

CS211: Programing For Operating Systems

Robert Davidson

Contents

1	Intro to C	4
1.1	Hello World	4
1.2	Variables	4
1.3	An Example	4
1.4	Operators	5
1.5	Control Structure	5
1.5.1	For loop	5
1.5.2	While loop	6
1.5.3	Do While loop	6
1.6	Output	6
1.7	Input	7
1.8	Functions	7
1.9	Call-by-Value and Pointers	7
1.10	Characters	8
1.11	Strings	8
1.11.1	String Functions	8
1.11.2	String Output	9
1.11.3	String Input	9
2	Arrays	9
3	Arrays	9
3.1	Explanation of Array Element Access in C	10
4	Files	10
4.1	Declaring a file identifier:	10
4.2	Opening a file:	10
4.3	Closing a File	10
4.4	Reading from a file	11
4.5	Navigating a file	11
4.6	Writing to a file	11
4.7	Issues concerning the use of files in C, we should be aware of:	12
5	The Process	12
5.1	Process Creation	13
5.2	Process Identification Number	13
5.2.1	unistd.h functions	13
5.3	Process Programming	14
5.4	Signals	14
5.5	Inter Process Communication	15
5.5.1	Direct Communication	15

Useful headers

- `stdio.h` : Standard input/output library
- `stdlib.h` : Standard library
- `string.h` : String manipulation functions (`strncpy`, `strcat`, `strcmp`, `strstr`, `strlen`)
- `unistd.h` : Standard library for system calls (`fork`, `getpid`, `getppid`)

1 Intro to C

It is a very small language and relies heavily on libraries. The compiler must be told in advance how these functions should be used. So before the compilation process, the **preprocessor** is run to include the function prototypes. The compiler then compiles the code into an object file.

1.1 Hello World

Listing 1: Hello World in C

```
1  #include <stdio.h>
2  int main(){
3      printf("Hello World\n");
4      return 0;
5  }
6
```

- **Line 1** : `#include <stdio.h>` is a preprocessor directive that tells the compiler to include the standard input/output library. This library contains the `printf` function.
- In C almost every line is either a preprocessor directive, variable declaration, or a function call.
- C uses curly braces to delimit blocks of code and semicolons to terminate statements.
- **Line 4**: In our case, we assume `main` is called by the Operating System, so `return 0` is used to indicate that the program has run successfully.

1.2 Variables

In C all variables must be declared before they are used. The declaration should have a type; telling the compiler what sort of data the variable will hold. The types of variables are:

- **int** : Integer (1, 2, 3, 4, 5, ...)
- **float** : Floating-point number (7 decimal digits)
- **double** : Double-precision floating-point number (15 decimal digits)
- **char** : Character (a, b, c, ...)
- **void** : No type (used for functions that do not return a value)

We can also declare arrays as follows:

Listing 2: Declaring Arrays

```
1  int arr[5]; // Array of 5 integers
2  char name[10]; // Array of 10 characters
```

To access the first element of `arr` we can do `arr[0]`

1.3 An Example

Listing 3: Example of Variables

```
1  int d=-101;
2  float f=1.23456;
3  char c='a';
4  printf("Values of d, f, c are: %d, %f, %c\n", d, f, c);
```

Explanation: In this case, `%d` is a placeholder for an integer, `%f` is a placeholder for a float, and `%c` is a placeholder for a character.

1.4 Operators

Operator	Description	Example
+	Addition	a + b
-	Subtraction	a - b
*	Multiplication	a * b
/	Division	a / b
%	Modulus	a % b

Table 1: Arithmetic Operators

Operator	Description	Example
=	Assignment	a = b
+=	Add and assign	a += b
-=	Subtract and assign	a -= b
*=	Multiply and assign	a *= b
/=	Divide and assign	a /= b
%=	Modulus and assign	a %= b
++	Increment	a++
-	Decrement	a--

Table 2: Assignment and Arithmetic Assignment Operators

Operator	Description	Example
==	Equal	a == b
!=	Not Equal	a != b
>	Greater	a > b
<	Less	a < b
>=	Greater or Equal	a >= b
<=	Less or Equal	a <= b

Table 3: Relational Operators

Operator	Description	Example
&&	Logical AND	a && b
	Logical OR	a b
!	Logical NOT	!a

Table 4: Logical Operators

1.5 Control Structure

Listing 4: If-Else

```

1  int a = 10;
2  if(a > 10){
3      printf("a is greater than 10\n");
4  }else if(a == 10){
5      printf("a is equal to 10\n");
6  }else{
7      printf("a is less than 10\n");
8  }
9

```

Logical operators, && and || can be used to make more complex conditions.

