Master Thesis

Design and implementation of a verifier for sequential programs using the Hoare calculus

submitted by: Florian Wege
Student number: 15856
Field of studies: Information and Communication Systems
Merseburg University of Applied Sciences

supervised by: Prof. Dr. phil. Dr. rer. nat. habil. Michael Schenke
Merseburg University of Applied Sciences
Prof. Dr. rer. nat. habil. Andreas Spillner
Merseburg University of Applied Sciences

Merseburg, November 1, 2017

Table of Contents

List of Tables

List of Figures

Listings

Abstract

The ***Floyd-Hoare*** logic or calculus is a methodology for proving the partial or total correctness of computer programs developed by ***C.A.R. Hoare*** based on ideas of ***Robert W. Floyd*** and has awoken a wave of enthusiasm in the domain of program verification. Though the system has received a great deal of recognition, some fundamental problems in effectively using it remain to be solved, as they were found undecidable at large.

This document aims to build a bridge between the often only theoretically-contemplated ***Hoare*** calculus and the venture to implement such with an example, starting from scratch. It describes the construction of an LL(1) parser, the preparation of corresponding grammars, a transformation of the obtained syntax trees, the ***Hoare*** methodology itself and then delves into the issues of searching for loop invariants and the handling of logical and arithmetic expressions, seeking heuristics of the implication problem, resorting to user interaction where automated solutions fall short.

Chapter 1

1 Introduction

1.1 Motivation

Since the introduction of computers, more and more of humanity's activities experienced a shift into the direction of digital handling. That transition streamlined a lot of things but also called for a new profession facing up to the proper control of those machines, which would soon become known under the term ***software engineering***. As there is a myriad of processes to be described and accounted for, the phenomenon had been bound to fan out. Thus the emergence of specialized engineers for diverse systems and their hybrid forms gradually came to life. "Programming" in its accustomed associations has turned into a basic skill and some politicians actually want to integrate it firmly into the curriculums of elementary schools [Kam16]. This discipline has also adapted a certain trait of creativity. With the right idea in mind for an App, arranging the available components in a way of high usability, one can tap a market demand because a range of platforms and services are already in place for unleashing one's creative mind upon. Hardware, too, became more feasible and sophisticated in time but, as the term discloses, software stands for an elevated level of malleability, which initially fosters a trial-and-error-flavored development. Adding more and more layers of abstraction, the exact behavior of a program is often up for speculation. Unless one is working with embedded systems, which require a close-up treatment, being aware of the inner workings, to some extent at least, has been rendered increasingly dispensable.

> "At least once a semester I hear some kid yell, 'Wow! This is like magic!' and that really motivates them."
>
> —Alfred Thompson, computer science teacher [Kam16]

This aspect is in contradistinction to the foundations of computer science, which seeks to formalize and systematically find solutions to problems. And in fact, as the application of software engineering progressed, the domain of topics enlarged and everything became more complex. There is the so-called ***Law of leaky Abstractions*** [Spo02] as depicted by ***Joel Spolsky*** in 2002. It states that there is no perfect

abstraction of non-trivial procedures. Especially when things do not work as they should, the put-on mask falls off and implementation details resurface. Questions of optimization and concerns about security are catching up and thus a particularized insight into the groundwork is about to regain value. As noted above, most everyday business is already handled by software and there are a couple of different applications where utmost accuracy is key:

- monetary transactions: automatic teller machines, to debit the right account, transfering ability to where it is needed
- infrastructure: e.g. ensuring the proper behavior of vehicles, switching and communication systems
- dealing with customer (private) data
- ...

Since it is more economic to do so, most software companies are content with the density of errors below a priorly specified threshold. That is, the amount of errors per lines of code is measured and weighed against a target value set within the analysis phase. For applications where an error could cost the life of a human being, the common pick is a limit of 0.5 per 1000 lines (0.05%) [Wik17b]. Yet one may argue that risks of that kind should be diminished completely to zero and that an individual life would not be up for quantification. From a historical viewpoint, a broad range of different causes for malfunctioning software could be recorded: A comma in lieu of a dot, a wrong signum leading a numeric expression, the usage of a wrong formula, racing conditions, an insufficient domain of definition, protocol errors, imprecision of floating point operations, overload, buffer overflow/underflow, non-considered constellations and many more [Tan16][Kle09] pp. 4-6. Upcoming are trends like ***IoT*** (***Internet of Things***) or autonomous driving that pose new layers of networks and challenge established safety aspects. Another famous concern is cost efficiency: It is well known that the later a software mistake is discovered, the more expensive it is to fix it. After the development phase ended, the team that initially wrote the program often moved on to newer shores. Or in a case like the Mars rover ***Curiosity***, once deployed, replacing the software a posteriori appears rather challenging. Moreover, often enough, the source code is not published. Demanded requirements can change eventually and glitches may manifest themselves without displaying any symptoms right away but which may infect the system nonetheless and deal a blow to its expandability later on.

Summarizing this section, the sources of programming errors are multifarious. There is a lot of potential hidden in between and it is often vital to know that a piece of code is indeed working correctly before shipping or utilizing it. Hence is implied a stricter methodology of scrutinizing software if not one for its systematic development.

1.2 Analysis vs simulation

To decrease the number of errors, a range of actions is at the software engineer's disposal. Most often that involves peer reviews, i.e. an independent surveyor evaluates one's code. Another idea is to simulate the behavior by carrying out dynamic test cases, directly running units or whole modules [McC08]. Therefore, positive test cases are written that present well-formed inputs or conditions for an algorithm, then that algorithm is executed and the results are checked for their integrity. Conversely, negative tests are to confirm that bad input or precondition scenarios will yield a proper error handling. The program is not supposed to end in an unregarded segmentation fault (stemming from an invalid access of memory), maybe should instead display a message box and append the information of the exception to a log file. However, those tests cover but a part of the possible instances the code allows for, therefore fail to vindicate an overall correctness as a famous quote by ***E. W. Dijkstra*** alleges:

> "Program testing can best show the presence of errors but never their absence."
>
> —Edsger W. Dijkstra [Dij69]

On the other hand, when speaking about verification in the environment of theoretical computer science, the term denotes a genuine proof of the absence of errors within a program according to a specification using formal means. It therefore poses an exact method to evaluate the quality of a software, which, as hinted above, turns out to be crucial at some points and as a consequence rightfully contributes to the discipline of software engineering.

1.3 Basic approaches

Currently, there are two main approaches known to this stipulation: model checking and deductive means. Model checking is the method of deciding whether a program or a model of it suffices a given specification by exploring its state-space. At this, a model serves an abstraction of the reality. The idea is to examine the model in order to draw conclusions about the actual system. It needs to be fitting to the task at hand, should be reduced as far as possible to simplify the issue but still contain all the relevant information to make the decision. Different models can be mixed to acquire new information but such course of action is quick to decline the collective operability. The ***state-space*** is a set or graph of constellations of the values of variables and the current point of execution. This vector describes the state of the program in its entirety. By going through the program code, a verifying tool shifts between the states in order

to find all possible execution paths. Those are then checked against constraints, e.g. invariants like a combination of variable values that should never occur. If an execution path is discovered that violates these conditions, it will be exposed and the programmer can observe the execution path that lead to the error to hopefully fix its root cause. This approach basically traverses all accessible variations of execution before it marks the program as approved. That is why there is an exponential growth in computation time and required memory involved, rendering the algorithm impractical fairly quickly. Model checking also necessitates a closed, finite system (or an algorithm to render it as such). Otherwise the program could keep allocating memory and the number of states would not exhaust, thus the verifier may never come to a conclusion. Dynamic data structures may be examined by dedicated methods like shape analysis [Wik17f]. Both the model and the specifications are described in appropriate languages that allow the verifier to work with. Due to the intent of exploring the state space, the modeling language must project a finite state machine. Examples are ***PROMELA*** (***Process Meta Language***), ***Timed Automata*** or ***Petri*** nets [Kle09]. The specifications or properties checked for are usually decorated by logical expressions like temporal logic as introduced in programs by ***A. Pnueli*** [Pnu77], are tacit (a division by zero should never occur) or may be integrated in the modeling language itself, e.g. ***PROMELA*** permits to insert assertions as part of the control flow [Wik17e].

Another way of verifying a program and the approach presented to be in this documentis by deductive resolution of theorems. This idea was first introduced by ***Alan Turing*** on a conference in 1949 [FLM84]. Due to typographical mistakes and other circumstances, it went hidden for a bit but other researchers had retaken the topic, ultimately. The important aspect back then was the notion that the problem of proving the correctness of programs could be modularized and that a program (***Turing*** used flowcharts) could be decorated with assertions. Later, in 1969, ***C.A.R. Hoare*** invented a set of axioms and rules, the so-called ***Hoare*** triples, that would point out a relation between an elementary program instruction or control flow and its effect on what can be logically assumed from what the semantics of this code snippet are to imply. For example, the following listing increments a numerical variable x by 1.

```
1    x:=x+1
```

Listing L1: Simple increment of a variable

Now it can be said that prior to this assignment, the variable had been smaller by 1 compared to its new state. Or more confusingly, before the assignment, every occurrence of x in an assertion had been substituted by the expression of the new value comparing to the ensuing outcome.

```
1  PRE {true}
2    z:=x+y;
3    z:=z*2;
4    z:=z-(x+y)
5  POST {z=x+y}
```

Listing L2: Disadvantages of state-space exploration

The above Listing L2 shall serve as an easily comprehensible example for when deductive means outclass the procedure of state exploration. Assuming that x and y are only 2 byte integer variables and may take any value in their data type domain, that totals the combination of 32 bits or over 4 billion possibilities to check the postcondition for, which is what state exploration would do. On the other hand, a human being should be able to recognize the pattern without much effort. By substitution, one could argue the assignments can be reduced to a single one ($z := x + y$) and that straight appears to match the postcondition. So does the above program fulfill the surrounding specification? Maybe, maybe not. It should be considered that, first off, the conditions between the curly braces possess their own language with their own semantics, e.g. the operators may have their own meaning. Secondly, those are not exactly mathematical expressions. As hinted by x and y being 2 byte integer variables, z too might be restricted, thus the add and multiplication instructions may cause a buffer overflow, whereupon the semantics would have been altered by the substitution then. So of course it depends on the underlying system and that system respectively the semantics of the language have to be well-known in advance. Other than that, an axiomatic theorem solver like the human would identify the pattern, apply rules on the structure of the program to see what can be derived from it and then make statements about it.

Deductive program verification, however, comes with its own set of problems: Those usually revolve around the elementary control flow structures of imperative programming languages and the implications of those are not necessarily assessable in their entirety. The question whether a logic expression connotes another is notably undecidable. Furthermore, the later more precisely examined calculus only establishes relationships and does not exactly hand out an algorithm. From theoretical computer science it can be stated that, with no loss of generality, it is impossible to say if a program satisfies a set of specifications of any kind. However, it becomes more feasible when narrowed down to classes of programs and regarded languages.

1.4 What the document is about

The objective of this document shall be to outline the ***Hoare*** calculus, to make a design for a verifier that would present how its rationales can be applied starting from a raw string input, how the mathematical formulae that come with it could be transcribed to imperative algorithms and at which points the interaction with a human user is still required. The design is then to be implemented in the ***Java*** programming language along with an appropriate graphical user interface to portray the inductive procedure of ***Hoare***-style reasoning.

To conclude the introduction, it should be stated that both model checking and theorem solving rely on a proper specification of the issue. If that is already faulty, which may be the case, since the specification needs a strict formalization as well, any verification will be meaningless and is prone to invoke type II errors ("false negatives") because it fails to project the client's true intentions. Figure F1 reveals more origins of error. Even when establishing specifications and a model and even obtaining the program by transformation of the model in the target language, there are still risks of human failings in between that may falsify the verification result (and the tooling must be assumed to be working flawlessly). That poses another reason why even a formal verification should only be seen as an additional scheme in the quality assurance toolkit.

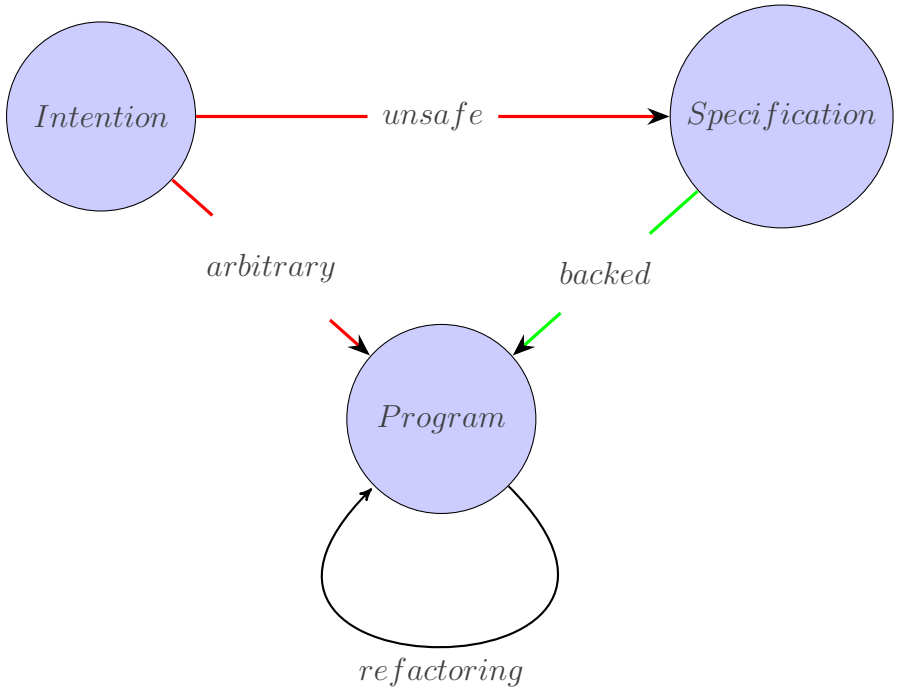

Figure F1: From intention to program.

Chapter 2
2 Preliminaries

2.1 Overview

Before plunging into the core topic of this document, it appears necessary to formalize the target of a prospective verifier. In order to make statements about the validity of a program, whether it holds to certain properties or not, both the program and the properties should be fixated. What could be considered secure knowledge anyway? Such a holistic view only makes sense under the presumption that some basic ideas can already be regarded as irrevocably intrinsic and then means of induction, analogy or suchlike are used to widen the scope and to declare more statements compatible to the existing knowledge base, verifying them or, if they appear as contradictory, objecting them. And the strategy here is like-minded: To know if a program fulfills some conditions, the meaning of the program and the conditions have to be exact. Since this entails lots and lots of programs and attributes in general, it becomes evident that rather than manually and pointlessly contemplating all possible variations, it deems better to ascribe it to some underlying scheme that can be unfolded on demand. Therefore the meaning, also called the semantics, of a program (and later also those of conditions) should be inductively synthesized using an appropriate model kit relating to a set of basic entities. Prior to determining the semantics, these entities also have to be identified as such, which is the part of the syntax analysis and shall be depicted as well.

Therefore the schedule is as follows: The rest of this chapter will give some further classification, tease about the purport and hand over a short preview. It may be skimmed or skipped over if the reader is fond of the contextual knowledge. Chapter 3: *Introduction of a Language* will formally start with the definition of a suitable language, how it is characterized and how it can be processed. Subsequently, the specific language subject to this documentand whose programs are to be verified is firmly presented along with some simple remarks about its significance. Chapter 4: *How to prove* first formalizes these semantics and then reasons about their usage, talks about the notion of correctness and introduces assertions by extending the language. Finally, a transition to the ***Hoare*** rule system will be conducted, how to use it for verification of sequential programs and what challenges come with it. Examples will be reviewed and ideas to overcome the challenges be discussed along with some hints to the implementability of

such endeavor. At this point, the theory and the general design will have been covered. The realization of the verifier using the aforementioned theory is carried out via the ***Java*** programming language and eyed in the hindmost Chapter 5: *Implementation* . Introduced shall be a simplified imperative language that later becomes target of the ***Hoare*** rule system which is derived from operational semantics. The language contains basic control flow elements like the composition of instructions, the selection routine and condition-controlled loops. More complex programs can be written by combining the aforementioned basic structures.

2.2 How to instruct computers

Computers by definition are devices that understand some sort of digitally represented information and can process it in compliance with a program. That program may be immutably ingrained or be loaded from a mounted memory storage as more dynamic machines permit, which is what bestows a great range of use cases upon them and made them ubiquitous. Yet those machines are set up at some point and consist of a number of rigid hardware components providing their specific functionality and each of that hardware piece speaks a certain language that needs to be addressed for. To be able to have this orchestra flawlessly work in unison, besides complying with a couple of basic interfaces, there is usually a mediator called the ***operating system*** in between and the concept of drivers further helps to identify the spoken language of each component. Hardware and operating system together are then referred to as the platform, serving as a layer to host user-written programs on and more layers can be stacked on top if required. But the platform is essentially the lowest layer to have the angularity of the hardware components relaxed. At this point, everything channels through its digital interface and is therefore unified in the language referred to as ***machine code***.

Still, machine code, as the name indicates, varies between different machines. In fact, in the beginning, software engineers tended to write in ***assembly*** language, which is a more human-readable representation of machine code yet still platform-dependent. To not have to rewrite the same program logic for different platforms over and over again, more levels of abstractions were piled up and thus high level languages were born. High level languages like ***C*** aggregate universal coding paradigms like variables or control structures and can combine elementary instructions to larger compounds. This makes it easier for the software engineer to assess the functionality of a program, which in turn is kind of a first step to boost the drafting of correct programs. For the platform to be able to use such high level programs, of course it appears necessary to reduce them to executable machine code again. The standard procedure is depicted in Figure F2 . The user-manufactured code may be exposed to a preprocessor, which

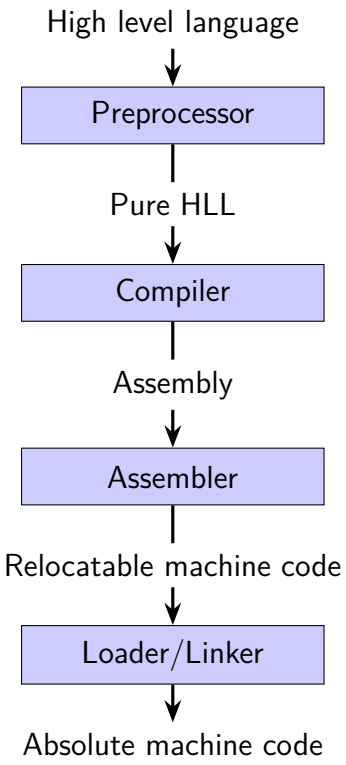

Figure F2: High level code to machine code.

takes care of some preparatory tasks like the inclusion of other script files or alternative substitutions like those carried out by the ***#define*** directive in the ***C*** language. This yields the pure high level language as understandable by a ***compiler***. The compiler does the main part of the translation and outputs assembly code which only needs to be transcribed to machine code and linked together to obtain the final executable version the hardware setup can be operated with.

The language as described in this document won't be in need of such a preprocessor and the verification is directly applied to the high level language during the compiler phase. Thus any kind of assembly output or lower level persistence is not required here and, in fact, the workings of a compiler can be split up further in detail.

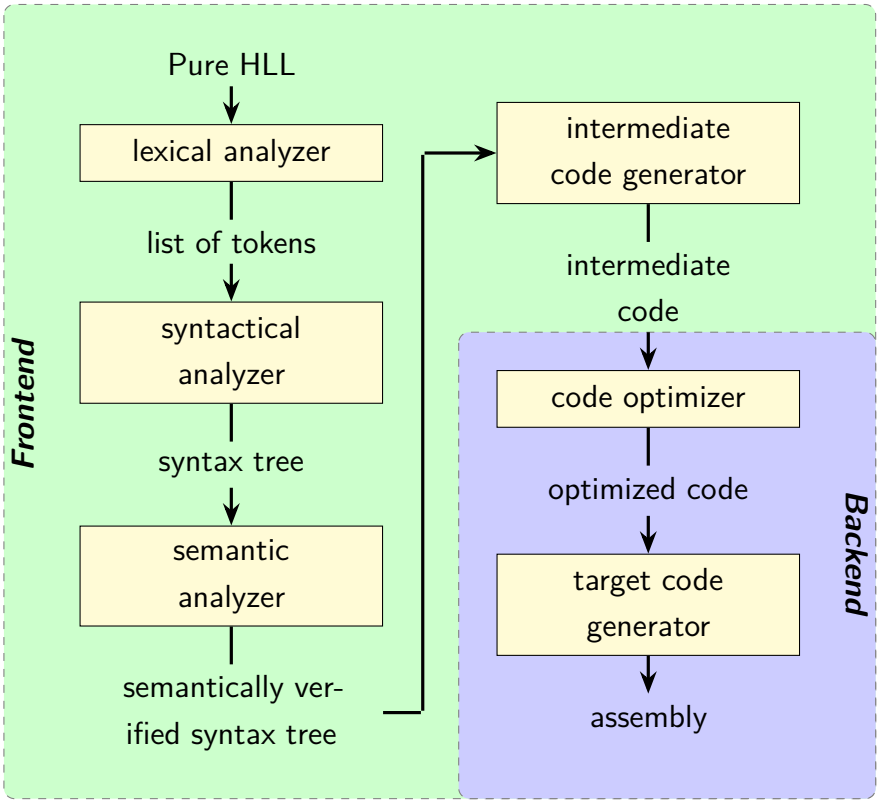

Figure F3: Processing chain of a compiler [Rav17].

Figure F3 shows the composition of the different components of a compiler. In a first step, a lexical analyzer, usually referred to as ***lexer*** or ***tokenizer***, surveys the raw input sequence of characters and contracts the to be as cohesive identified words (***lexemes***) to a sequence of tokens in the same order. This makes it easier for the syntactical analyzer (***parser***) to progress because it promotes the tokens to serve as the atomic symbols instead of the initial single characters. Both lexer and parser work with some grammar based on which the symbols are bestowed semantics but while the task of a lexer is to handle a less complex regular grammar (***Chomsky***'s level 3), which can be realized using regular expressions, parsers must cope with context-free grammars (***Chomsky***'s level 2) and normally it would be desirable for the parser to produce a tree structure incorporating rule precedence [Sas10]. The lexer can also be used to remove unnecessary white space and comments. More about the process can be read in Chapter 5: *Implementation* . After the syntactical analysis, there can be a semantic analysis that cross-checks the validity of the constructed syntax tree or sanitizes it, e.g. the typing in a variable assignment statement like:

$$x := y + 1 \tag{2.1}$$

Do variable x and the expression $y+1$ assigned to it actually match in their respective

data type? Since the type of the variable may be fixated (declared) far off the assignment instruction, it probably won't reside in the same branch/grammar production rule path. Moreover, the namespace for variables may be shared with other entities like functions, so it might make sense to examine whether the identifier does really denote a variable. Thus the semantic analyzer exposes a verified syntax tree. The ***Intermediate Code Generator*** translates the syntax tree into another intermediate representation, which serves as an interface between the high level language and the platform. The last two steps (***Code Optimizer*** and ***Target Code Generator***) can then be replaced per setup, so the other components are left untouched. The program verifier as described in this document is inserted right after the syntactical analyzer. It would ideally be done after a semantic analysis but the contemplated language and the samples are simple enough that such won't be required. Nowadays, the described analyses are often processed incrementally in background threads parallel to the programmer writing code and, in this way, assisted deductive program verification can be blended in on-the-fly but suchlike tool and verification in general are rather subject to specialized languages at this point in time. Examples of those languages are ***Spec#***, an extension to ***C#*** or ***JML (Java Modeling Language)***, which seeks to introduce verification specifications in the ***Java*** programming language by wilily wrapping the additional semantics required in backwards compatibility guaranteeing comment syntax.

Chapter 3

3 Introduction of a Language

3.1 On languages and grammars

3.1.1 Definitions

The considered programs are made up from a sequence of symbols of a given ***alphabet***. A sequence of symbols is said to be a ***word***.

Definition 1. *An alphabet is a set of symbols.*

Ex: $\{a, b, c\}$

Definition 2. *A word is a string or finite sequence of symbols (associated to a specific alphabet).*

Ex: $\{aaba, bbb, acb\}$ using the alphabet $\{a, b, c\}$

To later derive a meaning from it, some code must be established in advance and not just any word shall be accepted by the compiler but a well-defined set of words as denoted by a formal ***language***.

Definition 3. *A language is a set of words. Since those sets are usually infinite, a language is commonly described by a predicate.*

Ex: A language may be designated by the notation of a regular expression like for instance *a*b*, the asterisk being a quantifier for the preceding symbol, indicating "an arbitrary number of", so the given example would encompass the words b, ab, aab, $aaab$ and so on but regular expressions can only describe regular languages (***Chomsky***'s level 3) while there are other ways to address greater sets of languages. Since languages as defined above alone still lack a proper structure to bind semantics to, the concept of grammars is to be introduced. Those consist of a set of production rules to span a language incrementally, chunk and organize their words into a tree structure, called the ***tree of the syntax***. Grammars always relate to a (specific type of) language and are formalized as following:

Definition 4. *A grammar is a tuple of a set of variables (also called non-terminals), terminal symbols, production rules and a starting symbol (or set thereof).*

$$G = (V, T, P, S)$$

- *V - set of non-terminal symbols or variables*
- *T - set of terminal symbols*
- *P - production rules*
- *S - starting symbol(s)*

⟨*exp*⟩ ::= ⟨*exp*⟩ '+' ⟨*exp*⟩
| ⟨*exp*⟩ '*' ⟨*exp*⟩
| 'id'

⟨*bool_exp*⟩ ::= ⟨*bool_exp*⟩ '&' ⟨*bool_exp*⟩
| ⟨*bool_exp*⟩ '|' ⟨*bool_exp*⟩
| ⟨*exp*⟩ '<' ⟨*exp*⟩
| ⟨*exp*⟩ '>' ⟨*exp*⟩
| ⟨*exp*⟩ '<=' ⟨*exp*⟩
| ⟨*exp*⟩ '>=' ⟨*exp*⟩
| ⟨*exp*⟩ '=' ⟨*exp*⟩
| ⟨*exp*⟩ '<>' ⟨*exp*⟩
| 'true'
| 'false'

Figure F4: First example grammar.

The first example of a grammar in Figure F4 displays the standard ***Backus-Naur Form*** notation [Mignd] that will also be used throughout this document. In a mathematical tuple notation it corresponds to:

$$
\begin{aligned}
G = (\\
&V = \{\langle \text{exp} \rangle, \langle \text{bool\_exp} \rangle\},\\
&T = \{\text{`id'}, \text{`+'}, \text{`*'}, \text{`\&'}, \text{`|'}, \text{`<'}, \text{`>'}, \text{`<='}, \text{`>='}, \text{`='}, \text{`<>'}, \text{`true'}, \text{`false'}\},\\
&P = \{\langle \textit{exp} \rangle ::= \langle \text{exp} \rangle \text{ `+' } \langle \text{exp} \rangle,\\
&\langle \textit{exp} \rangle ::= \langle \text{exp} \rangle \text{ `*' } \langle \text{exp} \rangle,\\
&\langle \textit{exp} \rangle ::= \text{`id'},\\
&\langle \textit{bool\_exp} \rangle ::= \langle \text{bool\_exp} \rangle \text{ `\&' } \langle \text{bool\_exp} \rangle,\\
&\langle \textit{bool\_exp} \rangle ::= \langle \text{bool\_exp} \rangle \text{ `|' } \langle \text{bool\_exp} \rangle,\\
&\langle \textit{bool\_exp} \rangle ::= \langle \text{exp} \rangle \text{ `<' } \langle \text{exp} \rangle,\\
&\langle \textit{bool\_exp} \rangle ::= \langle \text{exp} \rangle \text{ `>' } \langle \text{exp} \rangle,\\
&\langle \textit{bool\_exp} \rangle ::= \langle \text{exp} \rangle \text{ `<=' } \langle \text{exp} \rangle,\\
&\langle \textit{bool\_exp} \rangle ::= \langle \text{exp} \rangle \text{ `>=' } \langle \text{exp} \rangle,\\
&\langle \textit{bool\_exp} \rangle ::= \langle \text{exp} \rangle \text{ `=' } \langle \text{exp} \rangle,\\
&\langle \textit{bool\_exp} \rangle ::= \langle \text{exp} \rangle \text{ `<>' } \langle \text{exp} \rangle,\\
&\langle \textit{bool\_exp} \rangle ::= \text{`true'},\\
&\langle \textit{bool\_exp} \rangle ::= \text{`false'}\},\\
&S = \{\langle \text{exp} \rangle\}\\
)
\end{aligned}
$$

Figure F5: Example grammar as a tuple.

This assumes that $\langle \text{exp} \rangle$ is indeed the starting symbol, which is not quite clarified in the first notation and will instead be separately stated when needed. Variables are those that appear on the lefthand side of the production rules and which form the non-terminal nodes of the syntax tree. Terminals are atomic symbols, which means they cannot be split up any further and become leaves of the syntax tree. They can only be found on the righthand side of the rules. Furthermore, production rules tell how the input words shall be broken down into variables and terminals. The starting symbol (or set thereof) determines what rule(s) to regard on the highest level. The pipe or vertical line symbol | in the ***Backus-Naur Form*** indicates an alternative. Thus the variable $\langle \text{exp} \rangle$ can either be derived to *exp + exp*, to *exp * exp* or to *id* here.

