Mathematical Logic in Software Development Documentation

Release 1

Kevin Sullivan

Feb 04, 2018

CONTENTS:

CHAPTER

ONE

REQUIREMENT, SPECIFICATIONS, AND IMPLEMENTATIONS

Software is an increasingly critical component of major societal systems, from rockets to power grids to healthcare, etc. Failures are not always bugs in implementation code. The most critical problems today are not in implementations but in requirements and specifications.

- **Requirements:** Statements of the effects that a system is meant to have in a given domain
- **Specification:** Statements of the behavior required of a machine to produce such effects
- **Implementation:** The definition (usually in code) of how a machine produces the specified behavior

Avoiding software-caused system failures requires not only a solid understanding of requirements, specifications, and implementations, but also great care in both the *validation* of requirements and of specifications, and *verification* of code against specifications.

- **Validation:** *Are we building the right system?* is the specification right; are the requirements right?
- **Verification:** *Are we building the system right?* Does the implementation behave as its specification requires?

You know that the language of implementation is code. What is the language of specification and of requirements?

One possible answer is *natural language*. Requirements and specifications can be written in natural languages such as English or Mandarin. The problem is that natural language is subject to ambiguity, incompleteness, and inconsistency. This makes it a risky medium for communicating the precise behaviors required of complex software artifacts.

The alternative to natural language that we will explore in this class is the use of mathematical logic, in particular what we call propositional logic, predicate logic, set theory, and the related field of type theory.

Propositional logic is a language of simple propositions. Propositions are assertions that might or might not be judged to be true. For example, *Tennys (the person) plays tennis* is actually a true proposition (if we interpret *Tennys* to be the person who just played in the French Open). So is *Tennys is from Tennessee*. And because these two propositions are true, so is the *compound* proposition (a proposition built up from smaller propositions) that Tennys is from Tennessee **and** Tennys plans tennis.

Sometimes we want to talk about whether different entities satisfy give propositions. For this, we introduce propositions with parameters, which we will call *properties*. If we take *Tennys* out of *Tennys plays tennis* and replace his name by a variable, *P*, that can take on the identify of any person, then we end up with a parameterized proposition, *P plays tennis*. Substituting the name of any particular person for *P* then gives us a proposition *about that person* that we can judge to be true or false. A parameterized proposition thus gives rise to a whole family of propositions, one for each possible value of *P*.

Sometimes we write parameterized propositions so that they look like functions, like this: *PlaysTennis(P)*. *PlaysTennis(Tennys)* is thus the proposition, *Tennys plays Tennis* while *PlaysTennis(Kevin)* is the proposition *Kevin plays Tennis*. For each possible person name, *P*, there is a corresponding proposition, *PlaysTennis(P)*.

Some such propositions might be true. For instance, *PlaysTennis(Tennys)* is true in our example. Others might be false. A parameterized proposition thus encodes a *property* that some things (here people) have and that others don't have (here, the property of *being a tennis player*).

A property, also sometimes called a *predicate*, thus also serves to identify a *subset* of elements in a given *domain of discourse*. Here the domain of discourse is the of all people. The subset of people who actually do *play tennis* is exactly the set of people, P, for whom *PlaysTennis(P)* is true.

We note briefly, here, that, like functions, propositions can have multiple parameters. For example, we can generalize from *Tennys plays Tennis **and** Tennys is from Tennessee** to *P plays tennis and P is from L,* where P ranges over people and L ranges over locations. We call a proposition with two or more parameters a *relation*. A relation picks out *combinations* of elements for which corresponding properties are true. So, for example, the *pair* (Tennys, Tennessee) is in the relation (set of *P-L* pairs) picked out by this parameterized proposition. On the other hand, the pair, (Kevin, Tennessee), is not, because Kevin is actually from New Hampshire, so the proposition *Kevin plays tennis **and** Kevin is from Tennessee** is not true. More on relations later!

CHAPTER

TWO

LOGICAL SPECIFICATIONS, IMPERATIVE IMPLEMENTATIONS

We've discussed requirements, specifications, and implementations as distinct artifacts that serve distinct purposes. For good reasons, these artifacts are usually written in different languages. Software implementations are usually written in programming languages, and, in particular, are usually written in *imperative* programming languages. Requirements and specifications, on the other hand, are written either in natural language, e.g., English, or in the language of mathematical logic.

This unit discusses these different kinds of languages, why they are used for different purposes, the advantages and disadvantages of each, and why modern software development requires fluency in and tools for handling artifacts written in multiple such languages. In particular, the educated computer scientist and the capable software developer must be fluent in the language of mathematical logic.

2.1 Imperative Languages for Implementations

The language of implementations is code, usually written in what we call an *imperative* programming language. Examples of such languages include Python, Java, C++, and Javascript.

The essential property of an imperative language is that it is *procedural*. Programs in these languages describe step-by-step *procedures*, in the form of sequences of *commands*, for solving given problem instances. Commands in turn operate (1) by reading, computing with, and updating values stored in a *memory*, and (2) by interacting with the world outside of the computer by executing input and output (I/O) commands.

Input (or *read*) commands obtain data from *sensors.* Sensors include mundane devices such as computer mice, track-pads, and keyboards. They also include sensors for temperature, magnetism, vibration, chemicals, biological agents, radiation, and face and license plate recognition, and much more. Sensors convert physical phenomena in the world into digital data that programs can manipulate. Computer programs can thus be made to *compute about reality beyond the computing machine*.

Output (or *write*) commands turn data back into physical phenomena in the world. The cruise control computer in a car is a good example. It periodically senses both the actual speed of the car and the desired speed set by the driver. It then computes the difference and finally finally it outputs data representing that difference to an *actuator* that changes the physical accelerator and transmission settings of the car to speed it up or slow it down. Computer programs can thus also be made to *manipulate reality beyond the computing machine*.

A special part of the world beyond of the (core of a) computer is its *memory*. A memory is to a computer like a diary or a notebook is to a person: a place to *write* information at one point in time that can then be *read* back later on. Computers use special actuators to write data to memory, and special sensors to read it back from memory when it is needed later on. Memory devices include *random access memory* (RAM), *flash memory*, *hard drives*, *magnetic tapes*, *compact* and *bluray* disks, cloud-based data storage systems such as Amazon's *S3* and *Glacier* services, and so forth.

Sequential progams describe sequences of actions involving reading of data from sensors (including from memory devices), computing with this data, and writing resulting data out to actuators (to memory devices, display screens, and physical systems controllers). Consider the simple assignment command, $x := x + 1$. It tells the computer to

first *read* in the value stored in the part of memory designated by the variable, *x, to add one to that value, and finally to *write* the result back out to the same location in memory. It's as if the person read a number from a notebook, computed a new number, and then erased the original number and replaced it with the new number. The concept of an updateable memory is at the very heart of the imperative model of computation.

2.2 Declarative Languages for Specifications

The language of formal requirements and specifications, on the other hand, is not imperative code but *declarative* logic. Expressions in such logic will state *what* properties or relationships must hold in given situation without providing a procedures that describes *how* such results are to be obtained.