Listing 5: Complex If-Else

```

1  if(a > 10 && a < 20){
2      printf("a is between 10 and 20\n");
3  }
4

```

1.5.1 For loop

for(initial val; continuation condition; increment/decrement){...}

Listing 6: Print numbers from 0 to 9

```

1  for(int i = 0; i < 10; i++){
2      printf("i is %d\n", i);
3  }

```

1.5.2 While loop

```
while(expression){...}
```

Listing 7: Print numbers from 0 to 9

```
1 int i = 0;
2 while(i < 10){
3     printf("i is %d\n", i);
4     i++;
5 }
```

1.5.3 Do While loop

```
do{...}while(expression);
```

Listing 8: Print numbers from 0 to 9

```
1 int i = 0;
2 do{
3     printf("i is %d\n", i);
4     i++;
5 }while(i < 10);
```

1.6 Output

`printf()` is used to print formatted output to the screen. It is a variadic function, meaning it can take any number of arguments. The first argument is a format string, followed by the values to be printed.

The format string may contain a number of escape characters, represented by a backslash. Some of the most common escape characters are:

Sequence	Description
<code>\a</code>	Produces a beep or flash
<code>\b</code>	Moves cursor to last column of previous line
<code>\f</code>	Moves cursor to start of next page
<code>\n</code>	New line
<code>\r</code>	Carriage return
<code>\t</code>	Tab
<code>\v</code>	Vertical tab
<code>\\</code>	Prints a backslash
<code>\'</code>	Prints a single quote

A conversion character is a letter that follows a `%` and tells `printf()` to display the value stored in the corresponding variable. Some of the most common conversion characters are:

Specifier	Description
<code>%c</code>	Single character (char)
<code>%d</code> or <code>%i</code>	Decimal integer (int)
<code>%e</code> or <code>%E</code>	Floating-point (scientific notation)
<code>%f</code>	Floating-point value (float)
<code>%g</code> or <code>%G</code>	Same as <code>%e/%E</code> or <code>%f</code> , whichever is shorter
<code>%s</code>	String (char array)
<code>%u</code>	Unsigned int
<code>%x</code>	Hexadecimal integer
<code>%p</code>	Pointer (memory address)
<code>%%</code>	Prints the <code>%</code> character

1.7 Input

`scanf()` reads input from standard input, format it, as directed by a conversion character and store the address of a specified variable.

Listing 9: Reading an integer

```
1  int number;
2  char letter;
3  printf("Enter a number and a char: ");
4  scanf("%d %c", &number, &letter);
5
6  printf("You entered: %d and %c\n", number, letter);
```

- The scan `scanf()` returns an integer equal to the number of successful conversions made.
- There is related function `fscanf()` that reads from a file. `scanf()` is really just a wrapper for `fscanf()` that treats the keyboard as a file.
- There are other useful functions for reading the standard input stream: `getchar()` and `gets()`.

Listing 10: Check for no input

```
1  int number;
2  printf("Enter a number between 1 and 30: ");
3  scanf("%d", &number);
4
5  while ((number<1) || (number>30))
6  {
7      printf("Invalid number. Please enter a number between 1 and 30: ");
8      scanf("%d", &number);
9  }
```

1.8 Functions

Def. Prototype and Definition

Prototype : A function prototype is a declaration of a function that tells the compiler what the function looks like. It includes the function name, return type, and parameter types. The prototype must be declared before the function is called.

Definition : A function definition is the actual implementation of the function. It includes the function name, return type, parameter types, and the body of the function. The definition must be declared after the function is called.

