Learn Verification With Cameleer

Verified Algorithms and Data Structures

Draft Version: August 31, 2025

© Pedro Gasparinho[†]
Mário Pereira[†]

[†] Nova School of Science and Technology, Portugal

Preface

This textbook is ongoing work and has temporarily been released in the form of a draft PDF file for the 16th edition of INForum, the Portuguese Symposium in Computer Science. Despite not being finished, we consider the current set of algorithms to be a good preview of the final version, and we expect that all of them will be present by then. We are open to suggestions, to discuss new ideas, to consider other algorithms, and much more. To contact the main author, readers may use the following email address: p.gasparinho@campus.fct.unl.pt

Contents

1 Introduction **1**

1.1 *OCaml* & *Opam* 1

1.1.1 Via Script 1

1.1.2 Via OS's Package Manager 2

1.1.3 Setting up *opam* 2

1.2 Installing *Why3* and provers 2

1.2.1 Installing *Why3* 2

1.2.2 Installing *Alt-Ergo* 3

1.2.3 Installing *cvc5* 3

1.2.4 Installing *Z3* 3

1.3 Installing Cameleer 3

1.4 Boolean Algebra 4

1.5 First-Order Logic 5

1.5.1 Hoare Logic 6

1.5.2 OCaml 7

1.5.3 GOSPEL and Cameleer 8

1.5.4 Cameleer and Why3 11

2 Arithmetic **15**

2.1 Extended Euclidean Algorithm 15

2.2 McCarthy 91 function 18

2.3 Euclidean Division 20

2.4 Fibonacci sequence 22

2.5 Revisiting Extended Euclidean Algorithm 25

2.6 Fast Exponentiation 29

2.7 Exercises 36

3 Searching **37**

3.1 Linear Search 37

3.2 Binary Search 39

3.3 Ternary Search 43

3.4 Depth-first Search in Binary Trees 47

3.5 Exercises 48

4 Sorting **49**
4.1 Integer Lists . . . 49
4.1.1 Small verification library . . . 49
4.1.2 Selection Sort . . . 54
4.1.3 Merge Sort . . . 58
4.1.4 Quick Sort . . . 62
4.2 Polymorphic Lists . . . 67
4.2.1 Revisiting the verification library . . . 69
4.2.2 Revisiting Selection Sort . . . 70
4.3 Integer Arrays . . . 71
4.3.1 Re-revisiting the verification library . . . 71
4.3.2 Swap-based sorting . . . 72
4.3.3 Insertion Sort . . . 73
4.4 Exercises . . . 76

5 Data Structures **79**

6 Selected Topics **81**
6.1 Exercises . . . 81

A Solutions **83**
A.1 Chapter 2 . . . 83
A.2 Chapter 3 . . . 89
A.3 Chapter 4 . . . 89

Chapter 1

Introduction

In this chapter we will go through the installation processes of our tools, as well as the required background for subsequent chapters. This includes reviewing basic Logic and OCaml concepts, in addition to introducing Hoare Logic, GOSPEL, Cameleer and Why3.

We recommend to our readers the use of a Unix operating system, since the tools used in this book have better support in these types of systems.

1.1 *OCaml* & *Opam*

The first step in this process is to install the *OCaml* programming language, or rather, it's package manager, *opam*, which comes with *OCaml's* compiler, the basic packages and auxiliary tools.

This can be done either through the operating system's package manager (not to be confused with a programming language package manager, such as *opam*), or using the provided script.

For a simple guide regarding *opam*'s installation process visit:

https://ocaml.org/install

For a more complete guide visit:

https://opam.ocaml.org/doc/Install.html

1.1.1 Via Script

Open the terminal an execute this command:

```
bash -c "sh <(curl -fsSL https://opam.ocaml.org/install.sh)"
```

1.1.2 Via OS's Package Manager

For debian, ubuntu, mint or similar users, one may use execute the following command in the terminal:

```
apt install opam
```

Opam is available in Homebrew and MacPorts for macOS users:

```
brew install opam # Homebrew
port install opam # MacPorts
```

For other operating systems check the complete guide mentioned above.

1.1.3 Setting up *opam*

After installing *opam*, one needs to initialize it using:

```
opam init
```

At the end of the last operation, a prompt appears to set the environment variables, it is recommended to answer **yes**. Otherwise, one must run the following command when accessing *opam*'s installation:

```
eval `opam config env`
```

1.2 Installing *Why3* and provers

Why3 is a platform for deductive program verification with use cases in both academia and industry. If features a rich specification library, along many other important features, however its main drawback, from an industrial standpoint, is that it only accepts directly programs written in its own programming and specification language, *WhyMl*. This language is not widely used as general-purpose programming language in the industry, when compared to *OCaml*. Despite this, *WhyMl* has been used as an intermediary language in various projects to prove more mainstream languages, such as *C*, *Java*, *Ada* or *OCaml*.

More information about installing *Why3* and the automated provers can be found at:

https://marche.gitlabpages.inria.fr/lecture-deductive-verif/install.html

1.2.1 Installing *Why3*

Why3 and its *IDE* can be installed through *opam*:

```
opam install why3 why3-ide
```

Why3 relies on third-party provers, which allows combining multiple provers in the same proof, and each may have its own strengths and limitations. To start with we recommend installing *Alt-Ergo*, *cvc5* and *Z3*.

1.2.2 Installing *Alt-Ergo*

Similarly, it can be installed through *opam*:

```
opam install alt-ergo
```

1.2.3 Installing *cvc5*

Unlike *Alt-Ergo*, *cvc5* and *Z3* are not available in *opam*, as of the release date of this version of the book. Instead, one must download the provers from the corresponding *github* pages.

The latest versions of *cvc5* include numerous options for each OS and architecture, which may be hard to distinguish which is the best suited for the user, one may experiment or go back to version 1.1.0, which features simpler variations.

To install version 1.1.0 for Linux, via terminal, one can use the following sequence of commands:

```
wget https://github.com/cvc5/cvc5/releases/download/cvc5-1.1.0/cvc5-Linux
sudo cp cvc5-Linux /usr/local/bin/cvc5
sudo chmod +x /usr/local/bin/cvc5
cvc5 --version
```

This sequence, by step, is equivalent to:

1. Downloading the desired file from *github*
2. Moving it from the working directory to */usr/local/bin*
3. Granting the file permission to execute
4. Checking the version (and if it is actually installed)

1.2.4 Installing *Z3*

Similarly to *cvc5*, to install the latest version (4.15.0) of *Z3*, via terminal, one may use the following sequence of commands:

```
wget https://github.com/Z3Prover/z3/releases/download/z3-4.12.2/z3-4.15.0-x64-glibc-2.39.zip
unzip z3-4.15.0-x64-glibc-2.39.zip
sudo cp z3-4.15.0-x64-glibc-2.39/bin/z3 /usr/local/bin
sudo chmod +x /usr/local/bin/z3
z3 --version
```

1.3 Installing Cameleer

For the reasons mentioned above, *Cameleer* emerged. This piece of software is used to verify OCaml programs with GOSPEL (Generic OCaml SPEcification

Language) annotations. *Cameleer*, internally, translates these programs into *WhyMl*, which can then be verified in the *Why3* platform. For more information check:

https://github.com/ocaml-gospel/cameleer

Cameleer can be installed via terminal with the following sequence of commands:

```
git clone https://github.com/ocaml-gospel/cameleer
opam pin add path/to/cameleer
cameleer --version
```

1.4 Boolean Algebra

The field of Formal Verification is closely related to Mathematics, with one of the most influential subfields being Logic. As such, it is important to start by disclosing it, through Boolean Algebra. This branch of algebra studies truth variables, and how these interact with each other. A truth variable may assume one of two values, true or false, and its negation can be obtained by preceding it with the $\neg$ symbol. To calculate the result of an expression, one may use a truth table, which has a column for each variable, one for the result, and potentially other auxiliary columns with intermediate results. In terms of rows, it usually has $2^{\#\text{variables}}$ to allow all possible combination between the values of the variable. For instance, the truth table of the negation operation is:

p	$\neg p$
T	F
F	T

Given the limited set of values in Boolean Algebra, this is the only unary operation, *i..e* only receives one argument. Most other operations are binary (2 arguments), and some of the most common include:

- Conjunction ($\wedge$), which is true when both variables are true.
- Disjunction ($\vee$), which is true when at least one variable is true.
- Consequence ($\implies$), which is true when the first variable is false or both are true.
- Equivalence ($\iff$), which is true when both variables have the same value.

p	q	$p \wedge q$	$p \vee q$	$p \implies q$	$p \iff q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

Note that when p is false, $p \implies q$ is true. This can be explained from the fact that we are in the context of false premises. Consider the following example:

$$p - \text{Going to the park}$$
$$q - \text{Feeding the ducks}$$
$$p \implies q - \text{If I go the park, then I will feed the ducks}$$

The only scenario where we would be "lying" is if we went to the park, but did not feed the ducks. In the event of not going to the park, it does not matter if we actually got to feed ducks (in any other place), since we do not state what we would be doing instead. Hence, when p is false, $p \implies q$ is true, independently of q.

1.5 First-Order Logic

Unlike Prepositional Logic, which exclusively uses Boolean Algebra, First-Order Logic expands upon the aforementioned concepts with the introduction of quantifiers and predicates. This family of logic systems include three basic building blocks:

- **Constants** - Which denote the objects in the logic system. A constant may only represent a single object.
- **Functions** - Which receive one or more objects to produce another. Functions are pure, *i.e.* they always produce the same output for a given input (there is no notion of state).
- **Predicates** - Which are properties or relations between objects that may be true or false. In first-order logic systems, predicates cannot be arguments in other predicates.

One common example of a First-Order Logic system is elementary algebra:

- Constants - $\mathbb{N}_0$ *i.e.* $\{0, 1, 2, ...\}$
- Unary Functions - $\{-, +, !, ...\}$ (1 argument)
- Binary Functions - $\{+, -, *, /, ^\wedge, \%, ...\}$ (2 arguments)
- Predicates - $\{=, \neq, >, \geq, <, \leq\}$

In addition to the basic building blocks, there are also quantifiers, Which apply the same property to each element in a given set (or subset) of objects. There are two quantifiers:

- For all ($\forall$) - If every single element in that set complies with the desired property, then the quantified expression is true.
- Exists ($\exists$) - If at least one element in that set complies with the desired property, then the quantified expression is true.

Examples:

$$\forall x \in \mathbb{N}_0 : x > -1 \text{ (true)}$$
$$\forall y \in \{1,2\} : 2y = 4 \text{ (false)}$$
$$\exists z \in \mathbb{N}_0 : 3z - 5 = 4 \text{ (true)}$$
$$\exists a, b \in \mathbb{N}_0 : a + b = 7 \text{ (true)}$$
$$\forall c \in \mathbb{N}_0 : \exists d \in \mathbb{N}_0 : 2c = d \text{ (true)}$$
$$\forall c \in \mathbb{N}_0 : \exists d \in \mathbb{N}_0 : c \neq d \wedge 2c = d \text{ (false)}$$

Exercise: What does each of the previous expressions mean?

1.5.1 Hoare Logic

Hoare Logic is the basis of deductive verification of software. It originated from the observation that before the execution of a program fragment the memory state must respect a set of logical conditions. Moreover, after the computation, the memory state may change and will respect a new set of logical conditions. These can be expressed as a Hoare Triple:

$$\{P\}\ S\ \{Q\}$$

Where P is the set of pre-conditions, S is a program (or a fragment) and Q is the set of post-conditions. A Hoare Triple can be understood as: "If P holds immediately before the execution of S, then after it terminates it produces a state where Q holds". This is partial correctness, since the termination is not assured by the triple. Total correctness is achieved when termination is also guaranteed. This is only problematic when dealing with recursion or `while` loops, since `for` loops have a finite number of iterations. Hoare's original work features a number of rules, based on language construct, which have been extended over the years. Of these rules, it is essential to know the while rule:

$$\frac{\{Inv \wedge Cond\}\ Exp\ \{Inv\}}{\{Inv\}\ \text{while}\ Cond\ \text{do}\ Exp\ \{Inv \wedge \neg Cond\}}$$

When we are dealing with the repetition of instructions, we stop thinking about pre- and post-conditions, to think about invariants. An invariant is a property that holds immediately before the start and immediately after the end of an iteration. In the case of a `while` loop, the loop condition is also respected when entering a new iteration, while its negation is respected when exiting the loop.

1.5.2 OCaml

OCaml is a functional-first programming language that also supports the imperative and object-oriented paradigms (although the latter will not be our focus). One of its main characteristics is type-safety, meaning that any compiled program will not produce type errors. This is particularly important in a formal verification setting, since it is a strong safety guarantee that we do not have to check ourselves. As a functional language, OCaml considers functions as primitive types, this allows for many possibilities, including passing functions as parameters or returning them. Consider the following function:

OCaml
```
let seconds_to_hours s =
  let h = s / 3600 in
  let r = s mod 3600 in
  let m = r / 60 in
  let s' = r mod 60 in
  (h, m, s')
```

As we can observe, the `let` keyword is used to name the expression after the equal sign. A function is distinguished by having other identifiers before `=`, in this case `s`. To define auxiliary values (including other functions) inside the body of a function, one must follow the `let` expression with the `in` keyword, this is due to scoping and avoiding ambiguities. Note that it is possible to chain `let` expressions, as seen above, with each identifier being available in the subsequent expressions. The readers might have noticed already that this function converts a single value in seconds (`s`) to a triple containing the equivalent amount of time in hours (`h`), minutes (`m`) and seconds (`s'`). This can be achieved by using the integer division (/), to obtain the highest whole value, and the remainder operation (`mod`), to spread across the subunits. For instance, by dividing the original amount by 3600 (number of seconds in an hour), we obtain the maximum number of complete hours:

$$\left\lfloor \frac{3600}{3600} \right\rfloor = 1 \qquad \left\lfloor \frac{3661}{3600} \right\rfloor = 1 \qquad \left\lfloor \frac{7200}{3600} \right\rfloor = 2$$

Another important feature in OCaml is pattern matching, which allows deconstructing complex data types in a case by case analysis using the different patterns, generally from the various constructors that combined make the data type. Consider a function that calculates the number of instances of a given element in a list:

OCaml
```
let rec count x l =
  match l with
  | [] -> 0
  | h::t -> (if x = h then 1 else 0) + count x t
```

The two most common patterns used when deconstructing a list is the empty list ([]) and the list with at least one element (`h::t`), where `h` is the first element (head) and `t` is the sub-list containing the remaining elements (tail). Note that `h` and `t` are just naming conventions, other identifiers could have been used. The `count` function recursively traverses the list element by element. In OCaml recursive functions must contain the `rec` keyword after the corresponding `let`. Also note that `if-blocks` can be used as expressions in many functional languages, in contrast to imperative languages, where these are treated as statements. Another language detail is the following syntactic sugar:

```ocaml
let rec count x = function
  | [] -> 0
  | h::t -> (if x = h then 1 else 0) + count x t
```

If we have a parameter that is immediately deconstructed in pattern matching by itself, then we may omit both of these with the `function` keyword.

Immutability is one of the main characteristics of the functional paradigm. In OCaml, however, the programmer is not limited by immutability, since the language also features numerous imperative constructs. This includes mutable variables, through references, arrays, and loops. Observe the imperative version of the previously presented `count` function:

```ocaml
let count_imp x a =
  let r = ref 0 in
  for i = 0 to Array.length a - 1 do
    if a.(i) = x then r := !r + 1
  done;
  !r
```

Unlike other languages, OCaml's `for` loop is quite different, it does not directly support early stopping (can still be achieved by using exceptions) nor defining a different step. The `to` keyword is used to increment the loop variable by one in each iteration. Alternatively, the `downto` keyword is used for decremental iterations, with these two keywords being the only available options for the loop's step. Moreover, the terminal value (`i.e.` the one that comes after `to` or `downto`) is inclusive, that is why we must subtract one from the array's length. Another particularity in OCaml is its syntax concerning array operations. To access an index of an array one must use `a.(i)` instead of the usual `a[i]`. Mutable variables, `i.e.` references, are declared using the `ref` keyword, which is placed immediately before the initial value. Operations to manipulate mutable variables include dereferencing (`!`), to read its current value, and updating (`:=`).

1.5.3 GOSPEL and Cameleer

The Generic OCaml SPEcification Language (GOSPEL), as the name states, is a specification language for OCaml programs that is not tied to a single tool or purpose, as such, other developers may use it as they see fit. Besides Cameleer, which is the focus of this work, other tools that use GOSPEL include `Ortac` and `Why3gospel`. Cameleer is a tool that enables the deductive verification of OCaml programs with GOSPEL annotations within the Why3 platform. Internally, these programs are translated into an WhyML equivalent, which is Why3's specification and programming language. Some advantages of this platform include the use of multiple third-party theorem provers, either interactive or automatic, and treating each proof goal independently. As we have mentioned before, the base of Deductive Verification is Hoare Logic. We can equip an OCaml function with pre- and post-conditions, similar to a Hoare triple, with GOSPEL as seen below:

GOSPEL + OCaml

```
let seconds_to_hours s =
  let h = s / 3600 in
  let r = s mod 3600 in
  let m = r / 60 in
  let s' = r mod 60 in
  (h, m, s')
(*@ h, m, s' = seconds_to_hours s
    requires s >= 0
    ensures 3600*h + 60*m + s' = s *)
```

GOSPEL annotations are written in the form of special comments, with the intent of OCaml's compilers ignoring these annotations and compiling successfully. To distinguish from regular comments, a special syntax with the at sign (@) is used: `(*@ ... *)`. Pre-conditions start with the `requires` keyword. In this case, the input parameter `s` (the number of seconds to be converted) must be a non-negative integer. On the other hand, post-conditions are represented with the `ensures` keyword, and in this context we must guarantee that the result is effectively correct, by re-converting each component to seconds, using the respective unit conversion rate, and summing the three to obtain the original value. In GOSPEL, by default, the parameters retain their original identifier, and if the function returns a value, then it can be accessed in the annotation with the identifier `result`. However, one may re-define these identifiers, as shown in the first line in the comment of the example above. In this case, that line also holds a special purpose, it explicitly deconstructs the tuple into single elements.

The previous function is automatically proven to terminate by the SMT solvers effortlessly, since it does not perform any kind of recursion or iteration. However, that is not always the case. For instance, consider the `count` function previously presented:

GOSPEL + OCaml

```
let rec count x l =
  match l with
  | [] -> 0
  | h::t -> (if x = h then 1 else 0) + count x t
(*@ r = count x l
    variant l
    ensures 0 <= r <= List.length l
    ensures r > 0 -> List.mem x l
    ensures r = 0 -> not List.mem x l *)
```

When dealing with recursive functions or `while` loops (not `for` loops since those have a guaranteed finite number of iterations), termination must be proven. This can be achieved with a monotonically decreasing expression that remains non-negative during iteration, in other words, the value of the expression in a given iteration must be strictly smaller than in the previous iteration, and both must be non-negative. In the context of the `count` function, using the length of the list suffices to prove its termination, since each recursive call deals with the tail of the current list, therefore each successive call receives a list with one less element than the previous, and the length of a list is undeniably non-negative. Alternatively, one may use the list itself, instead of `List.length l`, which checks the structure of the list, rather than just its length, however it works similarly.

If readers notice closely, this function returns the number of elements in a list that comply with a given property, this being the equality to a given element. However, since some elements may not comply with this property, it is not possible to quantify this exact amount with either the existential or universal quantifiers. To do so, we would need to introduce more complex GOSPEL constructs, which is not the objective of this chapter, but it will be done so in the next chapters of this textbook. So, for now, let us focus on partial correctness guarantees. In this field, it is important to be ambitious and aim to provide the strongest known safety guarantees, however that may not always be possible, for instance due to tool limitations, as such, knowing when to relax a problem is also a great quality. Whenever it is not possible to check for the exact result, then a more relaxed alternative is to restrict it to an interesting interval. In this case, the result ranges from 0 and the length of the list (both inclusive), since `x` (the value to be counted) may not be present in the list, or, at most, all elements of the list have the value of `x`. This leads to the second and third post-conditions, if the result is positive, then `x` must belong to the list, inversely, if the result is 0, `x` does not belong in the list.

Moving on to the imperative version of this function. It is important to take into account that `for` and `while` loops are also meant to be annotated, which leads to multiple GOSPEL annotations in the same function. In this case, `counter_imp` contains a single `for` loop, so, in total, it must contain two annotations: one applied to the function body, as a whole, and the other, internally, to the `for` loop. Starting with the function body:

GOSPEL + OCaml

```
let count_imp x a = (* ... *)
(*@ r = count_imp x l
    ensures 0 <= r <= Array.length l
    ensures r > 0 -> Array.mem x l
    ensures r = 0 -> not Array.mem x l *)
```

For the most part, the specification above is quite similar to its functional counterpart. The only real difference consists in the use of the operations provided by the array library, which should not be surprising, since we are dealing with arrays rather than lists. A possible approach to specify the `for` loop is as follows:

GOSPEL + OCaml

```
for i = 0 to Array.length a - 1 do
(*@ invariant 0 <= !r <= i
    invariant !r > 0 -> Array.mem x l
    invariant !r = 0 -> forall k. 0 <= k < i -> a.(k) <> x *)
  if a.(i) = x then r := !r + 1
done;
```

When specifying loops, it is important to remember that we are no longer able to use pre- and post-condition. Instead, invariants should be used, and these are logical properties that must hold both at the start and end of an iteration, including at the time of entering and exiting the loop. Finding the correct invariants is an arduous task, a general guideline is that they are related to function's post-conditions, although other invariants may be necessary. Also note that given the iterative nature of loops, at any given point only a subset of the arrays has been covered, hence, these properties may need to be adapted, based around the iteration variable (in this case i), instead of the array as a whole. This can be seen in the first invariant, where the upper bound becomes i, instead of the length of the array. This can be explained from the fact that when exiting a given iteration, the visited indexes range from 0 to i (both inclusive), and we can state for certain that, as most, r may hold the value of i. That property holds when entering the loop, since the upper bound is inclusive ($0 \leq$ `!r` ≤ 0). If we were to set a higher upper bound, namely the length of the list, that would logically mean that, when entering an intermediate iteration, `r` could already hold the length of the list, and at the time of exiting the loop, `r` could be incremented by one, which would break the loop invariant. The second loop invariant remains unchanged, since we are only confirming than a positive result leads to belonging in the list, once again this is a more relaxed condition, to preserve the simplicity of the example. By contrast, that is not the case when `r` holds 0, since occurrences of `x` may be present in the remainder of the list, which must be taken into account. The solution is to define the interval of indexes that have already been traversed, namely from 0, inclusive, up to i, exclusive. Note that the upper bound is exclusive ($<$), otherwise when entering a given iteration we would already be including a value that has not yet been processed, which would lead to an incorrect proof.