To make the difference between procedural and declarative styles of description clear, consider the problem of computing the positive square root of any given non-negative number, *x*. We can *specify* the result we seek in a clear and precise logical style by saying that, for any given non-negative number *x*, we require a value, *y*, such that $y^2 = x$. Such a *y*, squared, gives *x*, and this makes *y* a square root.

We would write this mathematically as $\forall x \in \mathbb{R} \mid x >= 0, y \in \mathbb{R} | y >= 0 \wedge y^2 = x$. In English, we'd pronounce this expression as, "for any value, *x*, in the real numbers, where *x* is greater than or equal to zero, the result is a value, *y*, also in the real numbers, where *y* is greater than or equal to zero and *y* squared is equal to *x*." (The word, *where*, here is also often pronounced as *such that*. Repeat it to yourself both ways until it feels natural to translate the math into spoken English.)

Let's look at this expression with care. First, the symbol, $\forall$, is read as *for all* or *for any*. Second, the symbol $\mathbb{R}$, is used in mathematical writing to denote the set of the *real numbers*, which includes the *integers* (whole numbers, such as *-1*, *0*, and *2*), the rational numbers (such as $2/3$ and *1.5*), and the irrational numbers (such as *pi* and *e*). The symbol, $\in$, pronounced as *in*, represents membership of a value, here *x*, in a given set. The expression, $\forall x \in \mathbb{R}$ thus means "for any value, *x*, in the real numbers," or just "for any real number, *x*".

The vertical bar followed by the statement of the property, *x >= 0*, restricts the value being considered to one that satisfies the stated property. Here the value of *x* is restricted to being greater than or equal to zero. The formula including this constraint can thus be read as "for any non-negative real number, *x*." The set of non-negative real numbers is thus selected as the *domain* of the function that we are specifying.

The comma is our formula is a major break-point. It separates the specification of the *domain* of the function from a formula, after the comma, that specifies what value, if any, is associated with each value in the domain. You can think of the formula after the comma as the *body* of the function. Here it says, assuming that *x* is any non-negative real numner, that the associated value, sometimes called the *image* of *x* under the function, is a value, *y*, also in the real numbers (the *co-domain* of the function), such that *y* is both greater than or equal to zero equal *and* $y^2 = x$. The symbol, $\wedge$ is the logical symbol for *conjunction*, which is the operation that composes two smaller propositions or properties into a larger one that is true or satisfied if and only if both constituent propositions or properties are. The formula to the right of the comma thus picks out exactly the positive (or more accurate a non-negative) square root of *x*.

We thus have a precise specification of the positive square root function for non-negative real numbers. It is defined for every value in the domain insofar as every non-negative real number has a positive square root. It is also a *function* in that there is *at most one* value for any given argument. If we had left out the non-negativity *constraint* on *y* then for every *x* (except *0*) there would be *two* square roots, one positive and one negative. We would then no longer have a *function*, but rather a *relation*. A function must be *single-valued*, with at most one "result" for any given "argument".

We now have a *declarative specification* of the desired relationship between *x* and *y*. The definition is clear (once you understand the notation), it's concise, it's precise. Unfortunately, it isn't what we call *effective*. It doesn't give us a way to actually *compute* the value of the square root of any *x*. You can't run a specification in the language of mathematical logic (at least not in a practical way).

2.3 Refining Declarative Specifications into Imperative Implementations

The solution is to *refine* our declarative specification, written in the language of mathematical logic, into a computer program, written in an imperative language: one that computes *exactly* the function we have specified. To refine means to add detail while also preserving the essential properties of the original. The details to be added are the procedural steps required to compute the function. The essence to be preserved is the value of the function at each point in its domain.

In short, we need a step-by-step procedure, in an imperative language, that, when *evaluated with a given actual parameter value*, computes exactly the specified value. Here's a program that *almost* does the trick. Written in the imperative language, Python, it uses Newton's method to compute *floating point* approximations of positive square roots of given non-negative *floating point* arguments.

```
def sqrt(x):
    """for x>=0, return non-negative y such that y^2 = x"""
    estimate = x/2.0
    while True:
        newestimate = ((estimate+(x/estimate))/2.0)
        if newestimate == estimate:
            break
        estimate = newestimate
    return estimate
```

This procedure initializes and then repeatedly updates the values stored at two locations in memory, referred to by the two variables, *estimate* and *newestimate*. It repeats the update process until the process *converges* on the answer, which occurs when the values of the two variables become equal. The answer is then returned to the caller of this procedure.

Note that, following good programming style, we included an English rendering of the specification as a document string in the second line of the program. There are however several problems using English or other natural language comments to document specifications. First, natural language is prone to ambiguity, inconsistency, imprecision, and incompleteness. Second, because the document string is just a comment, there's no way for the compiler to check consistency between the code and this specification. Third, in practice, code evolves (is changed over time), and developers often forget, or neglect, to update comments, so, even if an implementation is initially consistent with a such a comment, inconsistencies can and often do develop over time.

In this case there is, in fact, a real, potentially catastrophic, mathematical inconsistency between the specification and what the program computes. The problem is that in Python, as in many everyday programming languages, so-called *real* numbers are not exactly the same as the real (*mathematical*) reals!

You can easily see what the problem is by using our procedure to compute the square root of 2.0 and by then multiplying that number by itself. The result of the computation is the number *1.41421356237*, which we already know has to be wrong to some degree, as the square root of two is an *irrational* number that cannot be represented by any non-terminating, non-repeating decimal. Indeed, if we multiply this number by itself, we get the number, *1.99999999999*. We end up in a situation in which *sqrt(2.0) * sqrt(2.0)* isn't equal to 2.0!

The problem is that in Python, as in most industrial programming languages, *so-called* real numbers (often called *floating point* numbers) are represented in just 64 binary digits, and that permits only a finite number of digits after the decimal to be represented. And additional *low-order* bits are simply dropped, leading to what we call *floating-point roundoff errors.* That's what we're seeing here.

In fact, there are problems not only with irrational numbers but with rational numbers with repeating decimal expansions when represented in the binary notation of the IEEE-754 (2008) standard for floating point arithmetic. Try adding *1/10* to itself *10* times in Python. You will be surprised by the result. *1/10* is rational but its decimal form is repeating in base-2 arithmetic, so there's no way to represent *1/10* precisely as a floating point number in Python, Java, or in many other such languages.

There are two possible solutions to this problem. First, we could change the specification to require only that *y* squared be very close to *x* (within some specified margin of error). The we could show that the code satisfies this approximate definition of square root. An alternative would be to restrict our programming language to represent real numbers as rational numbers, use arbitrarily large integer values for numerators and denominators, and avoid defining any functions that produce irrational values as results. We'd represent *1/10* not as a 64-bit floating point number, for example, but simply as the pair of integers *(1,10)*.

This is the solution that Dafny uses. So-called real numbers in Dafny behave not like *finite-precision floating point numbers that are only approximate* in general, but like the *mathematical* real numbers they represent. The limitation is that not all reals can be represented (as values of the *real* type in Dafny. In particular, irrational numbers cannot be represented exactly as real numbers. (Of course they can't be represented exactly by IEEE-754 floating point numbers, either.) If you want to learn (a lot) more about floating point, or so-called *real*, numbers in most programming languages, read the paper by David Goldberg entitled, *What Every Computer Scientist Should Know About Floating-Point Arithmetic.* It was published in the March, 1991 issue of Computing Surveys. You can find it online.