1.9 Call-by-Value and Pointers

In C it is important to distinguish between a variable and the value stored in it. A variable has a location in memory. The value of the variable is stored in that location. For example:

```
1  int i = 10;
```

tells the system to allocate a location in memory to store the value 10. The variable `i` is a pointer to that location in memory. One of the distinguishing features of C is that we can manipulate the memory address of the variable almost as easily as we can manipulate the value stored in it.

Pointers

- if `i` is a variable, then `&i` is a pointer to the location in memory where the value of `i` is stored.
- The declaration `int *p;` creates a variable `p` that can store the memory address of an integer. The `*` indicates that `p` is a pointer to an integer.
- If a memory address is stored in the variable `p`, then `*p` is the value stored at that address.

1.10 Characters

Character representation

In C, a character is just an unsigned integer. Each character is represented by an integer between 0 and 127.

Printing characters:

- `printf("%c", c)`
- `putchar(c)`

Reading characters:

- `scanf("%c", c)`
- `c = getchar()`

1.11 Strings

String representation

C does not have a string data type. Instead it uses arrays of type `char` to represent strings. For example if we make a declaration:

```
char greeting[20]="Hello. How are you?";
```

the system stores each character as an element of the array `greeting`.

1.11.1 String Functions

Useful functions defined in `string.h`:

```
char *strncpy(char *dest, char *src, int n)
```

Copies at most `n` characters from `src` to `dest`. The advantage of this is that we don't copy more characters to `dest` than it can hold (prevents buffer overflow). `strncpy()` does not append a null character to the end of the string, so we need to do that manually.

```
char *strcat(char *dest, char *src)
```

Concatenates the string `src` to the end of the string `dest`. The destination string must be large enough to hold the concatenated result. `strcat()` appends a null character to the end of the string.

```
int strcmp(char *str1, char *str2)
```

Compares two strings and returns an integer:

- 0 if the strings are equal
- A negative integer if `str1` comes first alphabetically
- A positive integer if `str2` comes first alphabetically

```
char *strstr(char *haystack, char *needle)
```

Searches for the first occurrence of the string `needle` in the string `haystack`. If found, it returns a pointer to the first occurrence of `needle` in `haystack`. If not found, it returns `NULL`.

```
int strlen(char *str)
```

Returns the length of the string `str` (not including the null character).

1.11 Strings (Continued)

1.11.2 String Output

We know how to use `printf()` to print strings:

- `printf("%s%s\n", "Good Morning ", name);`
- `printf("%s%8s\n", "Good Morning ", name);`

The second example, the field width specifier is given. This causes the string to be padded so it takes up a total of 8 spaces. If the string is shorter than 8 characters, it is padded with spaces on the left. If the string is longer than 8 characters, it is printed as is.

1.11.3 String Input

- `scanf("%s", name);` reads the next "word" from the input stream and stores it in the array `name`. A "word" is defined as a sequence of characters separated without a space, tab, or newline. The string is terminated with a null character.
- `getchar(name);` to get more control of the input in a loop
- `gets(string);` reads a line input and stores it all except the newline character. The string is terminated with a null character. `gets()` is not safe to use because it does not check the length of the input string. If the input string is longer than the array, it will cause a buffer overflow and overwrite other data in memory.
- `fgets(string, n, stdin);` reads in a line of text from the keyboard (standard input stream) and stores at most `n` characters in the array `string`. The string is terminated with a null character. If the input string is longer than `n`, it will be truncated and the rest will be discarded. `fgets()` is safer to use than `gets()` because it checks the length of the input string.

2 Arrays

3 Arrays

To declare a 3×4 matrix of floats, we write `float a[3][4];`. So:

$$\begin{bmatrix} a[0][0] & a[0][1] & a[0][2] & a[0][3] \\ a[1][0] & a[1][1] & a[1][2] & a[1][3] \\ a[2][0] & a[2][1] & a[2][2] & a[2][3] \end{bmatrix}$$

In general, an $n \times m$ array is declared as `float a[n][m];`. The first index is the row number and the second index is the column number. The first element of the array is `a[0][0]` and the last element is `a[n-1][m-1]`.

