Final Assignment – ELEC278

David Laeer

Queen’s University

Submitted on Dec 4th 2023

I, David Laeer, attest that all of the materials which I am submitting for this assignment are my own and were written solely by me. I have cited in this report any sources, other than the class materials,

which I used in creating any part of this assignment. Furthermore, this work adheres to the policy on generative artificial intelligence as documented in the instructions.

# Executive Summary

**Table of Contents**

[Executive Summary 2](#__RefHeading___Toc1_1913926204)

[Design Proposal and General Approach 4](#__RefHeading___Toc5_1913926204)

[1. Memory Safety 4](#__RefHeading___Toc7_1913926204)

[2. Exception Handling/Safety 5](#__RefHeading___Toc330_1913926204)

[3. Undefined Behavior 6](#__RefHeading___Toc336_1913926204)

# Design Proposal and General Approach

The general design philosophy used when approaching the problem of designing a CLI-based spreadsheet program reflects several goals and design philosophies, within the constraints and programming paradigms imposed by the C programming language. In no particular order, these include:

1. Memory safety: The program should handle ownership of memory in a safe, consistent manner, with references to allocated memory being either ‘owning’ or ‘non-owning’. This minimizes the risks and challenges associated with manual memory management in the C programming environment.
2. Exception handling and safety: Errors are to be handled in a consistent, safe manner, ensuring the program behaves in an expected manner from the end-user’s point of view. Erroneous or unexpected input should not cause errors, crashes, safety issues, or other undesirable behavior, and should be handled in a user friendly manner.
3. Undefined behavior: Such behavior is undesirable and is to be avoided entirely.
4. Efficiency: Algorithms and data structures used in the design of this program should leave no room for wasteful memory usage or computation.
5. User-friendly design: The program should be easy to use and user-agnostic, meaning that users who have never been exposed to the program’s user interface should face no difficulty when first using the software. The user interface should be easy to use and follow a minimalist design approach.
6. NFR (Non-Functional Requirement) and FR (Functional Requirement) compliance: The program should comply with all given FRs and NFRs, and should implement additional features when feasible given the existing time constraints.

## 1. Memory Safety

Some of the most common issues encountered by developers using the C programming language stem from C’s manually managed memory model: Invalid pointers and memory leaks. Invalid pointers occur when a pointer holds a memory address which is not associated with an area of dynamic program memory which has been explicitly allocated (acquired) by the program, while memory leaks occur when access to an area in memory which has been explicitly allocated is ‘lost’, meaning when there are no pointers holding that memory block’s address. To address these two issues, data structures using dynamically-allocated memory in this program fall into two categories[[1]](#footnote-2): non-owning and owning references (pointers)[[2]](#footnote-3). In essence, ownership indicates where the responsibility of managing the lifetime of the underlying memory lies. Non-owning pointers or references are generally temporary in nature, such as when data is passed by reference to a function. While this function may or may not modify the underlying data (as indicated by the “constness” of the passed pointer), the onus is on the caller to manage the lifetime of the memory associated with the pointer. This is fundamentally different to a pointer which “owns” the underlying data. An owning pointer’s lifetime is classified into three parts: creation, use, and destruction. Upon entering execution scope (or upon program start in the case of globally scoped pointers), owning pointers must either be assigned to a valid area in memory (using malloc() or equivalent), or must be explicitly set to NULL. This ensures that NULL-checks can be implemented throughout the program and can be relied upon for checking the state of the pointer, where a pointer with a value of NULL explicitly is in a non-owning state. This prevents the first issue outlined above, where references to invalid memory blocks may be used, causing program crashes. During the lifetime (use) of owning pointers, they may be passed by value to functions accepting non-owning pointers: this demonstrates the use of safe non-owning pointers by helper functions. They may not however be assigned new values (memory addresses) without first going through a new lifetime cycle, i.e. without first being destructed. Destruction of an owning pointer involves freeing the memory “owned” by that pointer, then assigning said pointer to the NULL pointer macro. In short, an owning pointer may be in one of two states: “dead”, having a value of NULL and owning no memory, or “alive”, having a non-NULL value. Only “live” pointers may be passed by copy (not by reference) to functions accepting non-owning pointers. As an aside, function accepting pointers-to-pointers accept these as owning pointers, and are responsible for proper destruction/creation if they choose to modify the memory address stored in the pointer.

## 2. Exception Handling/Safety

Functions whose tasks are not guaranteed to succeed are required to implement mechanisms to handle failure to complete, which must include a way of notifying the caller of the failure of the required task. In other languages such as C++ or Java, exception handling is explicitly supported by the language standard, effectively providing two paths for function return mechanisms: the non-exceptional path (return by value/reference) and the exceptional path, consisting of raising an exception resulting in the unwinding of the call stack until the exception is handled. However, C does not permit this type of exception handling, and the programmer must therefore use careful design procedures when writing functions which may result in a failure to evaluate. The approach used in the design of this software involves modifying the function signature, wherein the function which is subject to failure returns a “bool” value, indicating success or failure. The function then takes an extra parameter in the form of a pointer, which is to be passed as the address of the variable where the result is to be stored upon success. As seen in section 1, this pointer parameter is a non-owning pointer whose underlying value may be modified by the called function, in order to store the result.

## 3. Undefined Behavior

The C programming language standard specifies that the machine readable output of the C compiler must not adhere to the source code input in a line-by-line fashion, as long as the program behaves as would be expected based on the source code AND there is no undefined behavior (UB) present in the program. If there is undefined behavior present in the source code, the program may not be expected to do anything – i.e. anything is allowed to happen. This is obviously highly undesirable and does not align with the goals outlined above. Examples of undefined behavior include accessing an array out of bounds, signed integer overflow, or calling “free()” on a pointer which is not associated with properly allocated memory. Such undefined behavior is therefore to be avoided at all costs, and several tools such as clang-tidy or IntelliSense can provide warnings if UB is thought to occur.

## 4. Efficiency

Given the limited nature of memory and compute cycles, the software developed in the context of this assignment must make every effort to use the most efficient algorithms available to solve the task at hand, and to limit the use of memory to what is required of the program and no more. This stems from the concept that a user’s time and resources are more valuable than those of the developer, since there may be 10,000 users for every developer. Thus, it makes sense for the developer to spend additional time improving his or her programs’ efficiency if it results even in a minor improvement for the end user.

## 5. User-friendly Design

While the code defining the user interface has already been provided by the ELEC278 teaching team, minor improvements have been made at the discretion of the student. Furthermore, user experience (UX) is influenced by the efficiency and responsiveness of the software, thus falling under item 4 listed above. This also encompasses certain program behavior, such as auto-capitalization of characters used in formulas referencing other cells.

## NFR and FR Compliance

The software must comply with all given Functional and Non-Functional Requirements.

### FR Compliance

* A user can navigate between cells and modify or clear the value of each: this FR is fulfilled. Cells can be navigated using a scroll wheel or up-down-left-right keys, and their values can be edited by typing into the edit window.
* When a user enters a new value, it is interpreted as either text, a number, or a formula: this FR is fulfilled.

### NFR Compliance

1. This approach is inspired from the concepts of “smart” (owning) pointers and RAII (Resource Acquisition Is Initialization) used in the C++ programming language. [↑](#footnote-ref-2)
2. The terms “pointer” and “reference” are used interchangeably throughout this report [↑](#footnote-ref-3)