1.5.4 Cameleer and Why3

As previously mentioned, Cameleer uses the Why3 platform in order to verify OCaml programs with possibly several SMT-solvers allowed by that platform. So, this may raise the question: how to use Cameleer? Assuming that we have an OCaml program in our file system, we can open a terminal in that directory and type:

```
cameleer [filename].ml
```

This will launch the Why3 IDE, which we will explain briefly in this subsection with various images and how to conduct a concrete proof, this being the `seconds_to_hours` function from before. To start, let us present the interface that is displayed immediately after the command above:

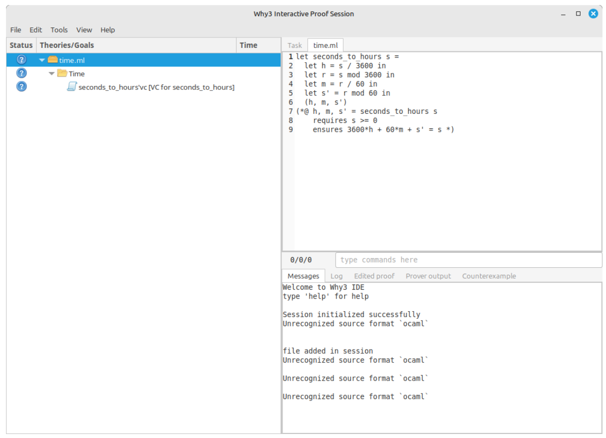

Figure 1.1: Why3 IDE

On the left side we can see the generated proof goals. In this case we can see three nested proof goals, the top-most being the file as a whole, and the innermost being the `seconds_to_hours` function. The goal in the middle is an implicit module that wraps all functions in the file. The more (external) functions we have in our file, the more proof goals will be generated. If we were using OCaml's module system (which we will cover in the last chapters) this would also generate more proof goals. To dispatch the SMT-solvers we can select any proof goal and click one of the following keys: 0, 1, 2 and 3. Each key has a different time limit imposed by Why3 due to the halting problem, which is the famous limitation of being impossible to create a program that can determine if another program will terminate execution or run forever. So, Why3 can not determine if the SMT-solvers will ever terminate checking a proof goal. This leads us to discussing the aforementioned keys and respective time limits:

- **0** – Time limit of 1s.
- **1** – Time limit of 5s.
- **2** – Starts with a time limit of 1s. If it fails, increases time limit to 10s.
- **3** – Starts with a time limit of 1s. If it fails, increases time limit to 5s. Finally, increases time limit to 30s, and may perform special proof goal splits.

When pressing one of these keys, it recursively dispatches the SMT-solvers to any children proof goals. Alternatively, if every child proof goal is successfully verified, then the parent is automatically updated. Since this is a simple case study it suffices to press 0 on any of the proof goals to successfully verify it:

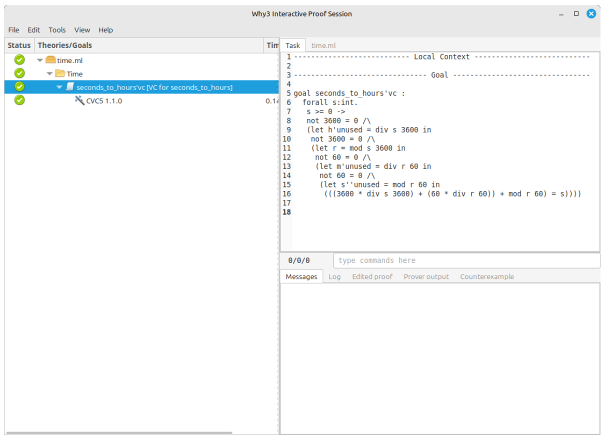

Figure 1.2: Successful proof

Taking a step back, the second most import window in Why3 is the `Task` window on the top right side. This window displays our current goal and the context behind it:

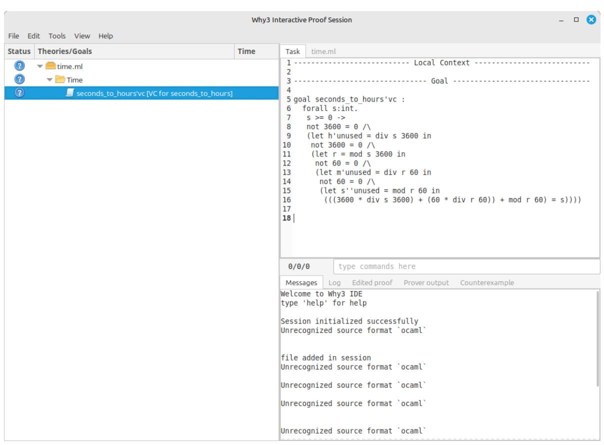

Figure 1.3: Before splitting

Despite the simplicity of the function, the goal looks complex. Using the **s** key will split the selected proof goal into smaller goals, and, if pressed repeatedly, also simplifies its descendants. Although, splitting may not always be possible.

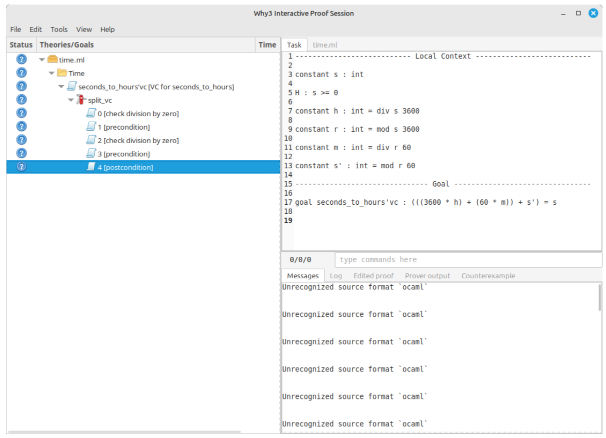

Figure 1.4: After splitting

By selecting one of the new sub-goals, we can observe how the logical context changes. For instance, proof goal 4 has a simpler expression, this being $3600 * h + 60 * m + s' = s$. Moreover, the other sub-goals are used as hypotheses, despite not being proven yet. Treating proof goals independently of each other is one of Why3's advantages. The proof is, also, successful after splitting:

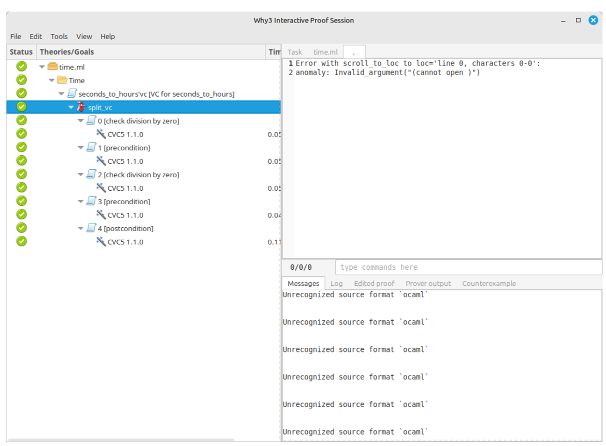

Figure 1.5: Successful proof with simpler goals

Chapter 2

Arithmetic

2.1 Extended Euclidean Algorithm

We begin our algorithmic journey with Euclid's classical method to calculate the greatest common divisor (gcd) of two numbers, for instance:

$$\gcd(72, 48) = 24$$

$$\text{Divisors of } 72 = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72\}$$
$$\text{Divisors of } 48 = \{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}$$

But, how does Euclid's algorithm work? This is the most important question to answer from both the programming and verification perspectives. This classical algorithm has been studied for centuries, with the original idea being based on the subtraction operation, while a more recent and optimized method uses the remainder operation. For the time being, we will concentrate on the latter:

Algorithm 1 (Optimized Euclidean Algorithm) *Given an integer, x, that differs from 0, and an integer, y, find their greatest common divisor.*

1. *If $y = 0$ then return n;*
2. *Calculate the remainder: $r = x \,\%\, y$;*
3. *Set $x \leftarrow y$, $y \leftarrow r$, go back to step (1).*

Not only that, but we will also consider the extended version of the algorithm. This version also calculates the Bézout's coefficients, two additional numbers, that comply with Bézout's Identity.

Lemma 1 (Bézout's Identity) *Let x and y be integers with d as their greatest common divisor. Then, there exists integers a and b such that x*a + y*b = d.*

This lemma is quite powerful, since it combines the two input numbers and the respective greatest common divisor in a single equation. A purely functional implementation of the extended Euclidean algorithm can be seen below:

OCaml

```
let rec extended_gcd x y =
  if y = 0 then (1, 0, x)
  else
    let q = x / y in
    let (a, b, d) = extended_gcd y (x - q * y) in
    (b, a - q * b, d)
```

Before analysing the code, we must first consider the input and output of the `extended_gcd`, it receives two parameters x and y, as expected, and recursively calculates the two Bézout's coefficients and the greatest common divisor of x and y, respectively, as an ordered triple. With this in mind, let's have a look into two examples:

$$\begin{aligned} &\text{egcd}(72, 48) = (1, -1, 24) \\ &\text{egcd}(48, 24) = (0, 1, 24) \\ &\text{egcd}(24, 0) = (1, 0, 24) \end{aligned} \qquad \begin{aligned} &\text{egcd}(1071, 462) = (-3, 7, 21) \\ &\text{egcd}(462, 147) = (1, -3, 21) \\ &\text{egcd}(147, 21) = (0, 1, 21) \\ &\text{egcd}(21, 0) = (1, 0, 21) \end{aligned}$$

The base case is simple to explain, the last call to the `extended_gcd` (`egcd` for short) function contains the result in parameter x and the value 0 in parameter y. As such, the Bézout's coefficients should be 1 and 0, respectively, to maintain Bézout's Identity:

$$\begin{aligned} 24 &= 24 * 1 + 0 * 0, \text{ when egcd}(24, 0) \text{ in egcd}(72, 48) \\ 21 &= 21 * 1 + 0 * 0, \text{ when egcd}(21, 0) \text{ in egcd}(1071, 462) \end{aligned}$$

One way to calculate the remainder is to use the Euclidean division lemma:

Lemma 2 (Euclidean Division) *Given two integers, a and b, with $b \neq 0$, then, there exists two unique integers, q and r, such that: $a = b * q + r$, with $0 \leq r < |b|$*

By applying this lemma to our context, we obtain:

$$\begin{aligned} &x = y * q + r \\ &r = x - y * q \text{ (q is the integer division between } x \text{ and } y) \\ &r = x - y * \lfloor x/y \rfloor \end{aligned}$$

Since each intermediate result respects Bézout's Identity, the recursive step can be obtained by comparing two consecutive calls:

$$d = x_n * a_n + y_n * b_n \text{ (Step } n\text{)}$$
$$d = x_{n+1} * a_{n+1} + y_{n+1} * b_{n+1} \text{ (Step } n+1\text{)}$$
$$\text{With } x_n = y_{n+1} \text{ and } y_n = x_{n+1} - q * y_{n+1}$$

$$d = x_n * a_n + y_n * b_n \equiv$$
$$d = y_{n+1} * a_n + (x_{n+1} + q * y_{n+1}) * b_n \equiv$$
$$d = y_{n+1} * a_n + x_{n+1} * b_n + q * y_{n+1} * b_n \equiv$$
$$d = x_{n+1} * b_n + y_{n+1} * (a_n + q * b_n)$$

$$\therefore a_{n+1} = b_n \text{ and } b_{n+1} = a_n - q * b_n$$

This result is exactly what is stated in `let (a, b, d) = extended_gcd y (x - q * y) in (b, a - q * b, d)`. The triple `(a, b, d)` corresponds to the n-th step, while `(b, a - q * b, d)` is the next. Also, note that `d`, the greatest common divisor, does not change between steps.

This previous discussion, although displayed somewhat informally, is a proof by induction, in which, one must present the base case, usually constant values that comply with a given formula, and the inductive step, where one has to reach the formula for step $n + 1$ from the previous step. From a machine-checked proof perspective, proofs by induction are quite powerful. Moreover, the fact we calculate the Bézout's coefficients for every function call is a very effective way guarantee that the Bézout's Identity is maintained every time. Alternatively, it would be possible to use the existential quantifier, however, these logical constructs are notoriously difficult to be checked by machines, due to potentially large value spaces. With the mathematical background out of the way, we present specified `OCaml` code:

GOSPEL + OCaml

```
let rec extended_gcd x y =
  if y = 0 then (1, 0, x)
  else
    let q = x / y in
    let (a, b, d) = extended_gcd y (x - q * y) in
    (b, a - q * b, d)
(*@ (a, b, d) = extended_gcd x y
    requires x <> 0
    variant abs y
    ensures d = a*x + b*y *)
```

The optimized version of the algorithm is prepared to deal with negative numbers, since it uses the remainder (although indirectly in our case), therefore the only restriction on the inputs is that x must be different from 0. This is due to x holding the result in the final functional call, and a divisor, by definition, is a value different from 0. Furthermore, y is the stopping condition, in the form of the value 0, as such, there are no additional requirements. The `ensures` clause is simply the Bézout's Identity formula, which, once more, is a very strong property that guarantees that `d` is effectively the greatest common divisor of x and y. Finally, the `variant` clause serves to prove the termination of `while` loops and recursive functions. This is obligatory due to the halting problem, a famous computational limitation which precludes the creation of a program that can always determinate if another program terminates. As such, we have to provide a non-negative expression that strictly decreases in every iteration. In this case, `abs y`, the absolute value is essential for dealing with initial values of x or y that are negative, since the subsequent values of y may bounce between positive and negative values, hence not making a clear monotonically decreasing expression.

2.2 McCarthy 91 function

An historical example in Formal Verification is the McCarthy 91 function. It was developed in 1970 by John McCarthy, Zohar Manna and Amir Pnueli, with the purpose of testing verification tools. In the past, it was viewed as a difficult problem due to its nested recursion, in particular, for automated tools. At the time of writing this book, it does not pose as much of a challenge any more due to significant advancements in automated tools. Mathematically, the 91 function is defined as:

$$M(n) = \begin{cases} M(M(n+11)), & \text{if } n \leq 100 \\ n - 10, & \text{if } n > 100 \end{cases}$$

The particularity of this function is that it converges to 91 for any integer value of $n \leq 100$. For $n = 101$ it also results in 91, however, from there it increases by 1 in comparison to the previous, for instance, $M(102) = 92$, $M(103) = 93$, and so forth. While this particularity is hard to visualize at first glance, it is clear when analysing the recursive calls for a given n, for example:

$$
\begin{aligned}
M(88) &= M(M(99)) \\
&= M(M(M(110))) \\
&= M(M(100)) \\
&= M(M(M(111))) \\
&= M(M(101)) \\
&= M(91) \\
&= M(M(102)) \\
&= M(92) \\
&= M(M(103)) \\
&= \ldots && \text{(The pattern from M(91) onwards repeats)} \\
&= M(100) \\
&= M(M(111)) \\
&= M(101) \\
&= 91
\end{aligned}
$$

Based on this example, it is possible to see that the recursive calls easily form patterns, such as the one from $M(M(99))$ to $M(M(101))$ or from $M(91)$ to $M(100)$.

Representing a recursive mathematical function in OCaml is quite straightforward, by using an `if-expression` to model the two branches:

GOSPEL + OCaml

```
let rec f91 n =
  if n <= 100 then f91(f91 (n + 11))
  else n - 10
(*@ r = f91 n
    variant 101 - n
    ensures n <= 100 -> r = 91
    ensures n > 100 -> r = n - 10 *)
```

Due to the simplicity of the function, we have also decided to present the specification. In terms of pre-conditions, there are no restrictions to the value of n, since this function also allows negative numbers, as such, we can omit the `requires` clause. The correctness of this function can be expressed conditionally, based on the two possible outcomes, with logical implications: one for $n \leq 100$ where the result is always 91, and another for $n > 100$, where the result is $n - 10$. Alternatively, in GOSPEL, one may use an `if-expression` (or even pattern matching) to express conditional properties:

GOSPEL

```
(*@ r = aux n
    variant 101 - n
    ensures if n <= 100 then r = 91
            else r = n - 10 *)
```

To prove termination we have to find a non-negative monotonically decreasing expression. In this case, the only variable at our disposal is n, as such, we have to include it somehow. If we analyse the outermost function calls in the $M(88)$ execution example, it is possible to observe that the argument is increasing, so to obtain a decreasing expression we must use $-n$ as a term. Another possible observation, is that n converges to 101, exactly one of the boundary values of function M, and the one that fits inside the non-recursive case. This leads to the expression $101 - n$ that can prove the termination.

2.3 Euclidean Division

Until now, we have covered two examples with purely functional implementations. So, in this section we will present an imperative version of the Euclidean Division algorithm. This algorithm is known to perform divisions through repeated subtractions, and is based on the previously mentioned lemma 2. The lemma states that for integers x and y the equation $x = y * q + r$ with $b \neq 0$ and $0 \leq r < |b|$ is unique. The second condition ($0 \leq r < |b|$) is exactly what restricts the equation to a single solution. So, if we, momentarily, disregard it, then it is possible to find multiple solutions, for instance:

$$
\begin{aligned}
&\text{Let } x = 13 \text{ and } y = 6, \text{ then} \\
&13 = 6 * 0 + 13 \quad (q = 0; r = 13) \\
&13 = 6 * 1 + 7 \quad\;\; (q = 1; r = 7) \\
&13 = 6 * 2 + 1 \quad\;\; (q = 2; r = 1)
\end{aligned}
$$

If we look closely at the previous example, then it is possible to find a pattern, if we increase q by unit then we must subtract y from r. This is exactly the process found in the Euclidean Division algorithm, and can easily be proven mathematically:

$$
\begin{aligned}
&x = y * (q + 1) + (r - y) \equiv \\
&x = y * q + y + r - y \equiv \\
&x = y * q + r
\end{aligned}
$$

Algorithm 2 (Euclidean Division) *Given a non-negative integer, x, and a positive integer, y, find the quotient, q, and remainder, r, that comply with Euclid's lemma.*

1. *Set $r \leftarrow x$ and $q \leftarrow 0$;*
2. *While $r \geq y$ do: set $r \leftarrow r - y$ and $q \leftarrow q + 1$*
3. *Return q and r.*

The first step effectively amounts to saying that x is equal to itself, since $q = 0$. Not only is this the safest choice possible, but it is also the only correct one, because when dealing with a smaller divided, x, in comparison to the divisor, y, it respects the following result:

Let $y > x$, then let $q = 0$ and $r = x$

$x = y * 0 + x \equiv$

$x = x$

Note that $0 \leq r < |y|$, since $0 \leq x < y$

$\therefore$ Euclid's lemma is valid in these conditions.

On the other hand, if we are dealing with a larger divided, eventually the remainder will be in the Euclid's lemma conditions, because the loop's exit condition is $r < y$, and given that in this implementation y is strictly positive, then it is equivalent to $r < |y|$, in this context. This algorithm can be implemented in OCaml as:

OCaml

```
let euclidean_div x y =
  let r = ref x in
  let q = ref 0 in
  while !r >= y do
    r := !r - y;
    q := !q + 1;
  done;
  (!q, !r)
```

Syntactically, a mutable variable is declared in OCaml with the `ref` keyword preceding the initial value, which can later be changed using the attribution operator (`:=`) or accessed using the `!` operator. Unlike other languages, such as C or Java, the `;` in OCaml does not represent the termination of a command, instead, it is used to sequence multiple operations. It is commonly used in conjunction with imperative features, since the result of a sequence operation is the result of its last expression, meaning that the previous results are discarded, and are, generally, expected to produce side effects, such as printing or altering the memory state.

The previous code can be proven with the following specification:

GOSPEL + OCaml

```
let euclidean_div x y = (* ... *)
(*@ (q, r) = euclidean_div x y
    requires x >= 0
    requires y > 0
    ensures x = y * q + r
    ensures 0 <= r < y *)
```

For presentation purposes we omitted the body of the function. However, it is worth noting that it contains a `while` loop that must also be specified, which can be found in the listing below. As previously mentioned, this implementation of the Euclidean Division algorithm is only capable of handling non-negative dividends ($x \geq 0$) and positive divisors ($y > 0$), since the division by 0 is not defined. The first `ensures` clause correspond to the Euclidean lemma equation, while second clause concerns the condition on the remainder to make it and the quotient unique values.

GOSPEL + OCaml

```
while !r >= y do
(*@ invariant x = y * !q + !r
    invariant 0 <= !r
    variant !r *)
        (* ... *)
done;
```

Inside the `while` loop the $0 \geq r < |y|$ is not valid, since $r > y$, however, we must guarantee that r remains positive, so that the condition is valid at the end of the loop. However, the equation is always respected as we have proven mathematically before. Given that the value of r is strictly positive and decreases in every iteration, it suffices to prove termination in the `variant` clause.