If a has the line `int a[4];` then the system creates three arrays, each of length four. More precisely, it:

- declares 3 pointers to type `int`: `a[0]`, `a[1]`, and `a[2]`
- space for storing an integer is allocated to each of addresses `a[0]`, `a[0]+1`, `a[0]+2`, `a[0]+3`, `a[1]`, `a[1]+1`, ..., `a[2]+3`

This mean is if `a[] []` is declared as a two-dimensional 3×4 array, then the following are equivalent:

- `a[1][2]`
- `*(a[1]+2)`
- `*(*(a+1)+2)`
- `*(&a[0][0]+4+2)`

3.1 Explanation of Array Element Access in C

`a[1][2]`

This is the standard way to access a two-dimensional array element. It directly fetches the element in the second row (index 1) and the third column (index 2).

`*(a[1]+2)`

- `a[1]` yields the second row, which decays to a pointer to its first element (i.e., equivalent to `&a[1][0]`).
- Adding 2 moves the pointer two elements forward in that row.
- The dereference operator `*` then accesses the element at that position, which is `a[1][2]`.

`*(*(a+1)+2)`

- `a+1` moves the pointer from the first row to the second row.
- `*(a+1)` dereferences that pointer to yield the address of the first element of the second row (again, equivalent to `a[1]`).
- Adding 2 moves to the third element in that row, and the outer `*` fetches its value—again, `a[1][2]`.

`*(&a[0][0]+4+2)`

- `&a[0][0]` gets the address of the very first element of the array.
- Since the array is stored in contiguous memory, pointer arithmetic treats it as a flat sequence. Adding 4+2 (i.e., 6) moves the pointer to the 7th element in that sequence.
- If the layout of the array is such that the element `a[1][2]` is the 7th element (this is true, for example, if the row length is at least 3), then dereferencing this pointer retrieves `a[1][2]`.

4 Files

Taking an input from a file is not much different than taking input from a keyboard. All we do is:

- Declare an identifier of type `FILE` to hold the file pointer.
- Open the file (`fopen()`)
- Read the file
- Close the file (`fclose()`)

4.1 Declaring a file identifier:

```
FILE *datafile;
```

The `datafile` is now a pointer we can associate with a file. The `FILE` type is defined in the `stdio.h` library.

4.2 Opening a file:

```
fileptr = fopen(char *filename, char *mode);
```

The `fopen()` is a function that is used for file opening. It takes two arguments: the name of a file and the mode it will operate in. A file pointer is returned. The mode can be:

- `r` : read (open an existing file for reading)
- `w` : write (overwrite the file or create a new one)
- `a` : append (add to the end of the file)

4.3 Closing a File

```
fclose(fileptr);
```

Once a file is “closed” we can no longer read from it or write to it, unless we open it again. If we don’t do this, the file will still be closed when the program terminates. But until then, no other program on the same node (computer) can work with the file, and it might but be fully written to storage

4.4 Reading from a file

```
fgets(char *str, int n, FILE *fileptr);
```

reads in a line of text from the `fileptr` stream and stores at most `n` characters in array `str`. The new line character is stored. If the string can't be read, because we have reached the end of the file, then `NULL` is returned.

```
fgetc(FILE *fileptr);
```

reads the next character in the file and stores it in the `char` variable `c`. If the end of the file has been reached, `EOF` is returned.

```
fscanf(FILE *fileptr, char *format, ...);
```

reads formatted input from the file. The format string is similar to the one used in `printf()`

4.5 Navigating a file

Each time a character is read from the input stream, a counter associated with the stream is incremented.

```
rewind(FILE *fileptr);
```

sets the indicator to the start of the file

```
ftell(FILE *fileptr);
```

is used to check the current value of the file position indicator in the form of a long int.

```
fseek(FILE *fileptr, long offset, int place);
```

the value of `offset` is the amount the indicator will be changed by, while `place` is one of:

- `SEEK_SET(0)` : the start of the file
- `SEEK_CUR(1)` : the current position in the file
- `SEEK_END(2)` : the end of the file

4.6 Writing to a file

To write to a file, we declare a file pointer:

```
FILE *outfile;
```

and open a new file in write mode:

```
outfile = fopen("myList.txt", "w");
```

to write to the file, we use one of:

- `fprintf(outfile, char *format, ...);` : works like `printf()` except its first argument is a file pointer
- `fputs(char *str, FILE *fileptr);` : writes the string `str` to the file pointed to by `fileptr`, without its trailing `'\0'` character. The string is not formatted.
- `fputc(int c, FILE *fileptr);` : writes the character `c` to the file pointed to by `fileptr`. The character is not formatted.