2.4 Why Not a Single Language for Programming and Specification?

The dichotomy between specification logic and implementation code raises an important question? Why not just design a single language that's good for both?

The answer is that there are fundamental tradeoffs in language design. One of the most important is a tradeoff between *expressiveness*, on one hand, and *efficient execution*, on the other.

What we see in our square root example is that mathematical logic is highly *expressive*. Logic language can be used so say clearly *what* we want. On the other hand, it's hard using logic to say *how* to get it. In practice, mathematical logic is clear but can't be *run* with the efficiency required in practice.

On the other hand, imperative code states *how* a computation is to be carried out, but generally doesn't make clear *what* it computes. One would be hard-pressed, based on a quick look at the Python code above, for example, to explain *what* it does (but for the comment, which is really not part of the code).

We end up having to express *what* we want and *how* to get it in two different languages. This situation creates a difficult new problem: to verify that a program written in an imperative language satisfies, or *refines*, a specification written in a declarative language. How do we know, *for sure*, that a program computes exactly the function specified in mathematical logic?

This is the problem of program *verification*. We can *test* a program to see if it produces the specified outputs for *some* elements of the input domain, but in general it's infeasible to test *all* inputs. So how can we know that we have *built a program* right, where right is defined precisely by a formal (mathematical logic) specification) that requires that a program work correctly for all (∀) inputs?

CHAPTER

THREE

PROBLEMS WITH IMPERATIVE CODE

There's no free lunch: One can have the expressiveness of mathematical logic, useful for specification, or one can have the ability to run code efficiently, along with indispensable ability to interact with an external environment provided by imperative code, but one can not have all of this at once at once.

A few additional comments about expressiveness are in order here. When we say that imperative programming languages are not as expressive as mathematical logic, what we mean is not ony that the code itself is not very explicit about what it computes. It's also that it is profoundly hard to fully comprehend what imperative code will do when run, in large part due precisely to the things that make imperative code efficient: in particular to the notion of a mutable memory.

One major problem is that when code in one part of a complex program updates a variable (the *state* of the program), another part of the code, far removed from the first, that might not run until much later, can read the value of that very same variable and thus be affected by actions taken much earlier by code far away in the program text. When programs grow to thousands or millions of lines of code (e.g., as in the cases of the Toyota unintended acceleration accident that we read about), it can be incredibly hard to understand just how different and seemingly unrelated parts of a system will interact.

As a special case, one execution of a procedure can even affect later executions of the same procedure. In pure mathematics, evaluating the sum of two and two *always* gives four; but if a procedure written in Python updates a *global* variable and then incoporates its value into the result the next time the procedure is called, then the procedure could easily return a different result each time it is called even if the argument values are the same. The human mind is simply not powerful enough to see what can happen when computations distant in time and in space (in the sense of being separated in the code) interact with each other.

A related problem occurs in imperative programs when two different variables, say x and y, refer to the same memory location. When such *aliasing* occurs, updating the value of x will also change the value of y, even though no explicit assignment to y was made. A piece of code that assumes that y doesn't change unless a change is made explicitly might fail catastrophically under such circumstances. Aliasing poses severe problems for both human understanding and also machine analysis of code written in imperative languages.

Imperative code is thus potentially *unsafe* in the sense that it can not only be very hard to fully understand what it's going to do, but it can also have effects on the world, e.g., by producing output directing some machine to launch a missile, fire up a nuclear reactor, steer a commercial aircraft, etc.

CHAPTER

FOUR

PURE FUNCTIONAL PROGRAMMING AS RUNNABLE MATHEMATICS

What we'd really like would be a language that gives us everything: the expressiveness and the *safety* of mathematical logic (there's no concept of a memory in logic, and thus no possibility for unexpected interactions through or aliasing of memory), with the efficiency and interactivity of imperative code. Sadly, there is no such language.

Fortunately, there is an important point in the space between these extremes: in what we call *pure functional,* as opposed to imperative, *programming* languages. Pure functional languages are based not on commands that update memories and perform I/O, but on the definition of functions and their application to data values. The expressiveness of such languages is high, in that code often directly refects the mathematical definitions of functions. And because there is no notion of an updateable (mutable) memory, aliasing and interactions between far-flung parts of programs through *global variables* simply cannot happen. Furthermore, one cannot perform I/O in such languages. These languages thus provide far greater safety guarantees than imperative languages. Finally, unlike mathematical logic, code in functional languages can be run with reasonable efficiency, though often not with the same efficiency as in, say, C++.

In this chapter, you will see how functional languages allow one to implement runnable programs that closely mirror the mathematical definitions of the functions that they implement.

4.1 The identify function (for integers)

An *identity function* is a function whose values is simply the value of the argument to which it is applied. For example, the identify function applied to an integer value, x, just evaluates to the value of x, itself. In the language of mathematical logic, the definition of the function would be written like this.

$$\forall x \in \mathbb{Z}, x.$$

In English, this would be pronounced, "for all ($\forall$) values, x, in ($\in$) the set of integers ($\mathbb{Z}$), the function simply reduces to value of x, itself. The infinite set of integers is usually denoted in mathematical writing by a script or bold Z. We will use that convention in these notes.

While such a mathematical definition is not "runnable", we can *implement* it as a runnable program in pure functional language. The code will then closely reflects the abstract mathematical definition. And it will run! Here's an implementation of *id* written in the functional sub-language of Dafny.

```
function method id (x: int): int { x }
```

The code declares *id* to be what Dafny calls a "function method", which indicates two things. First, the *function* keyword states that the code will be written in a pure functional, not in an imperative, style. Second, the *method* keyword instructs the compiler to produce runnable code for this function.

Let's look at the code in detail. First, the name of the function is defined to be *id*. Second, the function is defined to take just one argument, x, declared of type *int*. The is the Dafny type whose values represent integers (negative, zero, and positive whole number) of any size. The Dafny type *int* thus represents (or *implements*) the mathematical set, $\mathbb{Z}$,

of all integers. The *int* after the argument list and colon then indicates that, when applied to an int, the function returns (or *reduces to*) a value of type *int*. Finally, within the curly braces, the expression *x*, which we call the *body* of this function definition, specifies the value that this function reduces to when applied to any *int*. In particular, when applied to avalue, *x*, the function application simply reduces to the value of *x* itself.

Compare the code with the abstract mathematical definition and you will see that but for details, they are basicaly *isomorphic* (a word that means identical in structure). It's not too much of a stretch to say that pure functional programs are basically runnable mathematics.

Finally, we need to know how expressions involving applications of this function to arguments are evaluated. They fundamental notion at the heart of functional programming is this: to evaluate a function application expression, such as *id(4)*, you substiute the value of the argument (here *4*) for every occurence of the argument variable (here *x*) in the body of the function definition, the you evaluate that expression and return the result. In this case, we substite *4* for the *x* in the body, yielding the literal expression, *4*, which, when evaluated, yeilds the value *4*, and that's the result.