Now there are different classes of grammars. Depending on it, the required strategy of a parser will look different. The later introduced language shall suffice the context-free LL(1) type. This is why the following steps explain the constraints and construction of an LL(1) grammar. To obtain such one, ambiguity, left recursion and non-determinism shall be erased. Some examples are to be inspected and transformed accordingly before

stepping further and applying the learned techniques on the actual used language.

3.1.2 Ambiguity, associativity, precedence

Note: Most of the conductions and remarks in this section refer to the compiler design lectures by ***Ravindrababu Ravula*** [Rav17].

$$\langle exp \rangle \quad ::= \langle exp \rangle \text{ `+' } \langle exp \rangle \mid \text{`id'}$$

Figure F6: Two-sided recursive grammar.

In a first step, the grammar of Figure F6 depicts the concatenation of 'id' terminals by the '+' operator, namely the infix notation of addition. When exposing an input *id+id+id* to that grammar, the two different syntax trees shown in Figure F7 may be obtained. That means the derivation process is not definite. Even with the arithmetic addition of two numbers being associative and commutative (Abelian), ambiguity in grammars is not really desired. There shall exist no more than one possible syntax tree for the same input and grammar. Telling if a grammar is ambiguous in general is not decidable [Wik17a]. However, the ambiguity at hand is evidently induced because it is unclear whether the addition operator binds to the lefthand or righthand side. This can be taken care of by rewriting the production rules to not include the same non-terminal on both ends. The grammar of Figure F8 has the non-terminal situated at the ending, its syntax trees grow right-sided (rightmost derivation). The grammar of Figure F9 has the non-terminal situated at the beginning, its syntax trees grow left-sided (leftmost derivation). With the addition being commutative, it does not matter semantics-wise but in order to be capable of elucidating another point about leftmost derivation, it shall be persevered with.

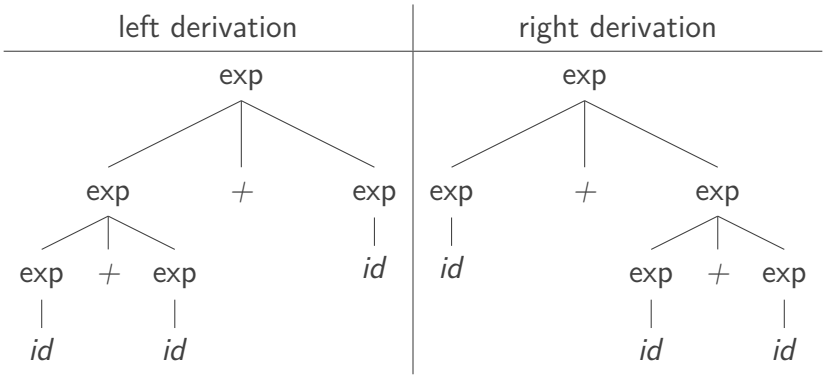

Figure F7: Syntax trees of the example grammar for *id+id+id*.

```
⟨exp⟩      ::= 'id' '+' ⟨exp⟩
             | 'id'
```

Figure F8: Right-most derivation grammar.

```
⟨exp⟩      ::= ⟨exp⟩ '+' 'id'
             | 'id'
```

Figure F9: Leftmost derivation grammar.

In the following step, the grammar is extended by multiplication according to Figure F11 . Again an example input *id+id*id* yields two different syntax trees as visible in Figure F10 . Moreover, they entail different semantics. When evaluating the semantics of an expression like applying the mathematical operations of addition and multiplication, it is not reasonable to re-synthesize the string containing the mathematical expression as that would again call for the necessity of analyzing the structure but rather the syntax tree should directly be worked on progressively. The children of a node would recursively be conflated before advancing to their parent. So in Figure F10 , the left tree would prioritize and execute the addition first and the resulting sum would become a factor in the multiplication, which would amount to a different value than what the mathematical expression *id+id*id* advises. The multiplication must be carried out before the summation directive. This raises the question on how to enforce precedence of operators within a grammar. Operations of higher precedence have to be on a deeper tree level. The solution is to split the grammar into more stages of variables.

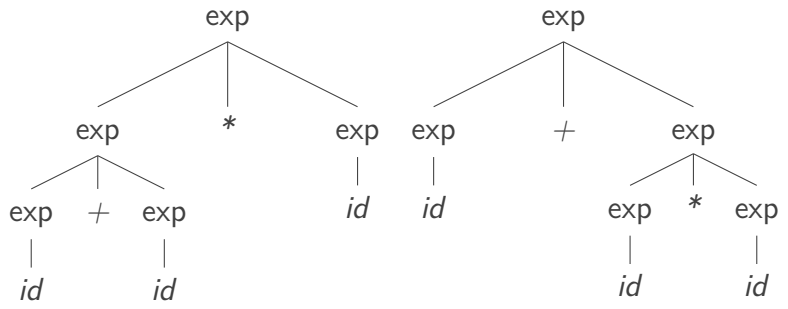

Figure F10: Syntax trees of the multiplication-extended ⟨exp⟩ grammar.

$$
\begin{array}{lll}
\langle exp \rangle & ::= & \langle exp \rangle \text{ `+' } \langle exp \rangle \\
& | & \langle exp \rangle \text{ `*' } \langle exp \rangle \\
& | & \text{`id'}
\end{array}
$$

Figure F11: Grammar of ⟨exp⟩ with multiplication.

Now, in the grammar of Figure F12 , the '+' and the '∗' operators are disconnected, they reside on different levels. Only the ⟨prod⟩ variable is able to contain multiplication and it cannot go back to ⟨exp⟩. The purpose of ⟨exp⟩ is to realize summation but it can derive to occurrences of ⟨prod⟩. So it realizes a one-way street and the sum derivation happens at the upper levels. The intrinsic ambiguity was eliminated as well. The raison d'être of the second production rule of ⟨exp⟩ is for the case that there is no summation involved, it should go straight to ⟨prod⟩ then. The second rule of ⟨prod⟩ acts as a terminator, otherwise the tree would keep on growing and it accounts for the case that maybe there exists no multiplication within the expression.

$$
\begin{array}{lll}
\langle exp \rangle & ::= & \langle exp \rangle \text{ `+' } \langle prod \rangle \\
& | & \langle prod \rangle \\
\langle prod \rangle & ::= & \langle prod \rangle \text{ `*' `id'} \\
& | & \text{`id'}
\end{array}
$$

Figure F12: Grammar with operator precedence.

In summarization, to fix associativity, the recursivity of the rules has to be adjusted (⟨exp⟩ ::= ⟨exp⟩ '+' `id' or ⟨exp⟩ ::= `id' '+' ⟨exp⟩ but no ⟨exp⟩ ::= ⟨exp⟩ '+' ⟨exp⟩). To fix precedence, a hierarchy of non-terminals has to be established. This information will be adduced when designing the language whose words shall be verified and that is up for implementation.

3.1.3 The problem with left recursion

When writing a grammar, it should be ensured that a real parser will have to be able to work with it. In a grammar as depicted in Figure F13 with the starting symbol being ⟨exp⟩, a ***top-down parser*** has to make a decision whether to pick the rule ⟨exp⟩ ::= ⟨exp⟩ '+' `id' or ⟨exp⟩ ::= `id'.

$$\begin{array}{lll} \langle exp \rangle & ::= & \langle exp \rangle \text{ `+' `id'} \\ & | & \text{`id'} \end{array}$$

Figure F13: Grammar with left recursion.

The basis for a specific decision is the input string. When entering the ⟨exp⟩ variable, the type of parser that will be illustrated here would investigate the first part of the first production rule ⟨exp⟩ ::= ⟨exp⟩ '+' 'id', which again is ⟨exp⟩. Without having made any progress, it finds itself in the same situation, the parser will try to derive ⟨exp⟩ and see ⟨exp⟩ ::= ⟨exp⟩ '+' 'id' as the path to pursue. It turns out to be a never-ending loop. This is why left recursion should be avoided in all production rules. To retain the generated language yet still get rid of left recursion, there is a simple conversion prescript demonstrated in Figure F14 . Another non-terminal is inserted that may right-recursively spawn new instances of α (everything that follows the initial non-terminal of the production rule causing the left recursion) or end with ϵ , which is the empty word. ϵ does not take any token from the input. Now, α and β may be substituted by any sequence of variables/terminals. To reform the above example grammar in Figure F12 and match the conversion pattern, α corresponds to '+' ⟨*prod*⟩ and β corresponds to ⟨*prod*⟩. The transformation is illustrated in Figure F15 . On top of that, the pattern can be extended for multiple α and β branches like in Figure F16 .

left recursion

$$\begin{array}{lll} \langle A \rangle & ::= & \langle A \rangle \ \alpha \\ & | & \beta \end{array}$$

right recursion

$$\begin{array}{lll} \langle A \rangle & ::= & \beta \ \langle A' \rangle \\ \langle A' \rangle & ::= & \alpha \ \langle A' \rangle \\ & | & \epsilon \end{array}$$

Figure F14: Elimination of left recursion.

left recursion	right recursion
$\langle exp \rangle$ ::= $\langle exp \rangle$ '+' $\langle prod \rangle$ | β	$\langle exp \rangle$ ::= $\langle prod \rangle$ $\langle exp' \rangle$ $\langle exp' \rangle$ ::= '+' $\langle prod \rangle$ $\langle exp' \rangle$ | ϵ

Figure F15: Grammar of $\langle \text{exp} \rangle$ with right recursion.

left recursion	right recursion
$\langle A \rangle$ ::= $\langle A \rangle$ α_1 | $\langle A \rangle$ α_2 | $\langle A \rangle$ α_3 ... | β_1 | β_2 | β_3 ...	$\langle A \rangle$ ::= β_1 $\langle A' \rangle$ | β_2 $\langle A' \rangle$ | β_3 $\langle A' \rangle$ ... $\langle A' \rangle$ ::= α_1 $\langle A' \rangle$ | α_2 $\langle A' \rangle$ | α_3 $\langle A' \rangle$ ... | ϵ

Figure F16: Elimination of left recursion with multiple instances of α and β.

Lastly, in order to produce a LL(1) grammar, non-determinism must be preempted. That means that the parser must be able to deduce which rule to pick looking only at the next token of the input sequence, never tracing back. Common prefixes in the production rules of the same variable have to be factored out to foster that feature. That process is also called left factoring and is visualized in Figure F17 .

$\langle A \rangle$ ::= α β_1 | α β_2 | ...	$\langle A \rangle$ ::= α $\langle A' \rangle$ $\langle A' \rangle$ ::= β_1 | β_2 | ...

Figure F17: Left factoring.

3.1.4 Construction of an LL(1) parser table

LL(1) stands for processing the input from left to right, right-most derivation and having a lookahead of 1 token, so no back tracing required. Using a parsing table, an LL(1) parser can directly make the rule picking decision by knowing the current non-terminal and the next terminal obtained from the input sequence: $NT \times T \mapsto P$. Before moving on to the actual language going to be used, the process of constructing an LL(1) parser table shall be outlined, which requires the concept of ***First*** and ***Follow***. ***First*** and ***Follow*** both describe sets of terminals. ***First*** can furthermore contain the empty word ϵ and ***Follow*** the terminating symbol \$ (which is just an extra symbol appended to the input sequence in order to mark the ending). Continuing to construct the parser table, each variable is going to be assigned a pair of ***First*** and ***Follow*** sets. Considering the grammar in Figure F18 , Table T1 must be filled in.

Table T1: Empty First-Follow table.

Non-terminal	First	Follow
S		
A		
B		
C		

$$
\begin{array}{lll}
\langle S \rangle & ::= & \langle A \rangle\ \langle C \rangle\ \langle B \rangle \\
 & | & \langle C \rangle\ \text{`b'}\ \langle B \rangle \\
 & | & \langle B \rangle\ \text{`a'} \\
\langle A \rangle & ::= & \text{`d'}\ \text{`a'} \\
 & | & \langle B \rangle\ \langle C \rangle \\
\langle B \rangle & ::= & \text{`g'} \\
 & | & \epsilon \\
\langle C \rangle & ::= & \text{`h'} \\
 & | & \epsilon
\end{array}
$$

Figure F18: Example grammar for the clarification of ***First*** and ***Follow***.

First: ***First*** of a variable $\langle X \rangle$ is obtained by taking a look at each of its production rules Q_i, processing its sequence of symbols P_i, collecting ***First*** of P_i. To get ***First***

of P_i, look at its first symbol. If it is a terminal, add it to the set and leave P_i. If it is a variable ⟨Sub⟩, get ***First*** of ⟨Sub⟩. The next step depends on if ***First*** of ⟨Sub⟩ contains the empty word ϵ, for then ⟨Sub⟩ might be erased in P_i while parsing. If ϵ is not included or if the variable being investigated is the last symbol of P_i, add all of ***First*** of ⟨Sub⟩ to the set and leave P_i. If ϵ was contained and ⟨Sub⟩ was not the last symbol of P_i, everything except ϵ is added and P_i advances to the next symbol.

Follow: ***Follow*** of a variable ⟨X⟩ is obtained by taking a look at each of its occurrences in every production rule Q_i of the grammar, processing its remaining symbols after the occurrence of ⟨X⟩ P_i, collecting ***Follow*** of P_i. Additionally, start variables automatically get the terminator symbol \$ bestowed. If P_i contains symbols, get ***First*** of P_i. If ***First*** of P_i contains the empty word ϵ, add everything of ***First*** of P_i to the set except for ϵ and also get ***Follow*** of the variable in which Q_i resides. If ϵ is not included, simply add everything of ***First*** of P_i. If P_i was empty to begin with, add ***Follow*** of the variable its original production rule Q_i resides in. Footnote: The ***Follow*** set never contains ϵ.

Since production rules may reference themselves or create a cyclic dependency, both algorithms should mark which non-terminals were already visited. Using these algorithms for ***First*** and ***Follow***, the table can be filled in like done in Table T2 (***Java*** listings are provided in Chapter 5: *Implementation*). Transcribing the ***First-Follow*** table, the promised predictive LL(1) parser table is about to erect. Therefore, each of the variables qualifies a row once again and the columns are made up of all terminals of the grammar, including the termination symbol \$.

Table T2: Filled First-Follow table.

Non-terminal	First	Follow
S	$\{a, b, d, g, h, e\}$	$\{\$\}$
A	$\{d, g, h, e\}$	$\{g, h, \$\}$
B	$\{g, e\}$	$\{a, g, h, \$\}$
C	$\{h, e\}$	$\{b, g, h, \$\}$

The procedure appears straightforward: For every variable ⟨X⟩ and every rule P, check the first symbol of P. If that symbol is a terminal, put P in the cell denoted by ⟨X⟩ and the actual terminal ($X \times t \mapsto$⟨X⟩ ::= t). If it is a non-terminal ⟨Y⟩, put P in every cell denoted by ⟨X⟩ and any of the terminals in the ***First*** set of ⟨Y⟩ ($\forall y \in First(Y)$: $X \times y \mapsto$⟨X⟩ ::= Y). If (as a last option) it should be the empty word ϵ, the rule will be to derive ⟨X⟩ to ϵ for all of the terminals of the ***Follow*** set of ⟨X⟩ ($\forall x \in Follow(X)$: $X \times x \mapsto$⟨X⟩ ::= ϵ).

Table T3: Predictive parser table.

NT \ T	a	b	d	g	h	$
S						
A			‘d’ ‘a’	⟨B⟩ ⟨C⟩		
B	ϵ			ϵ	ϵ	ϵ
C		ϵ		ϵ	ϵ	ϵ

If any of the cells should be object to multiple entries using the method just described, the grammar has not been LL(1) as seeing only the next token is not enough to make a decision in that case. All cells that remain empty are instances of failure. If the parser comes across such a combination, it has to throw an exception and the input must not be accepted. It should be noted that the above described algorithm for developing a grammar does not ensure LL(1) behavior. Left factorization lifts the ambiguity evoked by a common prefix in multiple production rules of the same variable but is purely syntactic. Variables, whose decomposition may yield the same prefix of terminals, are not of further interest, e.g. the rules ⟨A⟩ ::= ‘a’ ‘b’ and ⟨A⟩ ::= ⟨A’⟩ ‘b’ cannot be unified/left factored even if ‘a’ $\subseteq First(\langle$A’$\rangle)$. Additionally, there may be overlapping with the ***Follow*** sets. For a grammar to be LL(1), the ***First*** sets of all production rules per variable must be disjoint and the intersection of the ***First*** and ***Follow*** sets of a variable must be empty in case the variables has an ϵ production rule [Coc02]. One type of parser that can handle LL(1) grammars is those that descend recursively. It is presented in Chapter 5: *Implementation* .

3.2 Core language

3.2.1 Commands

After having previewed the example, the core language shall be designed now. The ***Hoare*** calculus provides rules for the typical elementary imperative flow control elements and statements: assignment of variables, branch selection, head-controlled loops and, of course, sequential composition. It matches that of ***while*** programs [Wik17g]. Some more commonly known structures can be extrapolated. Foot-controlled loops are semantically equivalent to head-controlled loops with the loop body duplicated once in front of the loop as shown in Listing L3 for example.

```
do {
  BODY;
} while (CONDITION)

//same as
BODY;
while (CONDITION) {
  BODY;
}
```

Listing L3: Conversion of foot-loop to while-loop (Java).

Count-controlled loops can be converted to head-controlled loops as well:

```
for (INIT; CONDITION; INCREMENT) {
  BODY;
}

//same as
INIT;
while (CONDITION) {
  BODY;
  INCREMENT;
}
```

Listing L4: Conversion of count-controlled loop to while-loop (Java).

The ternary conditional assignment can be expanded to a selection:

```
x = pred ? y : z;

//same as
if (pred) x = y; else x = z;
```

Listing L5: Conversion of conditional assignment to selection (Java).

Although converting old-school ***goto jump***s to loops may not be trivial and without the use of additional support variables, it is possible to do so. This just to state that the concepts presented here are transferable to more elaborated structures as they exist in real programming languages.

```
⟨skip⟩    ::= 'SKIP'
⟨assign⟩  ::= ⟨id⟩ ':=' ⟨exp⟩
⟨alt⟩     ::= 'IF' ⟨bool_exp⟩ 'THEN' ⟨prog⟩ 'ELSE' ⟨prog⟩ 'FI'
⟨loop⟩    ::= 'WHILE' ⟨bool_exp⟩ 'DO' ⟨prog⟩ 'OD'
```

Figure F19: Commands grammar.

The commands for variable assignment, if selection (alternative) and while loop are depicted in Figure F19 . The variable assignment ⟨assign⟩ assigns ⟨exp⟩ to ⟨var⟩ (no variable subscript/arrays here). The if selection ⟨alt⟩ checks the truth value of ⟨bool_exp⟩. Its evaluation being $true$ will trigger the ⟨prog⟩ of the ***THEN***-branch, otherwise it will execute the ⟨prog⟩ of the ***ELSE***-branch. The ⟨loop⟩ command checks the truth value of ⟨bool_exp⟩. Should it evaluate to $false$, the execution point will jump right after the loop. In case it is $true$, the inner ⟨prog⟩ will be called and afterwards the whole loop mechanism be repeated. Additionally, there is ⟨skip⟩, which does nothing of importance but can be placed to suffice the syntax (like maybe if the ***ELSE***-branch of the selection is superfluous). After having defined the elementary commands, they can be tied together via ⟨prog⟩ as shown in Figure F20 , which is also the starting symbol, and put in a sequential composition using the ';' separator. The first rule of ⟨prog⟩ displays left recursion which must be get rid of. This is easily resolved in Figure F21 . The addition of ⟨alt_else⟩ and refactoring of ⟨alt⟩ renders the else branch of selections optional for convenience.

```
⟨prog⟩    ::= ⟨prog⟩ ';' ⟨prog⟩
            | ⟨skip⟩
            | ⟨assign⟩
            | ⟨alt⟩
            | ⟨loop⟩
```

Figure F20: Shortened grammar of ⟨prog⟩ (raw).

⟨*prog*⟩ ::= ⟨*cmd*⟩ ⟨*prog'*⟩

⟨*prog'*⟩ ::= ';' ⟨*cmd*⟩ ⟨*prog'*⟩
| ϵ

⟨*cmd*⟩ ::= ⟨*skip*⟩
| ⟨*assign*⟩
| ⟨*alt*⟩
| ⟨*while*⟩

⟨*skip*⟩ ::= 'SKIP'

⟨*assign*⟩ ::= ⟨*id*⟩ ':=' ⟨*exp*⟩

⟨*alt*⟩ ::= 'IF' ⟨*bool_exp*⟩ 'THEN' ⟨*prog*⟩ ⟨*alt_else*⟩ 'FI'

⟨*alt_else*⟩ ::= 'ELSE' ⟨*prog*⟩
| ϵ

⟨*while*⟩ ::= 'WHILE' ⟨*bool_exp*⟩ 'DO' ⟨*prog*⟩ 'OD'

Figure F21: Shortened grammar of ⟨prog⟩ (left recursion eliminated).

3.2.2 Numeric expressions

The ⟨exp⟩ and ⟨bool_exp⟩ non terminals remain open for definition. ⟨exp⟩ describes an expression. In normal programming languages, this could be of any data type. Here, it is restrained to numeric expressions. Floating-point operations in numerical systems are commonly imprecise respectively on the bit level [Wik17d], which would make a semantic observation more difficult. Some techniques to cope with fractions will be covered later.

The indication of the initial grammar in Figure F22 is as it appears most intuitive. For example, a numeric expression might be a multiplication of two other ⟨exp⟩ or using any binary arithmetic operation for that matter. '+' stands for addition, '−' for subtraction, '∗' for multiplication, '/' for division, '^' for potentization and '!' for the factorial operation (which is unary). The terminal ⟨id⟩ matches a variable name (*[a-zA-Z][a-zA-Z0-9]**), 'num' is any integer literal (*[1-9][0-9]** | *0*). The grammar rules for ⟨exp⟩ contain left recursion and the precedence must be fixated to influence the setup of the syntax tree as described in Section 3.1: *On languages and grammars* .

```
⟨exp⟩      ::= ⟨exp⟩ '+' ⟨exp⟩
             | ⟨exp⟩ '−' ⟨exp⟩
             | ⟨exp⟩ '*' ⟨exp⟩
             | ⟨exp⟩ '/' ⟨exp⟩
             | ⟨exp⟩ '^' ⟨exp⟩
             | ⟨exp⟩ '!'
             | ⟨id⟩
             | ⟨exp_lit⟩

⟨id⟩       ::= [a-zA-Z][a-zA-Z0-9]*

⟨exp_lit⟩  ::= [1-9][0-9]*
             | '0'
```

Figure F22: Core grammar of ⟨exp⟩ (raw).

First off, a total order of the operators must be established. It seems obvious to do so abiding by the mathematical notation rules:

$$\text{`}+\text{'} \doteq \text{`}-\text{'} \lessdot \text{`}*\text{'} \doteq \text{`}/\text{'} \lessdot \text{`}\hat{}\text{'} \lessdot \text{`}!\text{'} \tag{3.1}$$

Table T4: Operator table of ⟨exp⟩.

	+	-	*	/	^	!
+	⋗	⋗	⋖	⋖	⋖	⋖
-	⋗	⋗	⋖	⋖	⋖	⋖
*	⋗	⋗	⋗	⋗	⋖	⋖
/	⋗	⋗	⋗	⋗	⋖	⋖
^	⋗	⋗	⋗	⋗	⋖	⋖
!	⋗	⋗	⋗	⋗	⋗	⋗

So addition and subtraction come with the lowest precedence, followed by multiplication and division, then follows exponentiation and finally the factorial operator stands at the top. The hierarchy is displayed in Table T4 , too. Moreover, this table denotes the associativity of the binary operators: addition through division are left-associative but exponentiation is not. The expression *2^2^3* shall denote $2^{2^3} = 2^8 = 256$ as opposed to $(2^2)^3 = 4^3 = 64$. While semantics-wise, associativity does not matter for addition and multiplication, it is fixed to left bias on default to reduce ambiguity. Using the methods

proposed in Section 3.1: *On languages and grammars* , the grammar fragment for ⟨exp⟩ can be arranged. The first version in Figure F23 shows the precedence levels. Associativity is applied in Figure F24 . In Figure F25 left recursion is abolished and finally the grammar has been exposed to left factoring in Figure F26 . The last version encloses the auxiliary rule ⟨exp_elem⟩ ::= '(' ⟨exp⟩ ')', whose parentheses' encapsulation permits the prioritization of any operation over others.

⟨*exp*⟩ ::= ⟨*sum*⟩

⟨*sum*⟩ ::= ⟨*sum*⟩ '+' ⟨*sum*⟩
| ⟨*sum*⟩ '−' ⟨*sum*⟩
| ⟨*prod*⟩

⟨*prod*⟩ ::= ⟨*prod*⟩ '∗' ⟨*prod*⟩
| ⟨*prod*⟩ '/' ⟨*prod*⟩
| ⟨*pow*⟩

⟨*pow*⟩ ::= ⟨*pow*⟩ '^' ⟨*pow*⟩
| ⟨*fact*⟩

⟨*fact*⟩ ::= ⟨*exp_elem*⟩ '!'
| ⟨*exp_elem*⟩

⟨*exp_elem*⟩ ::= ⟨*id*⟩
| ⟨*exp_lit*⟩

⟨*id*⟩ ::= [a-zA-Z][a-zA-Z0-9]*

⟨*exp_lit*⟩ ::= [1-9][0-9]*
| '0'

Figure F23: Grammar of ⟨exp⟩ (with fixed precedence).

⟨*exp*⟩ ::= ⟨*sum*⟩

⟨*sum*⟩ ::= ⟨*sum*⟩ '+' ⟨*prod*⟩
| ⟨*sum*⟩ '−' ⟨*prod*⟩
| ⟨*prod*⟩

⟨*prod*⟩ ::= ⟨*prod*⟩ '∗' ⟨*pow*⟩
| ⟨*prod*⟩ '/' ⟨*pow*⟩
| ⟨*pow*⟩

⟨*pow*⟩ ::= ⟨*fact*⟩ '^' ⟨*pow*⟩
| ⟨*fact*⟩

⟨*fact*⟩ ::= ⟨*exp_elem*⟩ '!'
| ⟨*exp_elem*⟩

⟨*exp_elem*⟩ ::= ⟨*id*⟩
| ⟨*exp_lit*⟩

⟨*id*⟩ ::= [a-zA-Z][a-zA-Z0-9]*

⟨*exp_lit*⟩ ::= [1-9][0-9]*
| '0'

Figure F24: Core grammar of ⟨exp⟩ (with fixed associativity).

```
⟨exp⟩      ::= ⟨sum⟩

⟨sum⟩      ::= '+' ⟨prod⟩ ⟨sum'⟩
             | '-' ⟨prod⟩ ⟨sum'⟩
             | ϵ

⟨prod⟩     ::= ⟨pow⟩ ⟨prod'⟩

⟨prod'⟩    ::= '*' ⟨pow⟩ ⟨prod'⟩
             | '/' ⟨pow⟩ ⟨prod'⟩
             | ϵ

⟨pow⟩      ::= ⟨fact⟩ '^' ⟨pow⟩
             | ⟨fact⟩

⟨fact⟩     ::= ⟨exp_elem⟩ '!'
             | ⟨exp_elem⟩

⟨exp_elem⟩ ::= ⟨id⟩
             | ⟨exp_lit⟩

⟨id⟩       ::= [a-zA-Z][a-zA-Z0-9]*

⟨exp_lit⟩  ::= [1-9][0-9]*
             | '0'
```

Figure F25: Core grammar of ⟨exp⟩ (right recursive).

$$
\begin{array}{lll}
\langle exp \rangle & ::= & \langle sum \rangle \\
\langle sum \rangle & ::= & \langle prod \rangle\ \langle sum' \rangle \\
\langle sum' \rangle & ::= & \text{`+'}\ \langle prod \rangle\ \langle sum' \rangle \\
 & | & \text{`-'}\ \langle prod \rangle\ \langle sum' \rangle \\
 & | & \epsilon \\
\langle prod \rangle & ::= & \langle pow \rangle\ \langle prod' \rangle \\
\langle prod' \rangle & ::= & \text{`*'}\ \langle pow \rangle\ \langle prod' \rangle \\
 & | & \text{`/'}\ \langle pow \rangle\ \langle prod' \rangle \\
 & | & \epsilon \\
\langle pow \rangle & ::= & \langle fact \rangle\ \langle pow' \rangle \\
\langle pow' \rangle & ::= & \text{`\^{}'}\ \langle pow \rangle \\
 & | & \epsilon \\
\langle fact \rangle & ::= & \langle exp\_elem \rangle\ \langle fact' \rangle \\
\langle fact' \rangle & ::= & \text{`!'} \\
 & | & \epsilon \\
\langle exp\_elem \rangle & ::= & \langle id \rangle \\
 & | & \langle exp\_lit \rangle \\
 & | & \text{`('}\ \langle exp \rangle\ \text{`)'} \\
\langle id \rangle & ::= & \text{[a-zA-Z][a-zA-Z0-9]*} \\
\langle exp\_lit \rangle & ::= & \text{[1-9][0-9]*} \\
 & | & \text{`0'}
\end{array}
$$

Figure F26: Grammar of ⟨exp⟩ (final).

