_convert_loop:
    popl  %edi
    popl  %ebx
    movl  %ebp, %esp
    popl  %ebp
    ret
```

Read from STDIN and write to STDOUT. The program doesn't open or close anything, because Linux already opened file descriptors 0 and 1:

```
    # Assemble with `as --32` and `ld -m elf_i386`.
    # Link with `0AK-05-00-convert-to-upper.o`.
    #
    # PURPOSE:
    #     Solution to Chapter 5, "Use the Concepts":
    #     convert STDIN to upper case and write it to
    #     STDOUT. No files are opened or closed: the
    #     shell already opened file descriptors 0
    #     and 1 for us.
    #
    # USAGE:
    #     echo "hello" | ./0AK-05-01-toupper-stdio
    #
    .include "006-01-linux.s"

    .section .bss
        .equ   BUFFER_SIZE, 500
        .lcomm BUFFER_DATA, BUFFER_SIZE

    .section .text
        .globl _start

_start:
_read_loop:
    movl  $SYS_READ, %eax
    movl  $STDIN, %ebx
    movl  $BUFFER_DATA, %ecx
    movl  $BUFFER_SIZE, %edx
    int   $LINUX_SYSCALL
    cmpl  $END_OF_FILE, %eax # End of file (0) or
    jle   _exit              # error (negative)?

    movl  %eax, %esi         # Bytes read.
    pushl $BUFFER_DATA
    pushl %esi
    call  _convert_to_upper
    addl  $8, %esp

    movl  $SYS_WRITE, %eax
```

```
40      movl  $STDOUT, %ebx
41      movl  $BUFFER_DATA, %ecx
42      movl  %esi, %edx
43      int   $LINUX_SYSCALL
44      jmp   _read_loop
45
46  _exit:
47      movl  $SYS_EXIT, %eax
48      movl  $0, %ebx
49      int   $LINUX_SYSCALL
```

```
echo "Hey, diddle 123!" | ./0AK-05-01-toupper-stdio
```

It prints `HEY, DIDDLE 123!`.

Change the size of the buffer and **use storage in the `.bss` section to store the file descriptors.** This version keeps the file descriptors in `.bss` with `.lcomm`, and uses a buffer of only 16 bytes. The result is the same; only the number of `read` and `write` calls changes:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       # Link with `0AK-05-00-convert-to-upper.o`.
3       #
4       # PURPOSE:
5       #     Solution to Chapter 5, "Use the Concepts":
6       #     `005-01-toupper` storing the file
7       #     descriptors in the .bss section instead of
8       #     the stack. The buffer is also smaller
9       #     (16 bytes), which only means more read and
10      #     write calls; the result is the same.
11      #
12      # USAGE:
13      #     ./0AK-05-02-toupper-bss input.txt output.txt
14      #
15      .include "006-01-linux.s"
16          .equ O_RDONLY,             0
17          .equ O_CREAT_WRONLY_TRUNC, 03101
18          .equ ST_ARGV_1,            8
19          .equ ST_ARGV_2,            12
20
21      .section .bss
22          .equ   BUFFER_SIZE, 16
23          .lcomm BUFFER_DATA, BUFFER_SIZE
24          .lcomm FD_IN,  4     # File descriptors.
25          .lcomm FD_OUT, 4
26
27      .section .text
28          .globl _start
29
30  _start:
31      movl  %esp, %ebp
32
33      movl  $SYS_OPEN, %eax    # Open the input file.
34      movl  ST_ARGV_1(%ebp), %ebx
35      movl  $O_RDONLY, %ecx
36      movl  $0666, %edx
```

```
37      int   $LINUX_SYSCALL
38      movl  %eax, FD_IN
39
40      movl  $SYS_OPEN, %eax    # Open the output file.
41      movl  ST_ARGV_2(%ebp), %ebx
42      movl  $O_CREAT_WRONLY_TRUNC, %ecx
43      movl  $0666, %edx
44      int   $LINUX_SYSCALL
45      movl  %eax, FD_OUT
46
47  _read_loop:
48      movl  $SYS_READ, %eax
49      movl  FD_IN, %ebx
50      movl  $BUFFER_DATA, %ecx
51      movl  $BUFFER_SIZE, %edx
52      int   $LINUX_SYSCALL
53      cmpl  $END_OF_FILE, %eax
54      jle   _close_files
55
56      movl  %eax, %esi         # Bytes read.
57      pushl $BUFFER_DATA
58      pushl %esi
59      call  _convert_to_upper
60      addl  $8, %esp
61
62      movl  $SYS_WRITE, %eax
63      movl  FD_OUT, %ebx
64      movl  $BUFFER_DATA, %ecx
65      movl  %esi, %edx
66      int   $LINUX_SYSCALL
67      jmp   _read_loop
68
69  _close_files:
70      movl  $SYS_CLOSE, %eax
71      movl  FD_OUT, %ebx
72      int   $LINUX_SYSCALL
73      movl  $SYS_CLOSE, %eax
74      movl  FD_IN, %ebx
75      int   $LINUX_SYSCALL
76
77      movl  $SYS_EXIT, %eax
78      movl  $0, %ebx
79      int   $LINUX_SYSCALL
```

Create a file called `heynow.txt` with the words "Hey diddle diddle!". `open` with the flags `03101` creates the file (or empties it if it already exists):

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 5, "Use the Concepts":
5       #     create the file `heynow.txt` and write
6       #     "Hey diddle diddle!" into it.
7       #
```

```
8       .include "006-01-linux.s"
9           .equ O_CREAT_WRONLY_TRUNC, 03101
10
11      .section .data
12          file_name:
13              .ascii "heynow.txt\0"
14          text:
15              .ascii "Hey diddle diddle!\n"
16          text_end:
17          .equ TEXT_LENGTH, text_end - text
18
19      .section .text
20          .globl _start
21
22  _start:
23      movl  $SYS_OPEN, %eax
24      movl  $file_name, %ebx
25      movl  $O_CREAT_WRONLY_TRUNC, %ecx
26      movl  $0666, %edx        # Permissions.
27      int   $LINUX_SYSCALL
28      movl  %eax, %esi         # File descriptor.
29
30      movl  $SYS_WRITE, %eax
31      movl  %esi, %ebx
32      movl  $text, %ecx
33      movl  $TEXT_LENGTH, %edx
34      int   $LINUX_SYSCALL
35
36      movl  $SYS_CLOSE, %eax
37      movl  %esi, %ebx
38      int   $LINUX_SYSCALL
39
40      movl  $SYS_EXIT, %eax
41      movl  $0, %ebx
42      int   $LINUX_SYSCALL
```

K.4.3 Going Further

- **What difference does the size of the buffer make?** A bigger buffer means fewer system calls, and each system call is slow compared with normal instructions, so the program runs faster, up to a point (a few kilobytes is usually enough). The cost is memory. A buffer of 1 byte works, but makes one `read` and one `write` for every character.
- **What error results can be returned by each of these system calls?** On failure, the system calls return a negative number, the error code with a minus sign. Some common ones (see `man 2 open`, `man 2 read`, ...):
  - `open`: `ENOENT` (2, the file doesn't exist), `EACCES` (13, no permission), `EISDIR` (21, it is a directory), `EMFILE` (24, too many open files), `ENOSPC` (28, the disk is full).
  - `read`: `EBADF` (9, bad file descriptor), `EFAULT` (14, the buffer is outside the program's memory), `EISDIR`, `EIO` (5, hardware error).
  - `write`: `EBADF`, `EFAULT`, `ENOSPC`, `EPIPE` (32, the other end of the pipe was closed).
  - `close`: `EBADF`, `EIO`.

- **Use the command-line arguments or STDIN and STDOUT, based on ARGC,** and **check the result of each system call.** This program does both. The messages go to `STDERR` instead of `STDOUT`, so that they are never mixed with the converted text:

```
        # Assemble with `as --32` and `ld -m elf_i386`.
        # Link with `0AK-05-00-convert-to-upper.o` and
        # `006-01-count-chars.o`.
        #
        # PURPOSE:
        #     Solution to Chapter 5, "Going Further":
        #     with two arguments, convert the input file
        #     into the output file; with no arguments,
        #     convert STDIN into STDOUT. Every system
        #     call is checked, and errors are reported.
        #
        # USAGE:
        #     ./0AK-05-04-toupper-checked in.txt out.txt
        #     echo "hi" | ./0AK-05-04-toupper-checked
        #
        # NOTES:
        #     The exercise asks for the messages on
        #     STDOUT, but they go to STDERR: that way
        #     they never get mixed with the converted
        #     text when STDOUT is redirected to a file.
        #     Linux returns errors as a negative number
        #     (-errno) in %eax.
        #
        .include "006-01-linux.s"
            .equ O_RDONLY,             0
            .equ O_CREAT_WRONLY_TRUNC, 03101
            .equ ST_ARGC,              0
            .equ ST_ARGV_1,            8
            .equ ST_ARGV_2,            12

        .section .data
            msg_usage:
                .ascii "Usage: toupper [input output]\n\0"
            msg_open_in:
                .ascii "Error: can't open input file\n\0"
            msg_open_out:
                .ascii "Error: can't open output file\n\0"
            msg_read:
                .ascii "Error: read failed\n\0"
            msg_write:
                .ascii "Error: write failed\n\0"

        .section .bss
            .equ   BUFFER_SIZE, 500
            .lcomm BUFFER_DATA, BUFFER_SIZE
            .lcomm FD_IN,  4
            .lcomm FD_OUT, 4

        .section .text
            .globl _start
```

```
51
52  _start:
53      movl  %esp, %ebp
54      movl  $STDIN, FD_IN      # Defaults.
55      movl  $STDOUT, FD_OUT
56
57      movl  ST_ARGC(%ebp), %eax
58      cmpl  $1, %eax           # No arguments.
59      je    _read_loop
60      cmpl  $3, %eax           # Two arguments.
61      je    _open_files
62      pushl $msg_usage
63      jmp   _fail
64
65  _open_files:
66      movl  $SYS_OPEN, %eax
67      movl  ST_ARGV_1(%ebp), %ebx
68      movl  $O_RDONLY, %ecx
69      movl  $0666, %edx
70      int   $LINUX_SYSCALL
71      cmpl  $0, %eax           # Negative = error.
72      jl    _fail_open_in
73      movl  %eax, FD_IN
74
75      movl  $SYS_OPEN, %eax
76      movl  ST_ARGV_2(%ebp), %ebx
77      movl  $O_CREAT_WRONLY_TRUNC, %ecx
78      movl  $0666, %edx
79      int   $LINUX_SYSCALL
80      cmpl  $0, %eax
81      jl    _fail_open_out
82      movl  %eax, FD_OUT
83
84  _read_loop:
85      movl  $SYS_READ, %eax
86      movl  FD_IN, %ebx
87      movl  $BUFFER_DATA, %ecx
88      movl  $BUFFER_SIZE, %edx
89      int   $LINUX_SYSCALL
90      cmpl  $0, %eax
91      jl    _fail_read
92      je    _close_files       # End of file.
93
94      movl  %eax, %esi
95      pushl $BUFFER_DATA
96      pushl %esi
97      call  _convert_to_upper
98      addl  $8, %esp
99
100     movl  $SYS_WRITE, %eax
101     movl  FD_OUT, %ebx
102     movl  $BUFFER_DATA, %ecx
103     movl  %esi, %edx
```