4.2 Data and function types

Before moving on to more interesting functions, we must mention the concepts of *types* and *values* as they pertain to both *data* and *functions*. Two types appear in the example of the *id* function. The first, obvious, one is the type *int*. The *values* of this type are *data* values, namely values representing integers. The second type, which is less visible in the example, is the type of the the function, *id*, itself. As the function takes an argument of type *int* and also returns a value of type *int*, we say that the type of *id* is $int \rightarrow int$. You can pronounce this type as *int to int*.

4.3 Other function values of the same type

There are many (indeed an uncountable infinity of) functions that convert integer values to other integer values. All such functions have the same type, namely $int \rightarrow int$, but they constitute different function *values*. While the type of a function is specified in the declaration of the function argument and return types, a function *value* is defined by the expression comprising the *body* of the function.

An example of a different function of the same type is what we will call *inc*, short for *increment*. When applied to an integer value, it reduces to (or *returns*) that value plus one. Mathematically, it is defined as $\forall x \in \mathbb{Z}, x + 1$. For example, *inc(2)* reduces to *3*, and *inc(-2)*, to *-1*.

Here's a Dafny functional program that implements this function. You should be able to understand this program with ease. Once again, take a moment to see the relationship between the abstract mathematical definition and the concrete code. They are basically isomorphic. The pure functional programmer is writing *runnable mathematics*.

```
function method inc (x: int): int { x + 1 }
```

Another example of a function of the same type is, *square*, defined as returing the square of its integer argument. Mathematically it is the function, $\forall x \in \mathbb{Z}, x * x$. And here is a Dafny implementation.

```
function method h (x: int): int { x * x }
```

Evaluating expressions in which this function is applied to an argument happens as previously described. To evaluate *square(4)*, for example, you rewrite the body, *x * x*, replacing every *x* with a *4*, yielding the expression *4 * 4*, then you evaluate that expression and return the result, here *16*. Function evaluation is done by substituting actual parameter values for all occurrences of corresponding formal parameters in the body of a function, evaluating the resulting expression, and returning that result.

4.4 Recursive function definitions and implementations

Many mathematical functions are defined *recursively*. Consider the familiar *factorial* function. An informal explanation of what the function produces when applied to a natural number (a non-negative integer), *n*, is the product of natural numbers from *1* to *n*.

That's a perfectly understandable definition, but it's not quite precise (or even correct) enough for a mathematician. There are at least two problems with this definition. First, it does not define the value of the function *for all* natural numbers. In particular, it does not say what the value of the function is for zero. Second, you can't just extend the definition by saying that it yields the product of all the natural numbers from zero to *n*, because that is always zero!

Rather, if the function is to be defined for an argument of zero, as we require, then we had better define it to have the value one when the argument is zero, to preserve the product of all the other numbers larger than zero that we might have multiplied together to produce the result. The trick is to write a mathematical definition of factorial in two cases: one for the value zero, and one for any other number.

$$factorial(n) := \forall n \in \mathbb{Z} \mid n >= 0, \begin{cases} \text{if n=0,} & 1, \\ \text{otherwise,} & n * factorial(n-1). \end{cases}$$

To pronounce this mathematical definition in English, one would say that for any integer, *n*, such that *n* is greater than or equal to zero, *factorial(n)* is one if *n* is zero and is otherwise *n* times *factorial(n-1)*.

Let's analyze this definition. First, whereas in earlier examples we left mathematical definitions anonymous, here we have given a name, *factorial*, to the function, as part of its mathematical definition. We have to do this because we need to refer to the function within its own definition. When a definition refers to the thing that is being defined, we call the definition *recursive.*

Second, we have restricted the *domain* of the function, which is to say the set of values for which it is defined, to the non-negative integers only, the set known as the *natural numbers*. The function simply isn't defined for negative numbers. Mathematicians usually use the symbol, $\mathbb{N}$ for this set. We could have written the definition a little more concisely using this notation, like this:

$$factorial(n) := \forall n \in \mathbb{N}, \begin{cases} \text{if n=0,} & 1, \\ \text{otherwise,} & n * factorial(n-1). \end{cases}$$

Here, then, is a Dafny implementation of the factorial function.

```
function method fact(n: int): int
   requires n >= 0 // for recursion to be well founded
{
    if (n==0) then 1
    else n * fact(n-1)
}
```

This code exactly mirrors our first mathematical definition. The restriction on the domain is expressed in the *requires* clause of the program. This clause is not runnable code. It's a specification: a *predicate* (a proposition with a parameter) that must hold for the program to be used. Dafny will insist that this function only ever be applied to values of *n* that have the *property* of being $>= 0$. A predicate that must be true for a program to be run is called a *pre-condition*.

To see how the recursion works, consider the application of *factorial* to the natural number, *3*. We know that the answer should be *6. The evaluation of the expression, *factorial(3)*, works as for any function application expression: first you subsitute the value of the argument(s) for each occurrence of the formal parameters in the body of the function; then you evaluate the resulting expression (recursively!) and return the result. For *factorial(3)*, this process leads through a

sequence of intermediate expressions as follows (leaving out a few details that should be easy to infer):

$$
\begin{aligned}
& factorial\ (3) && \text{; a function application expression} \\
& if\ (3 == 0)\ then\ 1\ else\ (3 * factorial\ (3-1)) && \text{; expand body with parameter/argument substitution} \\
& if\ (3 == 0)\ then\ 1\ else\ (3 * factorial\ (2)) && \text{; evaluate } (3-1) \\
& if\ false\ then\ 1\ else\ (3 * factorial\ (2)) && \text{; evaluate } (3 == 0) \\
& (3 * factorial\ (2)) && \text{; evaluate } ifThenElse \\
& (3 * (if\ (2 == 0)\ then\ 1\ else\ (2 * factorial\ (1)))) && \text{; etc} \\
& (3 * (2 * factorial\ (1))) \\
& (3 * (2 * (if\ (1 == 0)\ then\ 1\ else\ (1 * factorial\ (0))))) \\
& (3 * (2 * (1 * factorial\ (0)))) \\
& (3 * (2 * (1 * (if\ (0 == 0)\ then\ 1\ else\ (0 * factorial\ (-1)))))) \\
& (3 * (2 * (1 * (if\ true\ then\ 1\ else\ (0 * factorial\ (-1)))))) \\
& (3 * (2 * (1 * 1))) \\
& (3 * (2 * 1)) \\
& (3 * 2) \\
& 6
\end{aligned}
$$

The evaluation process continues until the function application expression is reduced to a data value. That's the answer!

It's important to understand how recursive function application expressions are evaluated. Study this example with care. Once you're sure you see what's going on, go back and look at the mathematical definition, and convince yourself that you can understand it *without* having to think about *unrolling* of the recursion as we just did.

Finally we note that the the precondition is essential. If it were not there in the mathematical definition, the definition would not be what mathematicians call *well founded*: the recursive definition might never stop looping back on itself. Just think about what would happen if you could apply the function to *-1*. The definition would involve the function applied to *-2*. And the definition of that would involve the function applied to *-3*. You can see that there will be an infinite regress.