3.2.3 Boolean expressions

The same procedure must be applied to boolean expressions. A ⟨bool_exp⟩ yields a boolean value. Here, it may either be a conjunction (‘&’), a disjunction (‘|’), a negation (‘~’) or an elementary entity: The comparison of two ⟨exp⟩s via the comparison operators less (‘<’), greater (‘>’), less or equal(‘<=’), greater or equal(‘>=’), equal (‘=’) or unequal (‘<>’) or the boolean literals ‘`true`’ or ‘`false`’.

$$\text{`|'} \lessdot \text{`\&'} \lessdot \text{` $\sim$ '} \lessdot \text{` < '} \doteq \text{` > '} \doteq \text{` <= '} \doteq \text{` >= '} \doteq \text{` = '} \doteq \text{` <> '} \tag{3.2}$$

Table T5: Operator table of ⟨bool_exp⟩

	|	&	~	<	>	<=	>=	=	<>
|	⋗	⋖	⋖	⋗	⋗	⋗	⋗	⋗	⋗
&	⋗	⋗	⋖	⋗	⋗	⋗	⋗	⋗	⋗
~	⋗	⋗	⋗	⋗	⋗	⋗	⋗	⋗	⋗
<	⋖	⋖	⋖	≐	≐	≐	≐	≐	≐
>	⋖	⋖	⋖	≐	≐	≐	≐	≐	≐
<=	⋖	⋖	⋖	≐	≐	≐	≐	≐	≐
>=	⋖	⋖	⋖	≐	≐	≐	≐	≐	≐
=	⋖	⋖	⋖	≐	≐	≐	≐	≐	≐
<>	⋖	⋖	⋖	≐	≐	≐	≐	≐	≐

⟨*bool_exp*⟩ ::= ⟨*bool_exp*⟩ '&' ⟨*bool_exp*⟩
| ⟨*bool_exp*⟩ '|' ⟨*bool_exp*⟩
| '~' ⟨*bool_exp*⟩
| ⟨*exp*⟩ '<' ⟨*exp*⟩
| ⟨*exp*⟩ '>' ⟨*exp*⟩
| ⟨*exp*⟩ '<=' ⟨*exp*⟩
| ⟨*exp*⟩ '>=' ⟨*exp*⟩
| ⟨*exp*⟩ '=' ⟨*exp*⟩
| ⟨*exp*⟩ '<>' ⟨*exp*⟩
| '`true`'
| '`false`'

Figure F27: Core grammar of ⟨bool_exp⟩ (raw).

Complying with the steps in accordance to the previous section, one arrives at Figure F28 . An analogous parentheses mechanism (⟨bool_ elem⟩ ::= '[' ⟨bool_ exp⟩ ']') is inserted but it uses brackets instead of parentheses. The reason is that ⟨bool_elem⟩ possesses rules starting with ⟨exp⟩. ⟨exp⟩ can already start with '(', using '(' again would break the LL(1) trait (***First*** sets of ⟨exp⟩ and ⟨bool_exp⟩ would not be disjunct) and are therefore not desirable. The reasoning parts of this document will still prefer parentheses over brackets in boolean expressions.

⟨*bool_exp*⟩ ::= ⟨*bool_or*⟩

⟨*bool_or*⟩ ::= ⟨*bool_and*⟩ ⟨*bool_or'*⟩

⟨*bool_or'*⟩ ::= '|' ⟨*bool_and*⟩ ⟨*bool_or'*⟩
| ϵ

⟨*bool_and*⟩ ::= ⟨*bool_neg*⟩ ⟨*bool_and'*⟩

⟨*bool_and'*⟩ ::= '&' ⟨*bool_neg*⟩ ⟨*bool_and'*⟩
| ϵ

⟨*bool_neg*⟩ ::= ⟨*bool_elem*⟩
| ' ' ⟨*bool_elem*⟩

⟨*bool_elem*⟩ ::= ⟨*exp*⟩ '<' ⟨*exp*⟩
| ⟨*exp*⟩ '<' ⟨*exp*⟩
| ⟨*exp*⟩ '>' ⟨*exp*⟩
| ⟨*exp*⟩ '<=' ⟨*exp*⟩
| ⟨*exp*⟩ '>=' ⟨*exp*⟩
| ⟨*exp*⟩ '=' ⟨*exp*⟩
| ⟨*exp*⟩ '<>' ⟨*exp*⟩
| '`true`'
| '`false`'
| '[' ⟨*bool_exp*⟩ ']'

Figure F28: Grammar of ⟨bool_exp⟩ (final).

This concludes the language definition subject to the forthcoming verifying methods. It will be extended by the proof specification decorations later on. The whole language (plus the later added assertion decorations) can be viewed in Appendix E: *Grammar for Hoare-decorated while programs* . Line breaks and white space is tolerated for readability and used as delimiters of keywords because e.g. *IFabc* should be regarded as an identifier $IFabc$ rather than the keyword $\mathbf{IF}$ plus the identifier a.

Note: The boolean operators '&', '|' and '~' are interchangeably used with the $\wedge/\vee/\neg$ symbols in the later chapters.

3.3 Semantic tree

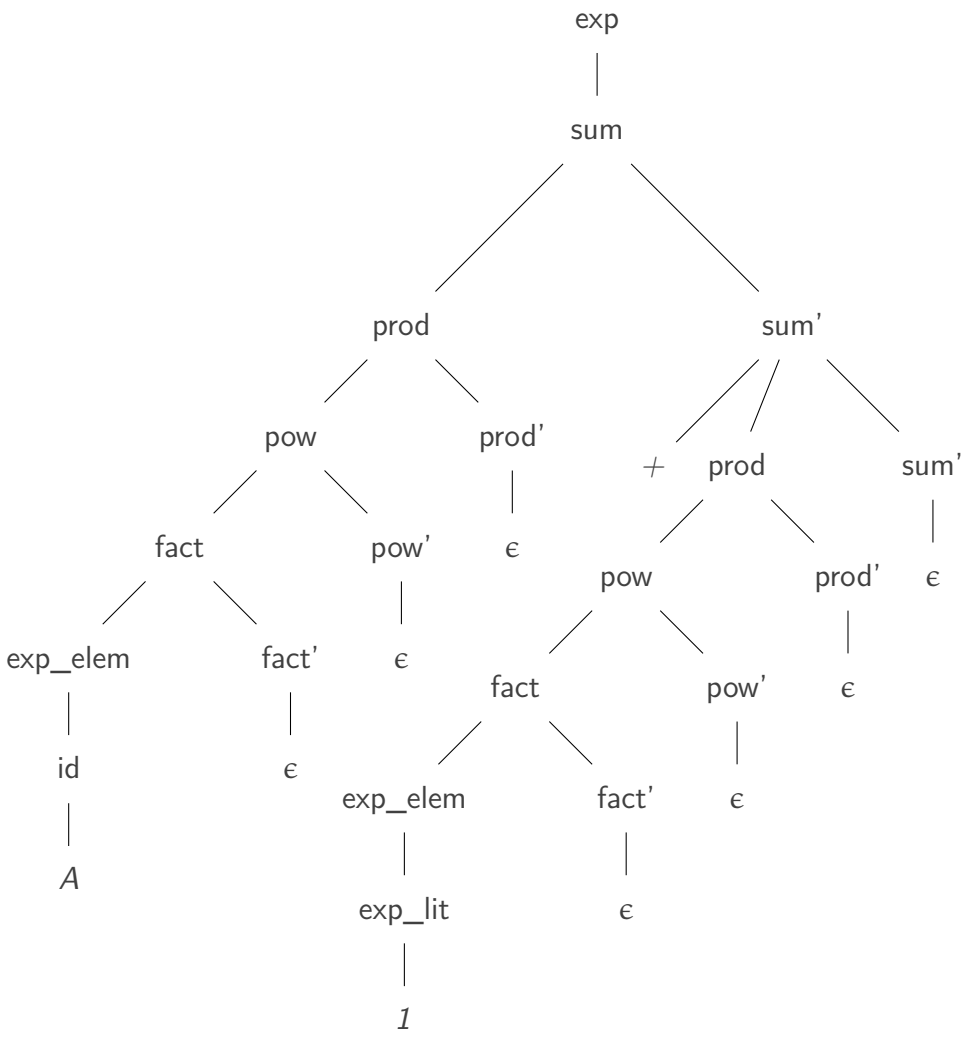

Figure F29: Extensive syntax tree of *A+1*.

The syntax tree constructed so far was meant to match the workings of an LL(1) parser. It creates a lot of unnecessary levels and the right recursion spawns extended cascades and ϵ-branches. Ex: The syntax tree of a simple expression *A+1* produces the syntax tree in Figure F29 . As can easily be observed, this representation is immensely oversized, contains redundancy and traversing it would be convoluted. Each additional summand appends another operator and another $\langle$prod$\rangle$-sub tree. It turns out to be impractical for further processing, which is why it should be converted into a more semantically meaningful tree. The deflated result of such is shown in Figure F30 . The expression is reduced to just a sum of an id and a numeric value, as one would intuitively identify it. The operator is also removed because it can be implied by the fact that the treated node is a sum (a minus sign could be realized by inserting another intermediate ***negation*** node, not defined yet). More on the technical aspects

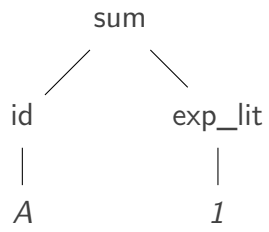

Figure F30: Semantic tree of *A+1*.

of typification of nodes and the transition from one tree to another are to be unveiled in the ***Implementation*** chapter. The considerations up to this point are to showcase the elements of the language to be verified and to give credit to the required preparatory steps. The author will henceforth be using the term ***semantic tree*** to refer to the new type when trying to emphasize a distinction between it and the original ***syntax tree***. The usual term found in literature is ***abstract syntax tree*** while ***semantic tree*** is reserved for a quite similar entity in logic [RK83]. The author reckons the meaning can be generalized to encompass the described topic and is fitting.

Chapter 4
4 How to prove

4.1 Of operational semantics

Speaking about verification of programs, it is of utmost importance to know what a program does exactly, namely its semantics. These are inductively defined and should be formally specified. The model checking part in the introduction mentioned that the current point of execution (the instruction position) and the values of the involved variables identify a snapshot of the program in its entirety. Theoretically, in a deterministic environment where the next instruction to handle is fixed, the behavior can be foretold as the machine would compute. Now, the idea is to formalize the semantics defined in the previous chapter in order to make statements about the execution of a given program, about computations. This is similar to actually running the program, traversing the entered lines/statements of code in succession and keeping memory of the current variable values. The mapping of all variables used inside the program as well as additional helper variables to specific values is called a state. As according to the introduced language, only the assignment instruction possesses the ability to alter the state.

Definition 5. *Be S a program. $var(S)$ denotes the set of all variables occurring in S.*

Ex: In Listing L6 $var(S_{var}) = \{x, y, z, q\}$

```
1 x := x + 1;
2 y := z;
3 IF z = q THEN
4   y := y + 1
5 FI
```

Listing L6: S_{var} example

Definition 6. *Be S a program. $change(S)$ denotes the set of all variables modified in S (each one that has at least one assignment, irrespective to the instruction actually being executed).*

Ex: In Listing L6 $change(S_{var}) = \{x, y\}$

Definition 7. *A state is a function, mapping a value to every variable in $var(S)$ as well as to auxiliary (on-the-fly created, originally not situated in the program) variables.*

Definition 8. *Be S a program and σ a state. The pair $< S, \sigma >$ is called a configuration.*

A program can shift between configurations through computations. E denotes the end of the program.

Ex: $< x := 1, \sigma(x) = 0 > \rightarrow < E, \sigma(x) = 1 >$, prior, the value of variable x was 0 but the assignment changed it to 1. Only the assignment was in the remaining execution buffer, what follows is the termination of the program.

The following axioms and rules of the ***transition system*** matching the introduced language were transcribed from page 59 of [APdBO10]:

$$< \mathbf{SKIP}, \sigma > \rightarrow < E, \sigma > \tag{4.1}$$

$$< u := t, \sigma > \rightarrow < E, \sigma[u := \sigma(t)] > \tag{4.2}$$

$$\frac{< S_1, \sigma > \rightarrow < S_2, \tau >}{< S_1; S, \sigma > \rightarrow < S_2; S, \tau >} \tag{4.3}$$

$$< \mathbf{IF}\ B\ \mathbf{THEN}\ S_1\ \mathbf{ELSE}\ S_2\ \mathbf{FI}, \sigma > \rightarrow < S_1, \sigma > \quad where\ \sigma \models B \tag{4.4}$$

$$< \mathbf{IF}\ B\ \mathbf{THEN}\ S_1\ \mathbf{ELSE}\ S_2\ \mathbf{FI}, \sigma > \rightarrow < S_2, \sigma > \quad where\ \sigma \models \neg B \tag{4.5}$$

$$< \mathbf{WHILE}\ B\ \mathbf{DO}\ S\ \mathbf{OD}, \sigma > \rightarrow < S; \mathbf{WHILE}\ B\ \mathbf{DO}\ S\ \mathbf{OD}, \sigma > \quad where\ \sigma \models B \tag{4.6}$$

$$< \mathbf{WHILE}\ B\ \mathbf{DO}\ S\ \mathbf{OD}, \sigma > \rightarrow < E, \sigma > \ \ where\ \sigma \models \neg B \tag{4.7}$$

(4.1) states that $\mathbf{SKIP}$ does not cause a state change and just transitions to ***E***. In (4.2), the state is altered by replacing the value of the variable u by t. (4.3) is the

propagation characteristic of the sequential composition: the first part is evaluated and continued by the second part. (4.4) and (4.5) handle alternatives and (4.6) together with (4.7) loops. It can be noticed that the assignment is the only statement to evoke a state change and that only the loop in (4.6) has the powerful as hazardous quality to have the impending "remaining" program to be processed larger than that of the source configuration. Thus it is the only one with potential for divergence: to make the program never end. With that comes a differentiation between ***partial*** and ***total correctness***. Latter avouches for the proper termination of a program in finite time in addition to other tested for properties while partial correctness is only about "under the assumption that it ends". The ***Halting Problem*** gives testimony that showing termination and/or establishing termination is no trivial request and that is why it is often separately analyzed. As hinted in the introduction, correctness is a somewhat vague term. For all it may concern, a program could be declared correct for halting, containing specific statements, fulfilling liveliness parameters (the program keeps visiting "good" configurations) or safety conditions (it never comes across "bad" configurations) for instance. At that, arguing about correctness in detail, one has to commit oneself.

4.2 Transition to Hoare calculus

The now presented ***Hoare*** calculus defines relations of input/output behavior. That is, if a program starts in a state satisfying a precondition p and executes a program S, it is guaranteed to have taken on a state fulfilling a postcondition q afterwards.

$$\{p\}\ S\ \{q\} \tag{4.8}$$

The notation is as shown in (4.8) and named ***Hoare triple***. The conditions, also called assertions, are put between curly braces although ***C.A.R. Hoare*** originally did it the other way around ($p\ \{S\}\ q$). The difference between assertion and state is that an assertion is a predicate for allowed states, it designates a set of states. Using assertions, the programs of the developed language can be decorated to express a supposed to prevail behavior:

```
1 PRE {x<y}
2   x:=x+y
3 POST {x<2*y}
```

Listing L7: Decoration example.

In that sense, of course, this is an arbitrary proposition that has to be verified. Do all states where x is smaller than y initially lead to a state where x is smaller than

$2 * y$ after having added y to x? It may be comprehensible in this case but less so for more complex problems. Fortunately, there is the ***Hoare*** calculus to help systematizing them.

HOARE CALCULUS (PW):

SKIP AXIOM:

$$\{p\}\ \mathbf{SKIP}\ \{p\} \tag{4.9}$$

ASSIGNMENT AXIOM:

$$\{p[u := t]\}\ u := t\ \{p\} \tag{4.10}$$

COMPOSITION RULE:

$$\frac{\{p\}\ S_1\ \{r\}, \{r\}\ S_2\ \{q\}}{\{p\}\ S_1; S_2\ \{q\}} \tag{4.11}$$

CONDITIONAL RULE:

$$\frac{\{p \wedge B\}\ S_1\ \{q\}, \{p \wedge \neg B\}\ S_2\ \{q\}}{\{p\}\ \mathbf{IF}\ B\ \mathbf{THEN}\ S_1\ \mathbf{ELSE}\ S_2\ \mathbf{FI}\ \{q\}} \tag{4.12}$$

LOOP RULE:

$$\frac{\{p \wedge B\}\ S\ \{p\}}{\{p\}\ \mathbf{WHILE}\ B\ \mathbf{DO}\ S\ \mathbf{OD}\ \{p \wedge \neg B\}} \tag{4.13}$$

CONSEQUENCE RULE:

$$\frac{p \to p_1, \{p_1\}\ S\ \{q_1\}, q_1 \to q}{\{p\}\ S\ \{q\}} \tag{4.14}$$

as listed in [APdBO10] p. 65f.

More precisely, there are two versions. The above one is for partial correctness only. The case of divergence, a program never halting, is not covered here. The proof system consisting of axioms and rules establishes a relationship between pre- and postconditions of a set of basic programming constructs. These are the groundwork for further verification ventures. The horizontal bar is a fancier notation for an implication:

If all of the conditions above the bar hold true, the statements below it are assured to be correct as well.

Again, the $SKIP$ axiom in (4.9) confirms that **SKIP** is unable to do anything to the state. The $ASSIGNMENT$ axiom says that the precondition matches the postcondition only that all occurrences of the variable are replaced by the new value within the precondition. This is a bit problematic since substitution is not a reversible (bijective) procedure, ergo a left to right evaluation becomes difficult. The composition displays its transitive properties once more in (4.11). To obtain the postcondition of a composition, the postcondition of its first part is fed as precondition to the second part or vice versa. The $CONDITIONAL$ rule (4.12) merges the triples of the individual branches with the respectively associated condition for entering that branch. Perhaps most intriguing is the rule responsible for loops in (4.13). The precondition becomes a conjunction with the negation of the loop condition but that is only the case (this transformation is only allowed to be conducted) if the conjunction of the precondition and the loop condition applied to the loop body ends in the precondition. p is called a loop invariant in that regard because it does not change within any of the iterations of the loop. Lastly, the binding material to plug the holes like enhancing the versatility of the $LOOP$ rule is found in the $CONSEQUENCE$ rule (4.14). A precondition can be strengthened by finding another one that implies the former precondition. On the other hand, a postcondition can always be relaxed by a weaker assertion. Essentially, the strongest predicate would be $\{false\}$, enveloping no state. A program annotated with $\{false\}$ at the end should never be found correct unless it diverges. The weakest assertion is $\{true\}$, encompassing all states, which is like the Cartesian product of all possible variable values. Both strengthening and weakening must be exerted with care, for overdoing it would elicit type I "false positive" errors. A program could be mistakenly identified as incorrect because e.g. the postcondition was unnecessarily rendered too weak and does no longer imply the final statement. ***S. Kleuker*** [Kle09] p. 228 additionally states:

$$\frac{\{p\}\ S_1\ \{q_1\}, \{p\}\ S_2\ \{q_2\}}{\{p\}\ \mathbf{IF}\ B\ \mathbf{THEN}\ S_1\ \mathbf{ELSE}\ S_2\ \mathbf{FI}\ \{q_1 \vee q_2\}} \tag{4.15}$$

and

$$\frac{\{p\}\ S_1\ \{q_1\}, \{p\}\ S_2\ \{q_2\}, var(B) \notin (change(S_1) \cup change(S_2))}{\{p\}\ \mathbf{IF}\ B\ \mathbf{THEN}\ S_1\ \mathbf{ELSE}\ S_2\ \mathbf{FI}\ \{(B \rightarrow q_1) \wedge (\neg B \rightarrow q_2)\}} \tag{4.16}$$

The ***Hoare*** calculus by itself does not specify an algorithm yet. There is some flexibility in there. The analysis of a program may commence from the beginning onwards or push up from the ending, or even a combination thereof. However, there are a couple of reasons why the second option seems preferable. The assignment axiom does contain an explicit instruction to receive the precondition from the postcondition whereas going from left to right in a variable assignment requires more thinking and case distinction. Assuming that the precondition p does not include the modified variable x. It would be intuitive that the strongest derived postcondition just adds the clause of x possessing the newly assigned value:

$$\{p\}\ x := 2\ \{p \wedge x = 2\} \tag{4.17}$$

If p does not contain x and the assigned value is a function of x, as there is no presumption about x, p will stay the same:

$$\{p\}\ x = x + 2\ \{p\} \tag{4.18}$$

or one could insert some auxiliary anchor variable:

$$\{p \wedge X = x\}\ x = x + 2\ \{p \wedge X + 2 = x\} \tag{4.19}$$

If p does contain x, the clauses in p that contain x would have to be discarded as those terms could not be found true or relevant anymore:

$$\{p \Rightarrow y = 1 \wedge x = 4\}\ x := 2\ \{q \Rightarrow y = 1 \wedge x = 2\} \tag{4.20}$$

or a stronger postcondition r may be found with $q \rightarrow r \wedge r \rightarrow p$ (find an intermediate condition). This is fractured and seldom suggested. More sustainable seems to be the ***wlp*** (weakest liberal precondition) algorithm by ***E. W. Dijkstra***:

$$wlp(\mathbf{SKIP}, q) \leftrightarrow q \tag{4.21}$$

$$wlp(u := t, q) \leftrightarrow q[u := t] \tag{4.22}$$

$$wlp(S_1; S_2, q) \leftrightarrow wlp(S_1, wlp(S_2, q)) \tag{4.23}$$

$$\begin{gathered} wlp(\textbf{IF } B \textbf{ THEN } S_1 \textbf{ ELSE } S_2 \textbf{ FI}, q) \\ \leftrightarrow \\ (B \wedge wlp(S_1, q)) \vee (\neg B \wedge wlp(S_2, q)) \end{gathered} \tag{4.24}$$

$$\begin{gathered} wlp(\textbf{WHILE } B \textbf{ DO } S_1 \textbf{ OD}, q) \wedge B \\ \rightarrow \\ wlp(S_1, wlp(\textbf{WHILE } B \textbf{ DO } S_1 \textbf{ OD}, q)) \end{gathered} \tag{4.25}$$

$$wlp(\textbf{WHILE } B \textbf{ DO } S_1 \textbf{ OD}, q) \wedge \neg B \rightarrow q \tag{4.26}$$

$$\models \{p\}\ S\ \{q\} \iff p \rightarrow wlp(S, q) \tag{4.27}$$

as listed in [APdBO10] p. 87f.

The wlp is a function supposed to return the weakest liberal precondition of a program and a postcondition. (4.23) indicates that the program is processed in reverse. In a composition, the wlp of S_1 depends on the wlp of S_2, so S_2 must be evaluated first. The already addressed skip and variable assignment handling is the same as before. The alternative is transformed into a logical disjunction of both branches. It is unknown which branch will be executed at runtime, so this can be imagined like the least common multiple sort of. The problem of finding a loop invariant remains but there are statements concerning it. The rough progressed algorithm is as follows: Apply wlp to the overall program (the root $\langle$prog$\rangle$) and the given postcondition. Depending on the current program part, act accordingly:

Skip: Return the postcondition.

Assignment: To get the precondition, replace all occurrences of the assigned variable in the postcondition by the new value. This means the syntax/semantic tree of the assertion must be recursively examined for the variable.

Composition: Find wlp of the rear program part using the given postcondition, then find wlp of the anterior part by supplying the previously received precondition to determine the precondition of the composition. Of course this can be nested/elongated. This

corresponds to a syntax tree from the language definition being descended rightwards, then working the way back up in accordance to a stack (recursive calls).

Alternative: Find wlp of the program in the **THEN**-branch (p_{then}) and the **ELSE**-branch (p_{else}) in arbitrary order, then return $B \wedge p_{then} \vee \neg B \wedge p_{else}$ with B being the condition of the alternative. This possesses the potential of easily inflating the precondition.

Loop: Try to find a loop invariant p automatically (some ideas are discussed in Section 4.5: *Finding invariants*), otherwise ask the user to present one. If it is indeed a loop invariant, it can simply be returned but it is unlikely to be sure of it (both in user query and automatic retrieval may fail), so executing the following inspection steps appears appropriate. Check if $p \wedge \neg B$ implies the available postcondition (if it is an equivalent or stronger version of it). It cannot be a fitting invariant if that is not the case, retry another one then. Find wlp of the loop body with p as the postcondition, then check the returned predicate whether it is implied by $p \wedge B$. It cannot be a fitting invariant if that is not the case, back to first step. With both checks being successful, p can be picked as a precondition of the loop. However, proving that one predicate (***Hoare*** is professed for predicate logic) does or does not imply another predicate is an undecidable problem of its own (see Section 4.4: *Resolving implications*). Thus it cannot be fully automatized, either, and must be user-supported.

Ex: A simple implementation for a ***Factorial*** procedure shall be outlined to clarify the application of the used wlp algorithm.

```
1 PRE {n>=1}
2   k := 1;
3   f := 1;
4
5   WHILE k < n DO
6     k := k + 1;
7     f := f * k
8   OD
9 POST {f=n!}
```

Listing L8: Factorial program.

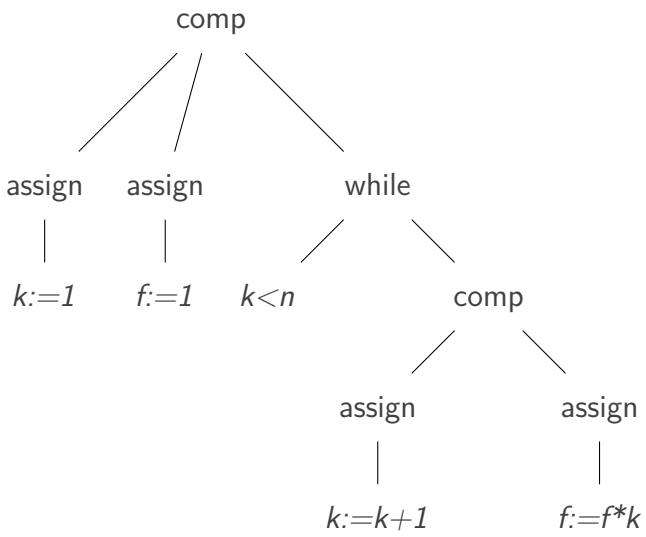

Figure F31: Tree for factorial program.

Starting from the bottom, the postcondition is $f = n!$ and the root is the main composition. The composition is processed from right to left, its last element being $while$, just passing the postcondition. The loop requires a loop invariant which is $f = k! \wedge 0 <= k \wedge k <= n$ in this case. This loop variant in conjunction with the negate of the loop condition $k < n$ yields $f = k! \wedge 0 <= k \wedge k <= n \wedge k >= n$ and must imply $f = n!$. Since $k <= n \wedge k >= n$ implies $k = n$, k can be substituted by n and the first comparison becomes $f = n!$. The implication holds true. Next on, wlp of the loop body and the invariant needs to be explored. Unpacking the inner composition again, the posterior assignment $f := f * k$ transforms $f = k! \wedge 0 <= k \wedge k <= n$ to $f * k = k! \wedge 0 <= k \wedge k <= n$ and $k := k + 1$ further to $f * (k + 1) = (k + 1)! \wedge 0 <= (k + 1) \wedge (k + 1) <= n$. To determine if it is truly a loop invariant that had been selected, $f * (k + 1) = (k + 1)! \wedge 0 <= (k + 1) \wedge (k + 1) <= n \wedge k < n$ (wlp result & loop condition) will be checked against $f = k! \wedge 0 <= k \wedge k <= n$ (just the invariant). $f * (k + 1) = (k + 1)!$ can be reduced to $f = k!$, $0 <= (k + 1) \rightarrow 0 <= k$ and $k < n \rightarrow k <= n$ are correct. All conditions of the invariant could be implied from

the inner wlp, too, hence the precondition of the loop is found to be $f = k! \wedge 0 <= k \wedge k <= n$. Supplying it to first $f := 1$, then $k := 1$ results in the final precondition of the program since the composition by itself does not invoke a change. wlp of the whole program is thereby $1 = 1! \wedge 0 <= 1 \wedge 1 <= n$. While the first two terms are tautologies, the third one depends on the value of n. What is missing is the check of the estimated precondition $n >= 1$ against $1 = 1! \wedge 0 <= 1 \wedge 1 <= n$. As this can be evaluated to true, the program is valid. Would the precondition be $n >= 0$ e.g., it would be incorrect as the scenario for $n = 0$ would not be covered.