```
    int   $LINUX_SYSCALL
    cmpl  $0, %eax
    jl    _fail_write
    jmp   _read_loop

_close_files:
    movl  $SYS_CLOSE, %eax   # Closing STDIN or
    movl  FD_OUT, %ebx       # STDOUT is harmless
    int   $LINUX_SYSCALL     # at exit.
    movl  $SYS_CLOSE, %eax
    movl  FD_IN, %ebx
    int   $LINUX_SYSCALL
    movl  $SYS_EXIT, %eax
    movl  $0, %ebx
    int   $LINUX_SYSCALL

_fail_open_in:
    pushl $msg_open_in
    jmp   _fail
_fail_open_out:
    pushl $msg_open_out
    jmp   _fail
_fail_read:
    pushl $msg_read
    jmp   _fail
_fail_write:
    pushl $msg_write

    # Write the message on top of the stack to
    # STDERR and exit with status 1.
_fail:
    call  _count_chars       # Length of message.
    movl  %eax, %edx
    popl  %ecx               # Message address.
    movl  $SYS_WRITE, %eax
    movl  $STDERR, %ebx
    int   $LINUX_SYSCALL
    movl  $SYS_EXIT, %eax
    movl  $1, %ebx
    int   $LINUX_SYSCALL
```

```
./0AK-05-04-toupper-checked /no/such/file out.txt
```

It prints `Error: can't open input file` and exits with status 1.

K.5 Chapter 6. Reading and Writing Simple Records

A correction first. The data of `006-01-write-records.s` had two addresses shorter than in the original book (`"Chicago, IL"` instead of `"Chicago, IL 12345"`, and `"500 Oakland"` instead of `"500 W Oakland"`), so the second and third records were not 324 bytes long and their ages were not where `RECORD_AGE` says. The programs that only print the names worked, but any program that reads the ages got garbage. The file is fixed in this edition, and the ages of `test.dat` are now 45, 29 and 36.

K.5.1 Know the Concepts

- **What is a record?** A group of related data items stored together and handled as one unit, such as the first name, last name, address and age of a person.
- **What is the advantage of fixed-length records over variable-length records?** Every field is at the same offset in every record, and every record has the same size. This makes them simple to read and write, and you can jump directly to record number `n` at position `n × RECORD_SIZE`. The cost is wasted space when the data is shorter than its field, and a hard limit when it is longer.
- **How do you include constants in multiple assembly source files?** Put the `.equ` definitions in one file and add `.include "file.s"` to every source file that needs them.
- **Why might you want to split up a project into multiple source files?** To reuse functions in several programs, to keep each file small and focused, to let several people work at the same time, and to reassemble only the files that changed.
- **What does the instruction `incl record_buffer + RECORD_AGE` do?** It adds 1 to the 4-byte number stored at the address `record_buffer + RECORD_AGE`, which is the age of the record in the buffer. It uses direct addressing, with a single operand. The assembler (and the linker) compute the address `record_buffer + 320` once, before the program runs; when the program runs, the processor only reads that memory location, increments it and writes it back.

K.5.2 Use the Concepts

Add another data member to the person structure. This version adds a 20-byte phone number after the age, so `RECORD_SIZE` changes from 324 to 344:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 6, "Use the Concepts":
5       #     the person record with a new data member,
6       #     a phone number (20 bytes) after the age.
7       #
8           .equ RECORD_FIRSTNAME,  0
9           .equ RECORD_LASTNAME,   40
10          .equ RECORD_ADDRESS,    80
11          .equ RECORD_AGE,        320
12          .equ RECORD_PHONE,      324   # New member.
13          .equ RECORD_SIZE,       344   # Was 324.
```

`_read_record` and `_write_record` use `RECORD_SIZE`, so they must be reassembled with the new definition. Their code doesn't change:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     `_read_record` and `_write_record` for the
5       #     record with a phone number. The code is the
6       #     same as in `006-01-read-record.s` and
7       #     `006-01-write-record.s`; only RECORD_SIZE
8       #     changes, so they must be reassembled.
9       #
10      # INPUT (both functions):
11      #     First argument  - Address of the buffer.
12      #     Second argument - File descriptor.
13      #
```

```
14      # OUTPUT:
15      #     %eax - Result of the read/write call.
16      #
17      .include "006-01-linux.s"
18      .include "0AK-06-01-record-def.s"
19          .equ ST_BUFFER,   8
20          .equ ST_FILEDES,  12
21
22      .section .text
23          .globl _read_record
24          .type  _read_record, @function
25  _read_record:
26      pushl %ebp
27      movl  %esp, %ebp
28      pushl %ebx
29      movl  ST_FILEDES(%ebp), %ebx
30      movl  ST_BUFFER(%ebp), %ecx
31      movl  $RECORD_SIZE, %edx
32      movl  $SYS_READ, %eax
33      int   $LINUX_SYSCALL
34      popl  %ebx
35      movl  %ebp, %esp
36      popl  %ebp
37      ret
38
39          .globl _write_record
40          .type  _write_record, @function
41  _write_record:
42      pushl %ebp
43      movl  %esp, %ebp
44      pushl %ebx
45      movl  ST_FILEDES(%ebp), %ebx
46      movl  ST_BUFFER(%ebp), %ecx
47      movl  $RECORD_SIZE, %edx
48      movl  $SYS_WRITE, %eax
49      int   $LINUX_SYSCALL
50      popl  %ebx
51      movl  %ebp, %esp
52      popl  %ebp
53      ret
```

The programs that write and read the records now handle the phone number. `.space N` reserves `N` zero bytes, which is shorter than `.rept`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       # Link with `0AK-06-01-record-io.o`.
3       #
4       # PURPOSE:
5       #     Write two records with a phone number to
6       #     `test-phone.dat`.
7       #
8       .include "006-01-linux.s"
9       .include "0AK-06-01-record-def.s"
10
```

```
11      .section .data
12          file_name:
13              .ascii "test-phone.dat\0"
14
15          # Each field is padded with zeros up to its
16          # size; `.space N` reserves N zero bytes.
17          record1:
18              .ascii "Fredrick\0"
19              .space 40 - 9
20              .ascii "Bartlett\0"
21              .space 40 - 9
22              .ascii "4242 S Prairie\nTulsa, OK 55555\0"
23              .space 240 - 31
24              .long 45
25              .ascii "555-0100\0"
26              .space 20 - 9
27          record2:
28              .ascii "Marilyn\0"
29              .space 40 - 8
30              .ascii "Taylor\0"
31              .space 40 - 7
32              .ascii "2224 S Johannan St\nChicago, IL\0"
33              .space 240 - 31
34              .long 29
35              .ascii "555-0199\0"
36              .space 20 - 9
37
38      .section .text
39          .globl _start
40
41  _start:
42      movl  $SYS_OPEN, %eax
43      movl  $file_name, %ebx
44      movl  $03101, %ecx       # Create, write, truncate.
45      movl  $0666, %edx
46      int   $LINUX_SYSCALL
47      movl  %eax, %esi         # File descriptor.
48
49      pushl %esi
50      pushl $record1
51      call  _write_record
52      addl  $8, %esp
53
54      pushl %esi
55      pushl $record2
56      call  _write_record
57      addl  $8, %esp
58
59      movl  $SYS_CLOSE, %eax
60      movl  %esi, %ebx
61      int   $LINUX_SYSCALL
62
63      movl  $SYS_EXIT, %eax
```

```
64      movl  $0, %ebx
65      int   $LINUX_SYSCALL
```

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       # Link with `0AK-06-01-record-io.o`,
3       # `006-01-count-chars.o` and
4       # `006-01-write-newline.o`.
5       #
6       # PURPOSE:
7       #     Print the first name and the phone number
8       #     of every record in `test-phone.dat`.
9       #
10      .include "006-01-linux.s"
11      .include "0AK-06-01-record-def.s"
12
13      .section .data
14          file_name:
15              .ascii "test-phone.dat\0"
16          separator:
17              .ascii ": "
18
19      .section .bss
20          .lcomm record_buffer, RECORD_SIZE
21
22      .section .text
23          .globl _start
24
25  _start:
26      movl  $SYS_OPEN, %eax
27      movl  $file_name, %ebx
28      movl  $0, %ecx           # Read only.
29      movl  $0666, %edx
30      int   $LINUX_SYSCALL
31      movl  %eax, %esi         # File descriptor.
32
33  _record_loop:
34      pushl %esi
35      pushl $record_buffer
36      call  _read_record
37      addl  $8, %esp
38      cmpl  $RECORD_SIZE, %eax # A whole record?
39      jne   _finished
40
41      pushl $record_buffer + RECORD_FIRSTNAME
42      call  _print_string
43      addl  $4, %esp
44
45      movl  $SYS_WRITE, %eax   # ": "
46      movl  $STDOUT, %ebx
47      movl  $separator, %ecx
48      movl  $2, %edx
49      int   $LINUX_SYSCALL
50
```

```
51      pushl $record_buffer + RECORD_PHONE
52      call  _print_string
53      addl  $4, %esp
54
55      pushl $STDOUT
56      call  _write_newline
57      addl  $4, %esp
58      jmp   _record_loop
59
60  _finished:
61      movl  $SYS_EXIT, %eax
62      movl  $0, %ebx
63      int   $LINUX_SYSCALL
64
65      # PURPOSE:
66      #     Write a null-terminated string to STDOUT.
67      #
68          .type _print_string, @function
69  _print_string:
70      pushl %ebp
71      movl  %esp, %ebp
72      pushl %ebx
73      pushl 8(%ebp)
74      call  _count_chars
75      addl  $4, %esp
76      movl  %eax, %edx         # Length.
77      movl  $SYS_WRITE, %eax
78      movl  $STDOUT, %ebx
79      movl  8(%ebp), %ecx
80      int   $LINUX_SYSCALL
81      popl  %ebx
82      movl  %ebp, %esp
83      popl  %ebp
84      ret
```

```
./0AK-06-01-write-records
./0AK-06-01-read-records
```

It prints:

```
Fredrick: 555-0100
Marilyn: 555-0199
```

Write 30 identical records to a file with a loop. *%edi* counts down from 30; `decl` sets the zero flag when it reaches 0, so `jnz` needs no `cmpl`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       # Link with `006-01-write-record.o`.
3       #
4       # PURPOSE:
5       #     Solution to Chapter 6, "Use the Concepts":
6       #     write 30 identical records to `test30.dat`
7       #     with a loop.
8       #
9       # OUTPUT:
```

```
10      #     A file of 30 * 324 = 9720 bytes.
11      #
12      .include "006-01-linux.s"
13      .include "006-01-record-def.s"
14
15      .section .data
16          file_name:
17              .ascii "test30.dat\0"
18          record:
19              .ascii "Fredrick\0"
20              .space 40 - 9
21              .ascii "Bartlett\0"
22              .space 40 - 9
23              .ascii "4242 S Prairie\nTulsa, OK 55555\0"
24              .space 240 - 31
25              .long 45
26
27      .section .text
28          .globl _start
29          .equ RECORD_COUNT, 30
30
31  _start:
32      movl  $SYS_OPEN, %eax
33      movl  $file_name, %ebx
34      movl  $03101, %ecx       # Create, write, truncate.
35      movl  $0666, %edx
36      int   $LINUX_SYSCALL
37      movl  %eax, %esi         # File descriptor.
38
39      movl  $RECORD_COUNT, %edi    # Loop counter.
40  _write_loop:
41      pushl %esi
42      pushl $record
43      call  _write_record
44      addl  $8, %esp
45      decl  %edi
46      jnz   _write_loop        # Until %edi = 0.
47
48      movl  $SYS_CLOSE, %eax
49      movl  %esi, %ebx
50      int   $LINUX_SYSCALL
51
52      movl  $SYS_EXIT, %eax
53      movl  $0, %ebx
54      int   $LINUX_SYSCALL
```

The file `test30.dat` is 9720 bytes long (30 × 324).