Similarly, if Dafny would allow the function to be applied to *any* value of type *int*, it would be possible, in particular, to apply the function to negative values, and that would be bad! Evaluating the expression, *factorial(-1)* would involve the recursive evaluation of the expression, *factorial(-2)*, and you can see that the evaluation process would never end. The program would go into an "infinite loop" (technically an unbounded recursion). By doing so, the program would also violate the fundamental promise made by its type: that for *any* integer-valued argument, an integer result will be produced. That can not happen if the evaluation process never returns a result. We see the precondition in the code, implementing the domain restriction in the mathematical definition, is indispensible. It makes the definition sound and it makes the code correct!

4.5 Dafny is a Program Verifier

Restricting the domain of factorial to non-negative integers is critical. Combining the non-negative property of ever value to which the function is applied with the fact that every recursive application is to a smaller value of *n*, allows us to conclude that no *infinite decreasing chains* are possible. Any application of the function to a non-negative integer *n* will terminate after exactly *n* recursive calls to the function. Every non-negative integer, *n* is finite. So every call to the function will terminate.

Termination is a critical *property* of programs. The proposition that our factorial program with the precondition in place always terminates is true as we've argued. Without the precondition, the proposition is false.

Underneath Dafny's "hood," it has a system for proving propositions about (i.e., properties of) programs. Here we see that It generates a propostion that each recursive function terminates; and it requires a proof that each such proposition is true.

With the precondition in place, there not only is a proof, but Dafny can find it on its own. If you remove the precondition, Dafny won't be able to find a proof, because, as we just saw, there isn't one: the proposition that evaluation of the function always terminates is not true. In this case, because it can't prove termination, Dafny will issue an error stating, in effect, that there is the possibility that the program will infinitely loop. Try it in Dafny. You will see.

In some cases there will be proofs of important propositions that Dafny nevertheless can't find it on its own. In such cases, you may have to help it by giving it some additional propositions that it can verify and that help point it in the right direction. We'll see more of this later.

The Dafny language and verification system is powerful mechansim for finding subtle bugs in code, but it require a knowledge of more than just programming. It requires an understanding of specification, and of the languages of logic and proofs in which specifications of code are expressed and verified.

CHAPTER

FIVE

INTEGRATING FORMAL SPECIFICATION WITH IMPERATIVE PROGRAMMING

To get a clear sense of the potential differences in performance between a pure functional program and an imperative program that compute the same function, consider our recursive definition of the Fibonacci function.

We start off knowing that if *n* is *0* or *1* the answer is *n*. In other words, the *sequence*, *fib(i)* of *Fibonacci numbers indexed by i*, starts with, $[0, 1, \ldots]$. We start already having the values of *fib(0)*, the first Fibonacci number and *fib(1)*, the second. The third, *fib(2)* is then the sum of the previous two. Note that by convention we index sequences starating at zero rather than one. The first element in such a sequence has index *0*, the second has index *1*, and the *n'th* has index *n - 1*.

Now, for any index *i >= 1*, the next element, *fib(i+1)* is the sum of the previous two elements, *fib(i-1)* and *fib(i)*. Let's call them *fib0=fib(i-1), fib1=fib(i)*, and *fib2=fib(i+1)*. Given a *fib0* and a *fib1* we compute *fib2* by adding *fib0* and *fib1*.

Our recursive definition, *fib(n)* is pure math: elegant and precise. And because we've written in a functional programming language, we can even run it if we wish. An imperative program, by constrast, will just repeated add the last two two known Fibonacci numbers together to get the next one until the desired *nth* one is computed.

Now let's consider the evaluation of each program given the value, *n = 7*. Start with the imperative program. The answers for the first two values are zero and one. If *n* is either zero or one the answer is just returned; otherwise it is computed and returned. In this case, the program will repeatedly add together the last two known values of the function (starting with the *0* and *1*) to obtain the next one. It will then store (remember) the previous and current values of the function to get ready for the next iteration of the loop, terminating once the *n'th* value in the sequence of Fibonacci numbers has been computed. The program returns that value.

Question: How many executions of the loop body are required to compute *fib(5)*? Well, we need to execute it for values of *i* of *2, 3, 4,* and *5*. It takes *4* **n-1* iterations. To compute the 10th element requires that the loop body execute for *i* in the range (inclusive of *[2, 3, . . . , 10]*, which means nine iterations of the loop will be required, or, again, *n-1*. Indeed, it's pretty easy to see that for any value of *n*, *n-1* iterations of the loop body will be required to compute the *nth* Fibonacci number.

The functional program, on the other hand, is evaluated by repeated unfolding of nested recursive definitions until values are computed, at which point the values are combined into a final result. Let's see if we can see a pattern. We'll measure computational complexity now in terms of the number of function evaluations (rather than loop bodies executed).

To compute $fib(0)* or $fib(1)$ requires just 1 function evaluation, as these are base cases with no recursive calls to solve subproblems. To compute *fib(2)* however requires *3* evalations of *fib*, one for *2* and one for each of *1* and *0*. Those count as just one each as there are no further recursive calls. So the relationship between *n* and the number of function evaluations currently looks like this: $\{(0, 1), (1, 1), (2, 3), ...\}$.

What about when *n* is *3*? Computing this requires answers for *fib(2)*, costing *3* evaluations, and *fib(1)*, costing one, for a total of *5* evaluations. Computing *fib(4)* requires answers for *fib(3)* and *fib(2)*, costing *5 + 3*, or *8* evaluations, plus the original evaluation is 9. For *fib(5)* we need *9 + 5*, or *14*, plus the original makes $15* evaluations. relation is like this: $\{(0, 1), (1, 1), (2, 3), (3, 5), (4, 9), (5, 15), ...\}$. So, in general, the number of evaluations needed to evaluate

fib(i+1) is the sum of the numbers required to compute *fib(i)* and *fib(i-1) + 1*. Now that we see the formula, we can compute the next entry in the sequence easily: the number of function evaluations needed to compute *fib(6)* is *15 + 9 + 1*, i.e., 25. Computing the value of *fib(7)* costs *41* evaluations; *fib(8), *67*l *fib(9), 109*, *fib(10), 177* and *fib(11), 286* function evaluations.

With out imperative program, the number of loop body interations grows linearly with *n*. We could say that the computational cost of running the imperative program to compute *fib(n)*, let's call it *cost(n) is just *n+1*. How does the cost of the (doubly) recursive program grow as a function of *n*? Well, one thing to notice is that the cost of computing the Fibonacci sequence is close to the Fibonacci sequence itself! The first two values in the *cost* sequence are *1* and *1*, and each subsequence element is the sum of the previous two *plus 1*. It's not exactly the Fibonacci sequence, but it turns out to grow at the same rate overall. Without getting into details, the Fibonacci sequence, and thus also the cost of computing it recursively, grows at an exponential rate, with an exponent of about *1.6*. Increasing *n* by *1* does quite double the previous cost, but it does multiply it by about *1.6*.