4.3 Assertions as language extension

⟨*prog*⟩ ::= ⟨*cmd*⟩ ⟨*prog'*⟩

⟨*prog'*⟩ ::= ';' ⟨*cmd*⟩ ⟨*prog'*⟩
| ϵ

⟨*cmd*⟩ ::= ⟨*skip*⟩
| ⟨*assign*⟩
| ⟨*alt*⟩
| ⟨*while*⟩
| ⟨hoare_block⟩

⟨*skip*⟩ ::= 'SKIP'

⟨*assign*⟩ ::= 'id' ':=' ⟨*exp*⟩

⟨*alt*⟩ ::= 'IF' ⟨*bool_exp*⟩ 'THEN' ⟨*prog*⟩ ⟨*alt_else*⟩ 'FI'

⟨*alt_else*⟩ ::= 'ELSE' ⟨*prog*⟩
| ϵ

⟨*while*⟩ ::= 'WHILE' ⟨*bool_exp*⟩ 'DO' ⟨*prog*⟩ 'OD'

⟨*hoare_block*⟩ ::= ⟨hoare_pre⟩ ⟨prog⟩ ⟨hoare_post⟩

⟨*hoare_pre*⟩ ::= 'PRE' '{' ⟨bool_exp⟩ '}'

⟨*hoare_post*⟩ ::= 'POST' '{' ⟨bool_exp⟩ '}'

Figure F32: ***Hoare***-extended grammar.

The projected verifier will have to provide input masks for the inspected program itself as well as its supposed pre- and postcondition. While those three things may seem

separable, it comes in handy to graft the assertions directly into the language. The simple remodification in Figure F32 encapsulates a ⟨prog⟩ and enforces the existence of a complete triumvirate whenever a 'PRE' token is scanned. It re-utilizes the definition of ⟨bool_exp⟩, though that might be replaced for mightier constructs depending on the desired semantics for assertions. It also permits nested ⟨hoare_block⟩s. Inner and further below positioned assumptions could be tested first before advancing to outer levels, modularizing the verification process.

```
PRE {X=x&Y=y}
    R:=X;
    PRE {X=y&R=x}
        X:=Y;
        Y:=R
    POST {X=y&Y=x}
POST {X=y&Y=x}
```

Figure F33: Nested ***Hoare*** blocks.

4.4 Resolving implications

4.4.1 The implication question

It could already be observed from the ***Factorial*** example that making a decision about implications is very difficult within the domain of predicate logic although the introduced language allows but a subset of it. In fact, predicate logic in general is undecidable. There could be much more arbitrary predicates like $x\ is\ a\ zero\ of\ the\ zeta\ function$ or $y\ is\ prime$. Quantifiers (universal quantifier, existential quantifier) were left out since there were no subscripted variables declared. Arithmetics with unlimited variable domains remain and those come with a non-decidability of their own. Proving, for instance, $x < x + 1$ under the premise $x \in [1, 10]$ could be verified by testing the condition for all possible values from the 1 to 10 range, checking $1 < 1 + 1$, $2 < 2 + 1$, ..., $10 < 10 + 1$. With in infinite domain, however, it is completely futile and also the Cartesian product of multiple variables is quick to induce a state explosion. The machine must be able to recognize the pattern as a human would. The question arises how to teach the computer to do just that. At this point of explanation, the boolean expression is a mere semantic tree matching the string input. Reviewing the ***Swap*** program in Listing L9 , the wlp is $X = y \wedge Y = x[Y := R][X := Y][R := X] \Rightarrow X = y \wedge R = x[X := Y][R := X] \Rightarrow Y = y \wedge R = x[R := X] \Rightarrow Y = y \wedge X = x$. What must be proven is $X = x \wedge Y = y \rightarrow Y = y \wedge X = x$, the terms are just in different order. That is a fundamental problem of the language: Syntax and semantics

are not bijective, the syntax for the same semantics may very well diverge. This is why it appears to be a good idea to try to restructure the expressions to a more unique (and possibly less convoluted) representation. The idea is to apply the same set of rules to both sides of the implication to have them at the same destination layout. That this only works partially can be seen later on. Aside from the boolean literals $true$ and $false$, boolean expressions in the given language are built on top of numeric expressions, so their reduction rules will be examined first. All of those rules base on mathematics and logic, of course.

```
1 PRE {X=x&Y=y}
2   R:=X;
3   X:=Y;
4   Y:=R
5 POST {X=y&Y=x}
```

Listing L9: Swap program.

4.4.2 Reduction of numeric expressions

$$\begin{gathered} 123 + n\hat{}2 + 5 * n \Rightarrow 1 + 2 + n * n + n + n + 3 * n + 5! \\ 1/2 \Rightarrow 2/4 \end{gathered} \tag{4.28}$$

The proposed language seems like it only allows for integers. Yet the operations enable the representation of rational and real numbers. An input of *1/2* would depict 0.5 as would *2^(0-1)*. This 0.5 value may be irrelevant for the most part and never be regarded along the lines of IEEE 754[1] as only symbolic transformations are conducted. An ⟨ExpLit⟩ in the sense of that document is pair of integers (opposed to the same-named earlier defined syntax construct, a semantic entity is meant now), a numerator and a denominator to represent a rational number. This induces an equivocation, any fraction can be expanded. Finding the greatest common divisor of numerator and denominator and reducing the fraction by this number unifies it again. The advantage is that, this way, rational numbers can be compacted and worked on in a single ⟨ExpLit⟩ rather than in a product of an integer with the negative exponentiation of another integer. Furthermore, elementary operations like the addition of two ⟨ExpLit⟩ can be carried out in a streamlined fashion, converting the fractions to a common denominator, totalizing the numerators and re-applying the greatest common divisor.

$$5! \Rightarrow 5 * 4 * 3 * 2 \Rightarrow 120 \tag{4.29}$$

With the argument to the factorial operator being an ⟨ExpLit⟩ (5), it can be dissolved to a ⟨Prod⟩ ($5 * 4 * 3 * 2$) or directly to an ⟨ExpLit⟩ (120).

[1] common format for floating-point numbers in computers [Wik17d]

$$(k+2)! \Rightarrow k! * (k+2) * (k+1) \tag{4.30}$$

If the argument is a sum, the ⟨ExpLit⟩ part can be extracted to a sequence of factors as shown in (4.30).

$$\begin{gathered} 2\hat{}4 \Rightarrow 2*2*2*2 \Rightarrow 16 \\ (a\hat{}b)\hat{}c \Rightarrow a\hat{}(b*c) \\ a\hat{}1 \Rightarrow a \\ a\hat{}0 \Rightarrow 1 \\ (a+b)\hat{}2 \Rightarrow a\hat{}2 + 2*a*b + b\hat{}2 \end{gathered} \tag{4.31}$$

An exponentiation consists of a base and an exponent. If both of them are ⟨ExpLit⟩, calculating a number from it will be trivial. That is, with a fractional exponent the result may be real and not fit into a ⟨ExpLit⟩ anymore. To avoid the loss of information, it may be wiser to leave it as it is then instead of rounding it. A nested exponentiation can be reduced to a product of the exponents. Edge cases should be considered as far as possible like a zero exponent degrading the exponentiation to an ⟨ExpLit⟩ of value 1.

$$\begin{gathered} 2*3*5*a \Rightarrow 30*a \\ a*a*a\hat{}3 \Rightarrow a\hat{}5 \\ 0*4*a*b \Rightarrow 0 \\ a*(b+c) \Rightarrow a*b + a*c \\ a*(b*c) \Rightarrow a*b*c \end{gathered} \tag{4.32}$$

In (4.32), the ⟨ExpLit⟩ parts of a product should be condensed. Multiple occurrences of the same variable may be turned into an exponentiation. The whole product becomes zero if there is any zero included. The distributivity law may be applied to sum factors and nested products unwrapped.

$$\begin{gathered} 1+2 \Rightarrow 3 \\ a+a+3*a \Rightarrow 5*a \\ a+(b+c) \Rightarrow a+b+c \end{gathered} \tag{4.33}$$

Sums are the addition of two or multiple numeric expressions. Those expressions could be literals, variables or other structures. Literals can be merged, so can variables of the same name to a product. The ⟨Sum⟩ node in the semantic tree would review its children and find that in $n+n+3*n$, the first two are of type ⟨Id⟩ and the last one is

⟨Prod⟩. To be able to add the last part, $3 * n$ could be transformed to $n + n + n$ first or the ⟨Prod⟩ is examined for its signature, cutting the n off, only an ⟨ExpLit⟩ remains, which is added to the coefficient of the new product. Nested sums can be unwrapped once more.

4.4.3 Reduction of boolean expressions

$$\begin{aligned} 1 = 2 &\Rightarrow false \\ 1 < 2 &\Rightarrow true \\ 1 <> 2 &\Rightarrow true \\ 2 * a = 0 &\Rightarrow a = 0 \\ a! + b\hat{}c = a! + b\hat{}c &\Rightarrow true \end{aligned} \tag{4.34}$$

The literals for boolean expressions are $true$ and $false$. Another ⟨BoolElem⟩ is the comparison of two numeric expressions by a less, greater, less equal, greater equal, equal or unequal operator. Actually, these operators implant ambiguity again. $a <= b$ could be expressed by $a < b \vee a = b$, $a >= b$ by $a > b \vee a = b$ and $a <> b$ by $a < b \vee a > b$. The expressions of both sides of the comparison must be reduced and the equation (or inequation) may be homogenized by subtracting the right expression from both sides or vice versa, leaving a zero on the other. Dividing zero by any number unequal to zero yields zero. Unnecessary coefficients may be erased. This only works if the remaining side is a product. Comparing two ⟨ExpLit⟩ according to the operator is trivial and returns either $true$ or $false$. A comparison of two identical sides is reduced to $0 < operator > 0$ due to the homogenization and therefore erased, too.

$$\begin{aligned} a = 1 \wedge b = 2 \wedge true &\Rightarrow 1 = 2 \wedge 2 = 3 \\ a = 1 \wedge a = 1 &\Rightarrow a = 1 \\ \neg(a <> 1 \wedge b <> 2) &\Rightarrow a = 1 \vee b = 2 \end{aligned} \tag{4.35}$$

The structural components of boolean expressions are the junctors conjunction and disjunction plus negation. There is a couple of laws for them:

ASSOCIATIVITY

$$\begin{aligned} (A \vee B) \vee C &\Rightarrow A \vee (B \vee C) \\ (A \wedge B) \wedge C &\Rightarrow A \wedge (B \wedge C) \end{aligned} \tag{4.36}$$

COMMUTATIVITY

$$\begin{aligned} (A \vee B) &\Rightarrow (B \vee A) \\ (A \wedge B) &\Rightarrow (B \wedge A) \end{aligned} \tag{4.37}$$

DISTRIBUTIVITY

$$\begin{aligned} A \vee (B \wedge C) &\Rightarrow (A \vee B) \wedge (A \vee C) \\ A \wedge (B \vee C) &\Rightarrow (A \wedge B) \vee (A \wedge C) \end{aligned} \tag{4.38}$$

ABSORPTION

$$\begin{aligned} A \wedge (A \vee B) &\Rightarrow A \\ A \vee (A \wedge B) &\Rightarrow A \end{aligned} \tag{4.39}$$

IDEMPOTENCY

$$\begin{aligned} A \wedge A &\Rightarrow A \\ A \vee A &\Rightarrow A \end{aligned} \tag{4.40}$$

IMPLICATION

$$\begin{aligned} false \rightarrow A &\Rightarrow true \\ A \rightarrow true &\Rightarrow true \\ A \rightarrow B &\Rightarrow \neg A \vee B \\ A \rightarrow B &\Rightarrow \neg B \rightarrow \neg A \end{aligned} \tag{4.41}$$

NEGATION AND DE'MORGAN

$$\begin{aligned} \neg\neg A &\Rightarrow A \\ \neg(A \wedge B) &\Rightarrow \neg A \vee \neg B \\ \neg(A \vee B) &\Rightarrow \neg A \wedge \neg B \\ A \vee \neg A &\Rightarrow true \end{aligned} \tag{4.42}$$

TRUE/FALSE

$$\begin{aligned} A \wedge true &\Rightarrow A \\ A \wedge false &\Rightarrow false \\ A \vee true &\Rightarrow true \\ A \vee false &\Rightarrow A \end{aligned} \tag{4.43}$$

Apart from turning an implication $A \vee B \rightarrow C \vee D$ into $\neg(A \vee B) \vee (C \vee D)$, it can also be split into $(A \rightarrow C) \wedge (B \rightarrow C) \vee (A \rightarrow D) \wedge (B \rightarrow D)$.

4.4.4 Ordering

The commutativity rules of boolean expressions hint at another problem. $X = x \wedge Y = y \rightarrow Y = y \wedge X = x$ is still to show. One possibility would be to start with $A \rightarrow B \Rightarrow \neg A \vee B$: $X = x \wedge Y = y \rightarrow Y = y \wedge X = x \Rightarrow \neg(X = x \wedge Y = y) \vee (Y = y \wedge X = x) \Rightarrow X <> x \vee Y <> y \vee Y = y \wedge X = x$ and see that there are complementary parts lodged. Another would be to try out all permutations of the right side and see that one is identical. A third more versatile option is to collect the terms of conjunction of the right side and see that all of those can be found on the left side as well. More conjunction terms on the left side would only further decrease the number of states to account for and a $false$ left side renders the implication true, anyway. Thus this inclusion check is fine. And the forth and last option described here is the concept of ordering the expressions. The claim is that a total order can be established of all sibling collections inside a semantic tree.

$$6 + a + b + c! + b\hat{}2 \Rightarrow c! + b\hat{}2 + a + b + 6 \tag{4.44}$$

This can be done by first ordering the node types of the root: $\langle$Fact$\rangle \gtrdot \langle$Pow$\rangle \gtrdot \langle$Prod$\rangle \gtrdot \langle$Sum$\rangle \gtrdot \langle$Id$\rangle \gtrdot \langle$ExpLit$\rangle$ and recursively applying the same to the children. Siblings that are of the same type are either identical, containers or $\langle$Id$\rangle$ or $\langle$ExpLit$\rangle$. $\langle$ExpLit$\rangle$ may be intuitively ordered for their value (e.g. numerator primarily, denominator secondarily) or like $\langle$Id$\rangle$s lexically. Two containers of the same type may be ordered by successively comparing their elements until the first mismatch. This would yield a human-readable representation as taught in school. Of course, the whole expression could just be seen as a string of characters, the operators included, and ordered lexically.

4.4.5 Substitution

$$erg = 2\hat{}(y - x) \wedge x = 0 \Rightarrow erg = 2\hat{}y \tag{4.45}$$

The assignment of variables causes substitutions in the predicates and often stirs them up in a way that they could tolerate another reduction. A reduction could indeed be conducted after every assignment directive. Likewise, an assertion can be unified by substitution of the available variables. To do that, an equation must be reorganized for one specific variable standing alone on left- or righthand side or the pattern surrounding it must exist somewhere else matching exactly.

Ex: Rearranging for k in $k! = 1 \wedge k! = 2\hat{}a$ is difficult, factorial does not even possess a closed-form inverse function. Going for a is problematic as well as the language

currently does not feature logarithms. But $k!$ does occur twice and is free to replace, ending in $1 = 2\hat{}a$.

Solving equations and systems thereof is not decidable. Handling inequations is another issue. $a < b$ expresses that a may have any value lower than b. That is a kind of range mapping opposed to the exact mapping found in equations. To still be able to carry out substitutions, inequations can transfer their property to the target expression.

Ex: $a < 10 \wedge erg = 2\hat{}a$ is convertible to $a < 10 \wedge erg < 100$, the substitution in $a < 10 \wedge erg < 2\hat{}a$ is fine, too. Replacing the a in $a < 10 \wedge b > a$ does not quite work. b could have any value above or below 10 as long as it is greater than a but it could instead be relaxed to $a < 10 \wedge (b > a \vee b >= 10)$.

Substitutions should only be done in pure conjunctions as disjunctions pose alternative mappings. When both sides of an implication are pure conjunctions, it is practicable to transfer the substitutions from the left to the right side as in $a < 10 \wedge erg < 2\hat{}a \rightarrow erg < 2\hat{}a \Rightarrow a < 10 \wedge erg < 100 \rightarrow erg < 100$.

4.4.6 Chosen approach

When facing the need of an implication check, both sides are revised into DNF (disjunctive normal form). This yields an expression of the shape $A_1 \vee A_2 \vee A_3 \ldots \vee A_m \rightarrow B_1 \vee B_2 \vee B_3 \ldots \vee B_n$. Splitting it into multiple implications results in $A_1 \rightarrow B_1 \wedge A_2 \rightarrow B_1 \wedge A_3 \rightarrow B_1 \ldots \wedge A_m \rightarrow B_1 \vee A_1 \rightarrow B_2 \vee A_2 \rightarrow B_2 \vee A_3 \rightarrow B_2 \ldots \wedge A_m \rightarrow B_2 \vee A_1 \rightarrow B_3 \wedge A_2 \rightarrow B_3 \wedge A_3 \rightarrow B_3 \ldots \wedge A_m \rightarrow B_3 \ldots \vee A_1 \rightarrow B_m \wedge A_2 \rightarrow B_m \wedge A_3 \rightarrow B_m \ldots \wedge A_n \rightarrow B_m$ ($m * n$ implications). All of those A and B terms are pure conjunctions then, which enables the aforementioned substitutions after other reduction and ordering means have been exhausted. Should either the left side be found $false$ or the right side $true$ will mean that the observed implication is $true$. Otherwise it can still be converted from $A \rightarrow B$ to $\neg A \vee B$ and mingled with the results from the other implications.

Had quantifiers of predicate logic been factored in, surely the normalization process would have been delegated to Skolemization or prenex normal form and contemplated possible scenarios from there.

4.4.7 Greatest common divisor

The Listing **??** shows an implementation the Euclidean algorithm for getting the greatest common divisor of two numbers. The postcondition reveals the introduction of a named function gcd that can easily be added to the existing language as an indexed ⟨Id⟩ with two ⟨Exp⟩ arguments. The loop invariant here is $gcd(x0, y0) = gcd(x, y) \& x >$

$0\&y > 0$. Checking the lower end, $gcd(x0, y0) = gcd(x, y)\&x > 0\&y > 0\&x = y$ is to imply $x = y\&x = gcd(x0, y0)$. Clearly, the $x = y$ is in common. x being equal to y means that $gcd(x, y) \Rightarrow gcd(x, x)$ and the greatest common divisor of two equal (positive) numbers is evidently the number itself. $gcd(x0, y0) = gcd(x, x)$ is reduced to $gcd(x0, y0) = x$, which fulfills the second term of the postcondition.

$$gcd(x0, y0) = gcd(x, y)\&x > 0\&y > 0\&x = y \rightarrow x = y\&x = gcd(x0, y0) \quad (4.46)$$

Replacing the x by $x - y$ as the last instruction inside the loop commands when searching for its wlp, $gcd(x0, y0) = gcd(x-y, y)\&x > 0\&y > 0$ will face the alternative next. The selection rule signifies that the state in front of it is one that satisfies the wlp of the chosen branch with its entering condition. Just using the wlp algorithm, a verifier cannot exclude either path (unless the predicate collapses to a constant). So it has to be the disjunction of both possibilities. An empty/non-existing ***ELSE***-branch can be regarded as containing a ***SKIP***. The result is $x < y\&gcd(x0, y0) = gcd(y - x, x)\&y - x > 0\&x > 0|x >= y\&gcd(x0, y0) = gcd(x - y, y)\&x - y > 0\&y > 0$. The upper check is $gcd(x0, y0 = gcd(x, y)\&x > 0\&y > 0\&x <> 0 \rightarrow x < y\&gcd(x0, y0) = gcd(y - x, x)\&y - x > 0\&x > 0|x >= y\&gcd(x0, y0) = gcd(x - y, y)\&x - y > 0\&y > 0)$. A couple of terms vanish through the ***law of excluded middle***[2] and it is to show that $gcd(x, y) = gcd(y - x, x)$ basically. The mathematical ***gcd*** function has multiple properties, one being "If m is any integer, then gcd(a+m*b,b)=gcd(a,b)" [Wik17c]. Adding special functions is the same as inbuilt operators, the properties have to be ingrained as rules to reason about it. The rest of the proof is trivial.

4.5 Finding invariants

4.5.1 Pointers

The other main challenge in using the ***Hoare*** calculus consists of the search for fitting loop invariants. The pointers for finding them are:

- $p \wedge B \rightarrow wlp(S, p)$
- $p \wedge \neg B \rightarrow q$

where B is the condition of the loop, S is the body of the loop, q the postcondition after the loop and p the loop invariant. $wlp(S, p)$, $p \wedge B$, $p \wedge \neg B$ are abbreviated by R, P and Q respectively onwards.

[2] $A| \sim A \Rightarrow true$, two or more terms being complementary.

$$\begin{aligned} p &= f(B, S, q) \\ B \times S \times q &\mapsto p \end{aligned} \tag{4.47}$$

Finding f is undecidable and the involved implication relations suggest that this might be an even harder venture but maybe an algorithm for finding those loop invariants does not require implication checks or only simple ones? Most sources do not state a direct methodology for seeking loop invariants and randomly building assertions appears ineffective. At least, since Q is supposed to imply q, it is argumentative to say that $var(p) \cup var(B) \supseteq var(q)$ (all variables of the postcondition should be included). R is derived from the assignments (substitutions) in the body. As has already been discussed earlier, substitutions are badly reversible. A number of examples are going to be contemplated hereafter. One should pay attention that postconditions after loops in existing code listings may not necessarily be the strongest possibility nor be verified when they were actually user input. The loop invariant is artificially tailored to fit the postcondition and the effect of the loop must rather be interpreted and the precondition known to find the exact postcondition.

4.5.2 Parallel counter

```
1 PRE {x=0&y=0}
2   WHILE x<5 DO
3     x:=x+1;
4     y:=y+1
5   OD
6 POST {x=5&y=5}
```

Listing L10: Parallel counter

$$\begin{aligned} & x < 5 \\ \times & x := x + 1; y := y + 1 \\ \times & x = 5 \wedge y = 5 \\ \mapsto & x = y \wedge x < 6 \end{aligned} \tag{4.48}$$

There are only the variables x and y in Listing L10 . It seems obvious that x and y are 5 after the loop. That is because they both start at the same value below the loop condition threshold and increase at the same pace. This common pace or distance is a constancy, an invariant. A suitable loop invariant is $x = y \wedge x < 6$ because $x = y \wedge x < 6 \wedge x >= 5 \Rightarrow x = y \wedge x = 5 \Rightarrow x = 5 \wedge y = 5$ implies the postcondition, directly at that, and $x = y \wedge x < 6[y := y + 1][x := x + 1] \Rightarrow x + 1 \wedge y + 1 \wedge x + 1 < 6 \Rightarrow x = y \wedge x < 5$ simply absorbs the loop condition $x < 5$. The example can be parametrized to generalize it a bit and get a better understanding.

```
1 PRE {x=0&y=0&UNTIL>=0}
2   WHILE x<UNTIL DO
3     x:=x+1;
4     y:=y+1
5   OD
6 POST {x=UNTIL&y=UNTIL}
```

Listing L11: Parallel counter (parametrized)

$$\begin{aligned} & x < UNTIL \\ \times & x := x + 1; y := y + 1 \\ \times & x = UNTIL \wedge y = UNTIL \\ \mapsto & x = y \wedge x < UNTIL + 1 \end{aligned} \tag{4.49}$$

The easiest parameter to alter appears to be the upper bound of the loop. It is clearly represented in q as well as in p. However, this only works if $UNTIL$ is greater than or equal to the starting value 0. A negative $UNTIL$ would mean that neither x nor y experience modification and remain zero.

```
1 PRE {x=START&y=START}
2   WHILE x<UNTIL DO
3     x:=x+1;
4     y:=y+1
5   OD
6 POST {x=UNTIL&y=UNTIL}
```

Listing L12: Parallel counter (start parametrized)

Granting the starting values of the variables a degree of freedom induces the possibility of not entering the loop (with $START >= UNTIL$) likewise. The postcondition must handle this case ($x = UNTIL \wedge y = UNTIL \vee x = START \wedge y = START$). What does the previous $R \Rightarrow x = y \wedge x < UNTIL + 1 \wedge x >= UNTIL$ lack to imply that? It misses exactly the alternative. The loop condition cannot be changed to accommodate for it, the invariant must incorporate it. Choosing $x = y \wedge x < UNTIL + 1 \vee x = START \wedge y = START$ for p makes $R\ x + 1 = y + 1 \wedge x < UNTIL + 1 \wedge x < UNTIL \vee x + 1 = START \wedge y + 1 = START \wedge x < UNTIL$, which does not imply p evidently. A relaxation to $x = y \wedge x < UNTIL + 1 \vee x >= START \wedge y >= START$ using the $>=$ operator accounts for the $< var >:=< var > +1$ substitutions but no longer implies q.

One rule can be derived: To pass the parts of a postcondition not depending on the changed variables inside the loop body to the precondition of the loop, it can simply be added to the invariant. Respectively that supplement can be omitted while observing the loop and re-added afterwards.

$$p = f(B, S, q) \wedge var(Z) \notin change(S) \rightarrow p \wedge Z = f(B, S, q \wedge Z) \tag{4.50}$$

$$p = f(B, S, q) \vee var(Z) \notin change(S) \rightarrow p \vee Z = f(B, S, q \vee Z) \tag{4.51}$$

That is due to the $wlp(S, Z) = Z$ or more pellucidly $R \rightarrow p \wedge Z$ becoming $p' \wedge B \wedge Z \rightarrow p \wedge Z$. The variables in Z are not modified and $p' \wedge B \wedge Z \rightarrow p \wedge Z \Rightarrow (p' \rightarrow p \vee B \rightarrow p \vee Z \rightarrow p) \wedge (p' \rightarrow Z \vee B \rightarrow Z \vee Z \rightarrow Z)$. The argumentation is analogous for the postcondition check and disjunctive operator. Z does not alter the outcome of the implications.

4.5.3 Transformation of loops and structural thoughts

The loop in the ***Parallel counter*** example is indeed a count-controlled loop. The order of the assignment lines does not matter either since they do not depend on each other. That is why there is potential for certain transformations and more so with subscripted variables. Listing L13 displays the split of a loop into three other loops responsible for one of the assignments of the original loop each. That is possible because the termination of the first loop only depends on x and x does not depend on any other variable. The number of iterations is enumerated and the values of x within each iteration to pass it to y. The order is preserved. Such remodeling may force smaller structures whose loop invariants are perhaps known or that leave less of a scope to generate loop invariants for. At least a dependency graph could unveil chances for reduction.

```
1  x:=0;
2  y:=1;
3  z:=3;
4  WHILE x<5 DO
5    x:=x+1;
6    y:=y*x;
7    z:=z!
8  OD
9
10 //same as
11 x:=0;
12 y:=1;
13 z:=3;
14 c0:=0;
15 WHILE x<5 DO
16   x:=x+1;
17   c0save[c0]=x;
18   c0:=c0+1
19 OD
20 c1:=0;
21 WHILE c1<c0 DO
22   y:=y*c0save[c1];
23   c1:=c1+1
```

```
24 OD
25 c2:=0;
26 WHILE c2<c0 DO
27   z:=z!;
28   c2:=c2+1
29 OD
```

Listing L13: Loop transformation

Some more thoughts on the structure of loop invariants: The invariant must withstand the upper and lower delimiter checks. The negation of the condition of the loop can fulfill the postcondition on its own or part thereof. In that case, that burden is lifted from the invariant. It does certainly depend on the kind of assignments and substitutions. If the postcondition is a correct one, it deems the chance is high that the invariant will have roughly the same function with just different parameter restrictions. One cannot conclude a factorial relationship from proportionality, the interface between the different operations is lacking where parametrization could have an effect.

Chapter 5
5 Implementation

5.1 Java, surface

The verifier tool is implemented using the ***Java*** programming language. Since the user input codes may vary, should be able to be changed on-the-fly for experimentation purposes and more user input and information exchange is required during the verification, a graphical user interface seems plausible. Moreover, verifying assistance should ideally be integrated into an ***IDE***[1], so that the context would be a better fit. Yet for simplicity, independence of implementation and concentration on the core algorithms, the idea of a standalone application surpasses the one of a plug-in for an existing IDE. ***JavaFX***[2] is chosen as a framework for the ***GUI***[3]. It enforces the ***MVC***[4] pattern, thereby separates the graphical representation from the programming logic in a uniform way. Since the framework lacks an inbuilt widget for so-called ***rich text***[5], which allows for individual styling of characters inside a text area, the ***RichTextFX*** library by ***TomasMikula*** [Mik17] is added in order to be able to properly illustrate both inputs and outputs. That package also contains a dedicated widget for code areas. Features like line numbers, highlighting of keywords or breakpoints can be realized. Figure F34 shows the main window of the GUI. The program provides basic text editor functionality: opening, saving and creating new files. Multiple files can be opened at once, each one being represented by a tab. The displayed tab can be split into multiple views as Figure F35 indicates. Besides showing the input code (1), this can reveal the lexer-generated tokens (2) and the syntax tree composed by the parser (3) for introspection purposes. The branches that only contain the empty word are hidden on default since the tree can get pretty convoluted even without them. More output is visible in the console (4) and the tree chart in Figure F36 , which is an alternative representation of the syntax tree. After the code has been parsed, which is done automatically as the code area content changes on default, the interactive proving functionality becomes activatable (***H*** button).