Find the largest age and **the smallest age in the file.** Both programs are the same except for the conditional jump. The first record is always taken as the largest (or smallest) so far:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       # Link with `006-01-read-record.o`.
3       #
4       # PURPOSE:
```

```
5       #     Solution to Chapter 6, "Use the Concepts":
6       #     find the largest age in `test.dat` and
7       #     return it as the exit status code.
8       #     Create `test.dat` first with
9       #     `006-01-write-records`.
10      #
11      # VARIABLES:
12      #     %esi - File descriptor.
13      #     %edi - largest age so far.
14      #
15      .include "006-01-linux.s"
16      .include "006-01-record-def.s"
17
18      .section .data
19          file_name:
20              .ascii "test.dat\0"
21
22      .section .bss
23          .lcomm record_buffer, RECORD_SIZE
24
25      .section .text
26          .globl _start
27
28  _start:
29      movl  $SYS_OPEN, %eax
30      movl  $file_name, %ebx
31      movl  $0, %ecx           # Read only.
32      movl  $0666, %edx
33      int   $LINUX_SYSCALL
34      movl  %eax, %esi
35
36      movl  $0, %edi           # 0 if there are no
37      movl  $1, %ebx           # records; %ebx = 1
38                               # marks the first one.
39  _record_loop:
40      pushl %esi
41      pushl $record_buffer
42      call  _read_record
43      addl  $8, %esp
44      cmpl  $RECORD_SIZE, %eax
45      jne   _finished
46
47      movl  record_buffer + RECORD_AGE, %eax
48      cmpl  $1, %ebx           # First record: it is
49      je    _new_value         # the largest so far.
50      cmpl  %edi, %eax
51      jle   _record_loop       # Not larger.
52  _new_value:
53      movl  %eax, %edi
54      movl  $0, %ebx
55      jmp   _record_loop
56
57  _finished:
```

```
58      movl  $SYS_CLOSE, %eax
59      movl  %esi, %ebx
60      int   $LINUX_SYSCALL
61
62      movl  $SYS_EXIT, %eax
63      movl  %edi, %ebx        # The age is the
64      int   $LINUX_SYSCALL    # status code.
```

The minimum program only changes `jle` to `jge` (see `0AK-06-04-min-age.s`). With the `test.dat` of `006-01-write-records`, they return 45 and 29.

K.5.3 Going Further

- **Use command-line arguments to specify the filenames.** As in Chapter 5, the arguments are on the stack when the program starts: `8(%ebp)` is the address of the first filename and `12(%ebp)` the address of the second (after `movl %esp, %ebp`). Use them instead of `$file_name` in the `open` calls, and check `ARGC` (`0(%ebp)`) first. See `0AK-05-04-toupper-checked.s`.
- **Use `lseek` to write the modified records back to the same file.** After reading a record, `lseek` moves the file offset back one record, so the write replaces it:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       # Link with `006-01-read-record.o` and
3       # `006-01-write-record.o`.
4       #
5       # PURPOSE:
6       #     Solution to Chapter 6, "Going Further":
7       #     add a year to every age in `test.dat`,
8       #     writing each record back into the same
9       #     file.
10      #
11      # HOW IT WORKS:
12      #     The file is opened for reading and writing
13      #     (O_RDWR = 2). After reading a record, the
14      #     file offset points to the next record, so
15      #     `lseek(fd, -RECORD_SIZE, SEEK_CUR)` moves it
16      #     back to the start of the record just read
17      #     before writing it again.
18      #
19      .include "006-01-linux.s"
20      .include "006-01-record-def.s"
21          .equ SYS_LSEEK,  19
22          .equ SEEK_CUR,   1
23          .equ O_RDWR,     2
24
25      .section .data
26          file_name:
27              .ascii "test.dat\0"
28
29      .section .bss
30          .lcomm record_buffer, RECORD_SIZE
31
32      .section .text
33          .globl _start
```

```
34
35  _start:
36      movl  $SYS_OPEN, %eax
37      movl  $file_name, %ebx
38      movl  $O_RDWR, %ecx
39      movl  $0666, %edx
40      int   $LINUX_SYSCALL
41      movl  %eax, %esi         # File descriptor.
42
43  _record_loop:
44      pushl %esi
45      pushl $record_buffer
46      call  _read_record
47      addl  $8, %esp
48      cmpl  $RECORD_SIZE, %eax
49      jne   _finished
50
51      incl  record_buffer + RECORD_AGE
52
53      movl  $SYS_LSEEK, %eax   # Go back one record.
54      movl  %esi, %ebx
55      movl  $-RECORD_SIZE, %ecx
56      movl  $SEEK_CUR, %edx
57      int   $LINUX_SYSCALL
58
59      pushl %esi               # Overwrite it.
60      pushl $record_buffer
61      call  _write_record
62      addl  $8, %esp
63      jmp   _record_loop
64
65  _finished:
66      movl  $SYS_CLOSE, %eax
67      movl  %esi, %ebx
68      int   $LINUX_SYSCALL
69      movl  $SYS_EXIT, %eax
70      movl  $0, %ebx
71      int   $LINUX_SYSCALL
```

After running it on `test.dat`, the largest and smallest ages are 46 and 30, and the file size doesn't change.

- **Check *%eax* for error conditions and write a message to `STDERR`.** See the solution for Chapter 7, which does this for every system call of `007-01-add-year.s`.
- **Add a single record by reading the data from the keyboard.** This exercise is yours. A way to do it: clear a `RECORD_SIZE` buffer to zeros, `read` from `STDIN` into each field (at most its size minus one byte, so a null byte always remains at the end), replace the final newline with a null byte, store a default age, open the file with `O_WRONLY | O_APPEND` (`02001`) and write the record. The user signals the end of each field with Enter, or of the input with Ctrl+D (end of file).
- **Write `compare-strings` and return the records whose first name starts with 5 characters typed by the user.** The function compares up to 5 characters and stops at the end of the first string, so it also works with shorter prefixes:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 6, "Going Further": the
5       #     `_compare_strings` function, which compares
6       #     two strings up to 5 characters.
7       #
8       # INPUT:
9       #     First argument  - Address of string A.
10      #     Second argument - Address of string B.
11      #
12      # OUTPUT:
13      #     %eax - 1 if A is a prefix of B (comparing
14      #     at most 5 characters of A and stopping at
15      #     the null byte of A), 0 otherwise.
16      #     An empty A matches every string.
17      #
18          .equ MAX_CHARS, 5
19          .equ ST_STRING_A, 8
20          .equ ST_STRING_B, 12
21
22      .section .text
23          .globl _compare_strings
24          .type  _compare_strings, @function
25  _compare_strings:
26      pushl %ebp
27      movl  %esp, %ebp
28      pushl %ebx
29      pushl %esi
30      pushl %edi
31
32      movl  ST_STRING_A(%ebp), %esi
33      movl  ST_STRING_B(%ebp), %edi
34      movl  $0, %ecx           # Index.
35
36  _compare_loop:
37      cmpl  $MAX_CHARS, %ecx   # 5 characters done?
38      je    _match
39      movb  (%esi,%ecx,1), %al
40      cmpb  $0, %al            # End of A?
41      je    _match
42      movb  (%edi,%ecx,1), %bl
43      cmpb  %al, %bl
44      jne   _no_match
45      incl  %ecx
46      jmp   _compare_loop
47
48  _match:
49      movl  $1, %eax
50      jmp   _compare_end
51  _no_match:
52      movl  $0, %eax
53
```

```
_compare_end:
    popl  %edi
    popl  %esi
    popl  %ebx
    movl  %ebp, %esp
    popl  %ebp
    ret
```

```
    # Assemble with `as --32` and `ld -m elf_i386`.
    # Link with `0AK-06-06-compare-strings.o`,
    # `006-01-read-record.o`, `006-01-count-chars.o`
    # and `006-01-write-newline.o`.
    #
    # PURPOSE:
    #     Solution to Chapter 6, "Going Further":
    #     read up to 5 characters from STDIN and
    #     print the first name of every record in
    #     `test.dat` that starts with them.
    #
    # USAGE:
    #     echo Mar | ./0AK-06-07-find-records
    #
    .include "006-01-linux.s"
    .include "006-01-record-def.s"
        .equ INPUT_SIZE, 5

    .section .data
        file_name:
            .ascii "test.dat\0"

    .section .bss
        .lcomm record_buffer, RECORD_SIZE
        .lcomm input, INPUT_SIZE + 1  # + null byte.

    .section .text
        .globl _start

_start:
    movl  $SYS_READ, %eax    # Read the prefix.
    movl  $STDIN, %ebx
    movl  $input, %ecx
    movl  $INPUT_SIZE, %edx
    int   $LINUX_SYSCALL
    cmpl  $0, %eax           # Nothing read (or an
    jle   _exit              # error): stop.