2.4 Fibonacci sequence

The Fibonacci sequence is well-known for its primary characteristic: each element is the sum of the two previous values (with the exception of the first elements). Its first twelve elements are:

$$\text{Fibonacci sequence: } 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...$$

In this textbook we consider 0 to be the first element, although there is some discourse on whether the Fibonacci sequence starts with 0 or 1. Given our choice, the corresponding mathematical definition is:

$$\text{Fib}(n) = \begin{cases} 0, & \text{if } n = 0 \\ 1, & \text{if } n = 1 \\ \text{Fib}(n-1) + \text{Fib}(n-2), & \text{if } n \geq 2 \end{cases}$$

In contrast to the previously presented examples, the Fibonacci sequence is not described by a linear equation or simple conditional case study, but rather by the mathematical function above. As such, we present one more feature available in GOSPEL, logical functions:

GOSPEL

```
(*@ function rec fib (n: int) : int =
    if n <= 1 then n
    else fib (n-1) + fib (n-2) *)
(*@ requires n >= 0
    variant n *)
```

These functions can be used to express complex behaviours from a logical perspective. However, when multiple versions are available (for instance consider the recursive, memoized or the iterative versions of the Fibonacci sequence) it is recommended to pursue simplicity instead of performance, as the proof may become more demanding. For this reason, we have selected the recursive version of the Fibonacci sequence for the logical definition. Usually, when one defines a logical function, it is because there is no other way to express the corresponding behaviour, so, we have to manually ensure that it is correct. Although, it is possible to annotate the function with more general properties, such as only receiving non-negative numbers as input (`requires n >= 0`).

By using the recursive Fibonacci variant as a logical function, we are able to verify any Fibonacci implementation, including itself:

GOSPEL + OCaml

```
let rec recursive_fib n =
  if n <= 1 then n
  else recursive_fib (n-1) + recursive_fib (n-2)
(*@ res = recursive_fib n
    requires n >= 0
    variant n
    ensures res = fib n *)
```

The biggest difference is that we are now able to guarantee the correctness of the result, in other words, ensure that it is in fact the n-th number in the Fibonacci sequence. However, beware that this is not a good practice. Ultimately, what we did was to copy the implementation of our desired algorithm and adapted it to a logical function, not only is this very uninteresting from a verification perspective, since it is the same code with a few syntactic differences, but it may induce subtle errors, given that a faulty logical function will negatively condition the proof. Ideally, we should aim to verify a different version of the algorithm, for instance, dynamic programming applied to Fibonacci:

GOSPEL + OCaml

```
let fib_iter n =
  let y = ref 0 in
  let x = ref 1 in
  for i = 0 to n - 1 do
  (*@ invariant !y = fib i
      invariant !x = fib (i+1) *)
    let sum = !y + !x in
    y := !x;
    x := sum
  done;
  !y
(*@ res = fib_iter n
    requires n >= 0
    ensures res = fib n *)
```

Recursion, despite being a beloved feature by the functional programming enthusiast, has a clear archenemy, if used naively: finite memory, a sufficiently large input may generate more function calls than memory available. Moreover, the lack of memory is also a common problem, this means that the same input may be recalculated multiple times. The recursive Fibonacci is commonly used to exemplify these limitations, due to the two recursive calls. To solve these problems there are numerous optimization techniques, with one of the best being a domain-specific solution that iteratively calculates the current value (x) and the next (y). From a verification perspective, the annotation of the main function is quite similar from the previous example, the input number n should be non-negative, and the result should indeed correspond to the n-th number in the Fibonacci sequence. Given that this solution uses a `for` loop, which has a finite number of steps, there is no need to prove termination, however, we must guarantee a few invariant properties, i.e. properties that are true both at the start and end of an iteration, but may break in the middle of the iteration. In particular, the y variable must contain the value in the sequence of the current index, while x contains the next element.

Previously, we have introduced logical functions in GOSPEL, while, alternatively, it is also possible to write these constructs directly in OCaml, using GOSPEL tags:

GOSPEL + OCaml

```
let[@ghost][@logic] rec fib n =
  if n <= 1 then n
  else fib (n - 1) + fib (n - 2)
(*@ r = fib n
    requires n >= 0
    variant n *)
```

One of the advantages of using this technique is to make use of OCaml features that are not present in GOSPEL, such as type inference. OCaml functions, by default, are not visible in the logical domain, even within the corresponding annotation, for instance, the following example with the identity function produces an error:

GOSPEL + OCaml

```
let f x = x
(*@ r = f y
    ensures f r = y *)
```

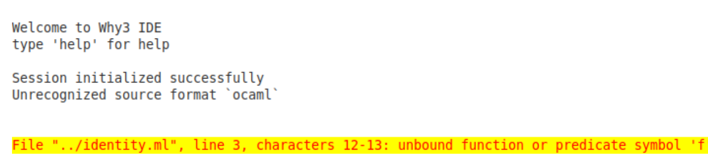

Figure 2.1: Scoping error from OCaml to GOSPEL

While we are allowed to write f in the first line of the annotation, this line only serves the purpose of renaming variables, in this case, *result* (default and hidden name for the function's result) to r, and x to y. However, when specifying any kind of behaviour, calling f is prohibited, since it is not considered in scope. The `logical` tag, could be used for this purpose, however, only works for the functions below it, so a corrected (and expanded) version of the previous example would be:

GOSPEL + OCaml

```
let[@logic] f x = x
(*@ r = f y
    ensures r = y *)

let g x = f x
(*@ ensures result = f x *)
```

The ghost tag, will be discussed in more detail in the next chapter, but the basic notion is that it must not affect the result, either directly or indirectly. So, the combination of these two tags perfectly resembles the behaviour of a GOSPEL logical function, those cannot be called by other OCaml functions given their representation as OCaml comments, but are available in later GOSPEL annotations. Ghost code can be called by other OCaml functions, but when doing so, whatever code associated with it must also be ghost.

2.5 Revisiting Extended Euclidean Algorithm

From a practical standpoint, when one uses the Euclidean Algorithm it is most likely to calculate the greatest common divisor. The extended version does have realistic use cases, however, in our context it is mainly used for its logic properties to facilitate the verification process. As such, returning a triple with the Bézout's coefficients and the greatest common divisor, similar to section 2.1, contains too much information. In this section we will revisit the extended Euclidean algorithm with an imperative and iterative implementation that uses ghost code for the Bézout's coefficients.

Contrary to the recursive function, the process to calculate the coefficients becomes slightly more complex, since we are computing in the "opposite direction". In this version, we must store both the current pair of Bézout's coefficients candidates and the next. The current pair will be associated with the current x, while the next pair is associated with the current y, since the next x will be the current y:

For step n, we know that:
$x_n = a_n * x + b_n * y$
$y_n = a_{n+1} * x + b_{n+1} * y$

Where:
- x and y are the numbers from the original input
- x_k and y_k are the derived numbers from the input at step k
- a_k and b_k are the coefficients at step k

For step $n+1$, and based on previous results, we know:

$$\begin{aligned} x_{n+1} &= y_n \\ &= a_{n+1} * x + b_{n+1} * y \\ y_{n+1} &= x_n \,\%\, y_n \\ &= x_x - y_n * q_n \end{aligned}$$

Where:
- % is the remainder operator
- q_k is the integer division of x_k by y_k

Then:

$$\begin{aligned} y_{n+1} &= x_x - y_n * q_n \\ &= (a_n * x + b_n * y) - (a_{n+1} * x + b_{n+1} * y) * q_n \\ &= (a_n * x) - (a_{n+1} * x * q_n) + (b_n * y) - (b_{n+1} * y * q_n) \\ &= (a_n - q_n * a_{n+1}) * x + (b_n - q_n * b_{n+1}) * y \\ &= a_{n+2} * x + b_{n+2} * y \end{aligned}$$

$$\therefore\ a_{n+2} = a_n - q_n * a_{n+1} \ \wedge\ b_{n+2} = b_n - q_n * b_{n+1}$$

The previous results demonstrate the formula to update the coefficients candidates, in particular, and using auxiliary variables:

$$\begin{aligned} a_{aux} &\leftarrow a_{current} & b_{aux} &\leftarrow b_{current} \\ a_{current} &\leftarrow a_{next} & b_{current} &\leftarrow b_{next} \\ a_{next} &\leftarrow a_{aux} - q * a_{next} & b_{next} &\leftarrow b_{aux} - q * b_{next} \end{aligned}$$

The last remaining detail that needs to be discussed is what values should be used to initialize the coefficient candidates:

At step 0, $x_0 = x$ and $y_0 = y$, as expected.
So, using the generic formulas from before:
$x_0 = a_0 * x + b_0 * y \equiv \qquad (x_0 = x)$
$x = a_0 * x + b_0 * y$

$y_0 = a_1 * x + b_1 * y \equiv \qquad (y_0 = y)$
$y = a_1 * x + b_1 * y$
The most natural candidates are:
$a_0 = 1$, $b_0 = 0$, $a_1 = 0$ and $b_1 = 0$

With this in mind, we can now present the algorithm implemented in OCaml:

GOSPEL + OCaml

```
let gcd x y =
  let xs = ref x and ys = ref y in
  let [@ghost] a = ref 1 and [@ghost] a_next = ref 0 in
  let [@ghost] b = ref 0 and [@ghost] b_next = ref 1 in

  while !ys > 0 do
    let[@ghost] q = !xs / !ys in
    let r = !xs mod !ys in
    xs := !ys;
    ys := r;

    let a' = !a in
    a := !a_next;
    a_next := a' - q * !a_next;

    let b' = !b in
    b := !b_next;
    b_next := b' - q * !b_next;

  done;
  !xs
```

This code closely follows what we have discussed previously, we start by initializing six references, so that the value may be changed later. Reference xs will, eventually, contain the result and is derived from the argument x, similarly, ys is derived from y, although it is used to check the termination of the algorithm. Additionally, a and b are the current coefficient candidates, a is associated with x, while b is related to y. Since, this version requires to be one step ahead, a_next and b_next contain the values of the coefficient candidates in the next step, respectively. By using the `[@ghost]` tag these values are strictly used for logical purposes. Inside the `while` loop, the new value of xs will be the current value of ys, while ys is updated to the remainder of xs by ys (before updating the values). In terms of the coefficients, we use the mathematical formulas we have reached and demonstrated previously. The main function can be specified as:

GOSPEL + OCaml

```
let gcd (x:int) (y:int) = (* ... *)
(*@ r = gcd x y
    requires x >= 0
    requires y >= 0
    ensures exists a,b. r = a*x+b*y *)
```

This implementation is not ready to deal with negative numbers, so for it to function well, we must restrict the domain of the inputs to the non-negative numbers. As previously mentioned, `exists` statements are notably hard for machines to prove, since the value space might be extremely large and checking every single value is not a valid strategy. Instead, we, as programmers, must help the machine, and this is possible with the following specification on the `while` loop:

GOSPEL + OCaml

```
while !ys > 0 do
(*@ invariant !xs >= 0
    invariant !ys >= 0
    invariant !xs = !a * x + !b * y
    invariant !ys = !a_next * x + !b_next * y
    variant !ys *)
  (* ... *)
done;
```

Undoubtably, the two last invariants, these being:

- `invariant !xs = !a * x + !b * y`

- `invariant !ys = !a_next * x + !b_next * y`

are very important conditions, why? The former guarantees that, when exiting the loop, the post-condition `ensures exists a,b. r = a*x+b*y` is true, since `xs` contains the final result, `r`, and we provide one example of a concrete instantiation for the existential quantifier (through the ghost references `a` and `b`). On the other hand, the latter `invariant` serves to guarantee that on the next iteration `xs` also complies with the former `invariant`, since the reference `xs` is updated with the value of the reference `ys`, as well as `a` and `b` with `a_next` and `b_next`, respectively. The two other invariants conditions, `!xs >= 0` and `!ys >= 0` serve to ensure that the values are well-behaved and are within the expected interval, which is the set of non-negative integers. To prove termination, the value of the `ys` reference (`!ys`) suffices, since it is positive and decreases each iteration.

2.6 Fast Exponentiation

Fast Exponentiation, also known as Exponentiation by Squaring, is an efficient algorithm to computer the power of a number, and is particularly relevant when dealing with large exponents. It is mathematically defined as:

For $n > 0$, then:

$$x^n = \begin{cases} (x^2)^{\frac{n}{2}}, & \text{if } n \,\%\, 2 = 0 \\ x * (x^2)^{\frac{n-1}{2}}, & \text{if } n \,\%\, 2 = 1 \end{cases}$$

This is possible due to the following properties:
- $n^a * n^b = n^{a+b}$
- $(n^a)^b = n^{a*b}$

So:
- when n is even: $x^n = x^{2*\frac{n}{2}} = (x^2)^{\frac{n}{2}}$
- when n is odd: $x^n = x * x^{n-1} = x * x^{\frac{2*(n-1)}{2}} = x * (x^2)^{\frac{n-1}{2}}$

From a computational perspective, this method allows to progressively calculate smaller components, in the form of powers of two, rather than a single larger exponent at once, for instance:

$$\begin{aligned}
3^5 &= 3 * (3^2)^{\frac{5-1}{2}} && \text{(simplify)} \\
&= 3 * 9^2 && \text{(apply fast exp.)} \\
&= 3 * (9^2)^{\frac{2}{2}} && \text{(simplify)} \\
&= 3 * (81)^1 && \text{(apply fast exp.)} \\
&= 3 * 81 * (81^2)^{\frac{1-1}{2}} && \text{(simplify)} \\
&= 3 * 81 * 6561^0 && \text{(simplify)} \\
&= 3 * 81 * 1 && \text{(simplify)} \\
&= 243
\end{aligned}$$

Although applying the fast exponentiation method when $n = 2$ or $n = 1$ is mathematically redundant, it is still computationally advantageous. By following the same procedure uniformly, the final result is always stored in a single variable, which simplifies both the program and its proof. This algorithm can be represented in pseudocode as:

Algorithm 3 (Fast Exponentiation) *Given an integer, x, and a non-negative integer, n, find x^n using the exponentiation by squaring technique.*

1. *Create $r \leftarrow 1$, $p \leftarrow x$ and $e \leftarrow n$;*
2. *While $e > 0$ do:*
   (a) *If e is odd then set $r \leftarrow r * p$;*
   (b) *Set $p \leftarrow p * p$;*
   (c) *If e is odd then set $e \leftarrow (e-1)/2$ else set $e \leftarrow e/2$*
3. *Return r.*

To calculate the final result we need three variables: r to store intermediate results, and eventually the correct value, p and e to keep the intermediate bases and exponents, respectively. The main idea behind this algorithm is that every step the equation $x^n = r * p^e$, until $e = 0$ and $x^n = r$. While the exponent is positive, the first operation of the loop body checks for its parity, if it is odd, then r is updated with the previous value times the current base p, this corresponds to the mathematical operation of separating x^n into $x * x^{n-1}$, with the exception that we do not update the exponent, right away, instead, it is done on the third operation. The second operation updates p by raising it to the power of two, or rather, by multiplying p with itself, this corresponds to the x^2 present in both cases. The previous example is calculated computationally as:

$$\begin{array}{lll} \text{(Step 0)} & r = 1; p = 3; e = 5 & \text{(Is } e > 0\text{? Yes!)} \\ \text{(Step 1)} & r = 3; p = 9; e = 2 & \text{(Is } e > 0\text{? Yes!)} \\ \text{(Step 2)} & r = 3; p = 81; e = 1 & \text{(Is } e > 0\text{? Yes!)} \\ \text{(Step 3)} & r = 243; p = 6561; e = 0 & \text{(Is } e > 0\text{? No!)} \end{array}$$

Result: 243

This algorithm can be implemented in OCaml as:

OCaml

```
let fastexp x n =
  let r = ref 1 in
  let p = ref x in
  let e = ref n in
  while !e > 0 do
    if !e mod 2 = 1 then r := !r * !p;
    p := !p * !p;
    e := !e / 2;
  done;
  !r
```

The most notable difference to the algorithm description is the lack of an `if`-statement on the third instruction inside the `while` loop body. This simplification is possible since `/` operator in OCaml represents the integer division. When e is odd, `e/2` and `(e-1)/2` yield the same result, because `e/2` mathematically produces a rational number, therefore the decimal place is truncated to retain the representation as integer and avoid over-approximations. Another important detail to notice is that the first sequence operator (`;`) refers to the `if`-statement as a whole, rather that solely to the `then` branch.

With this context, we are ready to prove the fast exponentiation algorithm. In the first place, we have to define a logical power function:

GOSPEL

```
(*@ function rec power (x n: int) : int =
    if n = 0 then 1
    else x * power x (n-1) *)
(*@ requires n >= 0
    variant n *)
```

Once more, the recursive and inefficient definition suffices as simplicity matters. The computation of x to the power of n is simply multiplying x by itself n times. In the context of this problem, we restrict the domain of n to the non-negative integers. This logical definition can be used to annotate the `fastexp` function:

GOSPEL + OCaml

```
let fastexp x n = (* ... *)
(*@ r = fastexp x n
    requires n >= 0
    ensures r = power x n *)
```

As expected, the result r should effectively correspond to x raised to the power of n. Additionally, the restriction on n is also applied. The `while` loop is slightly more complicated:

GOSPEL + OCaml

```
while !e > 0 do
(*@ invariant !r * power !p !e = power x n
    invariant !e >= 0
    variant !e *)
  (* ... *)
end;
```

Starting with the termination proof, in this case it is as simple as the value of the reference e, since it decreases every iteration by approximately half, which also guarantees that it says positive given that the integer division between two positive numbers does not return a negative number, at most it is 0, which is the expected value in the last iteration. The second invariant clause serves to guarantee that the exponent does not become negative, due to what we have explained before. However, when launching the provers in the Why3 platform, even with the maximum time limit available, it is clear that the proof is incomplete, why is this?

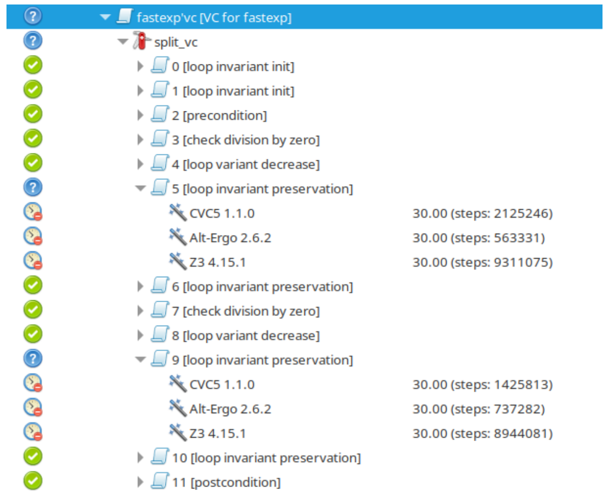

Figure 2.2: Failed Verification Attempt

The previous algorithms could be verified very quickly, additionally, the presented code does not seem to be that much more complex than the rest. This statement is true, time itself is not the issue. Is the previous specification incorrect? Not exactly, it correctly models the logical properties we have discussed beforehand. Instead, there are a few properties concerning the power operation that the theorem provers are not aware. Computers, in general, not just theorem provers or proof assistants, are very good in the domains of mathematics and logic, however, their deduction capabilities are not so stellar, as they are not aware of many properties that may seem intuitive to us as humans. The research and development teams behind verification tools make serious efforts to provide their users with powerful verification libraries with properties such as lemmas, axioms, predicates or even logical functions, however, these libraries must not contain errors, otherwise the logic will be faulty, which is a considerable effort, and many properties will have to be user defined.