[1] ***Integrated Development Environment***.
[2] ***GUI***-Toolkit for ***Java*** applications, successor to ***AWT***/***Swing***.
[3] Graphical User Interface.
[4] ***Model View Controller***.
[5] Formatting or multimedia enriched text.

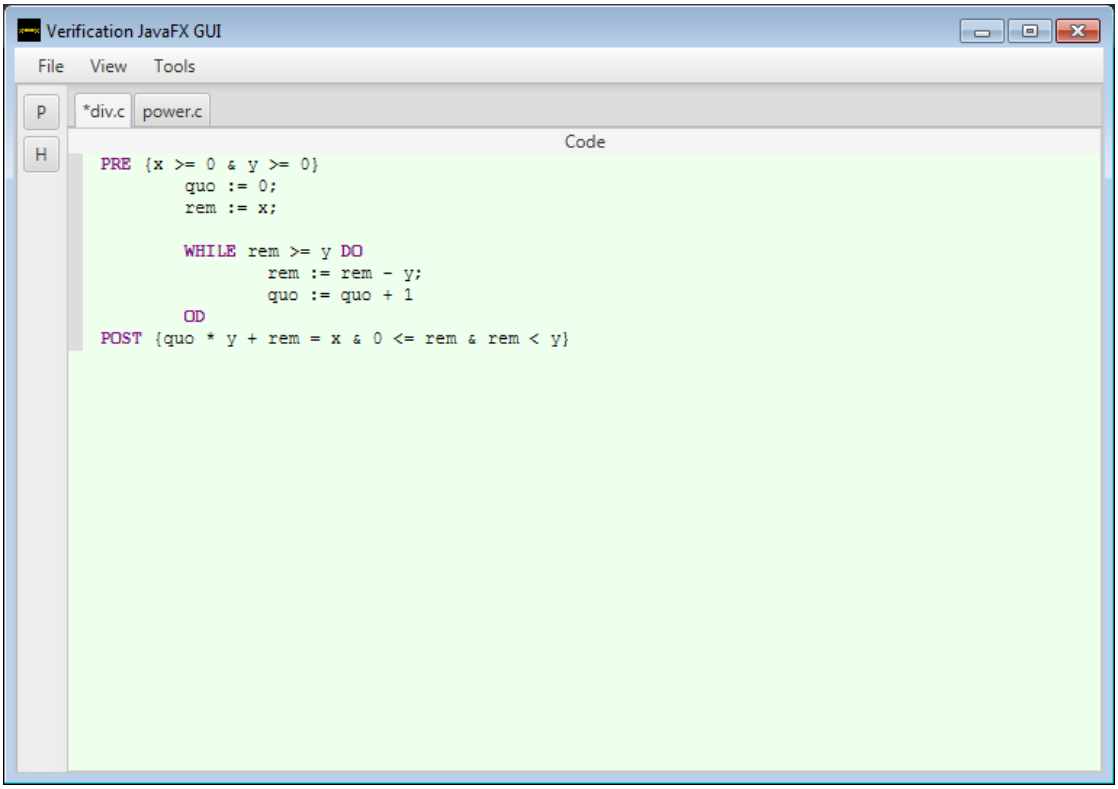

Figure F34: Main window.

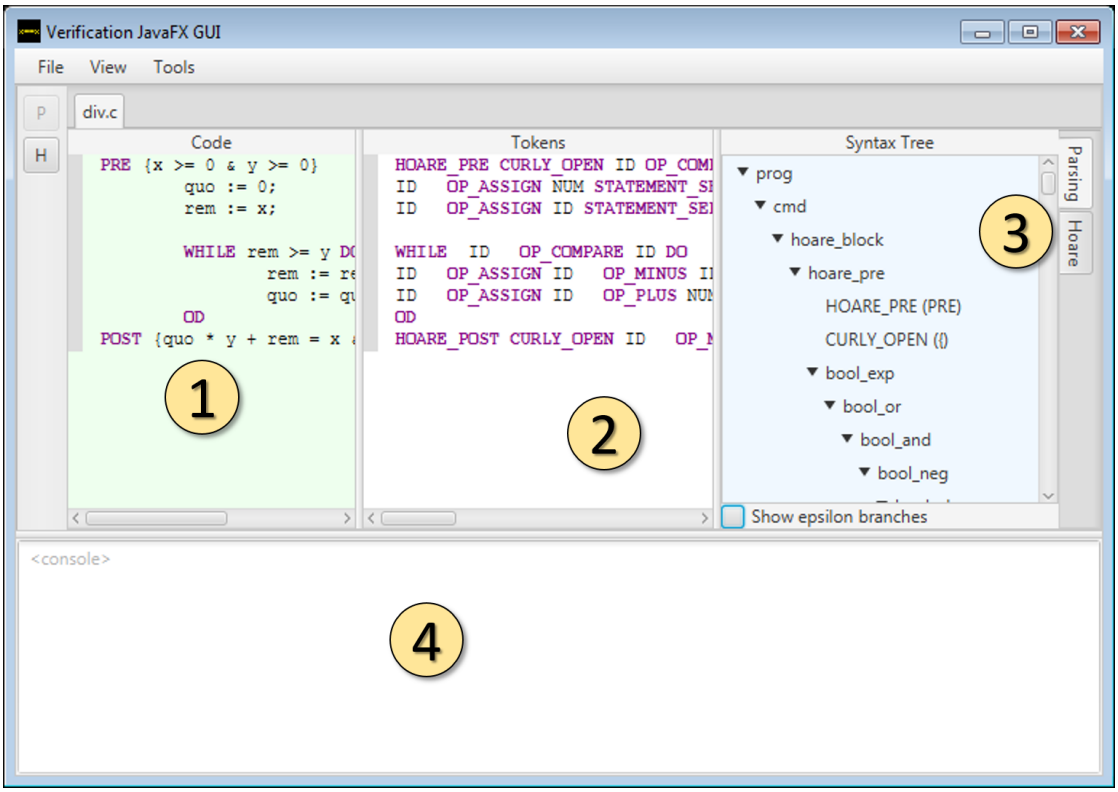

Figure F35: Views.

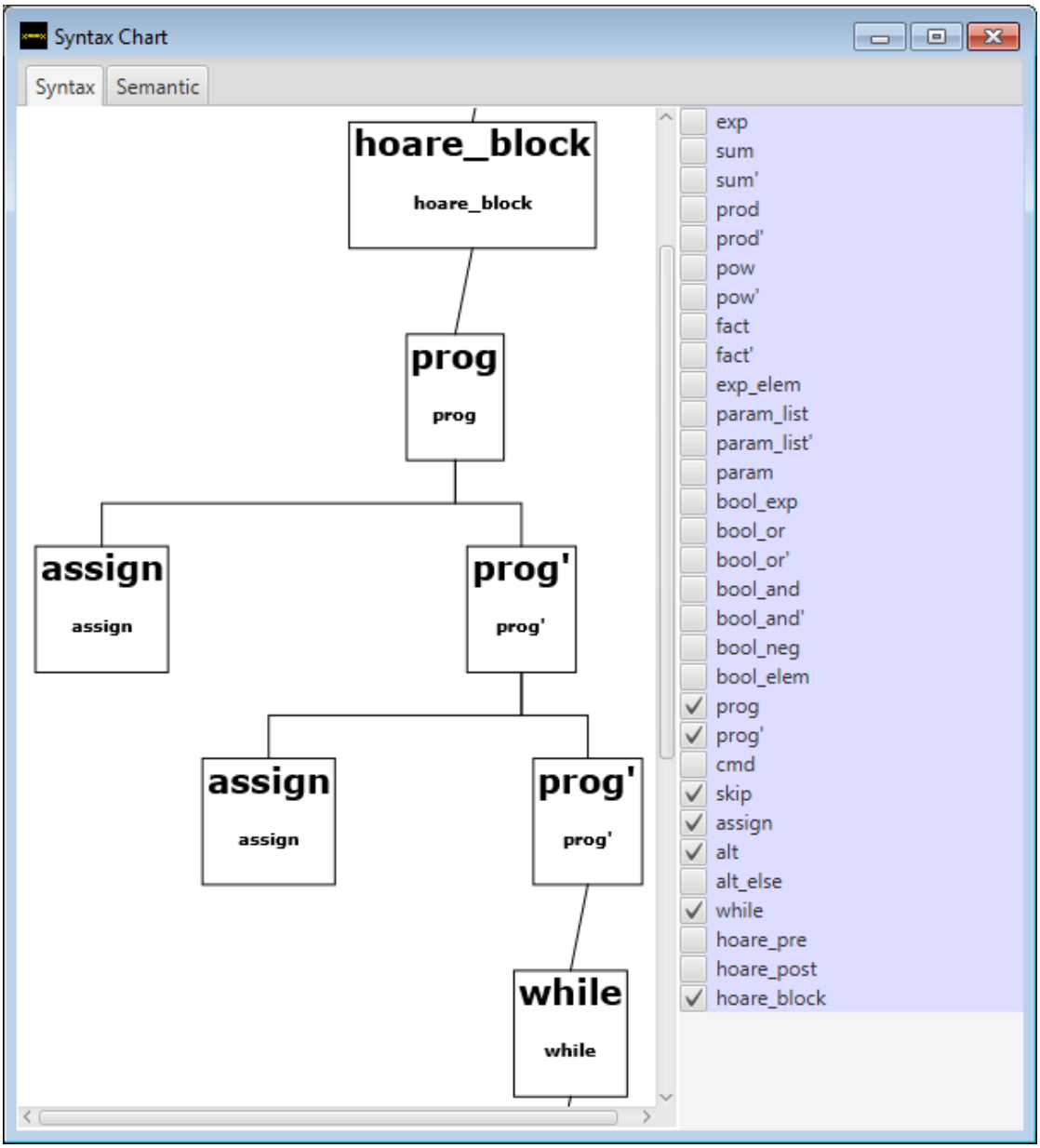

Figure F36: Syntax chart.

5.2 Grammar, lexer, parser

A grammar hosts terminals and non-terminal symbols, which come with their respective rules. Terminals are defined by lexer rules. Those are either regular expressions or fixed terms especially used for keywords. Parser rules for non-terminals consist of an ordered list of a combination of non-terminals and terminals or ϵ. Therefore, ***Symbol*** was chosen as an abstract class generalizing ***Terminal*** and ***NonTerminal***. The relationship is depicted in Figure F37 and an example for the $\langle \text{exp} \rangle$ grammar is found in Listing L14 .

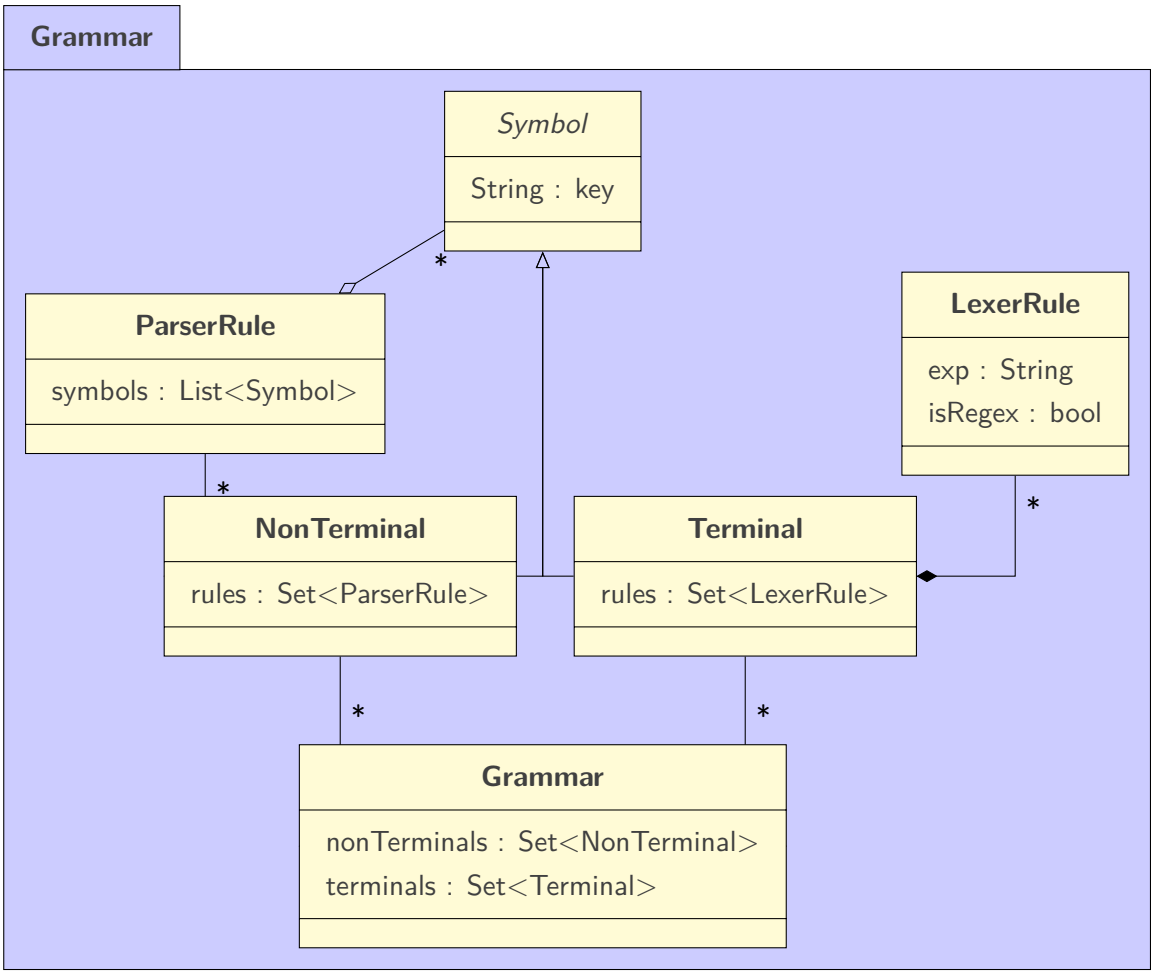

Figure F37: Grammar-related class diagram.

```
1  public ExpGrammar() {
2    super();
3
4    //lexer rules
5    TERMINAL_EXP_LIT = createTerminal("EXP_LIT");
6    TERMINAL_PAREN_OPEN = createTerminal("PAREN_OPEN");
7    TERMINAL_PAREN_CLOSE = createTerminal("PAREN_CLOSE");
8    TERMINAL_OP_PLUS = createTerminal("OP_PLUS");
9    TERMINAL_OP_MINUS = createTerminal("OP_MINUS");
10   TERMINAL_OP_MULT = createTerminal("OP_MULT");
11   TERMINAL_OP_DIV = createTerminal("OP_DIV");
12   TERMINAL_OP_POW = createTerminal("OP_POW");
13   TERMINAL_OP_FACT = createTerminal("OP_FACT");
14   TERMINAL_ID = createTerminal("ID");
15   TERMINAL_PARAM_SEP = createTerminal("PARAM_SEP").setSep();
16
17   TERMINAL_EXP_LIT.addRuleRegEx("[1-9][0-9]*");
18   TERMINAL_EXP_LIT.addRuleRegEx("0");
19
20   TERMINAL_PAREN_OPEN.addRule("(");
21   TERMINAL_PAREN_CLOSE.addRule(")");
22   TERMINAL_OP_PLUS.addRule("+");
23   TERMINAL_OP_MINUS.addRule("-");
24   TERMINAL_OP_MULT.addRule("*");
25   TERMINAL_OP_DIV.addRule("/");
26   TERMINAL_OP_POW.addRule("^");
```

```
27  TERMINAL_OP_FACT.addRule("!");
28
29  TERMINAL_ID.addRuleRegEx("[a-zA-Z][a-zA-Z0-9]*");
30
31  TERMINAL_PARAM_SEP.addRule(",");
32
33  //parser rules
34  NON_TERMINAL_EXP = createNonTerminal("exp");
35  NON_TERMINAL_SUM = createNonTerminal("sum");
36  NON_TERMINAL_SUM_ = createNonTerminal("sum'");
37  NON_TERMINAL_PROD = createNonTerminal("prod");
38  NON_TERMINAL_PROD_ = createNonTerminal("prod'");
39  NON_TERMINAL_POW = createNonTerminal("pow");
40  NON_TERMINAL_POW_ = createNonTerminal("pow'");
41  NON_TERMINAL_FACT = createNonTerminal("fact");
42  NON_TERMINAL_FACT_ = createNonTerminal("fact'");
43  NON_TERMINAL_EXP_ELEM = createNonTerminal("exp_elem");
44  NON_TERMINAL_PARAM_LIST = createNonTerminal("param_list");
45  NON_TERMINAL_PARAM_LIST_ = createNonTerminal("param_list'");
46  NON_TERMINAL_PARAM = createNonTerminal("param");
47
48  RULE_SUM = createRule(NON_TERMINAL_EXP, "sum");
49
50  RULE_PROD_SUM_ = createRule(NON_TERMINAL_SUM, "prod␣sum'");
51
52  RULE_OP_PLUS_PROD_SUM_ = createRule(NON_TERMINAL_SUM_, "OP_PLUS␣prod␣sum'");
53  RULE_OP_MINUS_PROD_SUM_ = createRule(NON_TERMINAL_SUM_, "OP_MINUS␣prod␣sum'");
54  createRule(NON_TERMINAL_SUM_, Terminal.EPSILON);
55
56  RULE_POW_PROD_ = createRule(NON_TERMINAL_PROD, "pow␣prod'");
57
58  RULE_OP_MULT_POW_PROD_ = createRule(NON_TERMINAL_PROD_, "OP_MULT␣pow␣prod'");
59  RULE_OP_DIV_POW_PROD_ = createRule(NON_TERMINAL_PROD_, "OP_DIV␣pow␣prod'");
60  createRule(NON_TERMINAL_PROD_, Terminal.EPSILON);
61
62  RULE_FACT_POW_ = createRule(NON_TERMINAL_POW, "fact␣pow'");
63
64  RULE_OP_POW_POW = createRule(NON_TERMINAL_POW_, "OP_POW␣pow");
65  createRule(NON_TERMINAL_POW_, Terminal.EPSILON);
66
67  RULE_EXP_ELEM_FACT_ = createRule(NON_TERMINAL_FACT, "exp_elem␣fact'");
68
69  RULE_OP_FACT_FACT_= createRule(NON_TERMINAL_FACT_, "OP_FACT␣fact'");
70  createRule(NON_TERMINAL_FACT_, Terminal.EPSILON);
71
72  RULE_ID_PARAM_LIST = createRule(NON_TERMINAL_EXP_ELEM, "ID␣param_list");
73  RULE_EXP_LIT = createRule(NON_TERMINAL_EXP_ELEM, "EXP_LIT");
74  RULE_PARENS_EXP = createRule(NON_TERMINAL_EXP_ELEM, "PAREN_OPEN␣exp␣PAREN_CLOSE"
        );
75
76  RULE_PARENS_PARAM_PARAM_LIST_ = createRule(NON_TERMINAL_PARAM_LIST, "PAREN_OPEN␣
        param␣param_list'␣PAREN_CLOSE");
77  createRule(NON_TERMINAL_PARAM_LIST, Terminal.EPSILON);
78
79  RULE_PARAM_SEP_PARAM_PARAM_LIST_ = createRule(NON_TERMINAL_PARAM_LIST_, "
        PARAM_SEP␣param␣param_list'");
80  createRule(NON_TERMINAL_PARAM_LIST_, Terminal.EPSILON);
81
82  RULE_EXP = createRule(NON_TERMINAL_PARAM, "exp");
83
84  //finalize
```

```
85    setStartSymbol(NON_TERMINAL_EXP);
86
87    updateParserTable();
88 }
```

Listing L14: Implementation of ⟨exp⟩ grammar (Java)

The ***Grammar*** class can be extended, e.g. ***ExpGrammar*** is inherited by ***WhileGrammar*** (the grammar that describes while Programs). This modularization approach concedes further flexibility when converting between string and syntax tree. An instance of ***Grammar*** both is used by the lexer and the parser. The ***Lexer*** class splits a string into a stream of tokens and the ***Parser*** class transforms the tokens into a syntax tree. ***Token*** is an aggregate of ***Terminal*** and contains additional details like the position it occupies relating to the input string. That information can be used for error reporting when checking the syntax or for other output arrangement. The inner workings of the lexer can be looked at in Appendix B: *Lexer, parser listings* . The method first removes comments and sanitizes the input from unnecessary line breaks. The current position is memorized and incorporated into the regular expression pattern. All of the terminals and rules are iterated over in order to find the longest match. Before doing that, the rules get sorted because the language for ⟨id⟩ is, in fact, a superset of most keywords like 'IF' or 'WHILE'. In that case, the keywords should be prioritized. If no match is found after trying everything, an exception with the current position will be thrown. Otherwise, the longest match will generate a new instance of ***Token*** and the lexer appends it to the output list. The pointer advances and the process is repeated until it transcends the end of the input string.

Using the terminals and non-terminals along with the information about the parser rules, a grammar can construct a predictive parser table. This table makes a direct assignment between a pair of ***NonTerminal*** and ***Terminal*** and ***ParserRule*** and is used by the parser to select the next rule. The parsing algorithm is depicted in Appendix B: *Lexer, parser listings* . Firstly, the terminator symbol '$' is annexed to the token list and the iterator gets pointed to the first token. Beginning with the designated starting rule of the grammar, the recursively invoked ***getNode*** method is called. It is supposed to create a single node of the syntax tree (paying attention to the current non-terminal and token) but triggers the construction of all children nodes in one fell swoop. The ***selectRule*** method fetches the rule to pursue from the predictive parser table and will report an error if there is no entry. Then the symbols of the rule are gone over: If a symbol is a terminal, it will be compared against the current token, added as a child and the iterator will take a step to point to the next token. In case of the empty word, the child is a special ϵ node. Lastly, non-terminals amount to a child as well but call the ***getNode*** method again to acquire their own respective children. Since the last case does not effectuate a change in the token iterator, the grammar is expected to indeed

be a LL(1) grammar as a different scenario would be prone to induce an infinite loop.

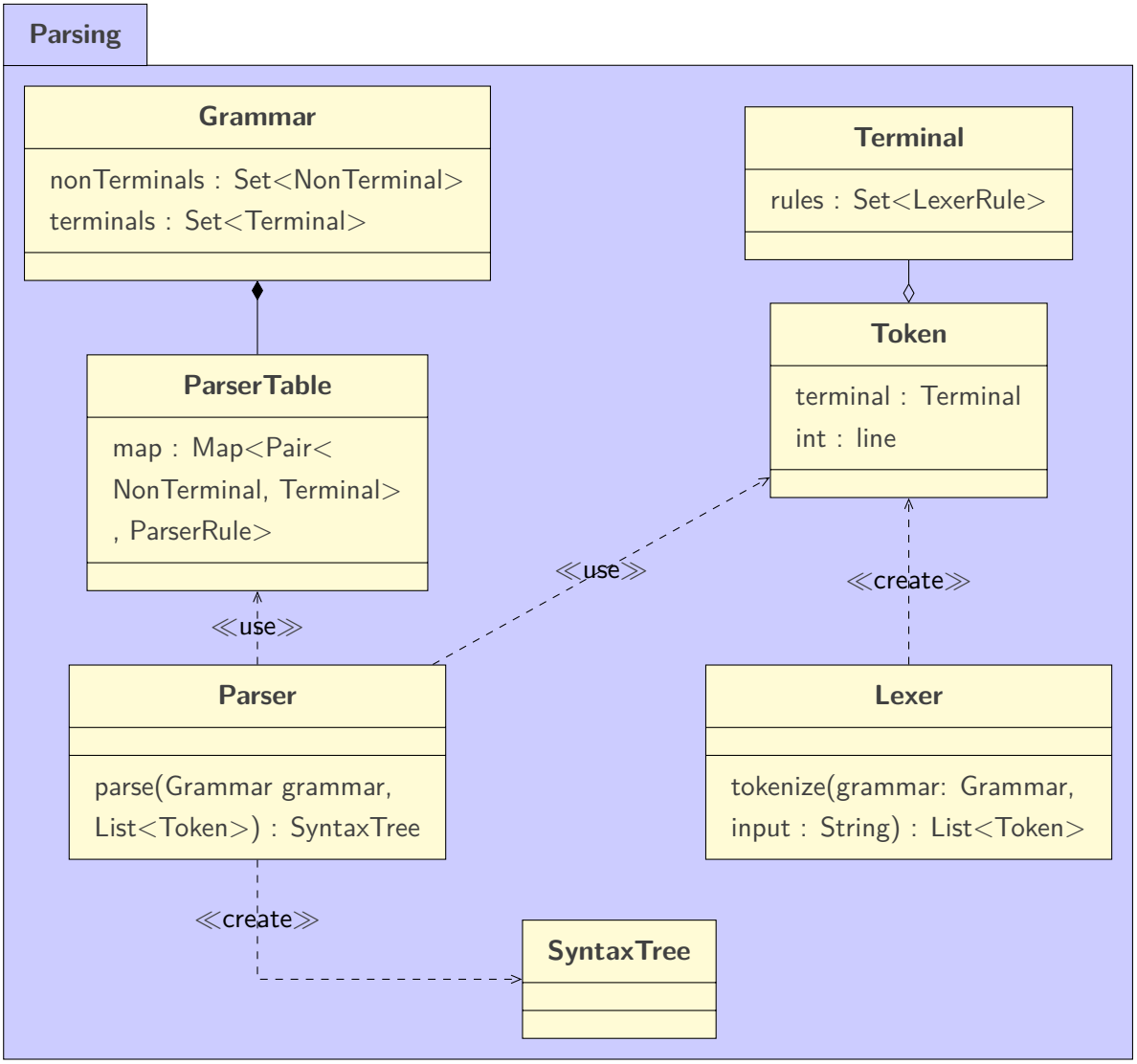

Figure F38: Parser-related class diagram.