No matter how small the exponent, exponential functions eventually grow very large very quickly. You can already see that the cost to compute *fib(n)* recursively for values of *n* larger than just ten or so is vastly greater than the cost to compute it iteratively. The math (the recursive definition clear but inefficient. The program is efficient, but woefully not transparent as to its function. We need the latter program for practical computation. But how do we ensure that hard to understand imperative code flawlessly implements the same function that we expressed so elegantly in mathematical logic and its computational expression in pure functional programming?

We address such problems by combining a few ideas. First, we use logic to express *declarative* specifications that precisely define *what* a given imperative program must do, an in particular what results it must return as a function of the arguements it received.

We can use functions defined in the pure functional programming style as specifications, e.g., as giving the mathematical definition of the *factorial* function that an imperative program is meant to implement.

Second, we implement the specified program in an imperative language in a way that supports logical reasoning about its behavior. What kind of support is needed to facilitate logical reasoning is broached in this chapter. For example, we have to specify not only the desired relationship between argument and result values, but also how loops are designed to work in our code; and we need to design loops in ways that make it easier to explain in formal logic how they do what they are meant to do.

Finally, we use logical proofs to *verify* that the program satisifies its specification.

We develop these idea in this chapter. First we explain how formal specifications in mathematical logic for imperative programs are often organized. Next we explore how writing imperative programs without the benefits of specification languages and verifications tools can make it hard to spot bugs in code. Next we enhance our implementation of the factorial function with specifications, show how Dafny flags the bug, and fix out program. Doing this requires that we deepen the way we understand loops. We end with a detailed presentation of the design and verification of an imperative program to compute elements in the Fibonacci sequence. Given any natural number *n*, our program must return the value of *fib(n)*, but it must also do it efficiently. The careful design of a loop is once again the very heart of the problem. We will see how Dafny can help us to reason rigorously about loops, and that, with just a bit of help, it can reason about them for us.

5.1 Logical Specification

First, we use mathematical logic to *declaratively specify* properties of the behaviors that we require of programs written in *imperative* languages. For example, we might require that, when given any natural number, n, a program compute and return the value of the $factorial$ of n, the mathematical definition of which we've given as $fact(n)$.

Specifications about required relationships between argument values and return results are especially important. They specify *what* a program must compute without specifying how. Specifications are thus *abstract*: they omit *implementation details*, leaving it to the programmer to decide how best to *refine* the specification into a working program.

For example we might specify that a program (1) must accept any integer valued argument greater than or equal to zero (a piece of a specification that we call a *precondition*), and (2) that as long as the precondition holds, then it must return the factorial of the given argument value (a *postcondition*).

In purely mathematical terms, a specification of this kind defines a *binary relation* between argument and return values, and imposes on the program a requirement that whenever it is given the first value in such a pair, it must compute a second value so that the $(firstvalue, secondvalue)$ pair is in the specified relation.

A binary relation in ordinary mathematics is just a set of pairs of values. A function is a special binary relation with at most one pair with a given first value. A function is said to be a *single-valued* relation.

For example, pairs of non-negative integers in the relation that constitutes the factorial function include $(0, 1), (1, 1), (2, 2), (3, 6), (4, 24)$ and $(5, 120)$, but not $(5, 25)$.

On the other hand, square root is a relation but not a *function*. It is not singled valued. Both $(4, 2)$ and $(4, -2)$, two pairs with the same first element but different second elements, are in the relation. That is because both *2* and *-2* are squarer roots of *4*. The *positive square root* relation, on the other hand, is a function, comprising those pairs in the square root relation where both elements are non-negative. It thus includes $(4, 2)$ but not $(4, -2)$.

We could formulate the square root *relation* as a *function* in a different way: by viewing it as a relation that associates with each non-negative integer the single *set* of its square roots. The pair $(4, \{2, -2\}$ is in this relation, for example. The relation is now also a function in that there is only one such pair with a given first element.

Now what we mean when we say that a program computes a function or a relation is that whenever it is given a valid argument representing the *first* value of a pair in the relation, it computes a *second* value such that the pair, $(first, second)$ is in the given relation. When we say, for example, that a program *computes the factorial function*, we mean that if we give it a non-negative number, *n*, it returns a number *m* such that the pair *(n,m)* is *in* the relation. And for *(n,m)* to be in the relation it must be that $m = fact(n)$. The program thus has to return $fact(n)$.

A program that computes a *function* is deterministic, in the sense that it can return at most one result: because there is at most one result. When a program computes a relation that is not a function, it can return any value, *m*, where *(n,m)* is in the specified relation.

5.2 Rigorous Implementation

Having written a formal specification of the required *input-output* behavior of a program, we next write imperative code in a manner, and in a language, that supports the use of formal logic to *reason* about whether the program refines (implements) its formal specification. One can use formal specifications when programming in any language, but it helps greatly if the language has strong, static type checking. It is even better if the language supports formal specification and logical reasoning mechanisms right alongside of its imperative and functional programming capabilities. Dafny is such a language.

In addition to choosing a language with features that help to support formal reasoning (such as strong, static typing), we sometimes also aim to write imperative code in a way that makes it easier to reason about formally (using mathematical logic). As we will see below, for example, the way that we write our while loops can make it easier or harder to reason about their correctness.

5.3 Formal Verification

Our ultimate aim to deduce that, as written, a program satisfies its input-output specification. In more detail, if we're given a program, *C* with a precondition, *P*, and a postcondition *Q*, we want a proof that verifies that if *C* is started in a state that satisfies *P* and if it terminates (doesn't go into an infinite loop), that it ends in a state that satisfies *Q*. We call this property *partial correctness*.

We write the proposition that *C* is partially correct in this sense (that if it's started in a state that satisfies the assertion, *P*, and if it terminates then, it will do so in a state that satisfies *Q*) as PCQ. This is a so-called *Hoare triple* (named after the famous computer scientist, Sir Anthony (Tony) Hoare. It is nothing other than a proposition that claims that *C* satisfies its specification.

In addition to a proof of partial correctness, we usually do want to know that a program also does always terminate. When we have a proof of both $P\{C\}Q$ and that the program always terminates, then we have a proof of *total correctness*. Dafny is a programming system that allows us to specify *P* amd *Q* and that then formally, and to a considerable extent automatically, verifies *P {C} Q* and termination. That is, Dafny produces proofs of total correctness.

It is important to bear in mind that a proof that a program refines its formal specification does not necessarily mean that it is fit for its intended purpose! If the specification is wrong, then all bets are off, even if the program is correct relative to its specification. The problem of *validating* specification againts real-world needs is separate from that of *verifying* that a given program implements its specification correctly.

5.4 Case Study: Implementing the Factorial Function

So far the material in this chapter has been pretty abstract. Now we'll see what it means in practice. To start, let's consider an ordinary imperative program, as you might have written in Python or Java, for computing the factorial function. The name of the function is the only indication of the intended behavior of this program. There is no documented specification. The program takes an argument of type nat (which guarantees that the argument has the property of being non-negative). It then returns a nat which the programmer implicitly claims (given the function name) is the factorial of the argument.

```
method factorial(n: nat) returns (f: nat)
{
    if (n == 0)
    {
        return 1;
    }
    var t: nat := n;
    var a: nat := 1;
    while (t !=  0)
    {
        a := a * n;
        t := t - 1;
    }
    f := a;
}
```

Sadly, this program contains a bug. Try to find it. Reason about the behavior of the program when the argument is 0, 1, 2, 3, etc. Does it always compute the right result? Where is the bug? What is wrong? And how could this logical error have been detected automatically?