In Cameleer, currently, there is not much support regarding the power operation, as such, we will have to define our own lemmas and prove them. And the most natural question to follow-up is: what lemmas do we need? First, let's analyse the first failed goal (number 5) and the respective hypothesis. For goal

5 (using mathematical notation):

$$\begin{aligned}
&H_0\colon\ e_1 \,\%\, 2 = 1\\
&H_1\colon\ e_1 > 0\\
&H_2\colon\ e_1 >= 0\\
&H_3\colon\ r_1 * p_1^{e_1} = x^n\\
&H_4\colon\ n >= 0
\end{aligned}$$

$$\begin{aligned}
\text{Let:}\ & r = (r_1 * p_1)\\
& p = (p_1 * p_1)\\
& e = \lfloor e_1/2 \rfloor
\end{aligned}$$

$$\text{Goal:}\ r * p^e = x^n$$

Let's expand the right-hand side of the equation in hypothesis number three:

$$\begin{aligned}
r_1 * p_1^{e_1} &= r_1 * (p_1^2)^{e_1/2}\\
&= r_1 * p_1 * (p_1^2)^{\lfloor e_1/2 \rfloor}\\
&= (r_1 * p_1) * (p_1 * p_1)^{\lfloor e_1/2 \rfloor}\\
&= r * p^e
\end{aligned}$$

Despite the variable names, this process is the same as saying $x_n = x * (x^2)^{(n-1)/2}$, when n is odd. The last step is trivial to the provers, it simply replaces variables names with their define. The issue is between steps one and two (for presentation purposes is separated into two steps, but may be represented computationally as one). Ideally, we want a lemma that states:

$$\forall n, x \in \mathbb{Z} : n \geq 0 \wedge n \,\%\, 2 = 1 \rightarrow x^n = x * (x^2)^{\lfloor n/2 \rfloor}$$

This lemma can be implemented in GOSPEL as:

GOSPEL
```
(*@ lemma power_odd : forall x n: int.
    n >= 0 && mod n 2 = 1 ->
      power x n = x * (power (x*x) (div n 2)) *)
```

Unlike functions, lemmas do not receive parameters, any variable must be declared with a quantifier. In GOSPEL, a quantifier declaration ends with a dot (.), and type annotations are preceded by a colon (:) (sometimes can be omitted). One syntactical difference in GOSPEL, when compared to OCaml, is that `div` and `mod` are treated as functions, rather than operators, therefore these names precede the input numbers, which are the arguments. Once this lemma is placed in the program (before the function `fastexp`), the previously mentioned goal is now easily cleared. Furthermore, a proof goal for the lemma was also generated, some lemmas can be discharged automatically by the provers, in this case we have to prove it, but we will save it for later. For now, let's consider the second failed goal (number 9), using mathematical notation:

$$
\begin{aligned}
H_0&\colon\ e_1 \,\%\, 2 \neq 1\\
H_1&\colon\ e_1 > 0\\
H_2&\colon\ e_1 >= 0\\
H_3&\colon\ r * p_1^{e_1} = x^n\\
H_4&\colon\ n >= 0\\
\\
\text{Let}&\colon\ p = (p_1 * p_1)\\
&\ \ e = e_1/2\\
\text{Goal}&\colon\ r * p^e = x^n
\end{aligned}
$$

Not surprisingly, we can mathematically prove the previous goal with the following procedure:

$$
\begin{aligned}
r * p_1^{e_1} &= r * (p_1^2)^{e_1/2}\\
&= r * (p_1 * p_1)^{e_1/2}\\
&= r * p^e
\end{aligned}
$$

Similarly, the provers are not aware of the property used in the first step. So, we need to define a similar lemma, mathematically defined as:

$$\forall n, x \in \mathbb{Z} : n \geq 0 \land n \,\%\, 2 = 0 \rightarrow x^n = (x^2)^{\frac{n}{2}}$$

And written in GOSPEL as:

GOSPEL

```
(*@ lemma power_even : forall x n: int.
    n >= 0 && mod n 2 = 0 ->
      power x n = (power (x*x) (div n 2)) *)
```

Once more, this lemma is not automatically discharged by the provers yet. However, we can observe that the `fastexp` function is now fully verified. So, now we have to prove the lemmas. Why is this important? Well, because the Why3 platform uses the lemma as a hypothesis in the next proof goals, independently of being proven beforehand or not. On one hand, this design decision is very useful for prototyping lemmas and prove them afterwards. On the other hand, it puts more responsibility on the user, and may induce lesser experienced users in error, since the lemma itself might be logically inconsistent. So, how can we prove a lemma in GOSPEL? Simple lemmas may be automatically discharged by the provers, when that is not the case, we need to defined what is called as a lemma function. Instead of using the lemma construct in GOSPEL, we will define a function in OCaml with the lemma tag. The annotations on this function correspond to the lemma itself, while its body is the proof. One should start by expressing the specification first, then move to the proof itself. The previous lemmas can be considered obsolete, so we recommended adapting them to lemma functions, starting with the power_even lemma:

GOSPEL + OCaml
```
let[@lemma] power_even (x: int) (n: int) =
(* TODO *)
(*@ requires n >= 0
    requires mod n 2 = 0
    ensures power x n = (power (x * x) (div n 2)) *)
```

Ultimately, we are dealing with a regular OCaml function, so we can use the usual keywords, such as **requires**, **ensures** and **variant**. So, now the question is: how do we approach this proof? There are numerous methods that can be applied when proving, however, one important detail that is universal to all lemma functions is that the function itself must be of the unit type, effectively meaning that we cannot return any proper kind of value. Instead, we have to make clear for the provers that the post-condition is true under that context. Let's consider a concrete example, for instance 2 raised to the power of 16:

$$
\begin{aligned}
2^{16} &= (2^2)^{16/2} = 4^8 && \text{(True)}\\
4^8 &= (4^2)^{8/2} = 16^4 && \text{(True)}\\
16^4 &= (16^2)^{4/2} = 256^2 && \text{(True)}\\
256^2 &= (256^2)^{2/2} = 65536 && \text{(True)}
\end{aligned}
$$

Power	Result
2^{16}	65536
4^8	65536
16^4	65536
256^2	65536

As we can see in this example, however, even for a small base and a relatively small exponent, the resulting number is quite large, since it grows exponentially. Therefore, directly calculating any two inputs would be unfeasible. Instead, we must do a proof by induction, which can be achieved with recursion:

GOSPEL + OCaml
```
let[@lemma] rec power_even (x: int) (n: int) =
  if n > 1 then power_even x (n-2)
(*@ requires n >= 0
    requires mod n 2 = 0
    variant n
    ensures power x n = (power (x * x) (div n 2)) *)
```

Before explaining the body, it is important to notice the two differences with the previously presented power_even lemma function: it became a recursive definition with the **rec** keyword, and we added a **variant** clause with the value of n to prove termination, since n will decrease between every recursive call. Let's now focus on the body of the function, two questions may arise: "What is the base case?" and "What is the inductive step?". The answer to the latter, as one might suspect, is the **then** branch of the **if**-statement. The answer to the former, on the other hand, may be harder to notice: in OCaml, and other functional programming languages, an **if**-statement always produces a value, in contrast to the imperative languages, as such, omitting the **else** branch will produce the unit value when the tested condition fails, and as a consequence, the type checker enforces the **then** branch to evaluate to the unit value for type consistency. Based on the `requires` clauses, we know that the only number that fails the `if` check is 0. There is no need to use the `assert` construct, since the `ensures` clause applied to a given x and 0, $x^0 = (x^2)^0$, is trivial to prove given the logical definition of the `power` function, when the exponent is 0 it evaluates to 1 independently of the base value. The inductive step is trickier, the strategy behind it is to subtract two from the exponent:

$$\text{Let } n, x \in \mathbb{N} : n > 1, \text{ then:}$$

$$\begin{aligned} x^n &= x^2 * x^{n-2} \\ &= x^2 * (x^2)^{\frac{n-2}{2}} \\ &= x^2 * (x^2)^{\frac{n}{2}-1} \\ &= (x^2)^{\frac{n}{2}} \end{aligned}$$

So, why is this result, in particular, important? If we observe the third step closely, it is possible to see the resemblance between that mathematical expression and the `else` branch of the `power` logical function with arguments $x * x$ and `div n 2`, which is exactly the transition to the fourth step and that the provers can easily achieve. The simplification between steps two and three is also performed by the provers without further human assistance. The real difficulty lies in the first step, since the `power` logic function only subtracts one exponent unit at a time. Subtracting two at a time might seem obvious us humans, however, the computer is much more sceptical. That is why, we must help the provers by separating two exponent units at a time:

GOSPEL + OCaml

```
let[@lemma] power_odd (x: int) (n: int) =
  power_even x (n-1)
(*@ requires n >= 0
    requires mod n 2 = 1
    ensures power x n = x * (power (x * x) (div n 2)) *)
```

We can reuse `power_even` as proof for `power_odd`, by subtracting 1 from the exponent, for similar reasons: `power_even` states that $x^n = (x^2)^{n/2}$, so $x^{n+1} = x*(x^2)^{n/2}$ is easily verified based on the `power` logical function definition.

2.7 Exercises

Implement and specify the:

1. Euclidean division that supports negative numbers (Hint: study the 4 possible cases and develop a sign function)
2. Functional Euclidean division
3. Iterative factorial function
4. Tribonacci sequence (i.e. $0, 1, 1, 2, 4, 7, 13, 24, 44, 81, ...$)
5. Functional fast exponentiation

Chapter 3

Searching

Undoubtably, a common use for computers is to store data, especially as a group. There are numerous possible layouts to the structure containing the data, and, naturally, a problem that arises, no matter the organization, is how to search for a particular element. The various solutions to this problem are intrinsically tied to the structure of the collection. We will start with linear data structures, such as lists and arrays, and, eventually, move on to more complex representations, for instance, trees.

3.1 Linear Search

Within linear structures, the most natural searching strategy is to traverse the data element by element from one end to the other, this is called linear search. Let's say we have the following data and want to find the value 0:

7	13	2	17	0	16	4	11	8	20	0	9
0	1	2	3	4	5	6	7	8	9	10	11

Figure 3.1: A sequence

There are two instances of the value 0, the first at index 4 and the second at index 10. In this particular case, it would actually be faster to search backwards, however, that is not always the case. As such, we have to define a consistent direction, for simplicity we choose to go from left to right, as usual.

Algorithm 4 (Linear Search) *Given a value, x, find its index, if it exists in a linear structure, s.*

1. *Create variable* $i \leftarrow 0$*;*
2. *While* $i < length(s)$ *do:*
   (a) *Compare* x *with* $s[i]$*:*
      i. *If* $x = s[i]$ *return* i
      ii. *If* $x \neq s[i]$ *set* $i \leftarrow i + 1$
   (b) *Go back to step* (2)
3. *Return error value (Not found)*

Another implementation decision originates from the multiple strategies to deal with the error case, i.e. when the desired value is not inside the linear data structure. One possible choice is to encode a value specifically to the error case. This value must not cause conflict in any way possible, which leads to commonly using -1 (or any other negative number, although less common). Another viable option is to use the `Option` data type, which encapsulates both successful and error cases, with the `Some` and `None` values, respectively. The `Some` expects an argument, while `None` does not. Alternatively, it is also possible to use the exception mechanism in OCaml in order to raise an error. In this chapter, we will explore all three possibilities, in that order.

Based on the previous decisions, we arrive at out OCaml implementation of the linear search algorithm for lists:

OCaml
```
let linear_search a v =
  let exception Break of int in
  try
    for i = 0 to Array.length a - 1 do
      if a.(i) = v then raise (Break i)
    done;
    -1
  with Break i -> i
```

Despite using the exception mechanism, our strategy with this implementation is to encode -1 as the not found value. The `Break` exception serves to stop the `for` loop earlier if the value was found, which otherwise would not be possible in OCaml. With language details out of the way, this implementation simply amounts to traversing an array from its first index until either the first instance of the desired element is found or the end of the array if not found.

Unlike the previous chapter there is no mathematical equation that we must comply to in every iteration. However, that does not mean that we cannot logically express the excluded area, and by excluded we mean what has already been searched:

Let's consider the example above, where $i = 3$, then this means that for every integer between 0 (inclusive) and 3 (exclusive), we know that the corresponding

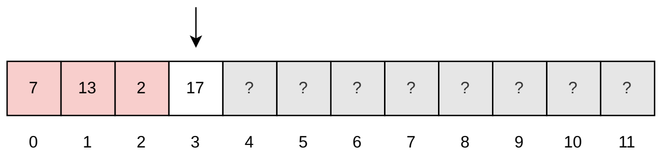

Figure 3.2: Linear Search Excluded Area

value in the array is different from the desired value. This property can be expressed logically with the for all quantifier:

$$\begin{array}{l}\text{Let } a \text{ be an array in} \\ \forall k \in \mathbb{Z} : 0 \leq k < i \leftarrow a[k] \neq v\end{array}$$

When dealing with arrays it is generally important to express the parts of the array that are already concluded. In this case, modelling the property above is crucial to prove the annotations of the `linear_search` function, and can be done so:

GOSPEL + OCaml

```
for i = 0 to Array.length a - 1 do
(*@ invariant forall k. 0 <= k < i -> a.(k) <> v *)
  (* ... *)
done
```

For the most part the `invariant` is quite similar, with some syntactic differences, these being that the integer type could be omitted (may not always be the case), to access an array position OCaml uses the `a.(i)` notation, which is quite different from most programming languages, and the different symbol is represented as `<>`. This condition is essential to prove the `linear_search` function:

GOSPEL + OCaml

```
let linear_search a v = (* ... *)
(*@ r = linear_search a v
    ensures r >= 0 -> a.(r) = v
    ensures r = -1 -> forall k. 0 <= k < Array.length a ->
      a.(k) <> v *)
```

If the element was not found, which happens when $r = -1$, then we state that for every single index from 0 (inclusive) to `length`(a) (exclusive) the element within is different from the desired value. Otherwise, when $r >= 0$, we must guarantee that corresponding index effectively contains the desired value.

3.2 Binary Search

In the worst case, the desired element of a potentially very large sequence is its last, which means traversing every single element. Even on average, we are expected to iterate over a substantial part of the sequence. So, how can we optimize the search process? Sometimes we can use context to our advantage: let's say we have a sorted sequence:

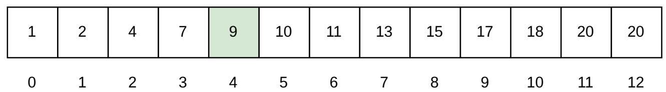

Figure 3.3: A sorted Sequence

In this case, we are looking for the number 9. We have two crucial pieces of information, the element we are looking for and that the sequence is sorted. In this situation, if we look at the content of a given index, we know for certain which direction to go next if the element is different:

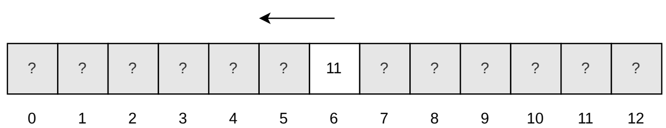

Figure 3.4: Which direction?

For instance, we are currently at index 6, then if we look at its element, 11, we know that the number we are looking for, 9, is to the left of our current position. Moreover, we can actually divide the sequence in half every iteration:

By having two pointers, one for the lower end and the other for the higher end of our search area, we can calculate the middle point, which will serve to decide the direction to seek next, if the element was not the correct one. Additionally, we can change the pointers to exclude the opposite direction and the middle point itself, and restrict the search area by half. There are other cases worth discussing, the three pointers may reference the same index, this means that there is only one position left to check, or when the higher end pointer is smaller than the lower end pointer, this means that all positions of the sequence have been excluded, therefore the desired value is not an element. This algorithm can be described as:

Algorithm 5 (Binary Search) *Given a value, x, find its index, if it exists in a sorted linear structure, s.*

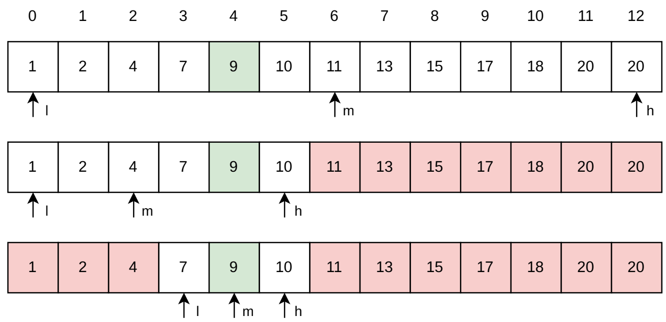

Figure 3.5: Binary Search example

1. *Create two variables:* $l \leftarrow 0$ *and* $h \leftarrow$ *length(s) - 1;*
2. *While* $l \leq h$ *do:*
   (a) *Calculate the middle point:* $m \leftarrow \lfloor (l+h)/2 \rfloor$*:*
   (b) *Compare* x *with* $s[m]$*:*
      i. *If* $x < s[m]$ *set* $h \leftarrow m - 1$
      ii. *If* $x > s[m]$ *set* $l \leftarrow m + 1$
      iii. *If* $x = s[m]$ *return* m
   (c) *Go back to step* (2)
3. *Return error value (Not found)*

Note that this algorithm only is beneficial in terms of speed if the cost of accessing a position is instantaneous. Linked lists and similar implementations are usually not adequate for this algorithm, unlike arrays. With this in mind, the binary search algorithm can be implemented in OCaml, with option values and arrays, as:

GOSPEL + OCaml

```
let binary_search a v =
  let l = ref 0 in
  let h = ref (Array.length a - 1) in
  let res = ref None in
  while !l <= !h do
    let m = (!h + !l)/ 2 in
    if a.(m) < v then l := m+1
    else if a.(m) > v then h := m-1
    else begin res := (Some m); l := m+1; h := m end
  done;
  !res
```

The option data type can be used to encapsulate both the successful and unsuccessful cases of an algorithm. It contains two values `None`, when there is no value to be returned, which can be used to express an error case, and `Some` x, which must always receive an argument with the value to return, in this case the index when the desired element was found. Another important implementation detail is how to break the loop when the element was found, to achieve this we set h to m and l to $m+1$,

Now to verify this implementation, we must remember that a pre-condition to this algorithm is that it must be sorted. How can we logically express that an array is sorted? Well, we could use a logical function, similar to when calculating the Fibonacci sequence, however, this is unusual when dealing with boolean results (unless the expression to calculate is harder to express logically rather than programmatically). Instead, we may use the following predicate defined logically as:

Let a be an array of integers, then:
$\forall i, j \in \mathbb{Z} : 0 \leq i \leq j < \text{length}(a) \rightarrow a[i] \leq a[j]$

Simply, this means that for every index i that precedes and index j (or when $i = j$), then the corresponding element of index i must be lesser or equal to the element in position j. Since this property ranges from 0 (inclusive) to `length`(a) (exclusive), then it effectively means that the array is sorted. In GOSPEL this predicate can be written as:

GOSPEL
```
(*@ predicate sorted (a: int array) =
    forall i j:int. 0 <= i <= j < Array.length a ->
      a.(i) <= a.(j) *)
```

And can be applied to the `binary_search` function as:

GOSPEL + OCaml
```
let binary_search a v = (* ... *)
(*@ r = binary_search a v
    requires sorted a
    ensures match r with
      | None -> forall k. 0 <= k < Array.length a -> a.(k) <> v
      | Some i -> a.(i) = v *)
```

Since the result of this function is encoded as an option type, we may use pattern matching to deconstruct r. If a value was found, *i.e.* when r is a `Some` i value, then we must confirm that the element at index i is effectively the value we are searching for, v. In case it is `None`, then it means that every index from 0 (inclusive) to `length`(a) (exclusive) has a different element from v. And now for the `while` loop:

GOSPEL + OCaml
```
while !l <= !h do
(*@ invariant 0 <= !l
    invariant !h < Array.length a
    invariant match !res with
```

```
      | None -> forall k. 0 <= k < !l \/
        !h < k < Array.length a -> a.(k) <> v
      | Some i -> a.(i) = v
    variant !h - !l *)
  (* ... *)
done;
```

With the first two invariants and the loop condition we effectively express that the lower and higher pointers are within the boundaries of the array (`0 <= !l <= !h < Array.length a`) during the search process. These conditions are separated for good reasons: (1) we cannot define a direct relation between l and h as an invariant, since it will break when exiting the loop; (2) the lower end only grows, so it is best to avoid defining an upper limit, since it might not hold when the lower limit surpasses the upper limit, in either case for termination (finding the desired element or excluding all elements); (3) similarly, we should not define a lower limit for h. Regarding the current result, in the reference `res`, we must also deconstruct it using pattern matching. If the value is found, the condition is identical to the previous annotation. The main difference is the `None` case, in which we have to exclude the elements to the left of l and to the right of h, within the array length of course. To achieve the union of these two disjoint sets of elements, we must use the logical `or` operator. Finally, to prove termination we can use the expression `!h - !l`, since the upper and lower limits are approaching each other.

3.3 Ternary Search

What if instead of diving an array by half, we could divide it into three parts and focus on a single one? That is the idea behind the ternary search algorithm. Despite its noble intentions, ternary search does not achieve significant increases of performance, and, at times, may actually be slower than binary search. Nonetheless, it is an interesting experiment from both the algorithmic and formal verification perspectives. Conceptually, it still uses a lower and a higher limit, however, it calculates two middle points instead of one:

Ternary Search can be described as:

Algorithm 6 (Ternary Search) *Given a value, x, find its index, if it exists in a sorted linear structure, s.*

1. *Create two variables:* $l \leftarrow 0$ *and* $h \leftarrow$ *length(s) - 1;*
2. *While* $l \leq h$ *do:*
   (a) *Calculate the middle points:*

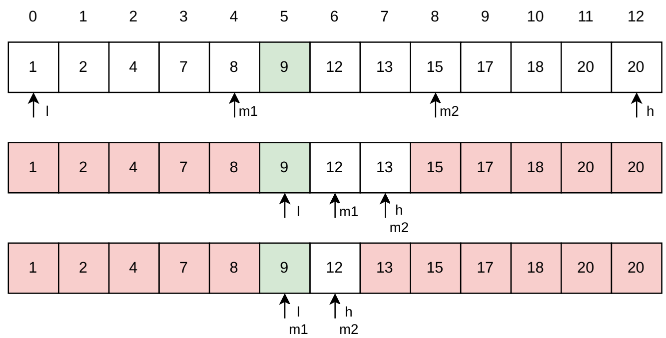

Figure 3.6: Binary Search example

        i. $m_1 \leftarrow l + \lfloor (h-l)/3 \rfloor$
        ii. $m_2 \leftarrow h - \lfloor (h-l)/3 \rfloor$

    (b) *Compare* x *with* $s[m]$*:*

        i. *If* $x = s[m_1]$ *return* m_1
        ii. *If* $x = s[m_2]$ *return* m_2
        iii. *If* $x < s[m_1]$ *set* $h \leftarrow m_1 - 1$
        iv. *If* $x > s[m_2]$ *set* $l \leftarrow m_2 + 1$
        v. *If* $s[m_1] < x < s[m_2]$ *set* $l \leftarrow m_1 + 1$ *and* $h \leftarrow m_2 - 1$

    (c) *Go back to step (2)*

3. *Return error value (Not found)*

Compared to binary search, this algorithm is considerably more complex in terms of the number of instructions. The middle points are obtained by dividing the space between the lower and higher boundaries in three parts with approximately the same size (due to the integer division there may be slightly differences between the three parts). By having two middle points the array is divided into three larger parts plus the two middle points, meaning that there are, effectively, five different cases. Ternary Search can be implemented in OCaml, using arrays and options, as:

OCaml

```
let ternarySearch a v =
  let l = ref 0 in
  let u = ref (Array.length a - 1) in
  let res = ref None in
  while !l <= !u do
    let m1 = !l + (!u - !l)/3 in
    let m2 = !u - (!u - !l)/3 in
    if (a.(m1) = v) then begin
      res := Some m1; l := m1+1; u := m1
```

```
    end
    else if (a.(m2) = v) then begin
      res := Some m2; l := m2+1; u := m2
    end
    else if (v < a.(m1)) then u := m1 - 1
    else if (v > a.(m2)) then l := m2 + 1
    else begin l := m1 + 1; u := m2 - 1 end
  done;
  !res
```

Note that the `begin ... end` blocks in the first two cases are optional and used for display purposes only, while the last is to avoid possible ambiguities stemming from the sequence operator. So, how can we verify this function?