5.2.1 First, Follow

The algorithms for the concept of ***First*** and ***Follow*** were already outlined in Chapter 3: *Introduction of a Language* . Specific ***Java*** implementations are provided along with the piecing together of the parser table in Appendix A: *First, Follow, parser table listings* .

```
1 public Set<Terminal> getFirst(List<Symbol> symbols, Set<NonTerminal> recursiveSet)
      {
2   if (symbols.contains(Terminal.EPSILON)) return new LinkedHashSet<>(Arrays.asList
      (new Terminal[]{Terminal.EPSILON}));
3
4   Set<Terminal> ret = new LinkedHashSet<>();
5
```

```
  for (int i = 0; i < symbols.size(); i++) {
    Symbol symbol = symbols.get(i);

    if (symbol instanceof Terminal) {
      ret.add((Terminal) symbol); break;
    } else if (symbol instanceof NonTerminal) {
      Set<Terminal> setSub = getFirst((NonTerminal) symbol, recursiveSet);

      if (i < symbols.size() - 1 && setSub.contains(Terminal.EPSILON)) {
        setSub.remove(Terminal.EPSILON); ret.addAll(setSub);
      } else {
        ret.addAll(setSub); break;
      }
    }
  }

  return ret;
}

public Set<Terminal> getFirst(NonTerminal nonTerminal, Set<NonTerminal>
    recursiveSet) {
  Set<Terminal> ret = new LinkedHashSet<>();

  if (recursiveSet.contains(nonTerminal)) return ret;

  recursiveSet.add(nonTerminal);

  for (ParserRule p : nonTerminal.getRules()) {
    ret.addAll(getFirst(p.getSymbols(), recursiveSet));
  }

  return ret;
}

public Set<Terminal> getFirst(NonTerminal nonTerminal) {
  return getFirst(nonTerminal, new LinkedHashSet<>());
}
```

Listing L15: Implementation of ***First*** (Java)

```
public Set<Terminal> getFollow(NonTerminal nonTerminal, Grammar grammar, Set<
    NonTerminal> recursiveSet) {
  Set<Terminal> ret = new LinkedHashSet<>();

  if (recursiveSet.contains(nonTerminal)) return ret;

  recursiveSet.add(nonTerminal);

  if (grammar.getStartParserRule().equals(nonTerminal)) ret.add(Terminal.
      TERMINATOR);

  for (NonTerminal p : grammar.getNonTerminals()) {
    for (ParserRule rule : p.getRules()) {
      List<Symbol> symbols = rule.getSymbols();

      for (int i = 0; i < symbols.size(); i++) {
        Symbol symbol = rule.getSymbols().get(i);

        if (symbol.equals(nonTerminal)) {
          List<Symbol> restSymbols = (i < symbols.size() - 1) ? symbols.subList(i
              + 1, symbols.size()) : new ArrayList<>();
```

```
19
20          if (restSymbols.isEmpty()) {
21            ret.addAll(getFollow(p, grammar, recursiveSet));
22          } else {
23            Set<Terminal> subSet = getFirst(restSymbols, new LinkedHashSet<
                  NonTerminal>());
24
25            if (subSet.contains(Terminal.EPSILON)) {
26              subSet.remove(Terminal.EPSILON);
27
28              ret.addAll(subSet);
29
30              ret.addAll(getFollow(p, grammar, recursiveSet));
31            } else {
32              ret.addAll(subSet);
33            }
34          }
35        }
36      }
37    }
38  }
39
40  return ret;
41 }
42
43 public Set<Terminal> getFollow(NonTerminal nonTerminal, Grammar grammar) {
44   return getFollow(nonTerminal, grammar, new LinkedHashSet<NonTerminal>());
45 }
```

Listing L16: Implementation of ***Follow*** (Java)

```
1  public PredictiveParserTable(Grammar g) {
2    Map<NonTerminal, Set<Terminal>> firstMap = new LinkedHashMap<>();
3    Map<NonTerminal, Set<Terminal>> followMap = new LinkedHashMap<>();
4
5    for (NonTerminal p : g.getNonTerminals()) {
6      firstMap.put(p, getFirst(p));
7      followMap.put(p, getFollow(p, g));
8    }
9
10   for (NonTerminal p : g.getNonTerminals()) {
11     for (ParserRule r : p.getRules()) {
12       List<Symbol> symbols = r.getSymbols();
13
14       if (symbols.contains(Terminal.EPSILON))
15         for (Terminal terminal : followMap.get(p)) {
16           set(p, terminal, r);
17         }
18       else {
19         Symbol symbol = r.getSymbols().get(0);
20
21         if (symbol instanceof Terminal) {
22           set(p, (Terminal) symbol, r);
23         } else if (symbol instanceof NonTerminal) {
24           for (Terminal terminal : firstMap.get((NonTerminal) symbol)) {
25             set(p, terminal, r);
26           }
27         }
28       }
29     }
30   }
```

```
}
```

Listing L17: Parser table (Java)

```
public LexerResult tokenize(String s) throws LexerException {
  s = removeComments(s);

  Vector<Terminal> terminals = new Vector<>(_grammar.getTerminals());

  terminals.sort(new Comparator<Terminal>() {
    private boolean isRegEx(Terminal terminal) {
      for (LexerRule rule : terminal.getRules()) if (rule.isRegEx()) return true;

      return false;
    }

    @Override
    public int compare(Terminal terminalA, Terminal terminalB) {
      if (terminalA.getRules().isEmpty() || terminalB.getRules().isEmpty()) return
          0;

      if (isRegEx(terminalA)) return 1;
      if (isRegEx(terminalB)) return -1;

      return 0;
    }
  });

  Terminal wsRule = new Terminal(new SymbolKey("WS"), true);

  wsRule.addRule(new LexerRule("\\s+", true));

  terminals.add(wsRule);

  int curPos = 0; Vector<Token> tokens = new Vector<>(); int x = 0; int y = 0;

  while (curPos < s.length()) {
    if ((s.length() - curPos >= System.lineSeparator().length()) && s.substring(
        curPos, curPos + System.lineSeparator().length()).equals(System.
        lineSeparator())) {
      curPos += System.lineSeparator().length(); x = 0; y++;

      continue;
    }

    int curLen = 0; LexerRule curRule = null; Terminal curTerminal = null;

    for (int i = 0; i < terminals.size(); i++) {
      Terminal terminal = terminals.get(i);

      for (LexerRule rule : terminal.getRules()) {
        String ruleS = (curPos > 0) ? String.format("^.{%d}(%s)", curPos, rule.
            getRegEx()) : String.format("^(%s)", rule.getRegEx());

          Pattern adjustedPattern = Pattern.compile(ruleS, Pattern.DOTALL);

        Matcher matcher = adjustedPattern.matcher(s);

        if (matcher.find() && (matcher.start(1) == curPos)) {
          int newLen = (matcher.end(1) - 1) - matcher.start(1) + 1;

```

```
            if (newLen > curLen) {
            curTerminal = terminal; curRule = rule; curLen = newLen;
          }
        }
      }
    }

    if (curRule == null) throw new LexerException(y, x, curPos, s);
    else {
      String text = s.substring(curPos, curPos + curLen);

      for (int i = 0; i < text.length();) {
        if ((text.length() - i >= System.lineSeparator().length()) && text.
            substring(i, i + System.lineSeparator().length()).equals(System.
            lineSeparator())) {
          i += System.lineSeparator().length();
        } else {
          i++;
        }
      }

      Token token = createToken(curTerminal, curRule, text, y, x, curPos);

      if (!token.getTerminal().isSkipped()) tokens.add(token);

      curPos += curLen;
      x += curLen;
    }
  }

  return new LexerResult(tokens);
}
```

Listing L18: Lexer (Java, shortened)

```
private ParserRule selectRule(NonTerminal nonTerminal, Token terminal) throws
    ParserException {
  try {
    ParserRule rule = _ruleMap.get(nonTerminal, terminal.getTerminal());

    if (rule == null) throw new Exception();

    return rule;
  } catch (Exception e) {
    if (terminal == null) throw new NoMoreTokensException(nonTerminal);
    else throw new NoRuleException(terminal, nonTerminal);
  }
}

private SyntaxTreeNode getNode(NonTerminal rule) throws ParserException {
  ParserRule nextRule = selectRule(rule, _token);

  SyntaxTreeNode thisNode = new SyntaxTreeNode(rule, nextRule);

  for (Symbol symbol : nextRule.getSymbols()) {
    if (symbol instanceof NonTerminal) {
      thisNode.addChild(getNode((NonTerminal) symbol));
    } else {
      if (symbol.equals(Terminal.EPSILON)) {
        thisNode.addChild(new SyntaxTreeNodeTerminal(null));

```

```
26          continue;
27        }
28
29        if (_token == null) throw new NoMoreTokensException(rule, (Terminal) symbol)
              ;
30        if (!_token.getTerminal().equals(symbol)) throw new WrongTokenException(
              _token, rule, symbol);
31
32        thisNode.addChild(new SyntaxTreeNodeTerminal(_token));
33
34        _token = _tokensItr.hasNext() ? _tokensItr.next() : null;
35      }
36    }
37
38    return thisNode;
39  }
40
41  public SyntaxTree parse(Vector<Token> tokens) throws ParserException {
42    _tokens = tokens;
43
44    if (_tokens.isEmpty()) throw new NoMoreTokensException(_grammar.
          getStartParserRule());
45
46    _tokens.add(Token.createTerminator(tokens));
47
48    _tokensItr = _tokens.iterator();
49
50    _token = _tokensItr.next();
51
52    SyntaxTreeNode root = getNode(_grammar.getStartParserRule());
53
54    if (!_token.getTerminal().equals(Terminal.TERMINATOR)) throw new
          SuperfluousTokenException(_token);
55
56    return new SyntaxTree(_grammar, root);
57  }
```

Listing L19: Parser (Java, shortened)

5.3 Semantic transformation, reduction, ordering

The syntax trees as produced by the parser are difficult to operate on, which is why the notion of semantic trees was mentioned earlier in Section 3.3: *Semantic tree* of Chapter 3: *Introduction of a Language* . The semantics are as needed: Their type-specific nature calls for individual treatment as a ⟨While⟩ node differs from a ⟨Id⟩ for example. In line with this, there is no uniform conversion from syntax to semantic tree. The semantic nodes are modeled in own ***Java*** classes, spanning a type hierarchy with abstract base and intermediates. The rough layout for the verifier is depicted in Figure F39 , Figure F40 and Figure F41 . The typification allows for proper case distinction using ***instanceof***[6], so do the interfaces and overloading of shared methods.

[6] ***Java*** operator that checks if an object is of a given type (or super types).

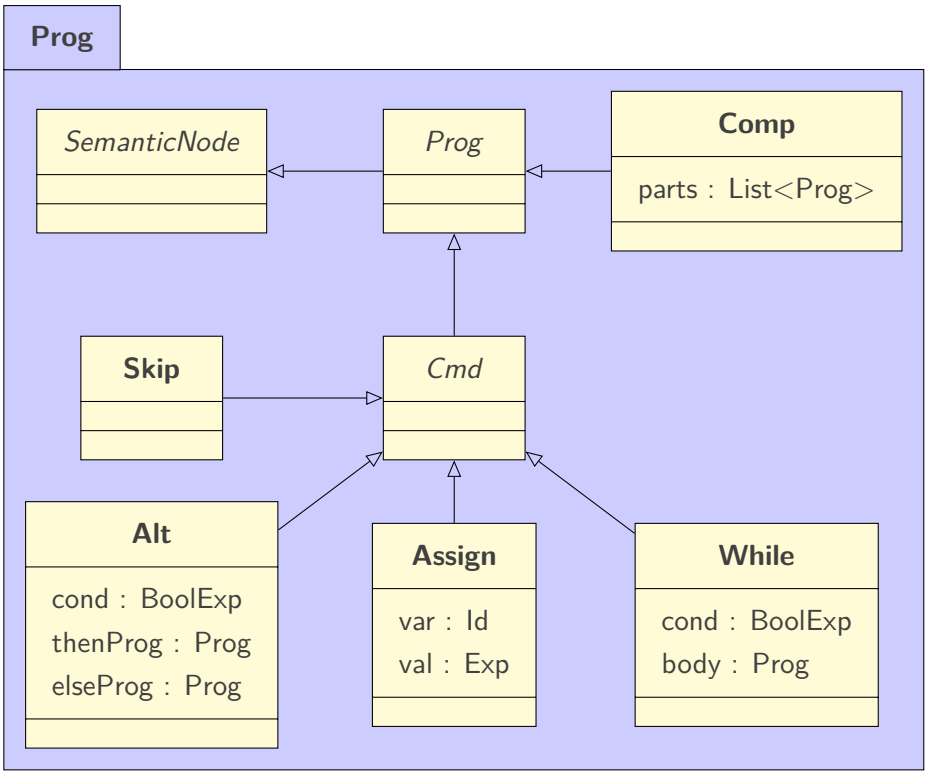

Figure F39: Type hierarchy of ⟨Prog⟩.

⟨Exp⟩ and ⟨BoolExp⟩ declare the methods ***reduce_spec***, ***order_spec*** and ***comp_spec*** for their children to implement. ***reduce_spec*** tries to apply reductions on the targeted object and further down in its node chain, presenting the result as a newly constructed node. The frequent manipulation of semantic nodes suggests to render the classes immutable[7]. For the ***reduce_spec*** method, returning a new object is a must because a ⟨Sum⟩ of ⟨ExpLit⟩ is to collapse to an ⟨ExpLit⟩ for example. ***order_spec*** sorts the children of a node in defined order by making comparisons using ***comp_spec***. Those methods are highly recursive and complex to re-enact normally. The base types define ***reduce***/***order***/***comp*** as wrapper methods to track the calls and stream them through a common gateway. ***comp*** additionally makes a comparison based on the class types before running the individually bound ***order_spec*** of the object in question. An example for those functionalities, albeit only a part of the recursive chain, is portrayed in Listing L20 .

[7] The attributes of the object are final, it cannot be modified.

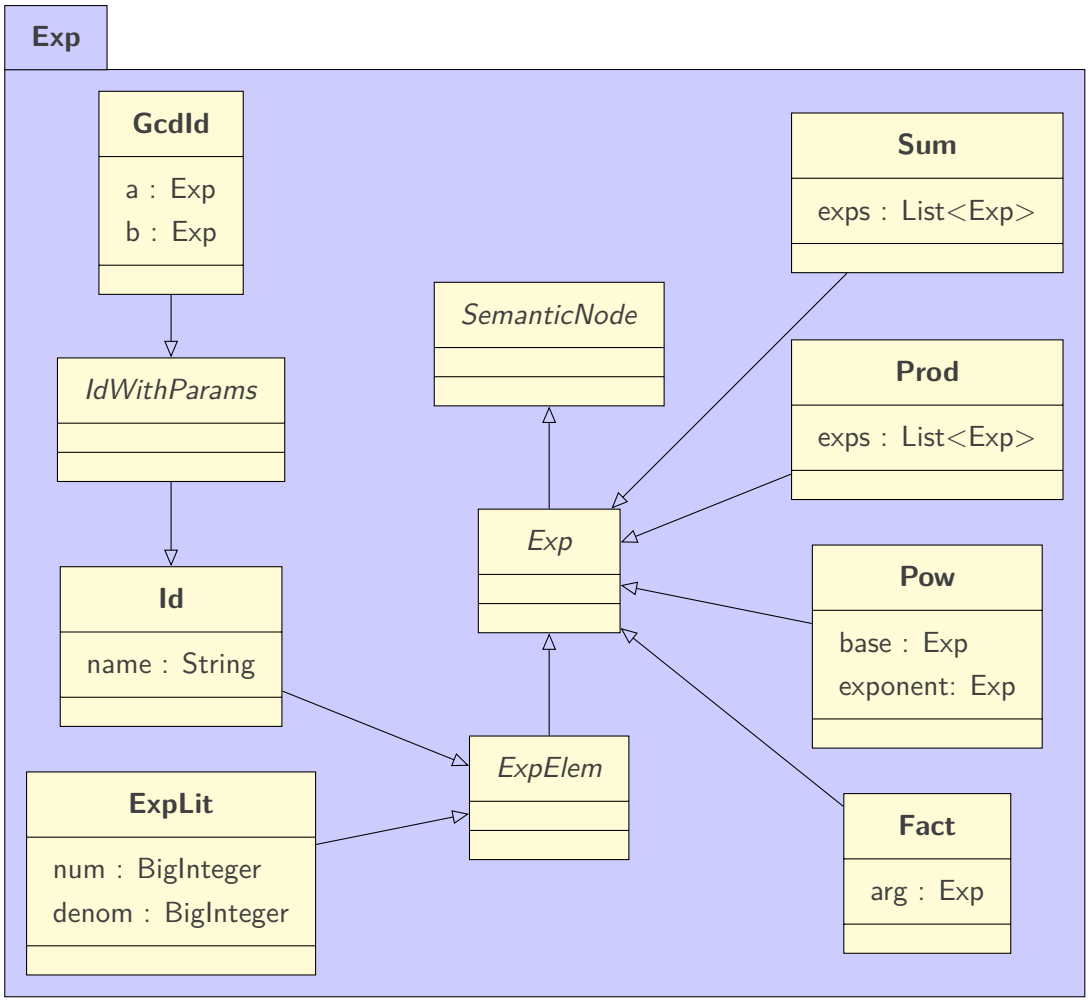

Figure F40: Type hierarchy of numeric expressions.

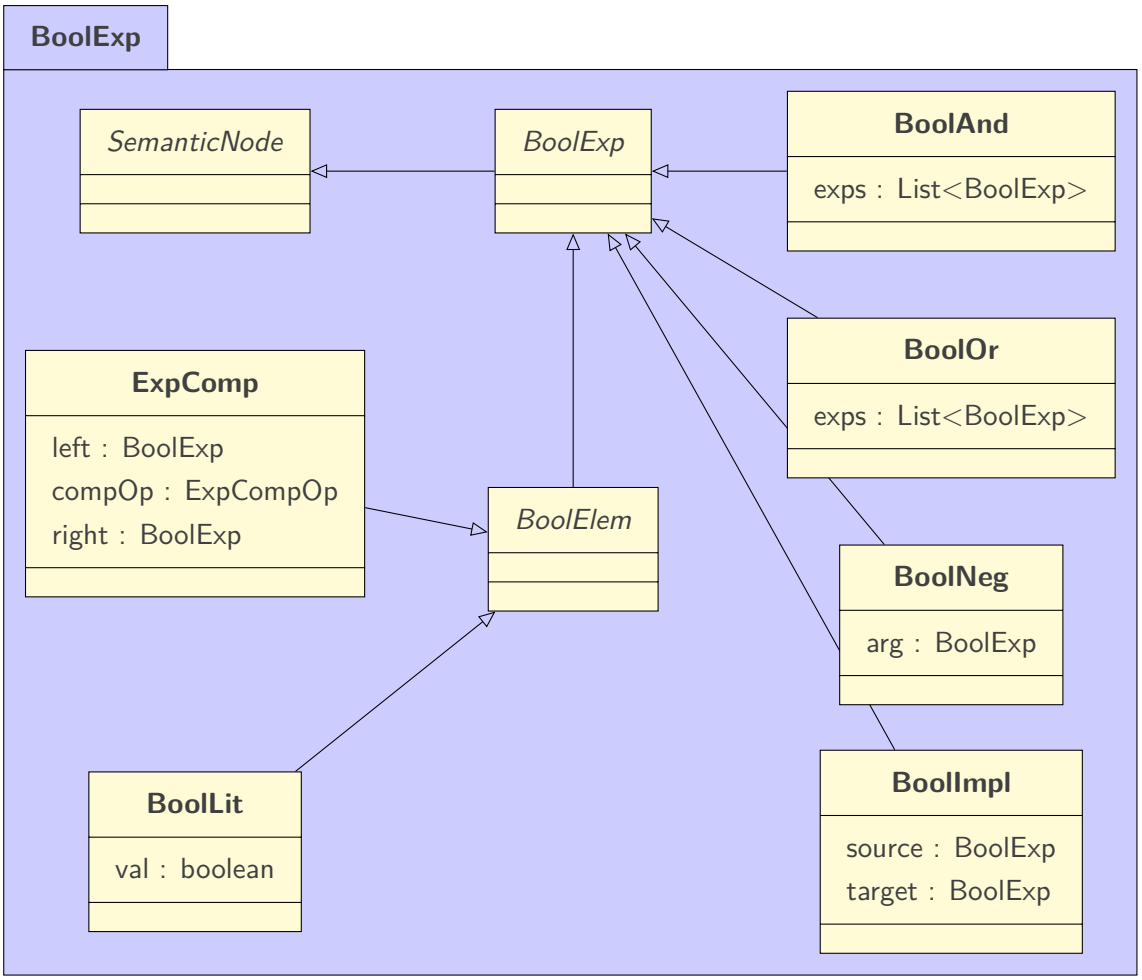

Figure F41: Type hierarchy of boolean expressions.

```
1  //Exp code
2
3  @CheckReturnValue
4  @Nonnull
5  public final Exp reduce() {
6    if (!getChildren().isEmpty()) {
7      _printer.println("enter␣" + getTypeName() + "->" + this);
8    }
9    _printer.begin();
10
11   _reduceStack.push(this);
12
13   Exp ret = reduce_spec();
14
15   _reduceStack.pop();
16
17   _printer.end();
18   if (!ret.getChildren().isEmpty()) {
19     _printer.println("leave␣" + getTypeName() + "->" + ret);
20   }
21
22   if (_reduceStack.isEmpty()) {
23     _printer.println("finished");
24   } else {
```

```
    _printer.println("reenter" + _reduceStack.peek().getTypeName());
  }

  return ret;
}

@CheckReturnValue
@Nonnull
public abstract Exp order_spec();

@CheckReturnValue
@Nonnull
public final Exp order() {
  return order_spec();
}

public abstract int comp_spec(Exp b);

public final int comp(Exp b) {
  List<Class<? extends Exp>> types = new ArrayList<>();

  types.add(ExpLit.class);
  types.add(Id.class);
  types.add(Sum.class);
  types.add(Prod.class);
  types.add(Pow.class);
  types.add(Fact.class);

  if (types.indexOf(getClass()) < types.indexOf(b.getClass())) return -1;
  if (types.indexOf(getClass()) > types.indexOf(b.getClass())) return 1;

  return comp_spec(b);
}

//Pow code

@Nonnull
@Override
public Exp reduce_spec() {
  Exp base = _base.reduce();
  Exp exponent = _exponent.reduce();

  if (base instanceof ExpLit && exponent instanceof ExpLit) {
    ExpLit ret = (ExpLit) base;

    ret = ret.pow((ExpLit) exponent);

    return ret;
  }

  if (base instanceof Pow) {
    exponent = new Prod(((Pow) base).getExponent(), exponent);

    base = ((Pow) base).getBase();
  }

  if (exponent.equals(new ExpLit(1))) return base;
  if (exponent.equals(new ExpLit(0))) return new ExpLit(1);

  return new Pow(base, exponent);
}
```

```
86
87  @Nonnull
88  @Override
89  public Pow order_spec() {
90    return new Pow(_base.order(), _exponent.order());
91  }
92
93  @Override
94  public int comp_spec(Exp b) {
95    int baseRet = _base.comp(((Pow) b).getBase());
96
97    if (baseRet != 0) return baseRet;
98
99    return _exponent.comp(((Pow) b)._exponent);
100 }
```

Listing L20: Logic snippet for ⟨Pow⟩ nodes.

5.4 Hoare

Starting the ***Hoare***-style verification opens up a special menu next to the code area shown in Figure F42 . The mechanism walks the semantic tree from the root in search of a ⟨HoareBlock⟩, consequently initiates the wlp approach with the inner ⟨Prog⟩ node and the postcondition. Each step displays a new dialog for the user to notice and to understand the rationale for the ongoing decision making while marking the currently considered piece of code with pointing arrows in the code area. These description texts are adjusted to integrate the actually seen values. The dialogs can be skipped over as far as possible with a checkbox selected. As this is generally not the case with loops and implication checks, there are adequate input options as required. Figure F43 displays the input box in the right lower part. The user may present a boolean expression as string or, if any loop invariants were found, select it from a combobox. The program can generally search for possibilities in parallel without blocking the GUI. The dynamically more complex consequence check dialog in Figure F44 has the implication split apart, trying to solve the shards individually but giving the user a veto/input possibility to make a potentially better/different choice before merging the results for the next level. A live proof outline can be eyed in the semantic tree chart view Figure F45 . The ***Hoare*** algorithm itself is in Appendix D: *Hoare listing* . As most of the implementation of a verifier proved to be, operating on the tree structure often ends in recursive calls. The dialogs necessitate stops in between. Callback interfaces were installed to emulate a calling stack without blocking the thread.

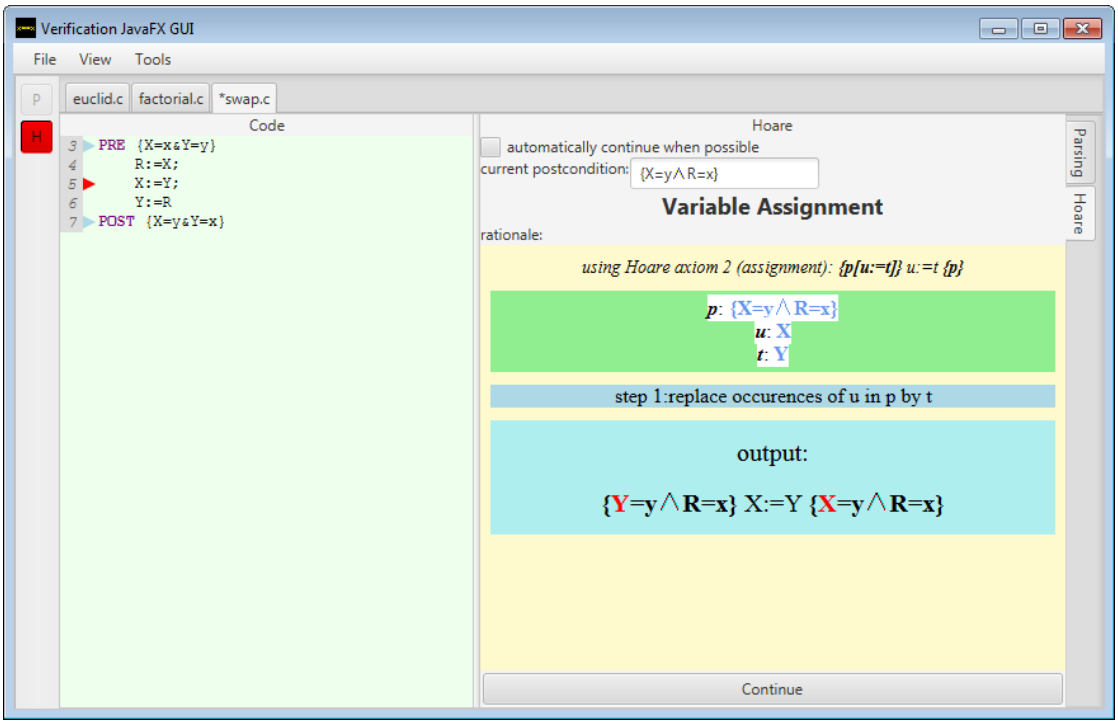

Figure F42: ***Hoare*** dialog and indicator.

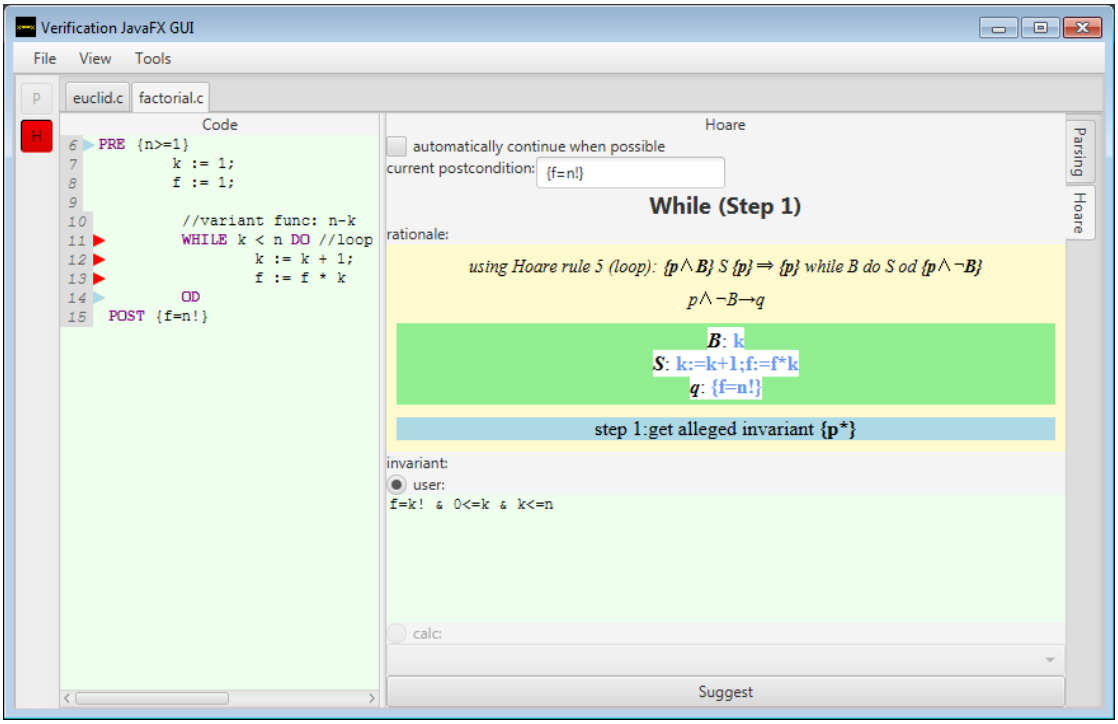

Figure F43: Loop invariant dialog.

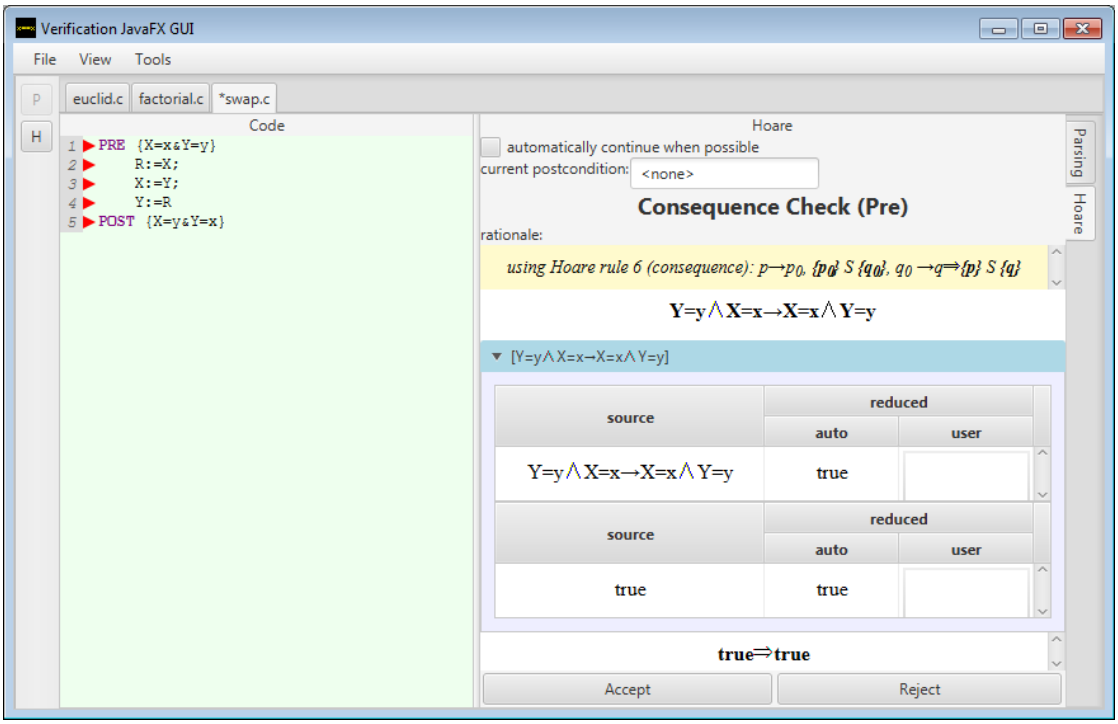

Figure F44: Consequence check dialog.