The problem is that the program lacks a complete specification. The program does *something*, taking a nat and possibly returning a nat (unless it goes into an infinite loop) but there's no way to analyze its correctness in the absence of a specification that defines what *right* even means.

Now let's see what happens when we make the specification complete. The precondition will continue to be expressed by the type of the argument, *n*, being *nat*. However, we have added a postcondition that requires the return result to be the factorial of *n*. Note that we used our functional definition of the *factorial* function in the *specification* of our imperative code. The pure functional program is really just a mathematical definition of factorial. What we assert with the postcondition is thus that the imperative program computes the factorial function as it is defined in pure mathematics.

```
method factorial(n: nat) returns (f: nat)
    ensures f == fact(n)
{
    if (n == 0)
    {
        return 1;
    }
    var t := n;
    var a := 1;
    while (t !=  0)
    {
        a := a * n;
        t := t - 1;
    }
    return a;
}
```

Dafny now reports that it cannot guarantee—formally prove to itself—that the *postcondition* is guaranteed to hold. Generating proofs is hard, not only for people but also for machines. In fact, one of seminal results of 20th century mathematical logic was to prove that there is no general-purpose algorithm for proving propositions in mathematical logic. That's good news for mathematicians! If this weren't true, we wouldn't need them!

So, the best that a machine can do is to try to find a proof for any given proposition. Sometimes proofs are easy to generate. For example, it's easy to prove *1 = 1* by the *reflexive* propery of equality. Other propositions can be hard to prove. Proving that programs in imperative languages satisfy declarative specifications can be hard.

When Dafny fails to verify a program (find a proof that it satisfies its specification), there is one of two reasons. Either the program really does fail to satisfy its specificaiton; or the program is good but Dafny does not have enough information to know how to prove it.

With the preceding program, the postcondition really isn't satisfied due to the bug in the program. But even if the program were correct, Dafny would need a little more information than is given in this code to prove it. In particular, Dafny would need a litte more information about how the while loop behaves. It turns out that providing extra information about while loops is where much of the difficulty lies.

5.5 A Formally Verified Implementation of the Factorial Function

```

```

Here's verified imperative program for computing factorial. We start by documenting the overall program specification.

```
method verified_factorial(n: nat) returns (f: nat)
    ensures f == fact(n)
```

Now for the body of the method. First, if we're looking at the case where *n==0* we just return the right answer immediately. There is no need for any further computation.

```
if (n == 0)
{
    return 1;
}
```

The rest of the code handles the case where *n > 1*. At this point in the program execution, we believe that *n* must be greater than zero, as we would have just returned if it were zero, and it can't be negative because its type is *nat*. We

can nevertheless formally assert (write a proposition about the state of the program) that *n* is greater than zero. Dafny will try to (and here will successfully) verify that the assertion is always true at this point in the program.

```
assert n > 0;
```

Strategy: use a while loop to compute the answer. We can do this by using a variable, a, to hold a "partial factorial value" in the form of a product of the numbers from n down to a loop index, "i," that we start at n and decrement down, terminating the loop when *n==0*. At each point just before, during, and right after the loop, *a* is a product of the numbers from *n* down to *i*, and the value of *i* represents how much of this product-computing work remains to be done. So, for example, if we're computing factorial(10) and a holds the value *10 * 9*, then *i* must be *8* because the task of multiplying *a* by the factors from *8* down to *1* remains to be done. A critical "invariant" then is that if you multiply *a* by the factorial of *i* you get the final answer, the factorial of *n*. And in particular, when *i* gets down to *0*, *a* must contain the final result, because *a * fact(0)* will then equal *fact(n)* and *fact(0)* is just *1*, so *a* must equal *fact(n)*. This is how we design loops so that we can be confident that they do what we want tem to do.

Step 1. Set up state for the loop to work. We first initializie a := 1 and i := n and check that the invariant holds. Note that we are using our pure functional math-like definition of fact as a *specification* of the factorial function we're implementing.

```
var i: nat := n;    // nat type of i explicit
var a := 1;         // can let Dafny infer it
```

In Dafny, we can use matnematical logic to express what must be true at any given point in the execution of a program in the form of an "assertion." Here we assert that our loop invariant holds. The Dafny verifier tries to prove that the assertion is a true propsition about the state of the program when control reaches this point in the execution of this program.

```
assert a * fact(i) == fact(n); // "invariant"
```

Step 2: Now evaluate the loop to get the answer. To evaluate a loop, first, evaluate the loop condition (i > 0).Then , if the result is false, terminate the loop. Otherwise, evaluate the loop body, then iterate (run the loop again, starting by evaluating the loop condition).

Note that we can deduce that the loop body is going to execute at least once. It will run if i > 0. What is i? We initialized it to n and haven't change it since then so it must still be equal to n. Do we know that n is greater than 0? We do, because (1) it can't be negative owning to its type, and (2) it can't be 0 because if it were 0 the program would already have returned. But we can now do better than just reasoning in our heads; we can use logic to express what we believe to be true and let Dafny try to check it for us automatically.

```
assert i > 0;
```

Let's just think briefly about cases. We know i can't be zero. It could be one. If it's one, then the loop body will run. The loop body will run. a, which starts at 1, will be multiplied by i, which is 1, then i will be decremented. It will have the value 0 and the loop will not run again, leaving a with the value 1, which is the right answer. So, okay, let's run the loop.

```
while (i >  0)
    invariant 0 <= i <= n
    invariant fact(n) == a * fact(i)
{
    a := a * i;
    i := i - 1;
}
```

At this point, we know that the loop condition is false. In English, we'd say it is no longer true that i is greater than zero." We can do better that saying this in natural language then forgetting it. We can use formal logic to formalize and document our belief and if we do this then Dafny pays us well for our effort by checking that our assertion is true.

```
assert !(i > 0);
```

We can also have Dafny check that our loop invariant still holds.

```
assert a * fact(i) == fact(n);
```

And now comes the most crucial step of all in our reasoning. We can deduce that a now holds the correct answer. That this is so follows from the conjunction of the two assertions we just made. First, that i is not greater than 0 and given that its type is nat, the only possible value it can have now is 0. And that's what we'd expect, because that's the condition on which the loop terminates, which is just did! But better than just saying it, let us also formalize, document, and check it.

```
assert i == 0;
```

Now it's easy to see. No matter what value i has, a * fact(i) == fact(n), and i == 0, so we have a * fact(0) == fact(n), and we know that fact(0) is 1 because we see that in the very mathematical definition of fact, so it must be that a = fact(n). Dafny can check!

```
assert a == fact(n);
```

We thus have the answer we need to return. Dafny verifies that our program satisfies its formal specification. We no longer have to pray. We *know* that our program is right and Dafny confirms our belief.

```
return a;
```

Mathematical logic is to software as the calculus is to physics and engineering. It's not just an academic curiosity. It is a critical intellectual tool, inceasingly used for precise specification and semi-automated reasoning about and verification of real programs.