GOSPEL + OCaml

```
let ternarySearch a v = (* ... *)
(*@ r = ternarySearch a v
    requires sorted a
    ensures match r with
      | None -> forall k. 0 <= k < Array.length a -> a.(k) <> v
      | Some i -> a.(i) = v *)
```

If we notice closely that is the same exact specification used in the binary search example, except for the function's name. Well, this is not surprising, since the same conditions are used in the context of the linear search algorithm, except for the pre-condition, which is not necessary in that context. What about the while loop?

GOSPEL + OCaml

```
while !l <= !u do
(*@ invariant 0 <= !l
    invariant !u < Array.length a
    invariant match !res with
      | None -> forall k. 0 <= k < !l \/
        !u < k < Array.length a -> a.(k) <> v
      | Some i -> a.(i) = v
    variant !u - !l *)
  (* ... *)
done;
```

To our surprise, the specification is the same. One may ask why, however, on closer inspection we realize the middle points do not impact the specification, in fact, it is not even possible to use them there, since the scope of an annotation on a loop does not include whatever is declared on its body. The important logical properties stem from the diminishing window comprised by the lower and upper bounds, which is exactly the same in this family of search algorithms: binary search, ternary search, quaternary search, or even nonary search and beyond.

Much like this algorithm can be seen as an experiment, so can this first part of this section. Our goal was to demonstrate that significant implementation details, such as the number of middle points, may not impact the specification. With this accomplished, we must return to our promise to demonstrate verify error values encoded as exceptions, which will use a slightly modified implementation of the ternary search:

OCaml
```
let ternarySearch a v =
  let exception Break of int in
  try
    let l = ref 0 in
    let u = ref (Array.length a - 1) in
    while !l <= !u do
      let m1 = !l + (!u - !l)/3 in
      let m2 = !u - (!u - !l)/3 in
      if (a.(m1) = v) then raise (Break m1)
      else if (a.(m2) = v) then raise (Break m2)
      else if (v < a.(m1)) then u := m1 - 1
      else if (v > a.(m2)) then l := m2 + 1
      else begin l := m1 + 1; u := m2 - 1 end
    done;
    raise Not_found
  with Break i -> i
```

Instead of using a reference to store the result (either as a number or an option), in this implementation we use exceptions to deal with the result. Similar to the linear search algorithm, we use the `Break` exception to escape the `while` loop and use a `try-with` block to return the corresponding argument, which allows omitting the instructions used in the previous implementations to break the loop. To deal with the unsuccessful case, we used the `Not_found` exception from the standard library. This exception is purposefully not caught as not to return a value. The `ternarySearch` function is adapted to:

GOSPEL + OCaml
```
let ternarySearch a v = (* ... *)
(*@ r = ternarySearch a v
    requires sorted a
    ensures a.(r) = v
    raises Not_found -> forall k. 0 <= k < Array.length a ->
      a.(k) <> v *)
```

The `raises` clause serves to denote the behaviour of the function when an uncaught exception is triggered. In this case, out of the two exceptions, only `Not_found` is uncaught, and in this scenario every element of the array must differ from the desired value. The condition itself does not change, only how to "unwrap" the result. Since an uncaught exception terminates a function abruptly without returning, then we can simply express the successful case as an `ensures` clause without any condition preceding it, unlike the previous implementations. The specification on the `while` loop also changes slightly:

GOSPEL + OCaml
```
while !l <= !u do
(*@ invariant 0 <= !l
    invariant !u < Array.length a
    invariant forall k. 0 <= k < !l \/ !u < k < Array.length a ->
```

```
    a.(k) <> v
  variant !u - !l *)
 (* ... *)
done;
```

Since we do not store the result any more, we can remove the `invariant` condition that expressed that it contained the correct index. We still, however, have to express the area that has been excluded. We need not worry about the `Not_found` exception since it is raised outside the loop.

3.4 Depth-first Search in Binary Trees

Moving on from linear data structures, a tree can either be empty or a group of nodes. Each node may be connected to multiple distinct nodes below it, known as its children, and to at most one node above it, called its parent. The only exception is the root node, which has no parent. Binary Trees are a special case of trees where each node may only have at most two children, and can easily be defined in OCaml using a variant:

```
type 'a tree = E | N of 'a tree * 'a * 'a tree                    OCaml
```

The `E` constructor represents an empty tree, which does not contain any kind of information. On the other hand, the `N` constructor represents a node comprised by the left subtree, the element and the right subtree. Note that a subtree is also either empty or another node.

One of the most common searching algorithms for trees is depth-first search, which amounts to visiting one of child node and their descendants before the other nodes with the same parent, generally from left to right:

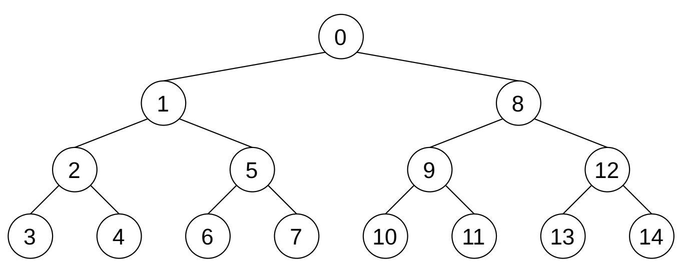

Figure 3.7: Depth-first search in a Binary Tree

This algorithm visits the nodes by the order of their identifiers, in other words, the first node that would be visited would be 0, then 1, then 2, and so on, until it would reach 14. Of course the algorithm should stop early if the desired value was found. A recursive depth-first search implementation in OCaml can be:

OCaml

```
let rec dfs v = function
  | E -> false
  | N (l, x, r) -> x = v || dfs v l || dfs v r
```

Using OCaml' shorthand for pattern matching, *i.e.* the `function` keyword it is possible to omit the parameter that contains the tree instance. In this version of the algorithm we simply wish to calculate if a value can be found in the tree, as such, if it is empty, then we simply evaluate to false. When traversing a node, then we must first compare the element in the node, if it has the same value as what we are looking for, then the `or` operators (——) are ignored. When the values differ, we call the `dfs` function with the left subtree first, which will fully evaluate (recursively) first before calling the right subtree, this will lead to the desired behaviour.

Since our objective with this algorithm is to find if an element belongs to the tree, then the specification should reflect exactly that. In order to avoid using the same algorithm as a logical function (trivializes the proof and may lead to subtle errors), one possible strategy would be to transform the tree into a list and use the `mem` operation. There are numerous ways to traverse a tree, one possibility is the prefix order, which is exactly the order we have described before: look at the current node, go left first, and explore the right side after:

GOSPEL

```
(*@ function rec prefix (t: 'a tree) : 'a list =
    match t with
    | E -> []
    | N l x r -> x::(prefix l) @ (prefix r) *)
(*@ variant t *)
```

This function can then be applied in the `dfs` function:

GOSPEL + OCaml

```
let rec dfs v = (* ... *)
(*@ r = dfs v t
    variant t
    ensures r <-> List.mem v (prefix t) *)
```

In both functions, `prefix` and `dfs`, we may use the structure of the tree to prove termination, similar to lists. The `ensures` clause is quite strong due to the use of the equivalent symbol, nonetheless, it is essential to guarantee that there are no false positives or false negatives, in other words, a value that does not belong to the tree but is marked as such or a value that is marked as negative despite belonging to the tree, respectively.

3.5 Exercises

Implement and specify the:

1. Backwards linear search on arrays with a while loop

Chapter 4

Sorting

Similarly to searching, one problem that may arise when dealing with data is how to sort it. The first step in this process is to find a suitable total order relation for the desired data type, in other words, any two elements must be comparable.

4.1 Integer Lists

The mathematical inequality operators ($<, \leq, >, \geq$), with the exception of the not equal operator ($\neq$), are total order relations for real numbers, and its subsets, including the integer numbers, since any two numbers (even if they are the same) can be compared. In this section, we will only consider integer numbers since Cameleer currently does not support the float data type. Moreover, for simplicity, duplicates are allowed, and the data will be sorted ascendingly, this means that we will use the $\leq$ operator in the following implementations.

4.1.1 Small verification library

Until now, we have dealt with either independent problems each with its own verification strategies (in chapter 2) or a problem class that is not logically intensive (in chapter 3). That is not the case with sorting problems. First, we need to define our concept of sorted sequence of elements, which is mathematically described as:

$$\begin{aligned}&\text{Let } s \text{ be a sequence of } n \text{ elements such that } s = s_0, ..., s_{n-1}\\&\text{Then } s \text{ is sorted if } \forall i, j \in \{0, ..., n-1\} : i \leq j \rightarrow s_i \leq s_j\end{aligned}$$

This definition is the basis for the predicate used in the Binary Search algorithm (see section 3.2). However, due to the explicit indexing used, this definition is not as natural for OCaml lists, instead we may traverse the list and compare two adjacent elements at a time:

GOSPEL
```
(*@ predicate rec sorted (l: int list) =
    match l with
    | [] | _::[] -> true
    | x::(y::ls) -> x <= y && sorted (y::ls) *)
(*@ variant l *)
```

Since we compare two elements at a time, both empty lists and lists with a single element are considered sorted by default. Otherwise, we must compare the first values with our total order relation. For a list to be considered sorted this must be true for every single pair of adjacent elements, that is why we must use the logical and operator (&&) and in the recursive call we still "propagate" y.

There are many strategies when it comes to sorting data. However, any (serious) sorting algorithm should only (potentially) reorder the original elements, this means that it is prohibited to insert, remove or change any element by the end. Although this may not necessarily be true in the middle of execution, more so when dealing with arrays and memory. This discussion leads to the concept of permutation, two lists are permutations of one another if they have exactly the same elements independently of their order. One possible way to define this concept is through the number of occurrences for each element, which must be equal in both lists. Assuming the existence of a logical function `occ`, we may model a permutation as the following predicate:

GOSPEL
```
(*@ predicate permut (l1 l2: int list) =
    forall x. occ x l1 = occ x l2 *)
```

Using the previously discussed GOSPEL tags, the `occ` function may be defined as:

GOSPEL + OCaml
```
let[@logic][@ghost] rec occ v = function
  | [] -> 0
  | h::t -> (if h = v then 1 else 0) + occ v t
(*@ res = occ v l
    variant l
    ensures 0 <= res <= List.length l
    ensures res > 0 <-> List.mem v l *)
```

Simply traversing the list and comparing its elements suffices for a logical function. One good practice is to equip the specification of a logical function with important properties, as a means to avoid having to define more axioms and lemmas (which have to be proved). In this case, we state that the number of occurrences is non-negative, and may only be as high as the number of elements in the list, since it is nonsensical to have a negative number of occurrences or have more occurrences of a single element than the number of elements in the list itself. Furthermore, a positive number of occurrences must correspond to belonging in the list, and vice versa.

These predicates are our basic verification blocks, however, by themselves, are quite fragile and SMT solvers will have a hard time verifying that these properties are maintained after an iteration. As such, we have to define axioms and lemmas that will help up. However, the first question that comes to mind is where do we begin? Well, the truth is that it is hard to predict what will be needed, a more natural workflow would be to start by annotating the algorithm, finding the needed predicates, and then analysing, within the Why3 platform, the failed proof goals in order to reach the missing properties. Since most of these lemmas are required in the various sorting algorithm we will present next, for presentation purposes we are not able to show this process. Instead, we will present these lemmas as a verification library. Most of these lemmas stem from a similar reason, this being basic list operations, namely the `cons` operator (::) and concatenation (@). Let us say we have two sorted lists, is their concatenation also sorted? Not necessarily, for instance:

$$\text{Let } a = [0,1,2],\ b = [1,2,3], \text{ and } c = [2,3,4]$$
$$\text{Then, } a \mathbin{@} b = [0,1,2,1,2,3], \text{ and } a \mathbin{@} c = [0,1,2,2,3,4]$$

The concatenation operation creates a new list where the elements of the left operand are followed by those of the right operand, so for the concatenation to remain sorted then it means that each element of the left operand must be lesser or equal to every element of the right operand:

GOSPEL + OCaml

```
let[@lemma] sorted_concat (l1: int list) (l2: int list) = (* TODO *)
(*@ sorted_concat l1 l2
    requires sorted l1
    requires sorted l2
    requires forall x y. List.mem x l1 -> List.mem y l2 -> x <= y
    ensures sorted (l1 @ l2) *)
```

So, how do we prove this lemma? An astute solution would be to obtain the last element of `l1`, by reversing it, and comparing it to the first element of `l2`, however, SMT solvers have a hard time checking this solution, and may require extra assertions, that may complicate the final proof. Instead, we may opt for comparing each element of $l1$ to every element of $l2$:

GOSPEL + OCaml

```
let[@lemma] rec sorted_concat (l1: int list) (l2: int list) =
  match l1 with
  | [] -> ()
  | h1::t1 ->
    match l2 with
    | [] -> ()
    | h2::t2 -> assert (h1 <= h2);
      sorted_concat l1 t2; sorted_concat t1 l2
(*@ sorted_concat l1 l2
    requires sorted l1
    requires sorted l2
    requires forall x y. List.mem x l1 -> List.mem y l2 -> x <= y
    variant l1, l2
```

```
    ensures sorted (l1 @ l2) *)
```

Similarly, the `cons` operation does not always guarantee the result is sorted if the list is sorted, instead it only happens if the element to be added is lesser or equal than every element on the list:

GOSPEL

```
(*@ lemma sorted_cons :
    forall x:int, l: int list.
    (sorted l /\
    (forall e. List.mem e l -> x <= e)) <->
    sorted (x::l) *)
```

Unlike the previous lemma, however, we opted from a stronger statement by using the equivalent sign. The reasoning behind this choice is related to the nature of the two operations. Concatenation is mostly used as a constructive operation, especially in the context of sorting algorithms, i.e. usually we want to build a bigger sorted list from two smaller sorted ones, rather than building two smaller sorted lists from one bigger sorted list. The `cons` operation, may be used both in a constructive manner, to iteratively build a sorted list element by element, or in a destructive way, when using pattern matching. If we separate the equivalent sign into two implications, we obtain:

Let l be an integer list in:

(1) $\forall x \in \mathbb{Z} : \text{sorted}(l) \wedge (\forall e \in l : x \leq e) \rightarrow \text{sorted}(x :: l)$

(2) $\forall x \in \mathbb{Z} : \text{sorted}(x :: l) \rightarrow \text{sorted}(l) \wedge (\forall e \in l : x \leq e)$

The first logical consequence denotes the constructive use of the `cons` operator, where an element can be inserted at the head of the list if it is smaller or equal to every single element in the list. This proof goal is easily dispatched by SMT solvers. By contrast, the second logical consequence models its destructive use. If a list with at least one element is sorted, then the element at its head is smaller or equal to every element in the tail, which remains sorted. This proof goal is not as trivial, and we even need to define an additional lemma (which must be placed before this one):

GOSPEL + OCaml

```
let[@lemma] rec sorted_head (h: int) (t: int list) =
  match t with
  | [] -> ()
  | x::tt -> assert (h <= x); sorted_head h tt
(*@ requires sorted (h::t)
    variant t
    ensures forall e. List.mem e t -> h <= e *)
```

By having `sorted(h::t)` as a requirement can recursively compare the elements in the tail to the head, by assert that the head is effectively lesser or equal to each element, which translates logically to the last ensures clause (`forall e. List.mem e t -> h <= e`).

Besides these lemmas related to the `sorted` predicate, the `permut` predicate also requires some logical support. One thing that may seem trivial to us, but is quite complex for SMT solvers to prove is that two permutations have the same length. The problem lies in the universal quantifier from the `occ` function. So, how do we go about proving that if the number of occurrences for every single element is the same between two lists then their length is the same? When a property looks trivial, but the provers cannot solve it, then it generally means that it is impossible to prove (it is an axiom), or it has a complex proof. In this case it is the latter. Complex proofs can be tedious and lead to several lost hours, for comfort purposes, sometimes it is okay to "cheat", instead of proving the lemma, we may consider it as an axiom. However, this practice should not be taken lightly, as it can quickly lead to possibly faulty programs being proved under false assumptions and inconsistent logic, which will cause more harm than good in real world software. As such, this practice, of transforming hard lemmas into axioms, must be avoided at all costs. This does not have any implications on real axioms, since there is no way to prove them. So, to ensure that a permutation of a list has the same length we define:

GOSPEL

```
(*@ axiom permut_len : forall l1 l2: int list.
    permut l1 l2 -> List.length l1 = List.length l2 *)
```

Finally, we also have to define the behaviour on the number of occurrences when concatenating two lists. This amounts to summing the elements of the two lists, since no element is changed, removed or inserted:

GOSPEL + OCaml

```
let[@lemma] occ_append (x: int) (l1: int list) (l2: int list) = (* TODO *)
(*@ occ_append x l1 l2
    ensures occ x (l1 @ l2) = occ x l1 + occ x l2 *)
```

For simplicity, we only consider one element at a time, in order to omit the universal quantifier, and streamline the post-condition. To prove this lemma, we do a proof by induction:

GOSPEL + OCaml

```
let[@lemma] rec occ_append (x: int) (l1: int list) (l2: int list) =
  let p = occ x (l1 @ l2) = occ x l1 + occ x l2 in
  match l1 with
  | [] -> assert (p)
  | _::t -> occ_append x t l2; assert (p)
(*@ occ_append x l1 l2
    variant l1
    ensures occ x (l1 @ l2) = occ x l1 + occ x l2 *)
```

We define `p`, as the property we want to prove, i.e. the post-condition, and recursively iterate over one of the lists. In the base case, `l1 = []`, which implies that `occ x ([] @ l2) = occ x [] + occ x l2`, and since the empty list does not contain any element, then it is trivial to prove that `occ x l2 = occ x l2`. The inductive step implicitly states that if `occ x (t @ l2) = occ x t + x l2` then `occ x (h::t @ l2) = occ x (h::t) + x l2`, where `l1 = h::t` (note that `h` is omitted in the implementation above). This can be proved by the SMT solvers since each side of the logical equality receives the same new element.

4.1.2 Selection Sort

One possible strategy to sort a sequence of elements is to find the minimum value and place it at the front of the sequence, then find the second smallest element and place it in the second position, and so on...

0	1	2	3	4	5
6	1	0	7	3	9
0	6	1	7	3	9
0	1	6	7	3	9
0	1	3	6	7	9
0	1	3	6	7	9
0	1	3	6	7	9
0	1	3	6	7	9

Figure 4.1: Selection sort example

However, shifting the sequence is unpractical and costly. In a functional setting, we can, instead, allow elements to be reorganized without any time complexity penalty. For instance, let us consider the iteration where 3 is the minimum value:

Minimum	Remaining	Processed
6	[7; 3; 9]	[ ]
6	[3; 9]	[7]
3	[9]	[7; 6]
3	[ ]	[7; 6; 9]

In this case 6 and 7 are swapped at the end of the iteration, this is because every element is placed at the end of processed list. At first one solution may seem to add the previous minimum candidate at the front of the list, however, for more complex examples this is interaction does not guarantee the original placement:

Minimum	Remaining	Processed
6	[8; 10; 12; 4; 5; 7; 3; 9]	[ ]
6	[10; 12; 4; 5; 7; 3; 9]	[8]
6	[12; 4; 5; 7; 3; 9]	[8; 10]
6	[4; 5; 7; 3; 9]	[8; 10; 12]
4	[5; 7; 3; 9]	[6; 8; 10; 12;]
4	[7; 3; 9]	[6; 8; 10; 12; 5;]
4	[3; 9]	[6; 8; 10; 12; 5; 7]
3	[9]	[4; 6; 8; 10; 12; 5; 7]
3	[ ]	[4; 6; 8; 10; 12; 5; 7; 9]

So, to simplify, it is best to place each processed element at the end of the list, which can be achieved using the `cons` operator (::), as we may see:

OCaml

```
let rec selection_aux min = function
  | [] -> (min, [])
  | x::r ->
    if min <= x then
      let (m, l) = selection_aux min r in m, x::l
    else
      let (m, l) = selection_aux x r in m, min::l
```

The `selection_aux` function has two parameters, the first is the minimum candidate, and the second is the list without that same element. By the end of the recursion, a pair with the minimum value and empty list is returned. When the list has at least one element we must compare its head to the current minimum candidate. If the minimum candidate is smaller or equal to the head element, then the minimum candidate for the next recursive call remains unchanged, and the head element is placed at the head of the resulting list. Otherwise, the minimum candidate is changed to the head element, and the previous minimum candidate is placed at the head of the resulting list.

The main function repeats this process if there are two or more elements in the received list or one of its sub-lists:

OCaml
```
let rec selection_sort l =
  match l with
  | [] -> []
  | [x] -> [x]
  | x::ls ->
    let m, r = selection_aux x ls in
    m::(selection_sort r)
```

By calling the `selection_aux` function we obtain the minimum value, `m`, and the sub-list with the remaining elements of `x::ls`. The result is obtained from inserting `m` of the list produced by the recursive call of `selection_sort` with `r` as its parameter. This corresponds to finding every element from lowest to highest and reconstructing it backwards to ensure that it is sorted in that order, since we are inserting at the head.