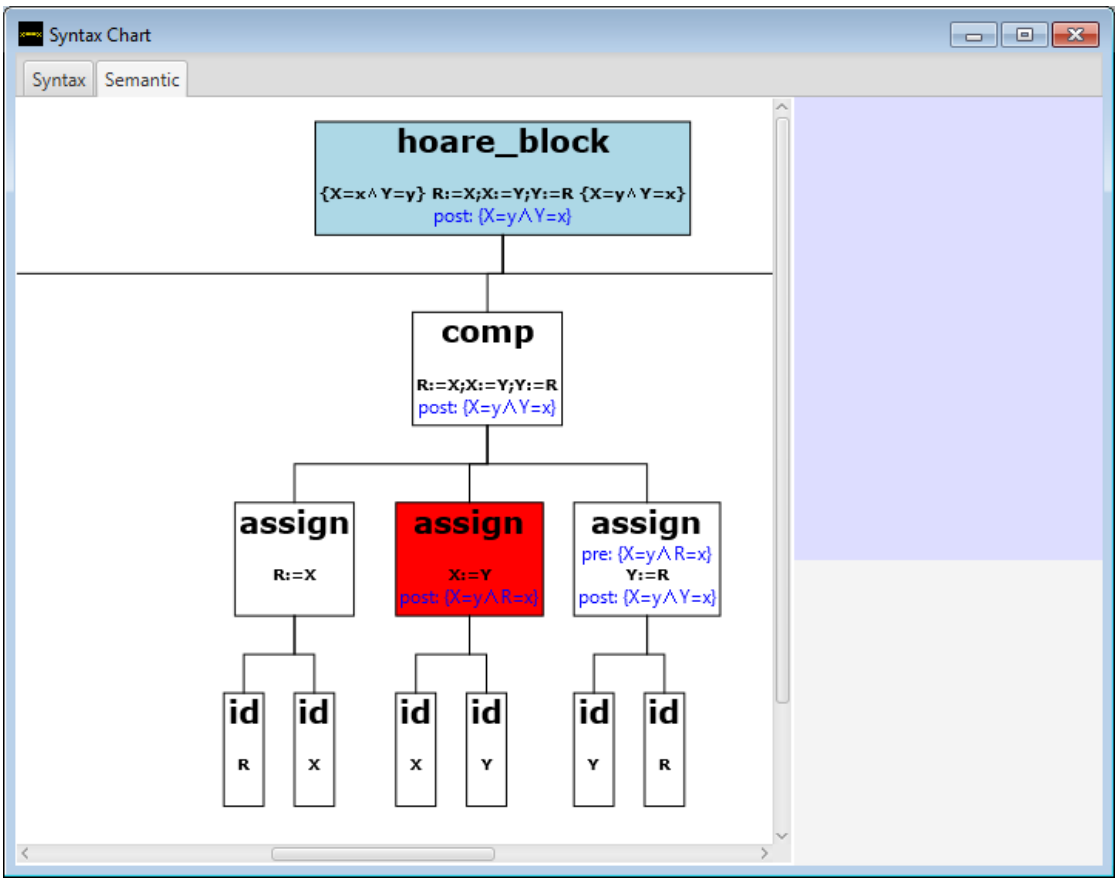

Figure F45: Semantic tree with proof outline.

Chapter 6
6 Conclusion

The ***Hoare*** calculus is good in theory but very difficult to apply and reenact since there are a lot of cavities and eventualities to account for. There is no single straightforward way to make use of it and the verification process must often be supported by the user. This is why a program should be annotated with assertions and loop invariants. The arising question is whether those annotations are chosen correctly then in order to meet the expectations of the developer. Program verification is a bit of a self-fulfilling prophecy, the software engineer inserts more information with the ambition of constraining malfunctioning scenarios, trusting that additional information (hopefully this is done by peers). The axioms and rules are general enough that the implementation and strategies are heavily dependent on the language. The semantics of the elements in assertions, the types of predicates and symbols, whose correctness must be ascertained, are the pivot point for what statements may be constructed. The topic is copious, can be scrutinized further for sure and concedes space for creativity. Finding loop invariants is usually regarded as an intuitive task. Maybe such vagueness could be combined with machine learning or databases be gradually fed with previously regarded proof outlines. Implication checks for the observed arithmetics are feasible but may fail in detail. Similarly to solving equations in school, sometimes it requires a ***sharp eye*** or the right application of conversion rules to get the proper result. The expansion of expressions appears to be very arbitrary, trial and error, but instead of only reducing them to a final format, which is ambiguous and more so with an enlarged language, intermediate comparisons and reshuffling multiple reduced representations should be able to solve more implication problems.

A verifier benefits from a test-driven and agile development. The verification rules are extendable and a lot of edge cases up for optimization. Frequent code refactoring may cause hard to track down issues. Test cases or other verification methods safeguard integrity and give an overview.

Bibliography

[APdBO10] K. Apt, A. Pnueli, F.S. de Boer, and E.R. Olderog. *Verification of Sequential and Concurrent Programs*. Texts in Computer Science. Springer, London, 2010. URL: books.google.de/books?id=9BGPVwLTkh4C.

[Coc02] Robin Cockett. Cpsc411 – compiler construction i: Ll(1) grammars and predictive top-down parsing. pages.cpsc.ucalgary.ca/ robin/-class/411/LL1.2.html, 2002. [Online; accessed 30-October-2017].

[Dij69] Edsger W. Dijkstra. Ew dijkstra quotes. wiki.c2.com/?EwDijkstraQuotes, 1969. [Online; accessed 30-October-2017].

[FLM84] C. B. Jones F. L. Morris. An early program proof by alan turing. pdfs.semanticscholar.org/dfd7/34b2de2cbcce6ac07e909011b0ed6ba32b01.pdf, 1984. [Online; accessed 30-October-2017].

[Gri82] David Gries. A note on a standard strategy for developing loop invariants and loops. *Science of Computer Programming*, 2(3):207 – 214, 1982. URL: www.sciencedirect.com/science/article/pii/0167642383900151, doi:dx.doi.org/10.1016/0167-6423(83)90015-1.

[Kam16] Anya Kamenetz. The president wants every student to learn computer science. how would that work? www.npr.org/sections/ed/2016/01/12/462698966/the-president-wants-every-student-to-learn-computer-science-how-would-that-work, 2016.

[Kapnd] Craig S. Kaplan. The craig web experience: Understanding the halting problem. www.cgl.uwaterloo.ca/csk/halt, n.d. [Online; accessed 31-October-2017].

[Kle09] S. Kleuker. *Formale Modelle der Softwareentwicklung: Model-Checking, Verifikation, Analyse und Simulation*. Vieweg Studium. Vieweg+Teubner Verlag, 2009. URL: books.google.de/books?id=Gql3pv5V85cC.

[Mat17] Richard J. Mathar. A java math.bigdecimal implementation of core mathematical functions. arxiv.org/abs/0908.3030v2, 2017. [Online; accessed 25-October-2017].

[McC08] James D. McCaffrey. The difference between unit testing and module testing. jamesmccaffrey.wordpress.com/2008/08/29/the-difference-between-unit-testing-and-module-testing, 2008. [Online; accessed 30-October-2017].

[Mignd] Matt Might. Grammar: The language of languages (bnf, ebnf, abnf and more). matt.might.net/articles/grammars-bnf-ebnf, n.d. [Online; accessed 20-June-2017].

[Mik17] Tomas Mikula. Rich-text area for javafx. github.com/FXMisc/RichTextFX, 2017. [Online; accessed 15-June-2017].

[Pnu77] Amir Pnueli. The temporal logic of programs. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science*, SFCS '77, pages 46–57, Washington, DC, USA, 1977. IEEE Computer Society. URL: dx.doi.org/10.1109/SFCS.1977.32, doi:10.1109/SFCS.1977.32.

[Rav17] Ravindrababu Ravula. Compiler design online lectures. www.youtube.com/playlist?list=PLEbnTDJUr_IcPtUXFy2b1sGRPsLFMghhS, 2017. [Online; accessed 31-August-2017].

[RK83] P. J. Hayes R. Kowalski. *Semantic Trees in Automatic Theorem-Proving*. Springer, Berlin, Heidelberg, 1983. URL: link.springer.com/chapter/10.1007/978-3-642-81955-1_13.

[Sas10] SasQ. parsing - lexers vs parsers - stack overflow. stackoverflow.com/questions/2842809/lexers-vs-parsers, 2010. [Online; accessed 20-June-2017].

[Spo02] Joel Spolsky. The law of leaky abstractions. www.joelonsoftware.com/2002/11/11/the-law-of-leaky-abstractions, 2002.

[Tan16] Gang Tan. A collection of well-known software failures. www.cse.psu.edu/ gxt29/bug/softwarebug.html, 2016. [Online; accessed 30-October-2017].

[Wik17a] Wikipedia. Ambiguous grammar — wikipedia, the free encyclopedia. en.wikipedia.org/wiki/Ambiguous_grammar#Recognizing_ambiguous_grammars, 2017. [Online; accessed 20-June-2017].

[Wik17b] Wikipedia. Fehlerquotient — wikipedia, die freie enzyklopädie. de.wikipedia.org/w/index.php?title=Fehlerquotient, 2017. [Online; accessed 24-August-2017].

[Wik17c] Wikipedia. Greatest common divisor — wikipedia, the free encyclopedia. en.wikipedia.org/wiki/Greatest_common_divisor#Properties, 2017. [Online; accessed 1-November-2017].

[Wik17d] Wikipedia. Ieee 754 — wikipedia, the free encyclopedia. en.wikipedia.org/wiki/IEEE_754, 2017. [Online; accessed 25-October-2017].

[Wik17e] Wikipedia. Model checking — wikipedia, the free encyclopedia. en.wikipedia.org/wiki/Model_checking, 2017. [Online; accessed 24-August-2017].

[Wik17f] Wikipedia. Shape analysis (program analysis) — wikipedia, the free encyclopedia. en.wikipedia.org/w/index.php?title=Shape_analysis_(program_analysis), 2017. [Online; accessed 24-August-2017].

[Wik17g] Wikipedia. While-programm — wikipedia, die freie enzyklopädie. de.wikipedia.org/w/index.php?title=WHILE-Programm, 2017. [Online; accessed 25-October-2017].

Appendix A

A First, Follow, parser table listings

```java
public Set<Terminal> getFirst(List<Symbol> symbols, Set<NonTerminal> recursiveSet) {
  if (symbols.contains(Terminal.EPSILON)) return new LinkedHashSet<>(Arrays.asList(new Terminal[]{Terminal.EPSILON}));

  Set<Terminal> ret = new LinkedHashSet<>();

  for (int i = 0; i < symbols.size(); i++) {
    Symbol symbol = symbols.get(i);

    if (symbol instanceof Terminal) {
      ret.add((Terminal) symbol); break;
    } else if (symbol instanceof NonTerminal) {
      Set<Terminal> setSub = getFirst((NonTerminal) symbol, recursiveSet);

      if (i < symbols.size() - 1 && setSub.contains(Terminal.EPSILON)) {
        setSub.remove(Terminal.EPSILON); ret.addAll(setSub);
      } else {
        ret.addAll(setSub); break;
      }
    }
  }

  return ret;
}

public Set<Terminal> getFirst(NonTerminal nonTerminal, Set<NonTerminal> recursiveSet) {
  Set<Terminal> ret = new LinkedHashSet<>();

  if (recursiveSet.contains(nonTerminal)) return ret;

  recursiveSet.add(nonTerminal);

  for (ParserRule p : nonTerminal.getRules()) {
    ret.addAll(getFirst(p.getSymbols(), recursiveSet));
  }

  return ret;
}

public Set<Terminal> getFirst(NonTerminal nonTerminal) {
  return getFirst(nonTerminal, new LinkedHashSet<>());
}
```

Listing L21: ***First*** (Java)

```java
public Set<Terminal> getFollow(NonTerminal nonTerminal, Grammar grammar, Set<
    NonTerminal> recursiveSet) {
  Set<Terminal> ret = new LinkedHashSet<>();

  if (recursiveSet.contains(nonTerminal)) return ret;

  recursiveSet.add(nonTerminal);

  if (grammar.getStartParserRule().equals(nonTerminal)) ret.add(Terminal.
      TERMINATOR);

  for (NonTerminal p : grammar.getNonTerminals()) {
    for (ParserRule rule : p.getRules()) {
      List<Symbol> symbols = rule.getSymbols();

      for (int i = 0; i < symbols.size(); i++) {
        Symbol symbol = rule.getSymbols().get(i);

        if (symbol.equals(nonTerminal)) {
          List<Symbol> restSymbols = (i < symbols.size() - 1) ? symbols.subList(i
              + 1, symbols.size()) : new ArrayList<>();

          if (restSymbols.isEmpty()) {
            ret.addAll(getFollow(p, grammar, recursiveSet));
          } else {
            Set<Terminal> subSet = getFirst(restSymbols, new LinkedHashSet<
                NonTerminal>());

            if (subSet.contains(Terminal.EPSILON)) {
              subSet.remove(Terminal.EPSILON);

              ret.addAll(subSet);

              ret.addAll(getFollow(p, grammar, recursiveSet));
            } else {
              ret.addAll(subSet);
            }
          }
        }
      }
    }
  }

  return ret;
}

public Set<Terminal> getFollow(NonTerminal nonTerminal, Grammar grammar) {
  return getFollow(nonTerminal, grammar, new LinkedHashSet<NonTerminal>());
}
```

Listing L22: ***Follow*** (Java)

```java
public PredictiveParserTable(Grammar g) {
  Map<NonTerminal, Set<Terminal>> firstMap = new LinkedHashMap<>();
  Map<NonTerminal, Set<Terminal>> followMap = new LinkedHashMap<>();

  for (NonTerminal p : g.getNonTerminals()) {
    firstMap.put(p, getFirst(p));
    followMap.put(p, getFollow(p, g));
  }

  for (NonTerminal p : g.getNonTerminals()) {
    for (ParserRule r : p.getRules()) {
      List<Symbol> symbols = r.getSymbols();

      if (symbols.contains(Terminal.EPSILON))
        for (Terminal terminal : followMap.get(p)) {
          set(p, terminal, r);
        }
      else {
        Symbol symbol = r.getSymbols().get(0);

        if (symbol instanceof Terminal) {
          set(p, (Terminal) symbol, r);
        } else if (symbol instanceof NonTerminal) {
          for (Terminal terminal : firstMap.get((NonTerminal) symbol)) {
            set(p, terminal, r);
          }
        }
      }
    }
  }
}
```

Listing L23: Parser table (Java)

B Appendix B

Lexer, parser listings

```
1  public LexerResult tokenize(String s) throws LexerException {
2    s = removeComments(s);
3
4    Vector<Terminal> terminals = new Vector<>(_grammar.getTerminals());
5
6    terminals.sort(new Comparator<Terminal>() {
7      private boolean isRegEx(Terminal terminal) {
8        for (LexerRule rule : terminal.getRules()) if (rule.isRegEx()) return true;
9
10       return false;
11     }
12
13     @Override
14     public int compare(Terminal terminalA, Terminal terminalB) {
15       if (terminalA.getRules().isEmpty() || terminalB.getRules().isEmpty()) return
             0;
16
17       if (isRegEx(terminalA)) return 1;
18       if (isRegEx(terminalB)) return -1;
19
20       return 0;
21     }
22   });
23
24   Terminal wsRule = new Terminal(new SymbolKey("WS"), true);
25
26   wsRule.addRule(new LexerRule("\\s+", true));
27
28   terminals.add(wsRule);
29
30   int curPos = 0; Vector<Token> tokens = new Vector<>(); int x = 0; int y = 0;
31
32   while (curPos < s.length()) {
33     if ((s.length() - curPos >= System.lineSeparator().length()) && s.substring(
         curPos, curPos + System.lineSeparator().length()).equals(System.
         lineSeparator())) {
34       curPos += System.lineSeparator().length(); x = 0; y++;
35
36       continue;
37     }
38
39     int curLen = 0; LexerRule curRule = null; Terminal curTerminal = null;
40
41     for (int i = 0; i < terminals.size(); i++) {
42       Terminal terminal = terminals.get(i);
43
44       for (LexerRule rule : terminal.getRules()) {
45         String ruleS = (curPos > 0) ? String.format("^.{%d}(%s)", curPos, rule.
               getRegEx()) : String.format("^(%s)", rule.getRegEx());
46
```

```
          Pattern adjustedPattern = Pattern.compile(ruleS, Pattern.DOTALL);

        Matcher matcher = adjustedPattern.matcher(s);

        if (matcher.find() && (matcher.start(1) == curPos)) {
          int newLen = (matcher.end(1) - 1) - matcher.start(1) + 1;

            if (newLen > curLen) {
            curTerminal = terminal; curRule = rule; curLen = newLen;
          }
        }
      }
    }

    if (curRule == null) throw new LexerException(y, x, curPos, s);
    else {
      String text = s.substring(curPos, curPos + curLen);

      for (int i = 0; i < text.length();) {
        if ((text.length() - i >= System.lineSeparator().length()) && text.
            substring(i, i + System.lineSeparator().length()).equals(System.
            lineSeparator())) {
          i += System.lineSeparator().length();
        } else {
          i++;
        }
      }

      Token token = createToken(curTerminal, curRule, text, y, x, curPos);

      if (!token.getTerminal().isSkipped()) tokens.add(token);

      curPos += curLen;
      x += curLen;
    }
  }

  return new LexerResult(tokens);
}
```

Listing L24: Lexer (Java)

```
private ParserRule selectRule(NonTerminal nonTerminal, Token terminal) throws
    ParserException {
  try {
    ParserRule rule = _ruleMap.get(nonTerminal, terminal.getTerminal());

    if (rule == null) throw new Exception();

    return rule;
  } catch (Exception e) {
    if (terminal == null) throw new NoMoreTokensException(nonTerminal);
    else throw new NoRuleException(terminal, nonTerminal);
  }
}

private SyntaxTreeNode getNode(NonTerminal rule) throws ParserException {
  ParserRule nextRule = selectRule(rule, _token);

  SyntaxTreeNode thisNode = new SyntaxTreeNode(rule, nextRule);

```

```
19    for (Symbol symbol : nextRule.getSymbols()) {
20      if (symbol instanceof NonTerminal) {
21        thisNode.addChild(getNode((NonTerminal) symbol));
22      } else {
23        if (symbol.equals(Terminal.EPSILON)) {
24          thisNode.addChild(new SyntaxTreeNodeTerminal(null));
25
26          continue;
27        }
28
29        if (_token == null) throw new NoMoreTokensException(rule, (Terminal) symbol)
              ;
30        if (!_token.getTerminal().equals(symbol)) throw new WrongTokenException(
              _token, rule, symbol);
31
32        thisNode.addChild(new SyntaxTreeNodeTerminal(_token));
33
34        _token = _tokensItr.hasNext() ? _tokensItr.next() : null;
35      }
36    }
37
38    return thisNode;
39  }
40
41  public SyntaxTree parse(Vector<Token> tokens) throws ParserException {
42    _tokens = tokens;
43
44    if (_tokens.isEmpty()) throw new NoMoreTokensException(_grammar.
          getStartParserRule());
45
46    _tokens.add(Token.createTerminator(tokens));
47
48    _tokensItr = _tokens.iterator();
49
50    _token = _tokensItr.next();
51
52    SyntaxTreeNode root = getNode(_grammar.getStartParserRule());
53
54    if (!_token.getTerminal().equals(Terminal.TERMINATOR)) throw new
          SuperfluousTokenException(_token);
55
56    return new SyntaxTree(_grammar, root);
57  }
```

Listing L25: Parser (Java)