    # End the text at the first newline, if any,
    # so "Mar\n" is used as "Mar".
    movl  $0, %ecx
_find_newline:
    cmpl  %eax, %ecx
    je    _open_file
    cmpb  $'\n', input(%ecx)
```

```
46      je    _cut
47      incl  %ecx
48      jmp   _find_newline
49  _cut:
50      movb  $0, input(%ecx)
51
52  _open_file:
53      movl  $SYS_OPEN, %eax
54      movl  $file_name, %ebx
55      movl  $0, %ecx
56      movl  $0666, %edx
57      int   $LINUX_SYSCALL
58      movl  %eax, %esi
59
60  _record_loop:
61      pushl %esi
62      pushl $record_buffer
63      call  _read_record
64      addl  $8, %esp
65      cmpl  $RECORD_SIZE, %eax
66      jne   _exit
67
68      pushl $record_buffer + RECORD_FIRSTNAME
69      pushl $input
70      call  _compare_strings
71      addl  $8, %esp
72      cmpl  $1, %eax
73      jne   _record_loop       # No match.
74
75      pushl $record_buffer + RECORD_FIRSTNAME
76      call  _count_chars
77      addl  $4, %esp
78      movl  %eax, %edx
79      movl  $SYS_WRITE, %eax
80      movl  $STDOUT, %ebx
81      movl  $record_buffer + RECORD_FIRSTNAME, %ecx
82      int   $LINUX_SYSCALL
83      pushl $STDOUT
84      call  _write_newline
85      addl  $4, %esp
86      jmp   _record_loop
87
88  _exit:
89      movl  $SYS_EXIT, %eax
90      movl  $0, %ebx
91      int   $LINUX_SYSCALL
```

`echo Mar | ./0AK-06-07-find-records` prints `Marilyn`, and `echo Fredrickson | ./0AK-06-07-find-records` prints `Fredrick`, because only the first 5 characters are read.

K.6 Chapter 7. Developing Robust Programs

K.6.1 Know the Concepts

- **What are the reasons programmers have trouble with scheduling?** They estimate the time to write the code for the normal case, but most of the work is in the rest: handling errors and unusual input, testing, fixing the bugs that testing finds, and requirements that change or were misunderstood.
- **Use your favorite program in a completely wrong manner and count the error scenarios.** This exercise is yours. Try files of the wrong type, empty and huge files, names with spaces or accents, invalid options, a full disk, no network, and closing windows at the wrong moment.
- **What are corner cases? Numeric examples?** Inputs at the limits of what a program accepts, where bugs tend to hide. Numeric examples: 0, 1, −1, the largest and smallest values that fit in a register (2147483647 and −2147483648 for a signed 32-bit number, 4294967295 for an unsigned one), the values just past each limit, and, for lists, an empty list and a list of one item.
- **Why is user testing so important?** Users do things the programmer never imagined, so they find the errors that the programmer's own tests can't, and they show whether the program is really usable.
- **What are stubs and drivers used for? What's the difference?** Both let you test one part of a program alone. A *driver* is a small program that calls the function you are testing with known inputs and checks the results. A *stub* replaces a function that the tested code calls but that isn't written yet (or that you want to control), returning fixed values.
- **What are recovery points used for?** They are places in the program where it can go back to a known good state after an error, and either try another way or report the problem cleanly, instead of handling every error everywhere.
- **How many different error codes should a program have?** As many as there are different errors that the user or another program needs to tell apart, and no more. Each code should identify where the error happened, and come with a message that says what to do.

K.6.2 Use the Concepts

Add error checking after every system call of `007-01-add-year.s`, and **read from STDIN if it can't open the file.** Every result is checked: a negative value is an error, and a read that returns part of a record means a damaged file. Opening `test.dat` is a recovery point: if it fails, the program warns the user and reads from `STDIN`:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       # Link with `006-01-read-record.o`,
3       # `006-01-write-record.o`, `007-01-error-exit.o`,
4       # `006-01-count-chars.o` and
5       # `006-01-write-newline.o`.
6       #
7       # PURPOSE:
8       #     Solution to Chapter 7, "Use the Concepts":
9       #     `007-01-add-year` with error checking after
10      #     every system call, and a recovery point: if
11      #     `test.dat` can't be opened, the records are
12      #     read from STDIN instead.
13      #
14      # USAGE:
15      #     ./0AK-07-01-add-year-robust
16      #     ./0AK-07-01-add-year-robust < other.dat
17      #
18      # NOTES:
```

```
19      #     System calls return a negative number
20      #     (-errno) on failure. A read that returns
21      #     more than 0 but less than a whole record
22      #     means the file is damaged.
23      #
24      .include "006-01-linux.s"
25      .include "006-01-record-def.s"
26          .equ O_CREAT_WRONLY_TRUNC, 03101
27
28      .section .data
29          input_file_name:
30              .ascii "test.dat\0"
31          output_file_name:
32              .ascii "testout.dat\0"
33          msg_recover:
34              .ascii "Warning: can't open test.dat, "
35              .ascii "reading STDIN\n"
36          msg_recover_end:
37          .equ RECOVER_LEN, msg_recover_end - msg_recover
38          code_output:
39              .ascii "0002: \0"
40          msg_output:
41              .ascii "Can't Open Output File.\0"
42          code_read:
43              .ascii "0003: \0"
44          msg_read:
45              .ascii "Can't Read Input File.\0"
46          code_partial:
47              .ascii "0004: \0"
48          msg_partial:
49              .ascii "Incomplete Record.\0"
50          code_write:
51              .ascii "0005: \0"
52          msg_write:
53              .ascii "Can't Write Output File.\0"
54          code_close:
55              .ascii "0006: \0"
56          msg_close:
57              .ascii "Can't Close Output File.\0"
58
59      .section .bss
60          .lcomm record_buffer, RECORD_SIZE
61
62      .section .text
63          .globl _start
64          # %esi - Input file descriptor.
65          # %edi - Output file descriptor.
66
67  _start:
68      movl  $SYS_OPEN, %eax
69      movl  $input_file_name, %ebx
70      movl  $0, %ecx           # Read only.
71      movl  $0666, %edx
```

```
72      int   $LINUX_SYSCALL
73      movl  %eax, %esi
74      cmpl  $0, %eax
75      jge   _open_output
76
77      # Recovery point: use STDIN instead.
78      movl  $STDIN, %esi
79      movl  $SYS_WRITE, %eax
80      movl  $STDERR, %ebx
81      movl  $msg_recover, %ecx
82      movl  $RECOVER_LEN, %edx
83      int   $LINUX_SYSCALL     # Nothing useful to do
84                               # if this one fails.
85  _open_output:
86      movl  $SYS_OPEN, %eax
87      movl  $output_file_name, %ebx
88      movl  $O_CREAT_WRONLY_TRUNC, %ecx
89      movl  $0666, %edx
90      int   $LINUX_SYSCALL
91      movl  %eax, %edi
92      cmpl  $0, %eax
93      jl    _error_output
94
95  _loop_begin:
96      pushl %esi
97      pushl $record_buffer
98      call  _read_record
99      addl  $8, %esp
100     cmpl  $0, %eax
101     jl    _error_read        # Read failed.
102     je    _loop_end          # End of file.
103     cmpl  $RECORD_SIZE, %eax
104     jne   _error_partial     # Damaged file.
105
106     incl  record_buffer + RECORD_AGE
107
108     pushl %edi
109     pushl $record_buffer
110     call  _write_record
111     addl  $8, %esp
112     cmpl  $RECORD_SIZE, %eax # Everything written?
113     jne   _error_write
114     jmp   _loop_begin
115
116 _loop_end:
117     movl  $SYS_CLOSE, %eax   # Closing the output
118     movl  %edi, %ebx         # can report a delayed
119     int   $LINUX_SYSCALL     # write error.
120     cmpl  $0, %eax
121     jl    _error_close
122
123     movl  $SYS_EXIT, %eax
124     movl  $0, %ebx
```

```
125     int   $LINUX_SYSCALL
126
127 _error_output:
128     pushl $msg_output
129     pushl $code_output
130     call  _error_exit
131 _error_read:
132     pushl $msg_read
133     pushl $code_read
134     call  _error_exit
135 _error_partial:
136     pushl $msg_partial
137     pushl $code_partial
138     call  _error_exit
139 _error_write:
140     pushl $msg_write
141     pushl $code_write
142     call  _error_exit
143 _error_close:
144     pushl $msg_close
145     pushl $code_close
146     call  _error_exit
```

```
./006-01-write-records
mv test.dat input.dat
./0AK-07-01-add-year-robust < input.dat
```

It prints `Warning: can't open test.dat, reading STDIN` and writes the records with the ages 46, 30 and 37 to `testout.dat`. With a damaged `test.dat` it prints `0004: Incomplete Record.` and exits with status 1.

Add error checking to one other program. See `0AK-05-04-toupper-checked.s` in the Chapter 5 solutions.

K.6.3 Going Further

- **What should you do if your error-reporting function fails?** Almost nothing: exit with an error status code. Trying to report the new error with the same function could fail again, or loop forever. The exit status still tells the caller that something went wrong.
- **Find a bug in an open-source program and file a bug report**, and **try to fix it.** This exercise is yours. A good report says what you did, what you expected, what happened instead, and the versions you used, with the smallest example that shows the bug. Look for projects that label issues as "good first issue".

K.7 Chapter 8. Sharing Functions with Code Libraries

K.7.1 Know the Concepts

- **What are the advantages and disadvantages of shared libraries?** Advantages: programs are smaller, the code is in memory only once for all the programs that use it, and fixing a bug in the library fixes it in every program. Disadvantages: the program depends on the right version of the library being installed, a change in the library can break programs, and loading and linking at run time takes a little time.
- **Given a library named 'foo', what would the library's filename be?** `libfoo.so` (and `libfoo.a` for a static library).
- **What does the `ldd` command do?** It lists the shared libraries that an executable needs, and where the dynamic linker would find each one.

- **How would you link `foo.o` and `bar.o` with the library 'kramer'?**

```
ld -m elf_i386 -o program foo.o bar.o -l kramer \
  -dynamic-linker /usr/lib32/ld-linux.so.2
```

- **What is *typedef* for?** It gives a new name to a C type, for example `typedef int myowntype;`. It doesn't create a new type; it makes declarations shorter and easier to read.
- **What are *structs* for?** They group several variables into one record, like the person records of Chapter 6. In assembly language, a struct is a block of memory and each member is at a fixed offset.
- **What is the difference between *int* and *int **?** An *int* holds a number. An *int ** holds the address of a number. To use an *int*, you read the memory where it is (`movl value, %eax`). To use the number an *int ** points to, you read the pointer first, and then read the memory at that address (`movl pointer, %ebx` and `movl (%ebx), %eax`).
- **What would be the command to create a shared library called 'bar' from `foo.o`?**

```
ld -shared -m elf_i386 -o libbar.so foo.o
```

- **What is the purpose of LD_LIBRARY_PATH?** It is a list of extra directories where the dynamic linker looks for shared libraries, before the standard ones, for example to use libraries that are not installed in the system.