Verification-wise, the major logic is placed in the auxiliary function, which leads to a relatively simple annotation for the main function (similar to most sorting algorithms):

GOSPEL + OCaml
```
let rec selection_sort l = (* ... *)
(*@ r = selection_sort l
    ensures sorted r
    ensures permut r l
    variant List.length l *)
```

As expected, the result should be sorted and a permutation of the original list. Moreover, since this function is applied to every single element in the list, to prove termination, we may simply use the length of the list.

GOSPEL + OCaml
```
let rec selection_aux min = (* ... *)
(*@ m, r = selection_aux min l
    variant l
    ensures m <= min
    ensures forall x. List.mem x r -> m <= x
    ensures permut (m::r) (min::l) *)
```

Similar to the main function, this one can be proven to be terminal using the list itself, since the function basically amounts to traversing the list from one end to the other (despite doing more than just that). In terms of post conditions, it is necessary to ensure that `m`, the resulting minimum value, can be lesser or equal to the minimum candidate from the parameters (`min`). Furthermore, `m` should not be greater that any value on the resulting list, to guarantee that it is indeed the minimum value, or in other words, it is lesser or equal to every element in `r`. The final ensures clause serves to maintain the property that at every iteration we produce a permutation of the previous one, therefore, by the end, the result will be a permutation of the original list.

Tail recursion

Does tail recursion have an impact on a program proof? The answer is likely yes. In many scenarios an accumulator variable is introduced and along with it some logical properties may change slightly, since part of the original input is now placed on the accumulator, and new requirements are usually introduced to reflect the properties of the data stored in the accumulator.

To update the auxiliary function, `selection_aux`, to be tail recursive, we may do this:

OCaml
```
let rec selection_aux min acc = function
  | [] -> (min, acc)
  | x::r ->
    if min <= x then
      selection_aux min (x::acc) r
    else
      selection_aux x (min::acc) r
```

In its original version, to build the pair of results when the list had at least one element (besides the minimum candidate) we had to first obtain the previous pair from the recursive call, which help build the new results on top of the previous ones. In the tail recursive version, the same behaviour is achieved by using an accumulator. When the current candidate is lesser or equal to the head of the list, assuming it has at least one element, the minimum candidate remains the same while the head element is placed at the head of the accumulator. On the other hand, if we have found a better minimum candidate, the first parameter is updated, and the old candidate is now placed at the head of the accumulator. By the end, the accumulator will contain the list of elements that are greater or equal to the minimum candidate.

GOSPEL + OCaml
```
let rec selection_aux min acc = (* ... *)
(*@ m, r = selection_aux min acc l
    requires forall x. List.mem x acc -> min <= x
    variant l
    ensures m <= min
    ensures forall x. List.mem x r -> m <= x
    ensures permut (m::r) (min::(l @ acc)) *)
```

The most significant change is the addition of a `requires` clause. Not just that, it is quite similar to one of pre-existing post conditions. This is due to the underlying relation between `acc` and `r`, since whatever is placed in `acc` during the final iteration will become `r`. So, the `acc` variable will contain the processed elements that are guaranteed to not be the minimum value, either due to being greater or equal to the current candidate. A question may arise, why is it a `requires` rather than an `ensures` clause? In a purely functional setting, such as this, data is immutable, so any property that impacts intermediate variables and that holds at the end of the iteration also holds at the start, thereby eliminating the need for post conditions related to intermediate variables, since these are only updated with new function calls. Therefore, it is mandatory for properties on intermediate variables to hold at the start of a given iteration. A small detail that has also change is in the last `ensures` condition, in which the input data is now split into two variables `l`, which contains the unprocessed data, and `acc`, which contains the processed data.

Moving on to the main function, `selection_sort`:

OCaml
```
let rec selection_sort acc = function
  | [] -> acc
  | [x] -> acc @ [x]
  | x::ls ->
    let m, r = selection_aux x [] ls in
    selection_sort (acc @ [m]) r
```

In this case, the accumulator will hold each consecutive minimum value, and each new one will be placed at the end of the list to guarantee the ascending sorting. The specification of this function also changes:

GOSPEL + OCaml
```
let rec selection_sort acc = (* ... *)
(*@ r = selection_sort acc l
    requires forall x y. List.mem x acc -> List.mem y l -> x <= y
    requires sorted acc
    ensures sorted r
    ensures permut r (l @ acc)
    variant List.length l *)
```

As we have previously mentioned, one of the new requirements is that the accumulator is sorted at the start of every iteration (implicitly at the end too due to immutability). The other pre-condition, however, can be more unnoticeable, but every element in `acc` is guaranteed to be lesser of equal to every element of `l`, since we select the minimum value from `l` and placed it at the end of `acc` in every iteration. This property is very important to ensure that the result, as well as the `acc` at every iteration, are sorted. This specification is not enough however, SMT solvers have a hard time recognizing that `m` belongs to `x::ls`, since we separate a minimum candidate (`x`) right from the start, so `m` does not necessarily belong to `ls` from the perspective of the auxiliary function, so we need to add an assertion to do just that:

GOSPEL + OCaml
```
let m, r = selection_aux x [] ls in
assert (List.mem m (x::ls));
selection_sort (acc @ [m]) r
```

4.1.3 Merge Sort

Another approach to problem-solving is to repeatedly divide a larger problem into smaller subproblems until each becomes simple enough to be solved directly, these can then be combined, in a way that maintains the validity of each intermediate result, to form the solution to the original problem. This is known as the divide and conquer strategy, which is the approach used in our current case study: merge sort. This algorithm is divided into two phases, split and merge. In the split phase, the recursively divided in half, for instance:

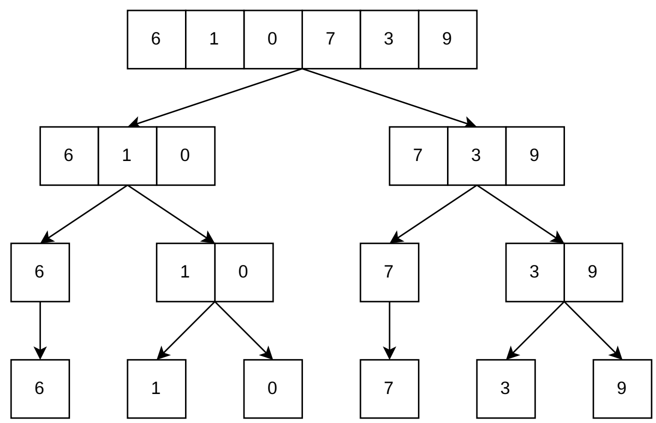

Figure 4.2: Merge sort: split phase example

At the end of the split phase, each sub-list will be sorted, since it only contains a single element. In the final stage, the sub-lists will be merged in a way that the intermediate results are also sorted, thereby guaranteeing that in the final iteration the original list will be sorted:

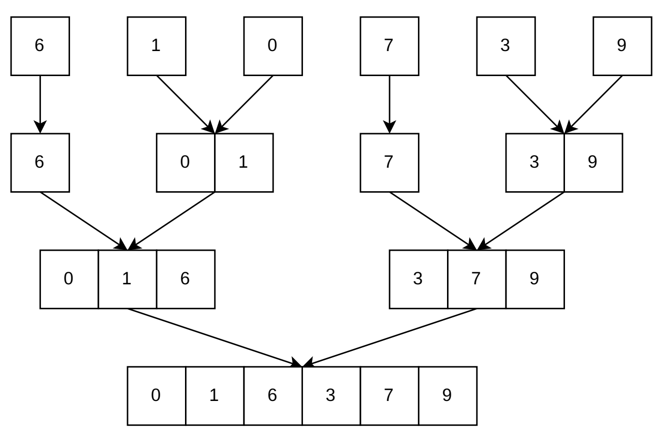

Figure 4.3: Merge sort: merge phase example

In a functional setting, such as the one in this case study, it is quite inconvenient to split a list exactly at its half point, since it would be necessary to know both the current index and the length of the original list. This translates into two unnecessary parameters. Note that the order of the elements before and after the split does not impact the performance of the merge sort algorithm, as long as the splitting strategy does not exceed linear time complexity. A more elegant splitting strategy is to send one element to the first sub-list and the next to the other sub-list, and repeating. This ensures that both lists have at most a difference of one element, in case the original list has an odd number of elements. This can be programmed as:

OCaml
```
let rec split (l: int list) =
  match l with
  | [] -> ([], [])
  | x::ls -> let ll, rl = split ls in (rl, x::ll)
```

The result of `split` function is a pair of lists, let us call the first element of the pair `ll` (left list) and the second element `rl` (right list). The quirk of this function is that at the end of every iteration the sub-lists are switching positions inside the pair, which allows fixating one of the members of the pair to receive the new element. This pattern leads exactly to the behaviour we desired, since we are not placing the new element twice in succession in the same list.

The merge phase, from an implementation perspective, is not as tricky:

OCaml
```
let rec merge l1 l2 =
  match l1, l2 with
  | z, [] | [], z -> z
  | x::ls, y::rs ->
    if x <= y then x::(merge ls (y::rs))
    else y::(merge (x::ls) rs)
```

As one might suspect from the previous figure, the `merge` function receives two (sorted) lists as parameters. Whenever one of these lists is empty, the result is simply the other list, since it has been sorted beforehand. If both lists have at least one element, then we must first compare their heads to finds which is the smallest, which is then appended to the head of the result. The recursive call also includes the other element, as not to miss any. This behaviour allows creating a sorted list from two smaller sorted lists via insertion.

Finally, the main function orchestrates the process between the phases:

OCaml
```
let rec merge_sort l =
  match l with
  | [] -> []
  | [x] -> [x]
  | _ -> let (a, b) = split l in
    merge (merge_sort a) (merge_sort b)
```

If we have at least two elements, we split the list and then recursively call the `merge_sort` function on each of these sub-lists to possibly be split further, and then the `merge` function combines the various intermediate results.

From a verification standpoint, the annotations on main function of a sorting algorithm might not change significantly in relation to other algorithm, and this is the case:

GOSPEL + OCaml

```
let rec merge_sort l = (* ... *)
(*@ r = merge_sort l
    ensures sorted r
    ensures permut r l
    variant List.length l *)
```

This is due to the main properties of each of the solutions being equal, each algorithm should produce a sorted list that is a permutation of the original list. Moreover, in functional programming these algorithms traverse the original list in the main function, which leads to the same termination proof, which is exactly the original list itself (or its length, which are equivalent).

To verify the `split` function, we may do it in such manner:

GOSPEL + OCaml

```
let rec split (l: int list) = (* ... *)
(*@ (r1, r2) = split l
    ensures permut l (r1 @ r2)
    ensures List.length r2 = List.length r1 \/
      List.length r2 = List.length r1 + 1
    ensures List.length r2 + List.length r1 = List.length l
    variant List.length l *)
```

Since we are splitting the original list, `l`, in two halves, we are effectively creating a permutation of `l`, meaning that no elements are inserted, removed or have its value altered, through the concatenation of the two sub-lists. Moreover, the sum of lengths of the sub-lists should be equal to the length of the original list, and the sub-lists cannot exceed a difference of an element in their size, otherwise it would not be a split in half.

Finally, the `merge` function:

GOSPEL + OCaml

```
let rec merge l1 l2 = (* ... *)
(*@ r = merge l1 l2
    requires sorted l1
    requires sorted l2
    ensures sorted r
    ensures permut r (l1 @ l2)
    variant List.length l1 + List.length l2 *)
```

As previously mentioned, the `merge` function receives two sorted lists and produces another sorted list, which permutation of both. To prove termination we use the length of both input lists, since we are iterating over both, and only removing one element of one of the lists at a time, meaning that at most we will iterate the same number of times of the sum of their lengths.

4.1.4 Quick Sort

Merge sort is not the only divide and conquer sorting algorithm, Quick sort applies the same principle with a different approach when breaking down the problem. The first step in this algorithm is to choose a pivot element, which will serve as a reference value to split apart the sequence. The remaining elements that are lesser or equal to the pivot will be placed in a separate sub-list from those that are strictly greater than the pivot. There are several methods to choose the pivot, with the simplest being selecting either the first or last element. Since we are dealing with linked lists, the only feasible method, without altering the time complexity, is to select the head of the list as pivot.

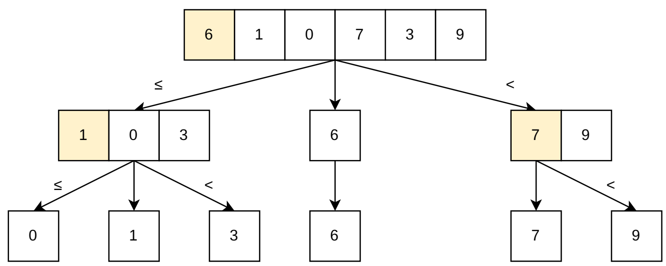

Figure 4.4: Quick sort example: breaking down the list

The pivots of each list before breaking down are highlighted in yellow. One other detail from the figure is that by the last iteration, once all elements are isolated, they are pretty much sorted. Note that this is just a visual representation, but the fact is that reconstructing sorted intermediate lists amounts to concatenating the sub-list with the smaller/equal values with the pivot and the sub-list of higher values.

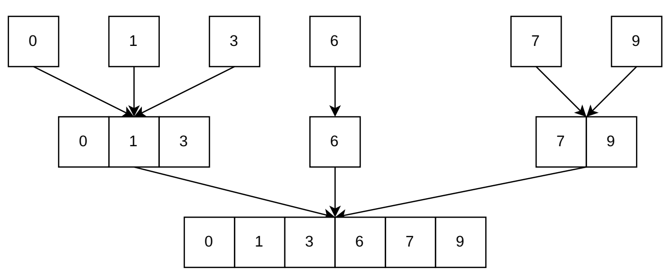

Figure 4.5: Quick sort example: breaking down the list

To define the behaviour of splitting the list, we will create an auxiliary function:

OCaml
```
let rec quick_aux p = function
  | [] -> ([], [])
  | x :: r ->
    let ll, lr = quick_aux p r in
    if x <= p then x :: ll, lr
    else ll, x :: lr
```

The main objective of this function is that given a pivot, `p`, and the remaining elements, we want to separate those that are lesser or equal to `p` from the ones that are higher, as such we will return a pair of lists. Assuming that the lesser or equal elements are placed in the first member of the pair, we start by performing the recursive call on the tail of the list, `r`, and we will obtain the pair (`ll`, `lr`), then insert at the head in the corresponding list, based on the comparison with the pivot. The main function, on the other hand, will contain the combination process:

OCaml
```
let rec quick_sort l =
  match l with
  | [] -> []
  | [x] -> [x]
  | p :: ls ->
    let (left, right) = (quick_aux p ls) in
    (quick_sort left) @  p :: quick_sort right
```

It is only sensible to perform a split if we have more than one element, since the first will be the pivot. After obtaining the `left` and `right` sub-lists, to combine the sub-lists it simply amounts to appending `left` to `p` and `right`, since both `left` and `right` were sorted beforehand and contain values based on the pivot, due to splitting. As per usual, the annotations on the main function, *i.e.* `quick_sort`, are as follows:

OCaml
```
let rec quick_sort l = (* ... *)
(*@ r = quick_sort l
    ensures sorted r
    ensures permut r l
    variant List.length l *)
```

The `quick_aux` function on the other hand:

OCaml
```
let rec quick_aux p = (* ... *)
(*@ ll, lr = quick_aux p l
    variant l
    ensures forall x. List.mem x ll -> x <= p
    ensures forall x. List.mem x lr -> x > p
    ensures permut l (ll @ lr) *)
```

Starting with the last `ensures` clause, since we are performing a split operation, we must guarantee that the result have the same elements as the original spread across the two sub-lists. Moreover, each list should respect the aforementioned properties, these being that every element of `ll` should be lesser or equal when compared to the pivot, while `lr` contains the values strictly greater than `p`.

Optimized tail recursion

One of the goals of tail recursion is to prevent stack overflows, however, when multiple recursive calls have to be made this is not guaranteed, and the calling order matters. Using quick sort as an example, if in the first call the sub-list contains more elements than the other sub-list, this means that we are making an inefficient use of stack space, since there will be a bigger number of consecutive function calls in memory, and by the time we do the second call, the tail call, the program might have stopped abruptly due to stack overflow or even if it doesn't the benefits of doing a tail call have diminished greatly. If we notice closely, the length of the smallest sub-list ranges from 0 to half of the number of elements in the original list (both inclusive), while the largest sub-list ranges from half of the number of elements and the total number of elements in the original list (both inclusive), this means that if we consistently call the largest sub-list first we will have expected linear stack space, however, if we call the smallest sub-list first we will have expected logarithmic stack space.

So, let's update out quick sort implementation to be tail recursive and optimized. Starting with the auxiliary function:

```ocaml
let rec quick_aux p left right = function
  | [] -> (left, right)
  | x::ls ->
    if x <= p then quick_aux p (x::left) right ls
    else quick_aux p left (x::right) ls
```

For `quick_aux` to be tail recursive we may use two additional parameters to accumulate the results, since the result is a pair of lists with distinct meanings, therefore `left` will store the values that are lesser or equal than the pivot, and `right` will store those that are strictly greater than `p`. The real challenge stems from the main function:

```ocaml
let rec quick_sort lacc racc = function
  | [] -> lacc @ racc
  | [x] -> lacc @ x::racc
  | p::ls ->
    let (left, right) = quick_aux p [] [] ls in
    if List.length left <= List.length right then begin
      let sorted_left = quick_sort lacc [] left in
      quick_sort (sorted_left @ [p]) racc right
    end else begin
      let sorted_right = quick_sort [] racc right in
      quick_sort lacc (p::sorted_right) left
    end
```

In a non-optimized tail call version of quick sort, we might have defined a precedence over one of the sub-lists, which would result in only one accumulator. However, that is not the case, since we are potentially alternating between going left or right first, then it means we are sorting the list on two fronts at the same time, and therefore we need two accumulators, one for each front. Moreover, the elements on `lacc` (left accumulator) must be lesser or equal than every element in the remainder of the list (omitted by the `function`) keyword, while the elements on `racc` (right accumulator) are strictly greater than those in the remainder of the list, and, consequently, greater than the elements on `lacc`. This means that if the remaining list to be process is empty, then we can simply concatenate `lacc` with `racc`. If the remaining list only contains one item, then it will be placed exactly in the middle of the two accumulators. If the remainder of the list has two or more elements we shall split its tail according to the pivot element, its head, and the `quick_aux` must be initialized with its accumulators as empty lists to avoid errors. The next step is to compare the lengths of the split sub-lists. If `left` is smaller or equal to `right`, then we must first perform the recursive call on `left`. This function call is initialized with `racc` as empty, otherwise it would be the same as placing the highest value elements in the original list in the middle of the list, which would be incorrect, in these intermediate calls we may only place the corresponding extreme of the list. Once all elements on the left side have been sorted, then we can proceed to sort the right side, and can be done so by another recursive call, now this time with the `racc` obtained previously and `sorted_left` sub-list with the pivot appended at the end since `p` is guaranteed to be greater or equal than every element of `left`, and consequently `sorted_left`, but also strictly smaller than every element in the `right` list, and consequently `racc` accumulator. Similarly, the first recursive call will have an empty `lacc`, since it would lead to incorrect values placed in the middle of the resulting list. Moreover, in the second call, since `p` is greater or equal than every element in the `left` list, and, consequently, the `lacc` accumulator, then it can be inserted at the head of the `sorted_right` (the new `racc`), since it is also strictly smaller than every element in right.

Verification-wise, the `quick_aux` function needs a strong set of post conditions to help verify the complex main function presented beforehand:

GOSPEL + OCaml

```
let rec quick_aux p left right = (* ... *)
(*@ ll, lr = quick_aux p left right l
    requires forall x. List.mem x left -> x <= p
    requires forall x. List.mem x right -> x > p
    ensures forall x. List.mem x ll -> x <= p
    ensures forall x. List.mem x lr -> x > p
    ensures permut (l @ left @ right) (ll @ lr)
    variant l *)
```

As expected, we must control what is placed on the accumulators, `left` and `right`, which is adapted from what they represent by the end of the computations, `ll` and `lr`, respectively. The first four clauses, two `requires` (for the accumulators) and two `ensures` (for the final results) conditions, represent exactly this, since one of the sub-lists must contain the elements that are lesser or equal to the pivot, and the other must contain the elements that are strictly greater than `p`. The remaining condition from the original specification is concerned with the permutation of the results from the results, which must be adapted, since the input is now split across three parameters rather than one. The two accumulators and the remainder of the list to be process when concatenated must contain all the elements present in both the resulting sub-lists, meaning that we can not introduce, remove or change any element.

Moving on to the main function:

GOSPEL + OCaml

```
let rec quick_sort lacc racc = (* ... *)
(*@ r = quick_sort lacc racc l
    requires forall x y.
      List.mem x racc -> List.mem y l -> x >= y
    requires forall x y.
      List.mem x l -> List.mem y lacc -> x >= y
    requires forall x y.
      List.mem x racc -> List.mem y lacc -> x >= y
    requires sorted lacc
    requires sorted racc
    ensures sorted r
    ensures permut r (lacc @ l @ racc)
    variant List.length l *)
```

Once more, since the input is now spread over three different parameters, these being `lacc`, `racc`, and the omitted list to be processed, we must update the permutation condition from before. In terms of new conditions, we need to add a staggering total of five `requires` clauses. The last two pre-conditions state that the accumulators must be sorted, otherwise it would not be possible to prove that at the end of the computations the result would be sorted. The first three pre-conditions serve to establish the relative order between each of the input lists, in the sense that any element in `lacc` is lesser or equal to any element in `l` (omitted parameter), which in turn are lesser or equal to the elements in `racc`. However, due to the complexity of this function and algorithm, these specifications by themselves are not enough. In fact, proving that the result is a permutation of the inputs combined is a quite troublesome affair for the SMT solvers. This can be solved with two simple lemmas (which are automatically proved):

GOSPEL

```
(*@ lemma permut_append_mem: forall l1 l2 l3: int list.
    permut l1 (l2 @ l3) ->
      (forall x. List.mem x l2 -> List.mem x l1) &&
      (forall x. List.mem x l3 -> List.mem x l1) *)

(*@ lemma permut_elems: forall l1 l2 l3: int list.
    permut l1 (l2 @ l3) ->
      (forall x. List.mem x l1 <-> List.mem x (l2 @ l3)) *)
```

The first auxiliary lemma, **permut_append_mem** states that if any list `l1` is a permutation of a concatenation of two other lists, `l2` and `l3`, then every element that belongs in either of those lists also belongs in `l1`. The second lemma, **permut_elems**, goes a bit further, it states that if `l1` is a permutation of `l2 @ l3`, then every element that belongs in `l1` also belongs in `l2 @ l3`.