4.7 Issues concerning the use of files in C, we should be aware of:

- There are 6 modes a file can have: `r`, `w`, `a`, `r+`, `w+`, `a+`
- To open a binary file, also add a `b` to the mode. For example, `rb` opens a file for reading in binary mode.
- `freopen()` attaches a new file to an existing file pointer. It is used to redirect the standard input or output to a file. For example, `freopen("myList.txt", "w", stdout);` redirects the standard output to the file `myList.txt`. This means that any output that would normally go to the screen will now go to the file.
- `tmpfile()` open a temporary file in binary read/write and is automatically deleted when closed or when the program terminates
- `fflush(fileptr);` flushes the output buffer of the file pointer. This means that any data that has been buffered but not yet written to the file will be written to the file.
- `remove("myList.txt");` deletes the file `myList.txt` from the disk.
- `rename("myList.txt", "myList2.txt");` renames the file `myList.txt` to `myList2.txt`. If the new name already exists, it will be overwritten.
- `int feof(FILE *fileptr);` returns a non-zero value if the end of the file has been reached. It is used to check if we have reached the end of the file while reading it.

5 The Process

"A process is a running program."

The operating system gives the impression many programs are running at the same time, but in reality, only one program is running at a time. This is made possible by abstracting the the concept of a running program as a process.

Every process has

- **The process text:** the program code
- **The program counter:** the address of the next instruction to be executed
- **The process stack:** temporary data, local variables, function parameters, return addresses
- **The data section:** global variables

A process is not just a program - if two users run the same program at the same time, they create different processes. Each process has its own memory space, so they do not interfere with each other. A program is a passive entity, while a process is an active / dynamic entity.

Operations OS must perform on a process

- **Create** a new process (open a new program)
- **Terminate / Destory** a process (close a program)
- **Wait** or pause a process until some event occurs (e.g. waiting for user input)
- **Supsend and Resume** similar to wait but more explicit
- **Status** report info about a process (e.g. how much memory it is using, how long it has been running, etc.)

States of a process

- **New** : the process is being created
- **Running** : instructions being executed
- **Block / Waiting** : waiting for some event to occur (e.g. I/O operation)
- **Ready** : waiting to be assigned to a processor
- **Terminated** : the process has finished executing

5.1 Process Creation

A parent creates a child process. The child process can create its own child, forming a tree of processes. After a parent creates a child process it may:

- **Execute** concurrently with the child process
- **Wait** until the child process terminates to continue

The parent may share all, none or some of its resources with the child process (memory space, open files, etc.)

5.2 Process Identification Number

All processes have a unique identifier called a **PID**. If we create a child process in C, using a `fork()` a new process is created:

- The new process runs **concurrently** with the parent, unless we instruct it to `wait()`.
- The subproc (child) is given a **copy of the parents memory space**
- At the time of creation, the two processes are identical, except the `fork()` returns the child process' PID to the parent and 0 to the child.

In order to use `fork()`, we must include the `unistd.h` library, which includes:

- `fork()` - creates a new process
- `getpid()` - returns the PID of the calling process
- `getppid()` - returns the PID of the parent process

5.2.1 `unistd.h` functions

```
pid_t fork(void);
```

- It takes no arguments
- It really returns an `int`
- It returns -1 if the fork failed
- Otherwise, it returns the PID of the newly created child process to the parent process
- It returns 0 to the child process
- The child process is distinct from the parent (it gets its own copy of the parent's memory space)
- Both parent and child process run concurrently
- Starting from the `fork()` call, the parent and child process execute the same instruction set.

```
pid_t getpid(void);
```

Returns the value of the process's own PID

```
pid_t getppid(void);
```

Returns the value of the parent process' PID. Since the parent and subproc (child) have copies of the same memory space and instruction set, `getpid()` and `getppid()` are useful for working out which is which.