K.7.2 Use the Concepts

Make a shared library with the `_factorial` function, link the main program with it dynamically, also link it with the C library, and display the result with `printf`, with an exit status of 0. First, the library:

```
1       # Assemble with `as --32`.
2       # Build the shared library with:
3       #     ld -shared -m elf_i386 \
4       #       -o libfactorial.so \
5       #       0AK-08-01-factorial-lib.o
6       #
7       # PURPOSE:
8       #     Solution to Chapter 8, "Use the Concepts":
9       #     the recursive `_factorial` function of
10      #     Chapter 4, alone in a file, to build the
11      #     shared library `libfactorial.so`.
12      #
13      # INPUT:
14      #     First argument - n.
15      #
16      # OUTPUT:
17      #     %eax - n!
18      #
19      # NOTES:
20      #     The recursive call uses a local label. A
21      #     call to the global name `_factorial` would
22      #     need a relocation in the code when the
23      #     library is loaded (DT_TEXTREL), because
24      #     another library could replace that name.
25      #
26      .section .text
```

```
        .globl _factorial
        .type  _factorial, @function
_factorial:
_factorial_local:           # Local name, see below.
    pushl %ebp
    movl  %esp, %ebp
    pushl %ebx              # Callee-saved register.

    movl  8(%ebp), %eax
    cmpl  $1, %eax          # 1! = 1 (and 0! = 1).
    jle   _end_factorial
    decl  %eax
    pushl %eax
    call  _factorial_local  # (n - 1)!
    addl  $4, %esp
    movl  8(%ebp), %ebx
    imull %ebx, %eax        # n * (n - 1)!

_end_factorial:
    popl  %ebx
    movl  %ebp, %esp
    popl  %ebp
    ret
```

Then the program, which calls `_factorial` from the library and `printf` and `exit` from the C library:

```
    # Assemble with `as --32`. Link dynamically with
    # the factorial library and the C library:
    #     ld -m elf_i386 \
    #       -o 0AK-08-02-factorial-printf \
    #       0AK-08-02-factorial-printf.o \
    #       -L . -l factorial -l c \
    #       -dynamic-linker /usr/lib32/ld-linux.so.2
    # Run with:
    #     LD_LIBRARY_PATH=. \
    #       ./0AK-08-02-factorial-printf
    #
    # PURPOSE:
    #     Solution to Chapter 8, "Use the Concepts":
    #     call `_factorial` from the shared library
    #     `libfactorial.so`, print the result with
    #     `printf` and exit with status 0.
    #
    # OUTPUT:
    #     The factorial of 5 is 120.
    #
    .section .data
        format:
            .ascii "The factorial of %d is %d.\n\0"

    .section .text
        .globl _start
        .equ NUMBER, 5

```

```
_start:
    pushl $NUMBER
    call  _factorial        # From libfactorial.so.
    addl  $4, %esp

    pushl %eax              # printf(format, n, n!)
    pushl $NUMBER
    pushl $format
    call  printf
    addl  $12, %esp

    pushl $0                # exit(0) flushes the
    call  exit              # printf buffer.
```

```
as --32 -o 0AK-08-01-factorial-lib.o 0AK-08-01-factorial-lib.s
ld -shared -m elf_i386 -o libfactorial.so \
  0AK-08-01-factorial-lib.o
as --32 -o 0AK-08-02-factorial-printf.o \
  0AK-08-02-factorial-printf.s
ld -m elf_i386 -o 0AK-08-02-factorial-printf \
  0AK-08-02-factorial-printf.o -L . -l factorial -l c \
  -dynamic-linker /usr/lib32/ld-linux.so.2
LD_LIBRARY_PATH=. ./0AK-08-02-factorial-printf
```

It prints `The factorial of 5 is 120.` and exits with status 0.

Rewrite `005-01-toupper` with the C library file functions. `fopen`, `fread`, `fwrite` and `fclose` replace the system calls. They return a `FILE` pointer (or `NULL`) and the number of items transferred:

```
    # Assemble with `as --32`. Link with
    # `0AK-05-00-convert-to-upper.o` and the C
    # library (see `make.bash`).
    #
    # PURPOSE:
    #     Solution to Chapter 8, "Use the Concepts":
    #     `005-01-toupper` using the C library file
    #     functions (fopen, fread, fwrite, fclose)
    #     instead of system calls.
    #
    # USAGE:
    #     ./0AK-08-03-toupper-libc input.txt output.txt
    #
    # NOTES:
    #     The C library functions preserve %ebx,
    #     %esi, %edi and %ebp, so the FILE pointers
    #     are kept in %esi and %edi.
    #
    .section .data
        mode_read:
            .ascii "r\0"
        mode_write:
            .ascii "w\0"
        msg_error:
            .ascii "Error: can't open the files\n\0"

```

```
27      .section .bss
28          .equ   BUFFER_SIZE, 500
29          .lcomm BUFFER_DATA, BUFFER_SIZE
30
31      .section .text
32          .globl _start
33          .equ ST_ARGV_1, 8
34          .equ ST_ARGV_2, 12
35
36  _start:
37      movl  %esp, %ebp
38
39      pushl $mode_read         # fopen(argv[1], "r")
40      pushl ST_ARGV_1(%ebp)
41      call  fopen
42      addl  $8, %esp
43      movl  %eax, %esi         # FILE * or NULL.
44
45      pushl $mode_write        # fopen(argv[2], "w")
46      pushl ST_ARGV_2(%ebp)
47      call  fopen
48      addl  $8, %esp
49      movl  %eax, %edi
50
51      cmpl  $0, %esi           # NULL means error.
52      je    _error
53      cmpl  $0, %edi
54      je    _error
55
56  _read_loop:
57      pushl %esi               # fread(buffer, 1,
58      pushl $BUFFER_SIZE       #       size, in)
59      pushl $1
60      pushl $BUFFER_DATA
61      call  fread
62      addl  $16, %esp
63      cmpl  $0, %eax           # 0 = end of file or
64      je    _close_files       # error.
65      movl  %eax, %ebx         # Bytes read.
66
67      pushl $BUFFER_DATA
68      pushl %ebx
69      call  _convert_to_upper
70      addl  $8, %esp
71
72      pushl %edi               # fwrite(buffer, 1,
73      pushl %ebx               #        count, out)
74      pushl $1
75      pushl $BUFFER_DATA
76      call  fwrite
77      addl  $16, %esp
78      jmp   _read_loop
79
```

```
80  _close_files:
81      pushl %edi
82      call  fclose
83      addl  $4, %esp
84      pushl %esi
85      call  fclose
86      addl  $4, %esp
87      pushl $0
88      call  exit
89
90  _error:
91      pushl $msg_error        # printf(msg_error)
92      call  printf
93      addl  $4, %esp
94      pushl $1
95      call  exit
```

K.7.3 Going Further

- **List the environment variables used by the dynamic linker.** The complete list is in `man 8 ld.so`. The most used are `LD_LIBRARY_PATH` (extra directories for libraries), `LD_PRELOAD` (libraries to load before all others), `LD_BIND_NOW` (resolve all symbols at start-up), `LD_DEBUG` (print what the linker does, for example `LD_DEBUG=libs`), `LD_SHOW_AUXV`, `LD_TRACE_LOADED_OBJECTS` (what `ldd` uses) and `LD_AUDIT`.
- **Research executable file formats.** Some important ones: a.out (the original UNIX format: simple, but hard to use with shared libraries), COFF (more flexible, used by older UNIX systems and as the base of Windows' format), ELF (Linux and most UNIX systems today: extensible, with good support for shared libraries and many architectures), PE/COFF (Windows), Mach-O (macOS and iOS, with support for several architectures in one file), and DOS `.COM` files (just the raw code, limited to 64 KB, with no header at all).
- **Find a library for an area you are interested in and use it.** This exercise is yours. The GNOME example in Appendix A shows how to call a graphics library from assembly language.
- **Use `LD_PRELOAD` with a library that contains the `exit` function.** With `LD_PRELOAD`, the dynamic linker loads the library before all the others, so its `exit` is found first and replaces the one in the C library:

```
1       # Assemble with `as --32`.
2       # Build the shared library with:
3       #     ld -shared -m elf_i386 \
4       #       -o libexitmsg.so 0AK-08-04-exit-message.o
5       # Use it with a 32-bit program linked with the
6       # C library:
7       #     LD_PRELOAD=./libexitmsg.so \
8       #       ./008-02-printf-example
9       #
10      # PURPOSE:
11      #     Solution to Chapter 8, "Going Further": a
12      #     shared library with its own `exit` function.
13      #     With LD_PRELOAD, the dynamic linker finds
14      #     this `exit` before the one in the C
15      #     library, so every call to `exit` writes a
16      #     message to STDERR first.
17      #
18      # NOTES:
```

```
19      #     This `exit` doesn't flush the C library
20      #     buffers, so text that `printf` wrote
21      #     without a final newline may be lost.
22      #     A shared library can't use the absolute
23      #     address of its data, because it doesn't
24      #     know where it will be loaded. `call` +
25      #     `popl` gets the current address, and the
26      #     message is found relative to it.
27      #
28          .equ SYS_WRITE, 4
29          .equ SYS_EXIT,  1
30          .equ STDERR,    2
31
32      .section .text
33          .globl exit
34          .type  exit, @function
35  exit:
36      call  _here             # Pushes the address of
37  _here:                      # `_here` and jumps to
38      popl  %ecx              # it; pop it to %ecx.
39      addl  $message - _here, %ecx  # %ecx = &message
40
41      movl  $SYS_WRITE, %eax
42      movl  $STDERR, %ebx
43      movl  $MESSAGE_LEN, %edx
44      int   $0x80
45
46      movl  $SYS_EXIT, %eax
47      movl  4(%esp), %ebx     # exit(status)
48      int   $0x80
49
50      message:
51          .ascii "exit() called: bye!\n"
52      message_end:
53          .equ MESSAGE_LEN, message_end - message
```

```
LD_PRELOAD=./libexitmsg.so ./008-02-printf-example
```

In a terminal it prints `Hi! Jonathan is the person number #3.` and then `exit() called: bye!`. When the output goes to a pipe or a file, only the second line appears: the C library keeps the text of `printf` in a buffer, and the real `exit` writes that buffer before ending the program, but this `exit` doesn't. Programs that don't call `exit` (such as the ones that use the system call directly) are not affected, and 64-bit programs ignore this 32-bit library.

K.8 Chapter 9. Intermediate Memory Topics

A correction first. In `009-02-alloc.s`, the check for regions that are in use jumped to `_allocate_init` instead of to the next region, as the original book does. With that bug, a program that allocated memory three times crashed with a segmentation fault. It is fixed in this edition.

K.8.1 Know the Concepts

- **Describe the layout of memory when a Linux program starts.** In this book's 32-bit programs: the code (`.text`) starts at address `0x08048000` or a little above it, followed by the initialized data (`.data`) and the zeroed data (`.bss`). The current break marks the end of the program's data. At the top of memory, below the kernel's area, is the stack, which holds the environment variables, the command-line arguments and `ARGC` when the program starts. Everything between the break and the stack is unmapped.
- **What is the heap?** The memory after the end of the `.bss` section that a program requests at run time (with `brk`) to store data whose size isn't known in advance.
- **What is the current break?** The address just after the last byte of the program's data memory. Memory beyond it is unmapped until the program moves the break up with the `brk` system call.
- **Which direction does the stack grow in?** Down, towards lower addresses.
- **Which direction does the heap grow in?** Up, towards higher addresses.
- **What happens when you access unmapped memory?** The processor can't translate the address, so it raises a page fault, and Linux stops the program with a segmentation fault (`SIGSEGV`).
- **How does the operating system prevent processes from writing over each other's memory?** With virtual memory. Each process has its own table that maps its virtual addresses to physical memory, so the same address in two processes points to different physical memory, and a process has no way to name the memory of another one.
- **Describe what happens if a piece of memory you are using is currently on disk.** The processor finds that the page is not in physical memory and raises a page fault. Linux suspends the process, finds a free page of physical memory (writing another page to disk if needed), reads the page from the disk into it, updates the page table and resumes the process at the same instruction, which now works. The program doesn't notice anything, except that it was slower.
- **Why do you need an allocator?** Because programs need memory of sizes they only know at run time, and they need to give it back and reuse it. Calling `brk` for every request would be slow and couldn't reuse memory that is freed in the middle of the heap. The allocator keeps track of which parts are free.