Even after all this trouble the proof is still not complete, however we are closer much than before. Only a few assertions are needed to terminate the proof:

GOSPEL + OCaml

```
(* ... *)
  | [x] -> assert (List.mem x l); lacc @ x::racc
(* ... *)
```

This assertion is essential to ensure that `x` is smaller than the elements in `racc` and greater or equal to the elements of `lacc`, thereby guaranteeing that the result is sorted.

GOSPEL + OCaml

```
(* ... *)
  | p::ls ->
    assert (List.mem p (p::ls));
    let (left, right) = quick_aux p [] [] ls in
    if List.length left <= List.length right then begin
      assert (permut l (left @ [p] @ right));
      let sorted_left = quick_sort lacc [] left in
      quick_sort (sorted_left @ [p]) racc right
    end else begin
      let sorted_right = quick_sort [] racc right in
      quick_sort lacc (p::sorted_right) left
    end
```

The first assertion might seem obvious (and it is in fact), however, in the context of `quick_aux` that is not the case, since `p` and `ls` are separate parameters. Within the auxiliary function the solvers know that `left @ right` is a permutation of `ls`, however `p` is not a part of it, that is that that condition is important. The case where we call the right side first is unexpectedly well-behaved, however, that is not when the left side is called first, and we have to assert that `l` is a permutation of `left @ [p] @ right`.

4.2 Polymorphic Lists

As we have previously discussed, to sort a sequence of elements with a given data type, then that data type must be equipped with a total order relation. In OCaml this can be achieved by using its module system:

OCaml

```
module type Cmp = sig
  type t
  val eq: t -> t -> bool
  val leq: t -> t -> bool
```

```
end
```

`Cmp` is a signature, which is a collection of definitions that must be present in any module that implements it. In this signature, we define our generic type, `t`, and provide two functions, one to test equality, `eq`, between two values of type `t`, and the other, `leq`, to test if the first value is considered lesser or equal than the second. By using a signature we are abstracting from concrete implementations, so that we can achieve a polymorphic type.

Signatures can also be annotated with GOSPEL, in fact this was one of its original uses, before being used for deductive verification with Cameleer. In particular, we need to ensure some basic properties regarding total order:

GOSPEL + OCaml

```
module type Cmp = sig
  type t

  val eq: t -> t -> bool [@@logic]
  (*@ b = eq x y
      ensures b <-> x = y *)

  (*@ function le: t -> t -> bool *)

  (*@ axiom reflexive : forall x. le x x *)
  (*@ axiom total : forall x y. le x y \/ le y x *)
  (*@ axiom transitive: forall x y z. le x y -> le y z -> le x z *)

  val leq: t -> t -> bool [@@logic]
  (*@ b = leq x y
      ensures b <-> le x y *)
end
```

When used, the `[@@logic]` tag enables OCaml definitions (in signatures) to be visible in subsequent annotations (not including in its own definition). The `eq` definition is used to avoid typing errors derived from WhyML, in which the equality operator (`=`) expected integer operands. The result of any implementation of `eq` must be equivalent to the logical equality between the same two elements. Similarly, the results of a concrete `leq` function must be equivalent to the logical `le` function. In GOSPEL it is also possible to provided logical definitions, such as `le`, that must be "implemented" logically. Furthermore, in this context we define the necessary axioms for the `le` definition to be considered a (non-strict) total order relation, these being: reflexivity ($x \leq x$ is true), totality (Let S be some set, then $\forall x, y \in S : x \leq y \lor y \leq x$), and transitivity (if $x \leq y$ and $y \leq z$, then $x \leq z$). Beware that any logical implementation of `le` must be carefully checked beforehand, since the axioms on top are considered true regardless of its correctness, and if it happens to be incorrect, then the proof will be flawed.

4.2.1 Revisiting the verification library

To make use of that signature, we now may make use of a functor, i.e. a module that is parameterized by other modules (or signatures):

OCaml

```
module SomeSort (E: Cmp) = struct
  type elt = E.t

  (* Omitted *)
end
```

We can use this formula for any sorting algorithm in order to allow polymorphism. The updated verification library should be inside this module for access to the `eq` and `leq` functions. So, starting with the function to calculate the number of occurrences:

GOSPEL + OCaml

```
let[@logic][@ghost] rec occ v = function
  | [] -> 0
  | h::t -> (if E.eq h v then 1 else 0) + occ v t
(*@ res = occ v l
    variant l
    ensures 0 <= res <= List.length l
    ensures res > 0 <-> List.mem v l *)
```

The only significant change is to update the if-statement condition by replacing the equality check, `h = v`, with `E.eq` function to `E.q h v`. The `permut` predicate remains unchanged, while the `sorted` predicate updated the `<=` operator to the `E.leq` function:

GOSPEL

```
(*@ predicate permut (l1 l2: elt list) =
    forall x. occ x l1 = occ x l2 *)

(*@ predicate rec sorted (l: elt list) =
    match l with
    | [] | _::[] -> true
    | x::(y::ls) -> E.leq x y && sorted (y::ls) *)
(*@ variant l *)
```

Lemma-wise, `occ_append` does not see any changes, while the remainder have the `<=` operator changed to the `E.leq` function:

GOSPEL + OCaml

```
let[@lemma] rec occ_append (x: elt) (l1: elt list) (l2: elt list) =
  let p = occ x (l1 @ l2) = occ x l1 + occ x l2 in
  match l1 with
  | [] -> assert (p)
  | _::t -> occ_append x t l2; assert (p)
(*@ occ_append x l1 l2
    variant l1
    ensures occ x (l1 @ l2) = occ x l1 + occ x l2 *)
```

```
let[@lemma] rec sorted_head (h: elt) (t: elt list) =
  match t with
  | [] -> ()
  | x::tt -> assert (E.leq h x); sorted_head h tt
(*@ requires sorted (h::t)
    variant t
    ensures forall e. List.mem e t -> E.leq h e *)

(*@ lemma sorted_cons :
    forall x: elt, l: elt list.
    (sorted l /\
    (forall e. List.mem e l -> E.leq x e)) <->
    sorted (x::l) *)

let[@lemma] rec sorted_append (l1: elt list) (l2: elt list) =
  match l1 with
  | [] -> ()
  | h1::t1 ->
    match l2 with
    | [] -> ()
    | h2::t2 -> assert (E.leq h1 h2);
      sorted_append l1 t2; sorted_append t1 l2
(*@ sorted_append l1 l2
    requires sorted l1
    requires sorted l2
    requires forall x y. List.mem x l1 -> List.mem y l2 -> E.leq x y
    ensures sorted (l1 @ l2) *)
```

4.2.2 Revisiting Selection Sort

Adapting from integer-specific code to a polymorphic implementation does not pose significant challenge, since it amounts to changing from concrete operators, such as $\leq$ or $=$, to the operations provided in the `Cmp` signature. In the case of the selection sort algorithm, there are no changes to the main function, since it does not use any of the aforementioned operators. Consequently, the specification of the `selection_sort` function also remains unchanged. By contrast, the auxiliary function has one slight change:

OCaml

```
let rec selection_aux min = function
  | [] -> (min, [])
  | x::r ->
    if E.leq min x then
      let (m, l) = selection_aux min r in m, x::l
    else
      let (m, l) = selection_aux x r in m, min::l
```

This change is in the if-statement condition, which is now `E.leq min x`, to convey that `min` is lesser or equal to `x`, independently of the criteria used to determine when a value is effectively lesser or equal than other for a given concrete data type. Similarly, the annotations also made of use of concrete operators, which need to be replaced:

GOSPEL + OCaml

```
let rec selection_aux min = (* ... *)
(*@ m, r = selection_aux min l
    variant l
    ensures E.leq m min
    ensures forall x. List.mem x r -> E.leq m x
    ensures List.length r = List.length l
    ensures permut (m::r) (min::l) *)
```

There are two slight changes in the specification, in particular in the first and second `ensures` clauses.

4.3 Integer Arrays

4.3.1 Re-revisiting the verification library

Besides syntactic differences in OCaml and GOSPEL, arrays and linked lists are fundamentally different in terms of accessing a given index. One one hand, arrays offer access in constant time complexity. While elements in linked lists, on the other hand, are access, on average, in linear time complexity. This performance "penalty" makes constructing an entirely new list more viable, while arrays may be sorted in-place, or at least with duplicate memory. This drastic change in approaches has repercussions in the verification library, since the sub-lists would be separate entities from the original list, and would be entirely sorted. Meanwhile, in the context of arrays, since we are using the same memory throughout the algorithm, only subsets of the array may be sorted at a given time, so this leads to the creation of a sorted interval predicate:

GOSPEL

```
(*@ predicate sorted_sub (a: int array) (l u: int) =
    forall i j: int. l <= i <= j < u -> a.(i) <= a.(j) *)

(*@ predicate sorted (a: int array) =
    sorted_sub a 0 (Array.length a) *)
```

To define a sorted interval within an array we need a lower and an upper bound. The lower bound is inclusive, while the upper bound is exclusive. For every two indexes inside that interval, such that one is smaller or equal to the other, then the corresponding value of the first must also be smaller or equal to the value in the second index. Additionally, to define a sorted array predicate, we may use an interval from 0 to the length of the array, effectively meaning that all indexes are inside that interval.

Besides the concept of sorted array, we must also define the concept of permutation, as a way to ensure that all elements are retained from one iteration to the other, this will be done through the number of occurrences, as as in the previous libraries:

GOSPEL
```
let[@logic][@ghost] occ v a =
  let r = ref 0 in
  for i = 0 to Array.length a - 1 do
  (*@ invariant 0 <= !r <= i
      invariant !r > 0 -> Array.mem v a
      invariant !r = 0 -> (forall k. 0 <= k < i -> a[k] <> v) *)
    if a.(i) = v then r := !r + 1
  done;
  !r
(*@ res = occ v a
    ensures 0 <= res <= Array.length a
    ensures res > 0 <-> Array.mem v a *)

(*@ predicate permut (a1 a2: int array) =
    forall x. occ x a1 = occ x a2 *)
```

To count the number of occurrences in an array, we may use a for loop. This comes with the cost of having to define invariants based on the post conditions we want to express, these being that the number of occurrences is non-negative, an may be at most the length of the array, in which case every element of the array would be `v`, the value we are looking for. The second post condition states that if the result is a positive number then the elements belongs in the array and vice-versa. The first loop invariant is based on the first post condition, at a given point of the iteration `r`, the reference that stores the result, is non-negative and may be at most `i`, which represents the current index at the start of an iteration, or the next index at the of an iteration (that is why there is no plus 1 after `i`). The other two invariants serve to prove the second post-condition. If `r` holds a positive number then the element must belong to the array. Otherwise, if `r`, in a given iteration, holds 0, then it means that up until that point, no such value was found within the interval of array that has been traversed. The `permut` predicate only sees a slightly change, which is the type of its arguments, since we are now using arrays instead of lists.

4.3.2 Swap-based sorting

One technique commonly present in sorting algorithms, for arrays, is to swap two elements at a time, for instance, with the following function:

OCaml
```
let swap (a: int array) i j =
  let t = a.(i) in
  a.(i) <- a.(j);
  a.(j) <- t
```

Since we are dealing with data that can be mutated, it is important to ensure exactly where and how the data was changed. To achieve this, we suggest the creation of a new predicate, called exchange:

GOSPEL
```
(*@ predicate exchange (a1 a2: int array) (i j: int) =
    Array.length a1 = Array.length a2 &&
    0 <= i < Array.length a1 &&
    0 <= j < Array.length a1 &&
    a1.(i) = a2.(j) &&
    a1.(j) = a2.(i) &&
    (forall k. 0 <= k < Array.length a1 && k <> i -> k <> j ->
      a1.(k) = a2.(k)) *)
```

Given two arrays of the same length (ideally the same memory before and after the changes or a copy that has seen some changes) and two indexes, that fit inside the arrays, *i.e.* they are within 0 (inclusive) and the length of the array (exclusive). These two arrays are considered an exchange from each other if the previous conditions are met, as well as the element in index `i` in each of the arrays is equal to the element in index `j` of the other array. Moreover, every other index, other than `i` and `j` must remain the same between the two arrays. As one might suspect, this predicate is quite strong, and if we notice closely, any two arrays that are an exchange from one another are also a permutation, since they only differ in two positions, which have their values swapped. As such, we must correlate these two predicates:

GOSPEL
```
(*@ axiom exchange_occ : forall a1 a2: int array, i j: int.
    exchange a1 a2 i j -> permut a1 a2 *)
```

With this, we can now proceed to the specification of the `swap` function:

GOSPEL + OCaml
```
let swap (arr: int array) i j = (* ... *)
(*@ requires 0 <= i < Array.length arr
    requires 0 <= j < Array.length arr
    ensures exchange arr (old arr) i j
    ensures permut arr (old arr) *)
```

To avoid invalid accesses we must restrict the values of `i` and `j` to be within the boundaries of the array `arr`. Furthermore, we use our newly created predicate that combines effortlessly with this function to ensure that only two indexes are changed and they come in the form of a swap between the corresponding values. Furthermore, this is a permutation, as previously mentioned.

4.3.3 Insertion Sort

Insertion sort is a classical sorting algorithm, and its main characteristic is that it takes an element and it will check position by position where that element belongs. In a functional setting this is done by traversing the sorted sub-list and stopping once the current element in the sub-list is greater than the value to insert. In an imperative context, this can be done by swapping. We assume that the first element is sorted by default and start from the second value onwards:

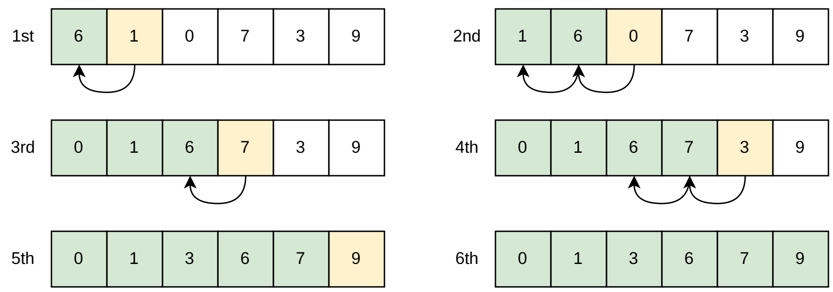

Figure 4.6: Selection sort example

So, we start by processing the second element, this amounts to checking the position immediately before it, and if it is lesser than that value, we perform the swap operation. This process is repeated iteratively for the value that we are placing (represented in yellow), until it reaches a value that it is smaller or equal, or once it reaches the beginning of the array.

This behaviour can be coded as:

OCaml

```
let in_sort arr =
  for i = 1 to (Array.length arr) - 1 do
    let j = ref i in
    while !j > 0 && arr.(!j - 1) > arr.(!j) do
      swap arr !j (!j - 1);
      j := !j - 1
    done
  done
```

As previously mentioned, we start by assuming that index 0 is already sorted, that is whay the `for` loop start at index 1. The element in index i is the value currently being processed (represented as yellow in the figure). So, create a pointer to the current position of the element we are processing, which starts as i, and may change due to swapping. After this, we begin the process of going backwards to find the correct position within previously sorted elements (all elements from 0, inclusive, to i, exclusive). This can be achieved with a `while` loop with two conditions, one to check if the loop has ended, note that this can only be performed if there is an element before index `j`, in other words, `j` must be at least one since it is "behind" on position, and the other condition is that the index immediately before `j` must be strictly greater than the value in `j` so that we can perform the swap operation. If these conditions are met, we can swap the value `j` with the value in `j-1` and decrease `j` by 1.

Verification-wise, this algorithm is not as simple as it might seem from a computational perspective. However, our verification library for arrays and the swapping function are already large steps in this endeavour. So, starting with the function itself:

GOSPEL + OCaml

```
let in_sort arr = (* ... *)
(*@ ensures sorted arr
    ensures permut arr (old arr) *)
```

These two `ensures` conditions are quintessential in any sorting algorithm. Since, we are no longer using recursive functions, unlike the previous sections, we no longer need to prove termination here, at least, and since we are dealing with mutable memory, we may use it in the post condtions, rather than a result variable. Moving on to the outer loop (`for` loop):

GOSPEL + OCaml

```
for i = 1 to (Array.length arr) - 1 do
(*@ invariant sorted_sub arr 0 i
    invariant permut arr (old arr) *)
  (* ... *)
done;
```

This loop reflects the post condtions in the main function, although to a partial degree, in particular, concerning the `sorted` predicate, since only a subset of the array will be sorted. This subsection corresponds to the elements of the left side of the loop variable, `i`, in other words, every index between 0, inclusive, and i exclusive, since from `i`, inclusive, onwards the elements have not been processed yet. This corresponds to using the `sorted_sub` predicate from 0 to i. Finally, the inner loop (`while` loop) can be specified as:

GOSPEL + OCaml

```
while !j > 0 && arr.(!j - 1) > arr.(!j) do
(*@ variant !j
    invariant 0 <= !j <= i
    invariant forall p q.
      0 <= p <= q <= i -> q <> !j -> arr.(p) <= arr.(q)
    invariant permut arr (old arr) *)
  (* ... *)
done
```

Reference `j` is the loop variable and is responsible for every access, directly or indirectly, as such, to avoid accessing invalid memory positions, we must bound `!j`. Since `j` references `i` at the start and decreases every iteration, it is clear that `!j <= i`. The left hand side of the equation in the first invariant is obtained from the fact that if the element to be processed is smaller than every other before it, then it will be placed in index 0, at the start of that iteration `j` will point to 1, and, at the end of that iteration it decreased by 1, which updates it to 0 and breaks the loop, therefore `0 <= !j <= i`. Moreover, termination of the `while` loop can be proven by the value pointed to by `j`, since it is a positive value that decreases every iterarion and remains non-negative throughout the loop. Additionally, we must also reflect the conditions on the code block above, similarly to before, since this is what allows to provethe condtions on that block step-by-step. Due to its simplicity, the `permut` predicate remains the same all throughout. However, the `sorted` predicate is a bit more complex.

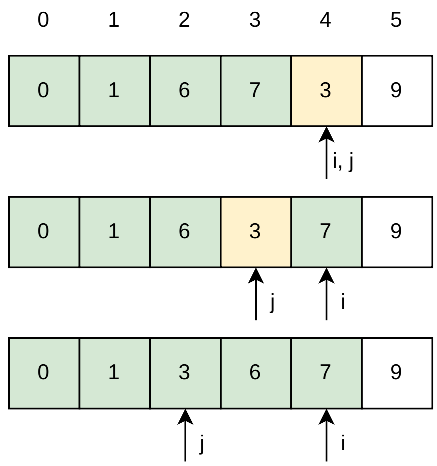

Figure 4.7: Selection sort example

If we extend our interval to include i, we can see that in most situations it is sorted, in fact, the only index that is not sorted coincides with the value of `!j`. Therefore, we may define an adaptation of the sorted predicate that excludes the `!j`, as that is exactly what we do: for any two values between 0 and i (both inclsuve), such that the largest is different from `!j`, then the corresponding value of the lowest index is lesser or equal to the corresponding value of the highest index. In the midst of this confusing condition a question may arise, should `p` not differ from `!j` too? The answer is, surprisingly, no, since if we consider `p = !j`, then everything that comes after `p` has been previously swapped, therefore the corresponding values are strictly higher that `arr.(!j)`.

4.4 Exercises

Implement and specify the:

1. Functional insertion sort
2. Tail recursive insertion sort
3. Polymorphic functional insertion sort
4. Optimized tail recursive selection sort (Hint: Use `::` instead of `@`. Beware of how data is stored).

5. Imperative selection sort (Hint: Use a swap-based implementation)
6. Polymorphic functional merge sort
7. Unoptimized tail recursive quick sort (Hint: Always go the same side first)
8. Polymorphic functional quick sort

Chapter 5

Data Structures

This chapter will be available soon.

Chapter 6

Selected Topics

This chapter will be available soon. For now, we leave readers with a few suggestions on what to do next in the form of exercises.

6.1 Exercises

Formal Verification is a vast field with numerous tools and techniques to learn. We encourage the readers to explore its many facets further, which may include:

- Verifying an algorithm that is not present in this book (beware of tool limitations)
- Learning a new automated deductive verification tool
- Trying a proof assistant (e.q. Rocq, Isabelle, etc.)
- Trying model checking
- Learning Separation Logic

N.B. This is by no means a comprehensive list nor a definitive roadmap. Instead, our intention is to provide a few suggestions on where to go next within this upmost interesting field, in our opinion. Readers who wish to continue studying Formal Verification should survey the current tools and techniques to decide their next step, according to their own interests and curiosity.