5.3 Process Programming

Often we don't want the parent to continue running while the child is running, the results may be non-deterministic. Recall a sub-proc will share the parents memory only in a sense that it receives a copy. The child process can mimic the parents execution or its memory space may be overlaid with a new program/set of instructions.

Often when a child process is created it is overlaid with another program. In C, this can be done with the `execlp()` function. In the following example, the sub-procs memory space is overlaid the program text of the `ls` command. Again we will use the `wait()` function.

The OS is responsible for **de-allocating the resources** of a process that has finished. It may also be responsible for terminating a process that is not responding.

Processes are terminated when

- The proc executes its last instruction and asks the operating system to delete it (`exit()`). At that time it will usually:
 - Output data from subproc to parent (via `wait()`)
 - Have its resources de-allocated by the OS
- Parent terminates a child process because:
 - Sub-proc has exceeded allocated resources
 - The task assigned to the sub-proc is no longer needed
- The parent is exiting and the OS does not allow subproc to continue if the parent is terminated

5.4 Signals

The `kill()` system call is an example of a signal - a form of communication from one process to another. These provide a facility for asynchronous event handling. Note - when the subproc sends the `kill()` signal to the parent, the subproc also terminates.

The `kill()` function can send other signals, but most (such as `SIGABRT`, `SIGILL`, `SIGQUIT`, `SIGTERM`) are just variants of `SIGKILL`. However there are signals that perform other tasks.

Types of Signals

- **SIGSTOP**: stops a process
- **SIGCONT**: continues a stopped process
- **SIGUSR1**: user defined signal 1
- **SIGUSR2**: user defined signal 2

The `kill` function can take two arguments:

```
kill(pid_t pid, int sig);
```

the PID of the process to send the signal to and the signal to send. The function returns 0 on success and -1 on failure. The `kill()` function can be used to send any signal to any process, including itself. With the `signal()` function, we can send a signal that tells the process to perform a specific action, when it receives a `SIGUSR1` or `SIGUSR2` signal.

5.5 Inter Process Communication

Inter process communication (IPC) is a mechanism that allows processes to communicate with each other. This is important because processes may need to share data or synchronize their actions

Types of Process Communication

- **Independent** : Cannot affect or be affected by each other
- **Co-operating** : Can be affected by the execution of each other

Why we allow IPC

- **Information sharing** - two procs might require access to the same file
- **Modularity** - Different procs might be dedicated to different system functions
- **Convenience** - a user might be running an editor, spell checker and printer all for the same file
- **Computational Speed** - on a multiprocessing system tasks are sub-divided and executed concurrently on different processors.

Communication between cooperative may be described in terms of the **producer consumer model**

Def. Producer Consumer Model

One process (editor) has information it wants to produce for consumption by another (printer). This may be done by a **mutual/shared buffer**. Producer write to the buffer and consumer reads from it.

Shared Buffer Types

- **Un-bounded** : no size limit placed on the buffer. The producer may continue to produce and write to the buffer as long as it wants to.
- **Bounded** : strict size limit on the buffer. If full, producer must wait until consumer removes some data.

How we implement shared buffers

- **Physically** by a set of shared variables (shared memory addresses), the implementation of this is the responsibility of the programmer.
- **Logically** by message passing using an Inter Process Communication. Such system is implemented by the OS.. The IPC provides a logical communication link via a message passing facility with two fundamental operations : **send message** and **receive message**.

The two standard forms of IPC are **Direct** and **Indirect** communication. Furthermore, IPC may also be **Symmetric** or **Asymmetric**.

5.5.1 Direct Communication

- Processes must nominate the other process they want to communicate with
- Pairs of communicating processes must know each other's ID's in order to send and receive messages
- A link is established automatically.
- There are exactly two processes in the link
- There can be at most one link between two processes

This is an example of **Symmetric addressing**. In the **Asymmetric addressing** model, the recipient listens out for any messages addressed to it (like making a phone call).

Disadvantages

- Processes must have details of each other before they can communicate

- One link between processes only
- Only two processes can communicate at a time