K.8.2 Use the Concepts

Make the memory manager initialize itself and **break up regions that are bigger than needed.** `_allocate` now calls `_allocate_init` when `heap_begin` is still 0. When the chosen free region is bigger than the request plus a new header (plus a minimum of 8 bytes), it is split, and the rest becomes a new free region with its own header:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 9, "Use the Concepts":
5       #     the memory manager of `009-02-alloc.s` with
6       #     two improvements:
7       #     1. `_allocate` calls `_allocate_init` by
8       #        itself the first time.
9       #     2. When the chosen free region is bigger
10      #        than needed, it is split in two: the part
11      #        that is used and a new free region with
12      #        its own header.
13      #     It also checks the result of `brk` the
14      #     right way: on failure, `brk` returns the
15      #     old break, not 0.
16      #
```

```
17      # MEMORY LAYOUT OF A REGION:
18      #     | available | size | size bytes of memory |
19      #       4 bytes    4 bytes  ^-- returned pointer
20      #
21      .section .data
22          heap_begin:
23              .long 0
24          current_break:
25              .long 0
26
27          .equ HEADER_SIZE,      8
28          .equ HDR_AVAIL_OFFSET, 0
29          .equ HDR_SIZE_OFFSET,  4
30          .equ UNAVAILABLE,      0
31          .equ AVAILABLE,        1
32          # Split only if the free part can hold a
33          # header and at least this many bytes.
34          .equ MIN_SPLIT,        8
35          .equ SYS_BRK,          45
36          .equ LINUX_SYSCALL,    0x80
37
38      .section .text
39
40      # PURPOSE:
41      #     Set heap_begin and current_break to the
42      #     current end of the program's memory.
43      #
44          .globl _allocate_init
45          .type  _allocate_init, @function
46  _allocate_init:
47      pushl %ebp
48      movl  %esp, %ebp
49      pushl %ebx
50      movl  $SYS_BRK, %eax     # brk(0) returns the
51      movl  $0, %ebx           # current break.
52      int   $LINUX_SYSCALL
53      movl  %eax, current_break
54      movl  %eax, heap_begin
55      popl  %ebx
56      movl  %ebp, %esp
57      popl  %ebp
58      ret
59
60      # PURPOSE:
61      #     Reserve memory.
62      #
63      # INPUT:
64      #     First argument - Number of bytes wanted.
65      #
66      # OUTPUT:
67      #     %eax - Address of the memory, or 0 if
68      #     there is no memory available.
69      #
```

```
70      # VARIABLES:
71      #     %ecx - Size requested.
72      #     %eax - Region being examined.
73      #     %ebx - Current break.
74      #     %edx - Size of the region being examined.
75      #
76          .globl _allocate
77          .type  _allocate, @function
78          .equ ST_MEM_SIZE, 8
79  _allocate:
80      pushl %ebp
81      movl  %esp, %ebp
82      pushl %ebx
83      pushl %esi
84
85      cmpl  $0, heap_begin     # Improvement 1:
86      jne   _initialized       # initialize on the
87      call  _allocate_init     # first call.
88  _initialized:
89      movl  ST_MEM_SIZE(%ebp), %ecx
90      movl  heap_begin, %eax
91      movl  current_break, %ebx
92
93  _alloc_loop_begin:
94      cmpl  %ebx, %eax         # End of the heap?
95      je    _move_break
96      movl  HDR_SIZE_OFFSET(%eax), %edx
97      cmpl  $UNAVAILABLE, HDR_AVAIL_OFFSET(%eax)
98      je    _next_location     # Region in use.
99      cmpl  %edx, %ecx         # Big enough?
100     jle   _allocate_here
101 _next_location:
102     addl  $HEADER_SIZE, %eax
103     addl  %edx, %eax
104     jmp   _alloc_loop_begin
105
106 _allocate_here:
107     # Improvement 2: split the region if the rest
108     # (size - requested - header) is big enough.
109     movl  %edx, %esi
110     subl  %ecx, %esi
111     subl  $HEADER_SIZE, %esi # %esi = size of the
112     cmpl  $MIN_SPLIT, %esi   # new free region.
113     jl    _mark_used
114     movl  %ecx, HDR_SIZE_OFFSET(%eax)
115     leal  HEADER_SIZE(%eax,%ecx,1), %edx
116     movl  $AVAILABLE, HDR_AVAIL_OFFSET(%edx)
117     movl  %esi, HDR_SIZE_OFFSET(%edx)
118 _mark_used:
119     movl  $UNAVAILABLE, HDR_AVAIL_OFFSET(%eax)
120     addl  $HEADER_SIZE, %eax
121     jmp   _allocate_return
122
```

```
_move_break:
    # Grow the heap by header + requested size.
    movl  %eax, %esi         # New region.
    addl  $HEADER_SIZE, %ebx
    addl  %ecx, %ebx         # %ebx = new break.
    movl  $SYS_BRK, %eax
    int   $LINUX_SYSCALL
    cmpl  %ebx, %eax         # brk returns the old
    jl    _error             # break on failure.

    movl  %esi, %eax
    movl  $UNAVAILABLE, HDR_AVAIL_OFFSET(%eax)
    movl  %ecx, HDR_SIZE_OFFSET(%eax)
    addl  $HEADER_SIZE, %eax
    movl  %ebx, current_break
    jmp   _allocate_return

_error:
    movl  $0, %eax

_allocate_return:
    popl  %esi
    popl  %ebx
    movl  %ebp, %esp
    popl  %ebp
    ret

    # PURPOSE:
    #     Give back memory reserved by _allocate.
    #
    # INPUT:
    #     First argument - Address returned by
    #     _allocate.
    #
        .globl _deallocate
        .type  _deallocate, @function
        .equ ST_MEMORY_SEG, 4
_deallocate:
    movl  ST_MEMORY_SEG(%esp), %eax
    subl  $HEADER_SIZE, %eax
    movl  $AVAILABLE, HDR_AVAIL_OFFSET(%eax)
    ret
```

This test program checks that allocations don't overlap, that freed memory is reused, and that regions are split:

```
    # Assemble with `as --32` and `ld -m elf_i386`.
    # Link with `0AK-09-01-alloc.o` (or with
    # `009-02-alloc.o` to compare).
    #
    # PURPOSE:
    #     Test a memory manager. The exit status is
    #     the sum of the checks that failed:
    #       1 - Two allocations overlap.
    #       2 - Freed memory is not reused.
```

```
10      #       4 - The free region was not split, so a
11      #           second small request grew the heap.
12      #     `0AK-09-01-alloc` returns 0; the book's
13      #     manager returns 4, because it doesn't split.
14      #
15      .section .data
16          failures:
17              .long 0
18
19      .section .text
20          .globl _start
21          # %esi = a, %edi = b, %ebx = c
22
23  _start:
24      call  _allocate_init
25
26      pushl $100              # a = allocate(100)
27      call  _allocate
28      addl  $4, %esp
29      movl  %eax, %esi
30
31      pushl $100              # b = allocate(100)
32      call  _allocate
33      addl  $4, %esp
34      movl  %eax, %edi
35
36      leal  100(%esi), %eax   # Check 1: b must not
37      cmpl  %eax, %edi        # start before the end
38      jae   _check_reuse      # of a.
39      addl  $1, failures
40
41  _check_reuse:
42      pushl %esi              # deallocate(a)
43      call  _deallocate
44      addl  $4, %esp
45
46      pushl $40               # c = allocate(40)
47      call  _allocate
48      addl  $4, %esp
49      movl  %eax, %ebx
50      cmpl  %esi, %ebx        # Check 2: c == a.
51      je    _check_split
52      addl  $2, failures
53
54  _check_split:
55      pushl $40               # d = allocate(40)
56      call  _allocate
57      addl  $4, %esp
58      cmpl  %edi, %eax        # Check 3: d must be
59      jb    _done             # in a's old region,
60      addl  $4, failures      # below b.
61
62  _done:
```