5.6 Case Study: Verified Implementation of the Fibonacci Function

Similarly, here an imperative implementation of the fibonacci function, without a spec.

```
method fibonacci(n: nat) returns (r: nat)
    ensures r == fib(n)
```

Now for the body. First we represent values for the two cases where the result requires no further computation. Initially, *fib0* will store the value of *fib(0)* and *fib1* will store the value of *fib(1)*.

```
var fib0, fib1 := 0, 1; //parallel assmt
```

Next, we test to see if either of these cases applies, and if so we just return the appropriate result.

```
if (n == 0) { return fib0; }
if (n == 1) { return fib1; }
```

At this point, we know something more about the state of the program than was the case when we started. We can deduce, which is to say that we know, that *n* has to be greater than or equal to *2*. This is because it initially had to be greater than or equal to zero due to its type, and then we would already have returned if it were *0* or *1*, to it must now be *2* or greater. We can document the belief that the current state of the program has to property that the value of the variable *n* is greater than or equal to *2*, and Dafny will verify this assertion for us.

```
assert n >= 2;
```

So now we have to deal with the case where *n >= 2*. Our strategy for computing fib(n) in this case is to use a while loop with an index i. Our design will be based on the idea that at the beginning and end of each loop iteration (we are currently at the beginning), we will have computed fib(i) and that its value is stored in fib1. We've already assigned the value of fib(0) to fib0, and of fib(1) to fib1, so to set up the desired state of affairs, we should initialize *i* to be *1*.

```
var i := 1;
```

We can state and Dafny can verify a number of conditions that we expect and require to hold at this point. First, *fib1* equals *fib(i)*. Now to compute the next (*i+1*) Fibonacci number, we need not only the value of $fib(i)* but also *fib(i-1)*. We will thus also want *fib0* to hold this value at the start and end of each loop iteration, and indeed we do have that state of affairs right now.

```
assert fib1 == fib(i);
assert fib0 == fib(i-1);
```

To compute *fib(n)* for any *n* greater than or equal to *2* will require at least one execution of the loop body. We'll thus set our loop condition to be $i < n$. This ensures that the loop body will run, as *i* is *1* and *n* is at least *2*, so the condition *i < n* is *true*, which dictates that the loop body must be evaluated.

Within the loop body we'll compute fib(i+1) (we call it *fib2* within the loop) by adding together *fib0* and *fib1*; then we increment i; then we update *fib0* and *fib1* so that for the *new* value of *i* they hold *fib(i-1)* and *fib(i)*. To do this we assign the initial value of *fib1* to *fib0* and the value of *fib2* to *fib1*.

Let's work an example. Suppose *n* happens to be *2*. The loop body will run, and after the one execution, *i* will have the value, *2*; *fib1* will have the value of $fib(2)$, and *fib0* will have the value of *fib(1)$. Because *i* is now *2* and *n* is still *2*, the loop condition will now be false and the loop will terminate. The value of *fib1* will of course be *fib(i)* but now we'll also have that *i == n* (it takes a little reasoning to prove this), so *fib(i)* will be *fib(n)*, which is the result we want and that we return.

We can also informally prove to ourself that this strategy gives us a program that always terminates and returns a value. That is, it does not go into an infinite loop. To see this, note that the value of *i* is initally less than or equal to *n*, and it increases by only *1* on each time through the loop. The value of *n* is finite, so the value of *i* will eventually equal the value of *n* at which point the loop condition will be falsified and the looping will end.

That's our strategy. So let's go. Here's the while loop that we have designed. And here, for the first time, we see something crucial. We tell Dafny about certain properties of the state of the program that hold both before and after every execution of the loop body. We call such properties *invariants*. Dafny needs to know these invariants to prove to itself (and to us) that the loop does what it is intended to do: that the result at the end will be as desired.

```
while (i < n)
    invariant i <= n;
    invariant fib0 == fib(i-1);
    invariant fib1 == fib(i);
{
    var fib2 := fib0 + fib1;
    fib0 := fib1;
    fib1 := fib2;
    i := i + 1;
}
```

The invariants are just the conditions that we required to hold for our design of the loop to work. First, *i* must never exceed *n*. If it did, the loop would spin off into infinity. Second, to compute the next (the *i+1st)* Fibonacci number we have to have the previous *two* in memory. So *fib0* better hold *fib(i-1)* and *fib1*, *fib(i)*. Note that these conditions do not have to hold *within* the execution of the loop body, but they do have to hold before before and after each execution.

The body of the loop is just as we described it above, and we can use our own minds to deduce that if the invariants hold before the loop body runs (and they do), then they will also hold after it runs. We can also see that after the loop terminates, it must be that *i==n*. This is because we know that it's always true that *i <= n* and the loop condition must

now be false, which is to say that *i* can no longer be strictly less than *n*, so *i* must now equal *n*. Logic says so, and logic is right. What is amazing is that we can write these assertions in Dafny if we wish to, and Dafny will verify that they are true statements about the state of the program after the loop has run. We have *proved* (or rather Dafny has proved and we have recapitulated the proof in this sequence of assertions) that we have without a doubt computed the right answer. Dafny has also proved to itself that the loop always terminates, and so we have in effect a formal proof of total correctness for this program.

```
assert i <= n;       // invariant
assert !(i < n);     // loop condition is false
assert (i <= n) && !(i < n) ==> (i == n);
assert i == n;       // deductive conclusion
assert fib1 == fib(i); // invariant
assert fib1 == fib(i) && (i==n) ==> fib1 == fib(n);
assert fib1 == fib(n);
return fib1;
```

5.7 What is Dafny?

Dafny is a cutting-edge software language and tooset developed at Microsoft Research—one of the top computer science research labs in the world—that provides such a capability. We will explore Dafny and the ideas underlying it in the first part of this course, both to give a sense of the current state of the art in program verification and, most importantly, to explain why it's vital for a computer scientist today to have a substantial understanding of logic and proofs along with the ability to *code*.

Tools such as TLA+, Dafny, and others of this variety give us a way both to express formal specifications and imperative code in a unified way (albeit in different sub-languages), and to have some automated checking done in an *attempt* to verify that code satisfies its spec.

We say *attempt* here, because in general verifying the consistency of code and a specification is a literally unsolvable problem. In cases that arise in practice, much can often be done. It's not always easy, but if one requires ultra-high assurance of the consistency of code and specification, then there is no choice but to employ the kinds of *formal methods* introduced here.

To understand how to use such state-of-the-art software development tools and methods, one must understand not only the language of code, but also the languages of mathematical logic, including set and type theory. One must also understand precisely what it means to *prove* that a program satisfies its specification; for generating proofs is exactly what tools like Dafny do *under the hood*.

A well educated computer scientist and a professionally trained software developer must understand logic and proofs as well as coding, and how they work together to help build *trustworthy* systems. Herein lies the deep relevance of logic and proofs, which might otherwise seem like little more than abstract nonsense and a distraction from the task of learning how to program.

CHAPTER

SIX

INDICES AND TABLES

- genindex
- modindex
- search