Appendix A

Solutions

A.1 Chapter 2

1. Euclidean division that supports negative numbers:

GOSPEL + OCaml

```
let sign n =
  if n >= 0 then 1
  else -1
(*@ r = sign n
    ensures n >= 0 -> r = 1
    ensures n < 0 -> r = -1 *)

let euclidean_div x y =
  let r = ref x in
  let q = ref 0 in
  let sx = sign x and sy = sign y in
  while not (0 <= !r && !r < abs y) do
  (*@ invariant x = y * !q + !r
      invariant x >= 0 -> 0 <= !r
      invariant x < 0 -> !r < abs y
      variant !r * sx + abs y *)
    r := !r - sx *  abs y;
    q := !q + 1 * sy * sx;
  done;
  (!q, !r)
(*@ (q, r) = euclidean_div x y
    requires y <> 0
    ensures x = y * q + r
    ensures 0 <= r < abs y *)
```

Explanation: The first step to verify this problem is to understand how the negative numbers affect the algorithm, with a concrete example:

	$y = 6$	$y = -6$
$x = 17$	$17 = 0 * 6 + 17$ $17 = 1 * 6 + 11$ $17 = 2 * 6 + 5$ Trend: $q \uparrow$, $r \downarrow$	$17 = 0 * (-6) + 17$ $17 = (-1) * (-6) + 11$ $17 = (-2) * (-6) + 5$ Trend: $q \downarrow$, $r \downarrow$
$x = -17$	$-17 = 0 * 6 - 17$ $-17 = (-1) * 6 - 11$ $-17 = (-2) * 6 - 5$ $-17 = (-3) * 6 + 1$ Trend: $q \downarrow$, $r \uparrow$	$-17 = 0 * (-6) - 17$ $-17 = 1 * (-6) - 11$ $-17 = 2 * (-6) - 5$ $-17 = 3 * (-6) + 1$ Trend: $q \uparrow$, $r \uparrow$

As one may observe, when the dividend x is positive, the remainder, r, otherwise r increases. The trend of the quotient, q, depends on both x and y, when both have the same sign q increases, otherwise, q decreases. For this effect, we define and specify the `sign` function:

GOSPEL + OCaml

```
let sign n =
  if n >= 0 then 1
  else -1
(*@ r = sign n
    ensures n >= 0 -> r = 1
    ensures n < 0 -> r = -1 *)
```

By defining additional variables with the sign of each of the inputs, we can accurately model the behaviours of the remainder and quotient:

GOSPEL + OCaml

```
let euclidean_div x y =
  let r = ref x in
  let q = ref 0 in
  let sx = sign x and sy = sign y in
  while not (0 <= !r && !r < abs y) do
    r := !r - sx *  abs y;
    q := !q + 1 * sy * sx;
  done;
  (!q, !r)
```

Another change is the loop condition, the remainder independently of starting as a positive or negative value, it will converge to a value between 0 (inclusive) and the absolute value of the dividend, y (exclusive). These changes reflect in the specification of the `while` loop, while the `euclidean_div` function remains intact:

GOSPEL + OCaml
```
while not (0 <= !r && !r < abs y) do
(*@ invariant x = y * !q + !r
    invariant x >= 0 -> 0 <= !r
    invariant x < 0 -> !r < abs y
    variant !r * sx + abs y *)
  (* ... *)
done;
```

With these changes, the previous `variant` clause (`!r`) becomes obsolete, since the remainder may grow in value when x is negative. So, we need to find a formula, possibly related to the remainder, that always decreases and remains non-negative throughout the loop. The solution that we propose stems from the observation that the remainder has different behaviours depending on the signal of x, so by multiplying these two values we obtain an ever-decreasing expression. However, if x is a negative, then so will r be until just before the last iteration, which implies that $\text{sign}(x) * r < 1$ exactly when that happens. As such, we have to find a suitable upper bound, the most natural choice would the absolute value of y, since the final value of r resides in the interval from 0 to y, so, this leads to $\text{sign}(x) * r + |y| > 0$.

2. Functional Euclidean division:

GOSPEL + OCaml
```
let rec eudiv_aux (x: int) y q r =
  if r < y then (q, r)
  else eudiv_aux x y (q+1) (r-y)
(*@ (q', r') = eudiv_aux x y q r
    requires y > 0
    requires r >= 0
    requires x = y * q + r
    ensures 0 <= r' < y
    ensures x = y * q' + r'
    variant r *)

let eudiv x y = eudiv_aux x y 0 x
(*@ (q, r) = eudiv x y
    requires x >= 0
    requires y > 0
    ensures x = y * q + r
    ensures 0 <= r < y *)
```

Explanation: In this exercise we propose an implementation does not support negative numbers, however, we also encourage readers to try more exercises on their own. The main function, `eudiv`, serves to initiate the values of the quotient as 0 and the remainder as the dividend. As such, the specification of this function does not differ from the imperative versions. In this algorithm the recursion strategy does not change significantly from the imperative version, which leads to the `eudiv_aux` function:

OCaml
```
let rec eudiv_aux (x: int) y q r =
  if r < y then (q, r)
  else eudiv_aux x y (q+1) (r-y)
```

The annotations on this function change slightly from the `while` loop in the imperative version, due to the special properties of the `invariant` clause: the condition must be true before and after every iteration. This type of clause is only available within loops, as such, we have to adapt it into pre- and post-conditions:

GOSPEL + OCaml
```
let rec eudiv_aux (x: int) y q r = (* ... *)
(*@     (q', r') = eudiv_aux x y q r
    requires y > 0
    requires r >= 0
    requires x = y * q + r
    ensures 0 <= r' < y
    ensures x = y * q' + r'
    variant r *)
```

Given the functional nature of this implementation, we now have, as parameters, the previous candidates for the quotient and remainder, q and r, respectively, as well as the next candidates, q' and r', respectively. Both of these pairs of candidates must respect the Euclidean lemma, and due to the immutability of the variables, q and r must respect the condition right from the start, while q' and r' are only available at the end, therefore are used in post-conditions. We must also guarantee that y stays positive and r stays non-negative every iteration. The termination proof remains the same as the imperative version, which is r, since it decreases every iteration.

3. Iterative factorial function:

GOSPEL + OCaml
```
(*@ function rec fact (n: int) : int   =
    if n = 0 then 1
    else n * fact (n-1) *)
(*@ requires n >= 0
    variant n *)

let rec factorial n =
  let r = ref 1 in
  for i = 1 to n do
  (*@ invariant !r = fact (i-1) *)
    r := !r * i
  done;
  !r
(*@ r = factorial n
```

```
    requires n >= 0
    ensures r = fact n *)
```

Explanation: Similar to the Fibonacci example, we must define a logical function to confirm the result of the factorial. This can be achieved using the mathematical definition, a recursive function. It is also worth noting this function is only applicable to non-negative numbers. The main function contains a `for` loop from 1 to n which allows calculating the factorial, if $n = 0$, then the loop is skipped and the result remains correct due to it being initialized as 1. The most notable condition in this example is the invariant: `!r = fact (i-1)`. This can be explained if we observe the behaviour when $i = 2$, if we were to use the condition `!r = fact i`, then, it would mean that at the start of the second iteration the reference r should contain the value of fact(2), which is not true since we are yet to multiply the previous result by 2, therefore the reference is one value behind.

4. Tribonacci sequence:

GOSPEL + OCaml

```
let[@ghost][@logic] rec trib n =
  if n = 0 then 0
  else if n <= 2 then 1
  else trib (n-1) + trib (n-2) + trib (n-3)
(*@ res = trib n
    requires n >= 0
    variant n *)

let tribonacci n =
  let z = ref 0 in
  let y = ref 1 in
  let x = ref 1 in
  for i = 0 to n - 1 do
  (*@ invariant !z = trib i
      invariant !y = trib (i+1)
      invariant !x = trib (i+2) *)
    let sum = !z + !y + !x in
    z := !y;
    y := !x;
    x := sum
  done;
  !z
(*@ res = tribonacci n
    requires n >= 0
    ensures res = trib n *)
```

N.B.: There is discussion on the first element of the Fibonacci sequence, and, even more so, on the first few elements of the Tribonacci sequence. However, from a verification perspective, this discussion is not really important, and what matters is to choose one variant and be consistent about it, or in other words, the logical function and the real implementation should denote the same variant for a successful verification process.

Explanation: As previously mentioned there are two ways to express a logical function, either as a GOSPEL function or an OCaml function with the `ghost` and `logic` tags. So to display both options, we opted to use the latter in this example. One possibility is to use the original Fibonacci example as basis, in which we need to add a new reference for the third value and update accordingly, with this we will calculate two values ahead, and must add an invariant clause to accompany this change.

5. Functional fast exponentiation:

GOSPEL + OCaml

```
(*@ function rec power (x n: int) : int =
    if n = 0 then 1
    else x * power x (n-1) *)
(*@ requires n >= 0
    variant n *)

let[@lemma] rec power_even (x: int) (n: int) =
  if n > 1 then power_even x (n-2)
(*@ requires n >= 0
    requires mod n 2 = 0
    variant n
    ensures power x n = (power (x * x) (div n 2)) *)

let[@lemma] power_odd (x: int) (n: int) =
  power_even x (n-1)
(*@ requires n >= 0
    requires mod n 2 = 1
    ensures power x n = x * (power (x * x) (div n 2)) *)

let rec exp x n =
  if n = 0 then 1
  else
    let r = exp (x * x) (n / 2) in
    if n mod 2 = 0 then r else x * r
(*@ r = exp x n
    requires n >= 0
    variant n
    ensures r = power x n *)
```

Explanation: We recommended using the same logical framework as before, i.e. the `power` logical function, the `power_even` and `power_odd` lemma functions. From an implementation standpoint, when the exponent n is 0, the function returns one, based on our logical definition. In the outer `else` branch, we first obtain the common factor between the two cases $(x^2)^{n/2}$, independently of the parity of n. The nested `if`-statement is used to calculate the final result, as when n is even, it suffices to return r by itself, however, when n is odd, we must also multiply x by r. The specification on the `exp` function is very similar to the imperative version, with the need for a `variant` clause. To prove termination we may use n, since it is a non-negative value that decreases every iteration until it reaches 0 in the end.

A.2 Chapter 3

1. Backwards linear search on arrays with a while loop:

GOSPEL + OCaml

```
let lsearch a v =
  let exception Break of int in
  try
    let i = ref (Array.length a - 1) in
    while !i >= 0 do
    (*@ invariant -1 <= !i < Array.length a
        invariant forall k. !i < k < Array.length a -> a.(k) <> v
        variant !i *)
      if v = a.(!i) then raise (Break !i)
      else i := !i - 1
    done;
    raise Not_found
  with Break i -> i
(*@ r = lsearch a v
    ensures a.(r) = v
    raises Not_found -> forall k. 0 <= k < Array.length a ->
      a.(k) <> v *)
```

Explanation: In this proposed solution we use the exception, however, any other of the taught techniques would be plausible (*i.e.* encoding with negative numbers or options). The main changes in the annotations are the ones on the `while` loop. The index variable i, varies from -1 (inclusive) and size(a) (exclusive), although it only reaches -1 when exiting the loop. This condition, alongside the loop condition guarantee that no invalid position of the array is accessed. Moreover, we need to exclude the previously check part of the array, since we are traversing from right to left the condition changes slightly, its lower limit is $!i$, which is exclusive, since at the start of the iteration we are yet to check index of the current $!i$. The upper limit is, naturally, the length of the array, also exclusive. To prove termination, we may use the value of $!i$ itself, since it decreases every iteration.

A.3 Chapter 4

1. Functional insertion sort:

GOSPEL + OCaml

```
(* Verification library omitted *)

let rec insert x l =
  match l with
  | [] -> [x]
  | y::ls ->
    if x <= y then x::y::ls
    else y::(insert x ls)
(*@ r = insert x l
    requires sorted l
    ensures sorted r
    ensures permut r (x::l)
    variant l *)

let rec insertion_sort l =
  match l with
  | [] -> []
  | [x] -> [x]
  | x::ls -> insert x (insertion_sort ls)
(*@ r = insertion_sort l
    ensures sorted r
    ensures permut r l
    variant l *)
```

Explanation: First we define an auxiliary function, `insert`, that takes a value and a sorted list so that it places the value inside the list in the first place that respects the sorted predicate. The main function, `insertion_sort`, inserts the head of the list using the auxiliary function in a sorted permutation of its tail, obtained from the recursive call.

2. Tail recursive insertion sort:

GOSPEL + OCaml

```
(* Verification library omitted *)

let rec insert x acc l =
  match l with
  | [] -> acc @ [x]
  | y::ls ->
    if x <= y then acc @ x::l
    else insert x (acc @ [y]) ls
(*@ r = insert x acc l
    requires sorted acc
    requires forall k. List.mem k acc -> k <= x
    requires forall k y. List.mem k acc -> List.mem y l -> k <= y
    requires sorted l
```

```
    ensures sorted r
    ensures permut r (acc @ (x::l))
    variant l *)

let rec insertion_sort l acc =
  match l with
  | [] -> acc
  | x::ls -> insertion_sort ls (insert x [] acc)
(*@ r = insertion_sort l acc
    requires sorted acc
    ensures sorted r
    ensures permut r (l @ acc)
    variant l *)
```

Explanation: Starting with the main function, `insertion_sort`, we need an accumulator parameter to store the results of the auxiliary. Note that this allows to swap the order of the function calls when compared to the non-tail recursive version. In that version the main function's recursive call was used as a parameter to the auxiliary function, which would contribute significantly to introducing stack overflows. Specification-wise, `acc` will contain the intermediate results, which are sorted, therefore we need to express this in order to prove that the final result is sorted. Moreover, since the original input is spread in both `l` and `acc`, their concatenation will be a permutation of `r`, the final result. Moving on to the auxiliary function, `insert`, the accumulator will contain the previously visited elements, in the same order as before, so that we can remove list operations with function calls as arguments. As such, we need pre-conditions that state that `acc` is sorted, and its elements are smaller than the element to be inserted, `x`, and every element that has not been processed yet.

3. Polymorphic functional insertion sort:

GOSPEL + OCaml

```
module InsertionSort (E: Cmp) = struct

  (* Verification library omitted *)

  let rec insert x l =
    match l with
    | [] -> [x]
    | y::ls ->
      if E.leq x y then x::y::ls
      else y::(insert x ls)
  (*@ r = insert x l
      requires sorted l
      ensures sorted r
      ensures permut r (x::l)
      variant l *)
```

```
  let rec insertion_sort l =
    match l with
    | [] -> []
    | [x] -> [x]
    | x::ls -> insert x (insertion_sort ls)
  (*@ r = insertion_sort l
      ensures sorted r
      ensures permut r l
      variant l *)

end
```

Explanation: Using the non-recursive implementation, we simply have to replace any $\leq$ or $=$ operators with the corresponding operations from `E`, the module with the comparison functions.

4. Optimized tail recursive selection sort:

GOSPEL + OCaml

```
(* Verification library omitted *)

(* selection_aux remains unchanged *)

let[@lemma] rec rev_permut (l: int list) =
  let l' = List.rev l in
  match l with
  | [] -> ()
  | h::t -> assert (List.mem h l'); rev_permut t
(*@ ensures permut l (List.rev l) *)

let rec selection_sort acc = function
  | [] -> List.rev acc
  | [x] -> List.rev (x::acc)
  | x::ls ->
    let m, r = selection_aux x [] ls in
    assert (List.mem m (x::ls));
    selection_sort (m::acc) r
(*@ r = selection_sort acc l
    requires forall x y.
      List.mem x acc -> List.mem y l -> x <= y
    requires sorted (List.rev acc)
    ensures sorted r
    ensures permut r (l @ acc)
    variant List.length l *)
```

Explanation: The `@` operator has linear time complexity, since the elements are placed at the end of the first list, and we do not have direct access to the final element of the first list. Meanwhile, the `::` operator has constant time complexity, since we have direct access to the first element of the list, and we place an element at its head. So, the objective of this exercise was to optimize the previously presented selection sort implementation. However, this change comes with a cost, since we are now placing elements at the head of the accumulator, then it is in descending order, which contrasts with our desired to sort ascendingly. Therefore, we must revert the result in the final iteration. Moreover, this has consequences in the annotations, the pre-condition that uses the `sorted` predicate must now take in consideration that it is only sorted when reversed. The SMT solvers seem to have a bit of trouble when dealing with reversed lists, as such we have defined the `rev_permut` lemma function, where for each element of a given list we assert that it also can be found in the reversed list, thereby proving that the reverse of a list is a permutation.

5. Imperative selection sort:

GOSPEL + OCaml

```
(* Verification library omitted *)

let sel_sort a =
  let n = Array.length a - 1 in
  for i = 0 to n do
  (*@ invariant sorted_sub a 0 i
      invariant permut a (old a)
      invariant forall x y. 0 <= x < i && i <= y <= n -> a.(x) <= a.(y) *)
    let m = ref i in
    for j = i+1 to n do
    (*@ invariant i <= !m < j
        invariant forall k. i <= k < j -> a.(!m) <= a.(k) *)
      if a.(j) < a.(!m) then m := j
    done;
    swap a i !m
  done
(*@ ensures sorted a
    ensures permut a (old a) *)
```

Explanation: The outer loop serves the purpose to place the $(i+1)^{\text{th}}$ minimum value in the i^{th} position using the swap function. On the other hand, the inner loop is used to find the index containing the current minimum value from the remaining elements to be processed. Unsurprisingly, the specification on the main function ensures that the array, `a`, is sorted, by the end of the process, and a permutation of the original memory disposition. The outer loop reflects these conditions, in particular, a permutation is always a permutation, however, regarding the sorted predicate, only a subset of the array will be sorted during the computations, in particular the positions between 0, inclusive, and `i`, exclusive, since these are the indexes that have already been processed. The third invariant, on the outer loop, states that every element that already has been processed, *i.e.* the ones that are already sorted are greater or equal than those that have not been processed, this is true since at every step we are selecting the smallest number available, therefore, the numbers that have not been processed must be greater or equal. The first invariant on the inner loop bounds the index `!m` to the area that has already been search, `i.e.` starting from `i` (inclusive), which is the first unprocessed element, and `j` (exclusive), which is the current position. The second invariant states that the value of index `!m` must be lesser or equal to every other value we have seen in the unprocessed interval, which is true, since we are looking for the minimum value in that subset, and `!m` must correspond to the best minimum candidate we have seen so far.

6. Polymorphic functional merge sort:

GOSPEL + OCaml

```
module MergeSort (E: Cmp) = struct

  (* Verification library omitted *)

  let rec split (l: elt list) =
    match l with
    | [] -> ([], [])
    | x::ls ->
      let ll, lr = split ls in (lr, x::ll)
  (*@ (r1, r2) = split l
      ensures permut l (r1 @ r2)
      ensures List.length r2 = List.length r1 \/
        List.length r2 = List.length r1 + 1
      ensures List.length r2 + List.length r1 = List.length l
      variant List.length l *)

  let rec merge l1 l2 =
    match l1, l2 with
    | z, [] | [], z -> z
    | x::ls, y::rs ->
      if E.leq x y then x::(merge ls (y::rs))
      else y::(merge (x::ls) rs)
  (*@ r = merge l1 l2
      requires sorted l1
      requires sorted l2
      ensures sorted r
      ensures permut r (l1 @ l2)
      variant List.length l1 + List.length l2 *)

  let rec merge_sort l =
    match l with
    | [] -> []
    | [x] -> [x]
    | _ ->
```

```
    let (a, b) = split l in merge (merge_sort a) (merge_sort b)
  (*@ r = merge_sort l
      ensures sorted r
      ensures permut r l
      variant List.length l *)

end
```

Explanation: Simply amounts to replacing any $\leq$ or $=$ operators with the corresponding operations from E, the module with the comparison functions.

7. Unoptimized tail recursive quick sort:

GOSPEL + OCaml

```
(* Verification library omitted *)

(* quick_aux, permut_append_mem, permut_elems also omitted *)

let rec quick_sort acc = function
  | [] -> acc
  | [x] -> x::acc
  | p::ls ->
    assert (List.mem p (p::ls));
    let (left, right) = quick_aux p [] [] ls in
    let sorted_right = quick_sort acc right in
    quick_sort (p::sorted_right) left
(*@ r = quick_sort acc l
    requires forall x y. List.mem x acc -> List.mem y l -> x >= y
    requires sorted acc
    ensures sorted r
    ensures permut r (l @ acc)
    variant List.length l *)
```

Explanation: Since this is an unoptimized, we may define which side to go first, for instance, let's say right. This decision allows us to reduce the number of accumulators from two to one, since we prioritize one side over the other. This simplifies both the implementation and specification significantly, in particular, we reduce the number of pre-conditions from 5 to 2. It is important to notice that, since we have chosen to always go right first, our accumulator always contains values greater or equal to those in the list of elements yet to be processed, including the pivot (p) itself.

8. Polymorphic functional quick sort:

GOSPEL + OCaml

```
module MergeSort (E: Cmp) = struct

  (* Verification library omitted *)

  let rec quick_aux p = function
```

```
    | [] -> ([], [])
    | x :: r ->
      let ll, lr = quick_aux p r in
      if E.leq x p then x :: ll, lr
      else ll, x :: lr
  (*@ ll, lr = quick_aux p l
      variant l
      ensures forall x. List.mem x ll -> E.leq x p
      ensures forall x. List.mem x lr -> E.g x p
      ensures permut l (ll @ lr) *)

  let rec quick_sort l =
    match l with
    | [] -> []
    | [x] -> [x]
    | p :: ls ->
      let (left, right) = (quick_aux p ls) in
      (quick_sort left) @  p :: quick_sort right
  (*@ r = quick_sort l
      ensures sorted r
      ensures permut r l
      variant List.length l *)

end
```

Explanation: Simply amounts to replacing any $\leq$ or $=$ operators with the corresponding operations from `E`, the module with the comparison functions.