```
63      movl  $1, %eax
64      movl  failures, %ebx
65      int   $0x80
```

Linked with `0AK-09-01-alloc.o` it returns `0`; linked with the book's `009-02-alloc.o` it returns `4`, because the second request of 40 bytes doesn't fit in what is left of the region. The program `0AK-09-03-alloc-auto-init.s` allocates memory without calling `_allocate_init`, writes 42 to it and returns that value.

Use the memory manager to get buffer memory instead of the `.bss`. The book already does this in `009-02-read-records.s`, which gets the record buffer with `_allocate`. The same change works for the buffer of `005-01-toupper`: call `_allocate` with `BUFFER_SIZE` at the start, keep the returned address in a register or a local variable, use it instead of `$BUFFER_DATA`, and call `_deallocate` at the end.

K.8.3 Going Further

- **Research garbage collection.** A garbage collector finds the memory that the program can no longer reach and frees it automatically. Advantages: no forgotten frees (memory leaks), no use of memory after it was freed, and simpler code. Disadvantages: it uses extra memory and processor time, it may pause the program at unpredictable moments, and the program doesn't control when memory is released.
- **Research reference counting.** Each block keeps a count of the pointers to it, and is freed when the count reaches 0. Advantages: memory is released as soon as it is no longer used, at predictable times, with no long pauses. Disadvantages: every pointer copy has to update the count, the count uses memory, and blocks that point to each other (cycles) are never freed.
- **Rename the functions to `malloc` and `free`, build them into a shared library and use it with `LD_PRELOAD`.** This exercise is yours, and it is harder than it looks. Besides the names, the C library expects `calloc`, `realloc` and `free(NULL)` to work, and `malloc` to return memory aligned to 16 bytes on 32-bit Linux; it may also call `malloc` before your library is ready. Programs that use `brk` themselves, or other threads, would corrupt this simple heap. Start with a small 32-bit C program of your own that only calls `malloc` and `free`, and use the technique of `0AK-08-04-exit-message.s` to reach your data from a shared library.

K.9 Chapter 10. Counting Like a Computer

K.9.1 Know the Concepts

- **Convert the decimal number 5,294 to binary. 1010010101110**.
- **What number does 0x0234aeff represent?** In binary **0000 0010 0011 0100 1010 1110 1111 1111**, in octal **0215127377** and in decimal **37007103**.
- **Add the binary numbers 10111001 and 101011. 11100100**.
- **Multiply the binary numbers 1100 and 1010110. 10000001000**.
- **Convert the results of the previous two problems into decimal.** 185 + 43 = **228**, and 12 × 86 = **1032**.
- **Describe how AND, OR, NOT, and XOR work.** They work bit by bit. AND gives 1 only if both bits are 1. OR gives 1 if at least one bit is 1. NOT inverts each bit of a single value. XOR gives 1 if the two bits are different.
- **What is masking for?** To select some bits of a value and ignore the rest: AND with a mask keeps only the bits that are 1 in the mask, OR with a mask sets them, and XOR inverts them.
- **What flags would you use for `open` to write a file, creating it if it doesn't exist?** `O_WRONLY | O_CREAT`, which is **0101** in octal (65 in decimal). Add `O_TRUNC` (01000) to also empty an existing file: `01101`.
- **How would you represent −55 in a 32-bit register?** In two's complement: **0xFFFFFFC9**, that is 1111 1111 1111 1111 1111 1111 1100 1001.
- **Sign-extend the previous quantity into a 64-bit register.** Copy the sign bit (1) into all the new bits: **0xFFFFFFFFFFFFFFC9**.

- **Describe the difference between little-endian and big-endian storage of words.** Little-endian processors, like x86, store the least significant byte of a word at the lowest address; big-endian processors store the most significant byte first. The number 0x12345678 is stored as the bytes `78 56 34 12` on x86 and as `12 34 56 78` on a big-endian machine.

K.9.2 Use the Concepts

Make the conversion base a parameter, and support bases greater than 10. This version of `_integer2string` takes the base as its third parameter and uses a table of digits, so bases from 2 to 36 work. It also returns the length of the text in *%eax* and preserves the registers that the calling convention says it must, which the book's version doesn't do with *%edi*:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 10, "Use the Concepts"
5       #     and "Going Further": `_integer2string`
6       #     with the base as a parameter, from 2 to 36.
7       #     Digits past 9 are the letters a to z, so
8       #     base 8 gives octal and base 16 gives
9       #     hexadecimal.
10      #
11      # INPUT:
12      #     First argument  - The (unsigned) number.
13      #     Second argument - Buffer for the text (33
14      #                       bytes is enough for any
15      #                       base: 32 digits + null).
16      #     Third argument  - The base (2 to 36).
17      #
18      # OUTPUT:
19      #     The buffer holds the null-terminated text.
20      #     %eax - Number of characters written.
21      #
22          .equ ST_VALUE,  8
23          .equ ST_BUFFER, 12
24          .equ ST_BASE,   16
25
26      .section .data
27          digits:
28              .ascii "0123456789"
29              .ascii "abcdefghijklmnopqrstuvwxyz"
30
31      .section .text
32          .globl _integer2string_base
33          .type  _integer2string_base, @function
34  _integer2string_base:
35      pushl %ebp
36      movl  %esp, %ebp
37      pushl %ebx              # Preserve the
38      pushl %edi              # callee-saved
39      pushl %esi              # registers.
40
41      movl  ST_VALUE(%ebp), %eax
42      movl  ST_BASE(%ebp), %edi
43      movl  $0, %ecx          # Digit count.
```

```
44
45  _conversion_loop:
46      movl  $0, %edx          # %edx:%eax / base:
47      divl  %edi              # %eax = quotient,
48                              # %edx = remainder.
49      movb  digits(%edx), %bl  # Remainder -> digit.
50      pushl %ebx              # Digits come out in
51      incl  %ecx              # reverse order, so use
52      cmpl  $0, %eax          # the stack to reverse
53      jne   _conversion_loop  # them.
54
55      movl  ST_BUFFER(%ebp), %edx
56      movl  %ecx, %esi        # Keep the count.
57  _copy_loop:
58      popl  %eax
59      movb  %al, (%edx)
60      incl  %edx
61      decl  %ecx
62      jnz   _copy_loop
63      movb  $0, (%edx)        # Null terminator.
64
65      movl  %esi, %eax        # Return the count.
66      popl  %esi
67      popl  %edi
68      popl  %ebx
69      movl  %ebp, %esp
70      popl  %ebp
71      ret
```

Print the results of previous programs instead of returning them in the exit status, and **return results in octal.** This program prints the factorial of 5, the factorial of 10 (which doesn't fit in an exit status code) and 255 in octal, hexadecimal, binary and base 36:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       # Link with `0AK-10-01-integer2string-base.o`,
3       # `0AK-08-01-factorial-lib.o` and
4       # `006-01-write-newline.o`.
5       #
6       # PURPOSE:
7       #     Solution to Chapter 10, "Use the Concepts":
8       #     print a result instead of returning it as
9       #     the exit status (the factorial of 5, which
10      #     no longer has the 255 limit: 10! works too),
11      #     and print 255 in several bases.
12      #
13      # OUTPUT:
14      #     120
15      #     3628800
16      #     377
17      #     ff
18      #     11111111
19      #     73
20      #
21      .include "006-01-linux.s"
```

```
22
23      .section .bss
24          .lcomm buffer, 33
25
26      .section .text
27          .globl _start
28
29  _start:
30      pushl $5                # 5!
31      call  _factorial
32      addl  $4, %esp
33      pushl $10               # In base 10.
34      pushl %eax
35      call  _print_number
36      addl  $8, %esp
37
38      pushl $10               # 10! = 3628800, too
39      call  _factorial        # big for an exit
40      addl  $4, %esp          # status code.
41      pushl $10
42      pushl %eax
43      call  _print_number
44      addl  $8, %esp
45
46      pushl $8                # 255 in octal,
47      pushl $255
48      call  _print_number
49      addl  $8, %esp
50      pushl $16               # hexadecimal,
51      pushl $255
52      call  _print_number
53      addl  $8, %esp
54      pushl $2                # binary
55      pushl $255
56      call  _print_number
57      addl  $8, %esp
58      pushl $36               # and base 36.
59      pushl $255
60      call  _print_number
61      addl  $8, %esp
62
63      movl  $SYS_EXIT, %eax
64      movl  $0, %ebx
65      int   $LINUX_SYSCALL
66
67      # PURPOSE:
68      #     Print a number in a base and a newline.
69      #
70      # INPUT:
71      #     First argument  - The number.
72      #     Second argument - The base.
73      #
74          .type _print_number, @function
```

```
75  _print_number:
76      pushl %ebp
77      movl  %esp, %ebp
78      pushl %ebx
79
80      pushl 12(%ebp)          # Base.
81      pushl $buffer
82      pushl 8(%ebp)           # Number.
83      call  _integer2string_base
84      addl  $12, %esp
85
86      movl  %eax, %edx        # Length.
87      movl  $SYS_WRITE, %eax
88      movl  $STDOUT, %ebx
89      movl  $buffer, %ecx
90      int   $LINUX_SYSCALL
91
92      pushl $STDOUT
93      call  _write_newline
94      addl  $4, %esp
95
96      popl  %ebx
97      movl  %ebp, %esp
98      popl  %ebp
99      ret
```

It prints:

```
120
3628800
377
ff
11111111
73
```

Write a function called `_is_negative`. The sign bit is bit 31, so shifting the number 31 places to the right leaves 1 for negative numbers and 0 for the rest:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 10, "Use the Concepts":
5       #     the `_is_negative` function.
6       #
7       # OUTPUT:
8       #     Exit status code 100:
9       #     is_negative(-5) * 100   -> 1 * 100
10      #     + is_negative(7) * 10   -> 0 * 10
11      #     + is_negative(0)        -> 0
12      #
13      .section .text
14          .globl _start
15
16  _start:
17      pushl $-5
```

```
18      call  _is_negative
19      addl  $4, %esp
20      imull $100, %eax, %esi
21
22      pushl $7
23      call  _is_negative
24      addl  $4, %esp
25      imull $10, %eax, %eax
26      addl  %eax, %esi
27
28      pushl $0
29      call  _is_negative
30      addl  $4, %esp
31      addl  %eax, %esi
32
33      movl  %esi, %ebx
34      movl  $1, %eax
35      int   $0x80
36
37      # PURPOSE:
38      #     Return 1 if the number is negative, 0 if
39      #     it is zero or positive.
40      #
41      # HOW IT WORKS:
42      #     In two's complement, the highest bit (bit
43      #     31) is the sign bit. Shifting the number 31
44      #     places to the right leaves only that bit.
45      #
46      # INPUT:
47      #     First argument - The number.
48      #
49      # OUTPUT:
50      #     %eax - 1 or 0.
51      #
52          .type _is_negative, @function
53  _is_negative:
54      movl  4(%esp), %eax
55      shrl  $31, %eax          # Logical shift: fills
56      ret                      # with zeros.
```

It returns `100`.

K.9.3 Going Further

- **Bases greater than 10.** See `0AK-10-01-integer2string-base.s` above.
- **Write `_number2integer`**, and **read a number from STDIN and convert it.** The function multiplies the result by 10 and adds each digit, until it finds a character that is not a digit. It accepts a minus sign. The program prints the result back with `_integer2string_base`, to check it:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       # Link with `0AK-10-01-integer2string-base.o`
3       # and `006-01-write-newline.o`.
4       #
```

```
5       # PURPOSE:
6       #     Solution to Chapter 10, "Going Further":
7       #     the `_number2integer` function, the reverse
8       #     of `_integer2string`. The program reads a
9       #     number from STDIN, converts it to an
10      #     integer, and prints it back with
11      #     `_integer2string_base` to test it.
12      #
13      # USAGE:
14      #     echo -0042 | ./0AK-10-04-number2integer
15      #     (prints -42)
16      #
17      .include "006-01-linux.s"
18          .equ INPUT_SIZE, 32
19
20      .section .data
21          minus:
22              .ascii "-"
23
24      .section .bss
25          .lcomm input, INPUT_SIZE + 1
26          .lcomm output, 33
27
28      .section .text
29          .globl _start
30
31  _start:
32      movl  $SYS_READ, %eax
33      movl  $STDIN, %ebx
34      movl  $input, %ecx
35      movl  $INPUT_SIZE, %edx
36      int   $LINUX_SYSCALL
37      cmpl  $0, %eax
38      jle   _exit
39      movb  $0, input(%eax)    # Null-terminate it.
40
41      pushl $input
42      call  _number2integer
43      addl  $4, %esp
44      movl  %eax, %esi         # The integer.
45
46      cmpl  $0, %esi           # Negative: print the
47      jge   _print             # sign and the
48      movl  $SYS_WRITE, %eax   # absolute value.
49      movl  $STDOUT, %ebx
50      movl  $minus, %ecx
51      movl  $1, %edx
52      int   $LINUX_SYSCALL
53      negl  %esi
54
55  _print:
56      pushl $10
57      pushl $output
```

```
58      pushl %esi
59      call  _integer2string_base
60      addl  $12, %esp
61
62      movl  %eax, %edx
63      movl  $SYS_WRITE, %eax
64      movl  $STDOUT, %ebx
65      movl  $output, %ecx
66      int   $LINUX_SYSCALL
67      pushl $STDOUT
68      call  _write_newline
69      addl  $4, %esp
70
71  _exit:
72      movl  $SYS_EXIT, %eax
73      movl  $0, %ebx
74      int   $LINUX_SYSCALL
75
76      # PURPOSE:
77      #     Convert decimal text to an integer.
78      #     An optional '-' sign is accepted at the
79      #     start; the conversion stops at the first
80      #     character that is not a digit (such as the
81      #     newline or the null byte).
82      #
83      # INPUT:
84      #     First argument - Address of the text.
85      #
86      # OUTPUT:
87      #     %eax - The integer.
88      #
89      # VARIABLES:
90      #     %eax - Result so far.
91      #     %edx - Address of the current character.
92      #     %ecx - Current character / digit value.
93      #     %ebx - 1 if the number is negative.
94      #
95          .globl _number2integer
96          .type  _number2integer, @function
97  _number2integer:
98      pushl %ebp
99      movl  %esp, %ebp
100     pushl %ebx
101
102     movl  8(%ebp), %edx
103     movl  $0, %eax
104     movl  $0, %ebx
105     cmpb  $'-', (%edx)       # Sign?
106     jne   _digit_loop
107     movl  $1, %ebx
108     incl  %edx
109
110 _digit_loop:
```

```
111     movzbl (%edx), %ecx      # Byte -> 32 bits.
112     subl  $'0', %ecx         # '0'..'9' -> 0..9.
113     cmpl  $9, %ecx           # Not a digit? (Also
114     ja    _digits_end        # catches < '0'.)
115     imull $10, %eax          # result = result*10
116     addl  %ecx, %eax         #          + digit
117     incl  %edx
118     jmp   _digit_loop
119
120 _digits_end:
121     cmpl  $1, %ebx
122     jne   _number_end
123     negl  %eax               # Apply the sign.
124
125 _number_end:
126     popl  %ebx
127     movl  %ebp, %esp
128     popl  %ebp
129     ret
```

`echo -0042 | ./0AK-10-04-number2integer` prints `-42`, and the limits `2147483647` and `-2147483648` come back unchanged.

- **Store likes and dislikes in a single machine word and compare two of them.** The low 16 bits are the likes and the high 16 bits the dislikes. An AND of the two words keeps what they have in common:

```
1       # Assemble with `as --32` and `ld -m elf_i386`.
2       #
3       # PURPOSE:
4       #     Solution to Chapter 10, "Going Further":
5       #     store likes and dislikes in a single word
6       #     and compare two people.
7       #
8       # LAYOUT OF THE WORD:
9       #     Bits 0 to 15  - Likes.
10      #     Bits 16 to 31 - Dislikes, same order.
11      #
12      # OUTPUT:
13      #     Exit status code: shared likes * 10 +
14      #     shared dislikes. For the people below:
15      #     books and games (2), sports (1) -> 21.
16      #
17          .equ MUSIC,   1 << 0
18          .equ BOOKS,   1 << 1
19          .equ MOVIES,  1 << 2
20          .equ SPORTS,  1 << 3
21          .equ COOKING, 1 << 4
22          .equ GAMES,   1 << 5
23          .equ ART,     1 << 6
24          .equ DISLIKE, 16     # Shift for dislikes.
25
26      .section .data
27          .equ A_LIKES,    MUSIC | BOOKS | GAMES
28          .equ A_DISLIKES, SPORTS | COOKING
```

```
29          .equ B_LIKES,    BOOKS | GAMES | ART
30          .equ B_DISLIKES, SPORTS | MOVIES
31          person_a:
32              .long A_LIKES | (A_DISLIKES << DISLIKE)
33          person_b:
34              .long B_LIKES | (B_DISLIKES << DISLIKE)
35
36      .section .text
37          .globl _start
38
39  _start:
40      movl  person_a, %eax
41      andl  person_b, %eax     # Bits set in both.
42      movl  %eax, %esi
43
44      andl  $0xffff, %eax      # Shared likes only.
45      pushl %eax
46      call  _count_bits
47      addl  $4, %esp
48      imull $10, %eax, %edi
49
50      movl  %esi, %eax
51      shrl  $DISLIKE, %eax     # Shared dislikes.
52      pushl %eax
53      call  _count_bits
54      addl  $4, %esp
55      addl  %eax, %edi
56
57      movl  %edi, %ebx
58      movl  $1, %eax
59      int   $0x80
60
61      # PURPOSE:
62      #     Count the bits set to 1 in a word.
63      #
64      # INPUT:
65      #     First argument - The word.
66      #
67      # OUTPUT:
68      #     %eax - Number of bits set.
69      #
70          .type _count_bits, @function
71  _count_bits:
72      movl  4(%esp), %edx
73      movl  $0, %eax
74  _count_loop:
75      cmpl  $0, %edx
76      je    _count_end
77      testl $1, %edx           # Lowest bit set?
78      jz    _count_next
79      incl  %eax
80  _count_next:
81      shrl  $1, %edx           # Next bit.
```

```
82      jmp   _count_loop
83  _count_end:
84      ret
```

It returns 21: two shared likes and one shared dislike.

K.10 Chapter 11. High-Level Languages

K.10.1 Know the Concepts

- **What is the difference between an interpreted language and a compiled language?** A compiled language is translated into machine code before it runs, once, and the result runs directly on the processor. An interpreted language is read and executed by another program, the interpreter, every time it runs. Compiled programs are usually faster; interpreted programs are easier to change and run on any machine that has the interpreter. Many modern languages are in between: they compile to a bytecode that an interpreter or a just-in-time compiler runs.
- **What reasons might cause you to need to learn a new programming language?** A new job or project that already uses it, a platform that requires it (web browsers, mobile devices), a problem that another language solves much better, the libraries available, or just to learn new ways of thinking about problems.

K.10.2 Use the Concepts

- **Re-code one of the programs in another language.** Here is the maximum program of Chapter 3 in C and in Python:

```c
/*
 * Solution to Chapter 11, "Use the Concepts": the maximum program
 * of Chapter 3 in C. Compile with `gcc -o 0AK-11-01-maximum-c-bin
 * 0AK-11-01-maximum.c`; it returns 222 as the exit status code.
 */
int main(void)
{
    int data_items[] = {3, 67, 34, 222, 45, 22, 11, 125, 0};
    int largest = data_items[0];

    for (int i = 1; data_items[i] != 0; i++) {
        if (data_items[i] > largest) {
            largest = data_items[i];
        }
    }
    return largest;
}
```

```python
#!/usr/bin/env python3
"""Solution to Chapter 11, "Use the Concepts": the maximum program of
Chapter 3 in Python. It returns 222 as the exit status code."""
import sys

data_items = [3, 67, 34, 222, 45, 22, 11, 125]
sys.exit(max(data_items))
```

Both return 222, like `003-02-maximum`.

- **What was automated?** In C: the registers (the compiler chooses them), the stack frame, the loop structure and the comparisons, and the program's start and exit (the C library calls `main` and passes its return value to `exit`). In Python, also the type and size of each value, the length of the list (no terminating 0), the search for the maximum (`max`), and the memory management.
- **Run each program 10,000 times and compare with `time`.** Measure it yourself, because the numbers depend on the machine. For example:

```
time (for i in $(seq 10000); do ./003-02-maximum; done)
time (for i in $(seq 10000); do python3 0AK-11-01-maximum.py; done)
```

  The assembly language version should come out ahead, and the Python version far behind. With such a small list, almost all the time is spent starting each process: the assembly program is tiny and makes a single system call, a C program also loads the C library, and Python has to start the whole interpreter before running one line.
- **How do the input/output methods of the language differ from the Linux system calls?** They are built on top of the same system calls, but they add buffering (fewer system calls), formatting (`printf` converts numbers to text), conversion between text encodings, error reporting with exceptions or special values instead of negative numbers, and the same interface on every operating system.

K.10.3 Going Further

- **Why did this book start with a language as verbose as assembly language?** Because it shows what the computer really does. After writing the loops, the stack frames and the system calls by hand, you understand what a high-level language does for you and what it costs, and you can reason about performance and debug problems that are invisible from the high-level code.
- **How have high-level languages affected the process of programming?** Programs can be written much faster, are shorter, easier to read and to move to other machines, and whole classes of errors disappear (such as memory errors in languages that manage memory). This made much larger programs possible. The cost is less control and some performance.
- **Why do so many languages exist?** Because they are designed for different problems (systems, web, data, scientific computing), different trade-offs (speed versus safety versus convenience), different ways of thinking (procedural, object-oriented, functional, logic), and because of history and the communities around them.
- **Learn two new high level languages and compare them.** This exercise is yours. For a strong contrast, try one compiled systems language (such as C or Rust) and one dynamic language (such as Python), or one functional language (such as Scheme or Haskell).

K.11 Chapter 12. Optimization

K.11.1 Know the Concepts

- **At what level of importance is optimization compared to the other priorities in programming?** Low. A program must first be correct, then clear and maintainable; it should be optimized only when it is measurably too slow, and only where it spends its time.
- **What is the difference between local and global optimizations?** Local optimizations make a specific piece of code faster without changing the structure of the program (for example a faster loop). Global optimizations change the structure of the program or its algorithms (for example caching results, or using a better data structure), and usually give much bigger gains.
- **Name some types of local optimizations.** Precomputing calculations, remembering the results of previous calculations, keeping data in registers instead of memory, inlining functions, using faster instructions for the same operation, choosing addressing modes well, and aligning data in memory.

- **How do you determine what parts of your program need optimization?** By measuring with a profiler (such as `gprof` or `perf`), which shows where the program spends its time. Optimize those parts only, and measure again to confirm that the change helped.
- **The same question again: why repeat it?** Because it is the most important lesson of the chapter, and the most forgotten one: optimizing too early wastes time and makes programs harder to read and to fix, usually in parts that don't matter.

K.11.2 Use the Concepts

- **Optimize the programs in this book.** This exercise is yours. Some ideas: keep loop variables in registers instead of memory (as `_power` does with −4(%ebp)), replace the recursive factorial with the loop of `0AK-04-03-factorial-loop.s`, use a bigger buffer in `005-01-toupper`, and replace `imull` by a power of 2 with a shift (`shll`).
- **Calculate the performance impact on your code under specific inputs.** This exercise is yours. Count how many times each instruction runs for an input: for example, the maximum program runs its loop once per item, so its time grows linearly with the length of the list; the recursive factorial makes `n` calls, each one with a stack frame. Then confirm the count by measuring.

K.11.3 Going Further

- **Ask the developers of a fast program about its optimizations**, and **profile a slow program.** These exercises are yours. To profile a C program with `gprof`, compile it with `gcc -pg`, run it once, and then run `gprof program gmon.out`. On Linux, `perf record` and `perf report` work without recompiling.
- **Has the compiler eliminated the need for local optimizations?** Mostly, yes: modern compilers do register allocation, inlining, loop transformations and instruction selection better than most people. But they can't change the algorithm or the data structures, they must keep the exact meaning of the code even when the programmer would accept a faster approximation, and they sometimes can't prove that an optimization is safe (for example because of pointers that may point to the same memory). So local optimization by hand is still useful in the few places where the profiler shows it matters.
- **What problems might a compiler run into when optimizing across function calls?** The called function may be in another file or in a shared library that the compiler can't see, or that can be replaced later (as `LD_PRELOAD` did with `exit`). Without knowing what the function does, the compiler must assume it can change any global memory and must keep the calling convention. Inlining everything would make the program much larger, and recursive functions can't be fully inlined.