Appendix C

Semantic Transformation Listing

```
1  private static SemanticNode transform(@Nonnull SyntaxNode syntaxNode) {
2    SemanticNode newNode = null;
3
4    Symbol symbol = syntaxNode.getSymbol();
5    ParserRule subRule = syntaxNode.getSubRule();
6
7    if (symbol.equals(_grammar.NON_TERMINAL_BOOL_EXP) && subRule.equals(_grammar.
         RULE_BOOL_OR)) {
8      SyntaxNode orSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_BOOL_OR);
9
10     if (orSyntaxNode != null) newNode = transform(orSyntaxNode);
11   } else if (symbol.equals(_grammar.NON_TERMINAL_BOOL_OR) || symbol.equals(
         _grammar.NON_TERMINAL_BOOL_OR_)) {
12     if (subRule.equals(_grammar.RULE_BOOL_AND_BOOL_OR_) || subRule.equals(_grammar
           .RULE_OP_OR_BOOL_AND_BOOL_OR_)) {
13       BoolOr boolOrNode = new BoolOr();
14
15       SyntaxNode andSyntaxNode = syntaxNode.findChild(_grammar.
             NON_TERMINAL_BOOL_AND);
16
17       if ((andSyntaxNode != null)) {
18         SemanticNode andNode = transform(andSyntaxNode);
19
20         if (andNode != null) boolOrNode.addBoolExp((BoolExp) andNode);
21       }
22
23       SyntaxNode or_SyntaxNode = syntaxNode.findChild(_grammar.
             NON_TERMINAL_BOOL_OR_);
24
25       if (or_SyntaxNode != null) {
26         SemanticNode or_Node = transform(or_SyntaxNode);
27
28         if (or_Node != null) boolOrNode.addBoolExp((BoolExp) or_Node);
29       }
30
31       if (boolOrNode.getChildren().size() > 1) {
32         newNode = boolOrNode;
33       } else if (!boolOrNode.getChildren().isEmpty()) {
34         newNode = boolOrNode.getChildren().get(0);
35       }
36     }
37   } else if (symbol.equals(_grammar.NON_TERMINAL_BOOL_AND) || symbol.equals(
         _grammar.NON_TERMINAL_BOOL_AND_)) {
38     if (subRule.equals(_grammar.RULE_BOOL_NEG_BOOL_AND_) || subRule.equals(
           _grammar.RULE_OP_AND_BOOL_NEG_BOOL_AND_)) {
39       BoolAnd boolAndNode = new BoolAnd();
40
41       SyntaxNode negSyntaxNode = syntaxNode.findChild(_grammar.
             NON_TERMINAL_BOOL_NEG);
42
```

```
43        if (negSyntaxNode != null) {
44          SemanticNode negNode = transform(negSyntaxNode);
45
46          if (negNode != null) boolAndNode.addBoolExp((BoolExp) negNode);
47        }
48
49        SyntaxNode and_SyntaxNode = syntaxNode.findChild(_grammar.
              NON_TERMINAL_BOOL_AND_);
50
51        if (and_SyntaxNode != null) {
52          SemanticNode and_Node = transform(and_SyntaxNode);
53
54          if (and_Node != null) boolAndNode.addBoolExp((BoolExp) and_Node);
55        }
56
57        if (boolAndNode.getChildren().size() > 1) {
58          newNode = boolAndNode;
59        } else if (!boolAndNode.getChildren().isEmpty()) {
60          newNode = boolAndNode.getChildren().get(0);
61        }
62      }
63    } else if (symbol.equals(_grammar.NON_TERMINAL_BOOL_NEG)) {
64      if (subRule.equals(_grammar.RULE_NEG_BOOL_ELEM)) {
65        SyntaxNode elemSyntaxNode = syntaxNode.findChild(_grammar.
              NON_TERMINAL_BOOL_ELEM);
66
67        if (elemSyntaxNode != null) newNode = new BoolNeg((BoolExp) transform(
              elemSyntaxNode));
68      } else if (subRule.equals(_grammar.RULE_BOOL_ELEM)) {
69        SyntaxNode elemSyntaxNode = syntaxNode.findChild(_grammar.
              NON_TERMINAL_BOOL_ELEM);
70
71        if (elemSyntaxNode != null) newNode = transform(elemSyntaxNode);
72      }
73    } else if (symbol.equals(_grammar.NON_TERMINAL_BOOL_ELEM)) {
74      if (subRule.equals(_grammar.RULE_BOOL_LIT)) {
75        SyntaxNode boolLitSyntaxNode = syntaxNode.findChild(_grammar.
              TERMINAL_BOOL_LIT);
76
77        if (boolLitSyntaxNode != null) newNode = transform(boolLitSyntaxNode);
78      } else if (subRule.equals(_grammar.RULE_EXP_OP_COMP_EXP)) {
79        SyntaxNode leftExpSyntaxNode = syntaxNode.findChild(_grammar.
              NON_TERMINAL_EXP, 0);
80        SyntaxNode expCompOpSyntaxNode = syntaxNode.findChild(_grammar.
              TERMINAL_OP_COMP);
81        SyntaxNode rightExpSyntaxNode = syntaxNode.findChild(_grammar.
              NON_TERMINAL_EXP, 1);
82
83        if ((leftExpSyntaxNode != null) && (expCompOpSyntaxNode != null) && (
              rightExpSyntaxNode != null)) {
84          Exp leftExpNode = (Exp) transform(leftExpSyntaxNode);
85          ExpCompOp expCompOpNode = (ExpCompOp) transform(expCompOpSyntaxNode);
86          Exp rightExpNode = (Exp) transform(rightExpSyntaxNode);
87
88          newNode = new ExpComp(leftExpNode, expCompOpNode, rightExpNode);
89        }
90      } else if (subRule.equals(_grammar.RULE_PAREN_BOOL_EXP)) {
91        SyntaxNode boolExpSyntaxNode = syntaxNode.findChild(_grammar.
              NON_TERMINAL_BOOL_EXP);
92
93        if (boolExpSyntaxNode != null) newNode = transform(boolExpSyntaxNode);
```

```
94      }
95    } else if (symbol.equals(_grammar.TERMINAL_BOOL_LIT)) {
96      newNode = new BoolLit((SyntaxNodeTerminal) syntaxNode);
97    } else if (symbol.equals(_grammar.TERMINAL_OP_COMP)) {
98      newNode = new ExpCompOp((SyntaxNodeTerminal) syntaxNode);
99    }
100
101   if (symbol.equals(_grammar.NON_TERMINAL_EXP)) {
102     newNode = transform(syntaxNode.findChild(_grammar.NON_TERMINAL_SUM));
103   } else if (symbol.equals(_grammar.NON_TERMINAL_SUM) || symbol.equals(_grammar.
        NON_TERMINAL_SUM_)) {
104     if (subRule.equals(_grammar.RULE_PROD_SUM_) || subRule.equals(_grammar.
          RULE_OP_PLUS_PROD_SUM_) || subRule.equals(_grammar.RULE_OP_MINUS_PROD_SUM_
          )) {
105       boolean positive = subRule.equals(_grammar.RULE_PROD_SUM_) || subRule.equals
            (_grammar.RULE_OP_PLUS_PROD_SUM_);
106
107       Sum sumNode = new Sum();
108
109       SyntaxNode prodSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_PROD)
            ;
110
111       if (prodSyntaxNode != null) {
112         Exp prodNode = (Exp) transform(prodSyntaxNode);
113
114         if (prodNode != null) {
115           Exp exp = prodNode;
116
117           if (!positive) exp = exp.makeNeg();
118
119           sumNode.addExp(exp);
120         }
121       }
122
123       SyntaxNode sum_SyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_SUM_)
            ;
124
125       if (sum_SyntaxNode != null) {
126         Exp sum_Node = (Exp) transform(sum_SyntaxNode);
127
128         if (sum_Node != null) sumNode.addExp(sum_Node);
129       }
130
131       if (sumNode.getExps().size() > 1) {
132         newNode = sumNode;
133       } else if (!sumNode.getExps().isEmpty()) {
134         newNode = sumNode.getExps().get(0);
135       }
136     }
137   } else if (symbol.equals(_grammar.NON_TERMINAL_PROD) || symbol.equals(_grammar.
        NON_TERMINAL_PROD_)) {
138     if (subRule.equals(_grammar.RULE_POW_PROD_) || subRule.equals(_grammar.
          RULE_OP_MULT_POW_PROD_) || subRule.equals(_grammar.RULE_OP_DIV_POW_PROD_))
           {
139       boolean positive = subRule.equals(_grammar.RULE_POW_PROD_) || subRule.equals
            (_grammar.RULE_OP_MULT_POW_PROD_);
140
141       Prod prodNode = new Prod();
142
143       SyntaxNode powSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_POW);
144
```

```
145       if (powSyntaxNode != null) {
146         Exp powNode = (Exp) transform(powSyntaxNode);
147
148         if (powNode != null) {
149           Exp exp = powNode;
150
151           if (!positive) exp = powNode.makeInv();
152
153           prodNode.addExp(exp);
154         }
155       }
156
157       SyntaxNode prod_SyntaxNode = syntaxNode.findChild(_grammar.
              NON_TERMINAL_PROD_);
158
159       if (prod_SyntaxNode != null) {
160         Exp prod_Node = (Exp) transform(prod_SyntaxNode);
161
162         if (prod_Node != null) prodNode.addExp(prod_Node);
163       }
164
165       if (prodNode.getExps().size() > 1) {
166         newNode = prodNode;
167       } else if (!prodNode.getExps().isEmpty()) {
168         newNode = prodNode.getExps().get(0);
169       }
170     }
171   } else if (symbol.equals(_grammar.NON_TERMINAL_POW) && subRule.equals(_grammar.
        RULE_FACT_POW_)) {
172     SyntaxNode factSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_FACT);
173
174     if (factSyntaxNode != null) {
175       Exp factNode = (Exp) transform(factSyntaxNode);
176
177       SyntaxNode pow_SyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_POW_)
              ;
178
179       if (pow_SyntaxNode != null) {
180         Exp pow_Node = (Exp) transform(pow_SyntaxNode);
181
182         if (pow_Node != null) newNode = new Pow(factNode, pow_Node); else newNode
              = factNode;
183       } else {
184         newNode = factNode;
185       }
186     }
187   } else if (symbol.equals(_grammar.NON_TERMINAL_POW_) && subRule.equals(_grammar.
        RULE_OP_POW_POW)) {
188     SyntaxNode powSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_POW);
189
190     if (powSyntaxNode != null) newNode = transform(powSyntaxNode);
191   } else if (symbol.equals(_grammar.NON_TERMINAL_FACT) && subRule.equals(_grammar.
        RULE_EXP_ELEM_FACT_)) {
192     SyntaxNode expElemSyntaxNode = syntaxNode.findChild(_grammar.
          NON_TERMINAL_EXP_ELEM);
193
194     if (expElemSyntaxNode != null) {
195       SyntaxNode fact_SyntaxNode = syntaxNode.findChild(_grammar.
            NON_TERMINAL_FACT_);
196
197       Exp exp = (Exp) transform(expElemSyntaxNode);
```

```
198
199       while (fact_SyntaxNode != null && fact_SyntaxNode.getSubRule().equals(
              _grammar.RULE_OP_FACT_FACT_)) {
200         fact_SyntaxNode = fact_SyntaxNode.findChild(_grammar.NON_TERMINAL_FACT_);
201
202         exp = new Fact(exp);
203       }
204
205       newNode = exp;
206     }
207   } else if (symbol.equals(_grammar.NON_TERMINAL_EXP_ELEM)) {
208     if (subRule.equals(_grammar.RULE_ID_PARAM_LIST)) {
209       SyntaxNode idSyntaxNode = syntaxNode.findChild(_grammar.TERMINAL_ID);
210
211       SyntaxNode paramListSyntaxNode = syntaxNode.findChild(_grammar.
              NON_TERMINAL_PARAM_LIST);
212
213       Id id = (Id) transform(idSyntaxNode);
214
215       if (id != null) {
216         ParamList paramList = (ParamList) transform(paramListSyntaxNode);
217
218         if (paramList != null) {
219           if (id.getName().equals("fact")) id = new FactId(paramList);
220           if (id.getName().equals("gcd")) id = new GcdId(paramList);
221         }
222
223         newNode = id;
224       }
225     } else if (subRule.equals(_grammar.RULE_EXP_LIT)) {
226       SyntaxNode numSyntaxNode = syntaxNode.findChild(_grammar.TERMINAL_EXP_LIT);
227
228       newNode = transform(numSyntaxNode);
229     } else if (subRule.equals(_grammar.RULE_PARENS_EXP)) {
230       SyntaxNode expSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_EXP);
231
232       newNode = transform(expSyntaxNode);
233     }
234   } else if (symbol.equals(_grammar.TERMINAL_ID)) {
235     newNode = new Id(((SyntaxNodeTerminal) syntaxNode).getToken().getText());
236   } else if (symbol.equals(_grammar.TERMINAL_EXP_LIT)) {
237     newNode = new ExpLit(new BigInteger(((SyntaxNodeTerminal) syntaxNode).getToken
              ().getText()), BigInteger.ONE);
238   } else if (symbol.equals(_grammar.NON_TERMINAL_PARAM_LIST) && subRule.equals(
        _grammar.RULE_PARENS_PARAM_PARAM_LIST_)) {
239     SyntaxNode paramSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_PARAM)
              ;
240
241     if (paramSyntaxNode != null) {
242       ParamList paramListNode = new ParamList();
243
244       SemanticNode paramNode = transform(paramSyntaxNode);
245
246       if (paramNode != null) paramListNode.addParam((Exp) paramNode);
247
248       SemanticNode paramList_Node = transform(syntaxNode.findChild(_grammar.
              NON_TERMINAL_PARAM_LIST_));
249
250       if (paramList_Node != null) paramListNode.addParamList((ParamList)
              paramList_Node);
251
```

```
252       newNode = paramListNode;
253     }
254   } else if (symbol.equals(_grammar.NON_TERMINAL_PARAM_LIST_) && subRule.equals(
        _grammar.RULE_PARAM_SEP_PARAM_PARAM_LIST_)) {
255     SyntaxNode paramSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_PARAM)
          ;
256
257     if (paramSyntaxNode != null) {
258       ParamList paramListNode = new ParamList();
259
260       SemanticNode paramNode = transform(paramSyntaxNode);
261
262       if (paramNode != null) paramListNode.addParam((Exp) paramNode);
263
264       SyntaxNode paramList_SyntaxNode = syntaxNode.findChild(_grammar.
            NON_TERMINAL_PARAM_LIST_);
265
266       if (paramList_SyntaxNode != null) {
267         SemanticNode paramList_Node = transform(paramList_SyntaxNode);
268
269         if (paramList_Node != null) paramListNode.addParamList((ParamList)
              paramList_Node);
270       }
271
272       newNode = paramListNode;
273     }
274   } else if (symbol.equals(_grammar.NON_TERMINAL_PARAM) && subRule.equals(_grammar
        .RULE_EXP)) {
275     newNode = transform(syntaxNode.findChild(_grammar.NON_TERMINAL_EXP));
276   }
277
278   if (symbol.equals(_grammar.NON_TERMINAL_PROG) || symbol.equals(_grammar.
        NON_TERMINAL_PROG_)) {
279     if (subRule.equals(_grammar.RULE_PROG_CMD_PROG_) || subRule.equals(_grammar.
          RULE_PROG__SEP_CMD_PROG_)) {
280       SyntaxNode cmdSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_CMD);
281
282       Comp comp = new Comp();
283
284       if (cmdSyntaxNode != null) {
285         SemanticNode cmdNode = transform(cmdSyntaxNode);
286
287         if (cmdNode != null) comp.addProg((Prog) cmdNode);
288       }
289
290       SyntaxNode prog_SyntaxNode = syntaxNode.findChild(_grammar.
            NON_TERMINAL_PROG_);
291
292       if (prog_SyntaxNode != null) {
293         SemanticNode prog_Node = transform(prog_SyntaxNode);
294
295         if (prog_Node != null) comp.addProg((Prog) prog_Node);
296       }
297
298       if (comp.getChildren().size() > 1) {
299         newNode = comp;
300       } else if (!comp.getChildren().isEmpty()) {
301         newNode = comp.getChildren().get(0);
302       }
303     }
304   } else if (symbol.equals(_grammar.NON_TERMINAL_CMD)) {
```

```
305     if (subRule.equals(_grammar.RULE_CMD_SKIP)) {
306       SyntaxNode skipNode = syntaxNode.findChild(_grammar.NON_TERMINAL_SKIP);
307
308       if (skipNode != null) newNode = transform(skipNode);
309     } else if (subRule.equals(_grammar.RULE_CMD_ASSIGN)) {
310       SyntaxNode assignNode = syntaxNode.findChild(_grammar.NON_TERMINAL_ASSIGN);
311
312       if (assignNode != null) newNode = transform(assignNode);
313     } else if (subRule.equals(_grammar.RULE_CMD_ALT)) {
314       SyntaxNode altNode = syntaxNode.findChild(_grammar.NON_TERMINAL_ALT);
315
316       if (altNode != null) newNode = transform(altNode);
317     } else if (subRule.equals(_grammar.RULE_CMD_WHILE)) {
318       SyntaxNode whileNode = syntaxNode.findChild(_grammar.NON_TERMINAL_WHILE);
319
320       if (whileNode != null) newNode = transform(whileNode);
321     } else if (subRule.equals(_grammar.RULE_HOARE_BLOCK)) {
322       SyntaxNode hoare_blockSyntayNode = syntaxNode.findChild(_grammar.
              NON_TERMINAL_HOARE_BLOCK);
323
324       if (hoare_blockSyntayNode != null) newNode = transform(hoare_blockSyntayNode
              );
325     }
326   } else if (symbol.equals(_grammar.NON_TERMINAL_SKIP) && subRule.equals(_grammar.
        RULE_SKIP)) {
327     newNode = new Skip();
328   } else if (symbol.equals(_grammar.NON_TERMINAL_ASSIGN) && subRule.equals(
        _grammar.RULE_ASSIGN)) {
329     SyntaxNode idSyntaxNode = syntaxNode.findChild(_grammar.TERMINAL_ID);
330     SyntaxNode expSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_EXP);
331
332     if ((idSyntaxNode != null) && (expSyntaxNode != null)) {
333       SemanticNode idNode = transform(idSyntaxNode);
334       SemanticNode expNode = transform(expSyntaxNode);
335
336       newNode = new Assign((Id) idNode, (Exp) expNode);
337     }
338   } else if (symbol.equals(_grammar.NON_TERMINAL_ALT) && subRule.equals(_grammar.
        RULE_ALT)) {
339     SyntaxNode boolExpSyntaxNode = syntaxNode.findChild(_grammar.
          NON_TERMINAL_BOOL_EXP);
340     SyntaxNode thenProgSyntaxNode = syntaxNode.findChild(_grammar.
          NON_TERMINAL_PROG);
341     SyntaxNode alt_elseSyntaxNode = syntaxNode.findChild(_grammar.
          NON_TERMINAL_ALT_ELSE);
342
343     if ((boolExpSyntaxNode != null) && (thenProgSyntaxNode != null) && (
          alt_elseSyntaxNode != null)) {
344       SemanticNode boolExpNode = transform(boolExpSyntaxNode);
345       SemanticNode thenProgNode = transform(thenProgSyntaxNode);
346       SemanticNode alt_elseNode = transform(alt_elseSyntaxNode);
347
348       newNode = new Alt((BoolExp) boolExpNode, (Prog) thenProgNode, (Prog)
            alt_elseNode);
349     }
350   } else if (symbol.equals(_grammar.NON_TERMINAL_ALT_ELSE) && subRule.equals(
        _grammar.RULE_ALT_ELSE)) {
351     SyntaxNode progSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_PROG);
352
353     if (progSyntaxNode != null) {
354       SemanticNode progNode = transform(progSyntaxNode);
```

```
355
356       if (progNode != null) newNode = progNode;
357     }
358   } else if (symbol.equals(_grammar.NON_TERMINAL_WHILE) && subRule.equals(_grammar
        .RULE_WHILE)) {
359     SyntaxNode boolExpSyntaxNode = syntaxNode.findChild(_grammar.
          NON_TERMINAL_BOOL_EXP);
360     SyntaxNode progSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_PROG);
361
362     if ((boolExpSyntaxNode != null) && (progSyntaxNode != null)) {
363       SemanticNode boolExpNode = transform(boolExpSyntaxNode);
364       SemanticNode progNode = transform(progSyntaxNode);
365
366       newNode = new While((BoolExp) boolExpNode, (Prog) progNode);
367     }
368   }
369
370   if (symbol.equals(_grammar.NON_TERMINAL_HOARE_BLOCK) && subRule.equals(_grammar.
        RULE_HOARE_PRE_PROG_HOARE_POST)) {
371     SyntaxNode hoare_preSyntaxNode = syntaxNode.findChild(_grammar.
          NON_TERMINAL_HOARE_PRE);
372     SyntaxNode progSyntaxNode = syntaxNode.findChild(_grammar.NON_TERMINAL_PROG);
373     SyntaxNode hoare_postSyntaxNode = syntaxNode.findChild(_grammar.
          NON_TERMINAL_HOARE_POST);
374
375     if ((hoare_preSyntaxNode != null) && (progSyntaxNode != null) && (
          hoare_postSyntaxNode != null)) {
376       SemanticNode hoare_preNode = transform(hoare_preSyntaxNode);
377       SemanticNode progNode = transform(progSyntaxNode);
378       SemanticNode hoare_postNode = transform(hoare_postSyntaxNode);
379
380       newNode = new HoareBlock((HoareCond) hoare_preNode, (Prog) progNode, (
            HoareCond) hoare_postNode);
381     }
382   } else if (symbol.equals(_grammar.NON_TERMINAL_HOARE_PRE) || symbol.equals(
        _grammar.NON_TERMINAL_HOARE_POST)) {
383     if (subRule.equals(_grammar.RULE_HOARE_PRE_CURLIES_BOOL_EXP_CURLY_CLOSE) ||
          subRule.equals(_grammar.RULE_HOARE_POST_CURLY_OPEN_BOOL_EXP_CURLY_CLOSE))
          {
384       SyntaxNode boolExpSyntaxNode = syntaxNode.findChild(_grammar.
            NON_TERMINAL_BOOL_EXP);
385
386       if (boolExpSyntaxNode != null) {
387         SemanticNode boolExpNode = transform(boolExpSyntaxNode);
388
389         newNode = new HoareCond((BoolExp) boolExpNode);
390       }
391     }
392   }
393
394   if (newNode != null) newNode._syntax = syntaxNode;
395
396   return newNode;
397 }
```

Listing L26: Transformation to semantic tree (Java)

Appendix D

Hoare listing

```
1  private class HoareNode {
2    private SyntaxTreeNode _actualNode;
3
4    private Vector<HoareNode> _children = new Vector<>();
5
6    public Vector<HoareNode> getChildren() {
7      return _children;
8    }
9
10   public void addChild(HoareNode child) {
11     _children.add(child);
12   }
13
14   public HoareNode(SyntaxTreeNode actualNode) {
15     _actualNode = actualNode;
16   }
17 }
18
19 private Vector<HoareNode> collectChildren(SyntaxTreeNode node) {
20   Vector<HoareNode> ret = new Vector<>();
21
22   for (SyntaxTreeNode child : node.getChildren()) {
23     Vector<HoareNode> hoareChildren = collectChildren(child);
24
25     ret.addAll(hoareChildren);
26   }
27
28   if ((node.getSymbol() != null) && node.getSymbol().equals(_grammar.
       nonTerminal_hoare_block)) {
29     HoareNode selfNode = new HoareNode(node);
30
31     for (HoareNode child : ret) {
32       selfNode.addChild(child);
33     }
34
35     ret.clear();
36
37     ret.add(selfNode);
38   }
39
40   return ret;
41 }
42
43 private interface ExecInterface {
44   public void finished() throws HoareException, LexerException, IOException,
       ParserException;
45 }
46
47 public static class Executer {
48   private HoareNode _node;
```

```
49  private int _nestDepth;
50  private HoareWhileGrammar _grammar;
51  private ObservableMap<SyntaxTreeNode, HoareCond> _preCondMap;
52  private ObservableMap<SyntaxTreeNode, HoareCond> _postCondMap;
53  private ExecInterface _callback;
54
55  private Vector<Executer> _execChain = new Vector<>();
56  private Iterator<Executer> _execChainIt;
57
58  public interface ImplicationInterface {
59    public void result(boolean yes) throws HoareException, LexerException,
      IOException, ParserException;
60  }
61
62  public interface InvariantInterface {
63    public void result(HoareCond invariant) throws HoareException, LexerException,
       IOException, ParserException;
64  }
65
66  private boolean check(HoareCond a) throws ScriptException {
67    /*ScriptEngineManager manager = new ScriptEngineManager();
68
69    ScriptEngine engine = manager.getEngineByName("JavaScript");
70
71    System.out.println(engine.eval(a.toString()));
72
73    return true;*/
74    return true;
75  }
76
77  private boolean implicates(HoareCond a, HoareCond b, ImplicationInterface
      callback) throws ScriptException, IOException, HoareException, LexerException,
       ParserException {
78    System.out.println("try␣implication␣" + a + "->" + b);
79
80    //TODO implicit check
81    boolean checkSuccess = false;
82    boolean checkResult = false;
83
84    if (checkSuccess) {
85      callback.result(checkResult);
86    } else {
87      new ImplicationDialog(a, b, callback, false).show();
88    }
89
90    return !check(a) || check(b);
91  }
92
93  private int _wlp_nestDepth = 0;
94  private int _wlp_printDepth = 0;
95
96  private void println_begin() {
97    _wlp_printDepth++;
98  }
99
100 private void println(String s) {
101   System.out.println(StringUtil.repeat("\t", _wlp_printDepth - 1) + s);
102 }
103
104 private void println_end() {
105   _wlp_printDepth--;
```

```
106   }
107
108   private interface wlp_callback {
109     public void result(HoareCond cond) throws IOException, HoareException,
      LexerException, ParserException;
110   }
111
112   private void wlp_assign(HoareCond postCond, String var, SyntaxTreeNode valNode,
      wlp_callback callback) throws IOException, HoareException {
113     println_begin();
114
115     HoareCond preCond = postCond.copy();
116
117     try {
118       Exp val = Exp.fromString(valNode.synthesize());
119
120       preCond.replace(_grammar.TERMINAL_ID, var, val.getBaseEx());
121
122       println("apply␣assignment␣rule:");
123       println("\t" + postCond.toStringEx(var + ":=" + valNode.synthesize()) + "␣"
    + var + "=" + valNode.synthesize() + "␣" + postCond.toStringEx());
124       println("\t->" + preCond.toStringEx() + "␣" + var + "=" + valNode.synthesize
    () + "␣" + postCond.toStringEx());
125
126       println_end();
127
128       callback.result(preCond);
129     } catch (ParserException | LexerException e) {
130       throw new RuntimeException(e);
131     }
132   }
133
134   private void wlp_composite(HoareCond postCond, SyntaxTreeNode first,
      SyntaxTreeNode second, wlp_callback callback) throws HoareException,
      IOException, LexerException, ParserException {
135     println_begin();
136
137     println("applying␣composition␣rule...");
138
139     wlp(second, postCond, new wlp_callback() {
140       @Override
141       public void result(HoareCond midCond) throws IOException, HoareException,
      LexerException, ParserException {
142         wlp(first, midCond, new wlp_callback() {
143           @Override
144           public void result(HoareCond preCond) throws IOException, HoareException
    , LexerException, ParserException {
145             String firstS = first.synthesize().replaceAll("\n", "");
146             String secondS = second.synthesize().replaceAll("\n", "");
147
148             //System.out.println("{" + postCondition + "}" + " -> " + "{" +
      midCondition + "}" + " -> " + "{" + ret + "}");
149             println("apply␣composition␣rule:");
150             println("\t" + preCond.toStringEx() + "␣" + firstS + "␣" + midCond.
      toStringEx() + ",␣" + midCond.toStringEx() + "␣" + secondS + "␣" + postCond.
      toStringEx());
151             println("\t" + "->");
152             println("\t" + preCond.toStringEx() + "␣" + firstS + ";␣" + secondS +
      "␣" + postCond.toStringEx());
153
154             println_end();
```

```
155
156             callback.result(preCond);
157           }
158         });
159       }
160     });
161   }
162
163   private void wlp_alt(HoareCond postCond, HoareCondBoolExpr altCond,
        SyntaxTreeNode first, SyntaxTreeNode second, wlp_callback callback) throws
        IOException, HoareException, LexerException, ParserException {
164     println_begin();
165
166     HoareCond preCond = postCond.copy();
167
168     String firstS = first.synthesize().replaceAll("\n", "");
169     String secondS = second.synthesize().replaceAll("\n", "");
170
171     //TODO
172     println("apply␣alternative␣rule:");
173     println("\t" + new HoareCondAnd(preCond, altCond).toStringEx() + "␣" + firstS
        + "␣" + postCond.toStringEx() + ",␣" + new HoareCondAnd(preCond, new
        HoareCondNeg(altCond)).toStringEx() + "␣" + secondS + "␣" + postCond.
        toStringEx());
174     println("\t" + "->");
175     println("\t" + preCond.toStringEx() + "␣if␣" + "(" + altCond + ")" + "{" +
        firstS + "}" + "␣else␣" + "{" + secondS + "}" + postCond.toStringEx());
176
177     println_end();
178
179     callback.result(preCond);
180   }
181
182   private void wlp_loop_acceptInvariant(HoareCond invariant, SyntaxTreeNode
        loopNode, wlp_callback callback) throws IOException, HoareException,
        LexerException, ParserException {
183     HoareCond loopCond = new HoareCondBoolExpr(loopNode.findChild(_grammar.
        NON_TERMINAL_BOOL_EXP));
184     SyntaxTreeNode body = loopNode.findChild(_grammar.NON_TERMINAL_PROG);
185
186     println("accept␣invariant␣" + invariant);
187
188     HoareCond preCond = new HoareCondAnd(invariant);
189
190     if (preCond==null) throw new RuntimeException("preCond␣null");
191     if (loopCond==null) throw new RuntimeException("loopCond␣null");
192
193     String bodyS = body.synthesize().replaceAll("\n", "");
194
195     println("apply␣loop␣rule:");
196     println("\t" + new HoareCondAnd(preCond, loopCond).toStringEx() + "␣" + bodyS
        + "␣" + preCond.toStringEx());
197     println("\t" + "->");
198     println("\t" + new HoareCondAnd(preCond).toStringEx() + "␣while␣" + "(" +
        loopCond + ")" + "{" + bodyS + "}" + "␣" + new HoareCondAnd(preCond, new
        HoareCondNeg(loopCond)).toStringEx());
199
200     println_end();
201
202     callback.result(preCond);
203   }
```

```
204
205   private void wlp_loop_tryInvariant(SyntaxTreeNode loopNode, HoareCond postCond,
        HoareCond invariantPost, wlp_callback callback) throws HoareException,
        IOException, LexerException, ParserException {
206     //TODO: auto-generate invariants
207
208     if (invariantPost == null) {
209       println("failed␣to␣guess␣invariant:␣ask␣user");
210
211       InvariantDialog diag = new InvariantDialog(_grammar, loopNode, postCond, new
         InvariantInterface() {
212         @Override
213         public void result(HoareCond invariant) throws HoareException, IOException
        , LexerException, ParserException {
214           if (invariant != null) {
215             wlp_loop_acceptInvariant(invariant, loopNode, callback);
216           } else {
217             throw new HoareException("aborted");
218           }
219         }
220       });
221
222       diag.show();
223     } else {
224       println("try␣invariant:␣" + invariantPost);
225
226       wlp(loopNode.findChild(_grammar.NON_TERMINAL_PROG), invariantPost, new
        wlp_callback() {
227         @Override
228         public void result(HoareCond invariantPre) throws HoareException,
        LexerException, IOException, ParserException {
229           println("tried␣invariant␣" + invariantPost + "␣resulted␣in␣" +
        invariantPre);
230
231           ImplicationDialog diag = new ImplicationDialog(invariantPre,
        invariantPost, new ImplicationInterface() {
232             @Override
233             public void result(boolean yes) throws HoareException, LexerException,
         IOException, ParserException {
234               if (yes) {
235                 wlp_loop_acceptInvariant(invariantPre, loopNode, callback);
236               } else {
237                 wlp_loop_tryInvariant(loopNode, postCond, null, callback);
238               }
239             }
240           }, true);
241
242           diag.show();
243         }
244       });
245     }
246   }
247
248   private void wlp_loop(HoareCond postCond, SyntaxTreeNode loopNode, wlp_callback
        callback) throws HoareException, IOException {
249     println_begin();
250
251     try {
252       println("applying␣loop␣rule...␣needs␣invariant");
253
254       //HoareCondition invariantPost = HoareCondition.fromString("erg==2^(y-x)");
```

```
255       HoareCond invariantPost = null;//HoareCond.fromString("y==z!");
256
257       wlp_loop_tryInvariant(loopNode, postCond, invariantPost, callback);
258     } catch (LexerException | ParserException e) {
259       throw new HoareException(e.getMessage());
260     }
261   }
262
263   private void wlp_consequence_pre(HoareCond origPreCond, HoareCond origPostCond,
      SyntaxTreeNode body, HoareCond newPreCond, HoareCond newPostCond, wlp_callback
       callback) throws IOException, HoareException, LexerException, ParserException
       {
264     println_begin();
265
266     String bodyS = body.synthesize().replaceAll("\n", "");
267
268     System.out.println("apply␣consequence␣rule");
269     System.out.println("\t" + newPreCond + "->" + origPreCond + ",␣" +
      origPostCond.toStringEx() + "␣" + bodyS + "␣" + origPostCond.toStringEx() + ",
      ␣" + origPostCond + "->" + newPostCond);
270     System.out.println("\t" + "->");
271     System.out.println("\t" + newPreCond.toStringEx() + "␣" + bodyS + "␣" +
      newPostCond.toStringEx());
272
273     println_end();
274
275     //TODO: for post as well, merged?
276     callback.result(newPreCond);
277   }
278
279   private void wlp(SyntaxTreeNode node, HoareCond postCondV, wlp_callback callback
      ) throws HoareException, IOException, LexerException, ParserException {
280     _wlp_nestDepth++;
281
282     final HoareCond postCond = postCondV.copy();
283
284     _postCondMap.put(node, postCond);
285
286     //System.out.println(StringUtil.repeat("\t", _wlp_nestDepth) + "postcond " +
      node);
287
288     wlp_callback retCallback = new wlp_callback() {
289       @Override
290       public void result(HoareCond cond) throws IOException, HoareException,
      LexerException, ParserException {
291         _preCondMap.put(node, cond);
292         _wlp_nestDepth--;
293
294         callback.result(cond);
295       }
296     };
297
298     if (node.getSymbol().equals(_grammar.NON_TERMINAL_PROG)) {
299       SyntaxTreeNode firstChild = node.getChildren().firstElement();
300       SyntaxTreeNode lastChild = node.getChildren().lastElement();
301
302       if (lastChild.findChild(_grammar.NON_TERMINAL_PROG) != null) {
303         wlp_composite(postCond, firstChild, lastChild.findChild(_grammar.
      NON_TERMINAL_PROG), retCallback);
304       } else {
305         wlp(firstChild, postCond, retCallback);
```

```
306       }
307     } else if (node.getSymbol().equals(_grammar.NON_TERMINAL_PROG_)) {
308       if (node.getSubRule().equals(_grammar.RULE_PROG__PROG))
309         wlp(node.findChild(_grammar.NON_TERMINAL_PROG), postCond, retCallback);
310       else
311         retCallback.result(postCond);
312     } else if (node.getSymbol().equals(_grammar.NON_TERMINAL_SKIP))
313       retCallback.result(postCond);
314     else if (node.getSymbol().equals(_grammar.NON_TERMINAL_ASSIGN)) {
315       SyntaxTreeNode idNode = node.findChild(_grammar.TERMINAL_ID);
316
317       SyntaxTreeNode expNode = node.findChild(_grammar.NON_TERMINAL_EXP);
318
319       String var = idNode.synthesize();
320       SyntaxTreeNode exp = expNode;
321
322       wlp_assign(postCond, var, exp, retCallback);
323     } else if (node.getSymbol().equals(_grammar.NON_TERMINAL_SELECTION)) {
324       if (node.getSubRule().equals(_grammar.RULE_SELECTION)) {
325         SyntaxTreeNode selectionElseRule = node.findChild(_grammar.
    NON_TERMINAL_PROG);
326
327         if (selectionElseRule.getSubRule().equals(Terminal.EPSILON)) {
328           wlp(node.findChild(_grammar.NON_TERMINAL_PROG), postCond, new
    wlp_callback() {
329             @Override
330             public void result(HoareCond thenCond) throws IOException,
    HoareException, LexerException, ParserException {
331               HoareCond elseCond = postCond;
332
333               retCallback.result(new HoareCondOr(thenCond, elseCond));
334             }
335           });
336         } else if (selectionElseRule.getSubRule().equals(_grammar.
    RULE_SELECTION_ELSE)) {
337           wlp(node.findChild(_grammar.NON_TERMINAL_PROG), postCond, new
    wlp_callback() {
338             @Override
339             public void result(HoareCond thenCond) throws IOException,
    HoareException, LexerException, ParserException {
340               wlp(node.findChild(_grammar.NON_TERMINAL_PROG, 2), postCond, new
    wlp_callback() {
341                 @Override
342                 public void result(HoareCond elseCond) throws IOException,
    HoareException, LexerException, ParserException {
343                   retCallback.result(new HoareCondOr(thenCond, elseCond));
344                 }
345               });
346             }
347           });
348         }
349       }
350     } else if (node.getSymbol().equals(_grammar.NON_TERMINAL_WHILE)) {
351       wlp_loop(postCond, node, retCallback);
352     } else if (node.getSymbol().equals(_grammar.nonTerminal_hoare_block)) {
353       wlp(node.findChild(_grammar.NON_TERMINAL_PROG), postCond, retCallback);
354     } else {
355       throw new HoareException("no␣wlp␣for␣" + node + "␣with␣rule␣" + node.
    getSubRule());
356     }
357   }
```

```
358
359   public void exec() throws IOException, HoareException, LexerException,
        ParserException {
360     SyntaxTreeNode preNode = _node._actualNode.findChild(_grammar.
        nonTerminal_hoare_pre);
361     SyntaxTreeNode postNode = _node._actualNode.findChild(_grammar.
        nonTerminal_hoare_post);
362
363     HoareCond preCondition = HoareCond.fromString(preNode.findChild(_grammar.
        NON_TERMINAL_BOOL_EXP).synthesize());
364     HoareCond postCondition = HoareCond.fromString(postNode.findChild(_grammar.
        NON_TERMINAL_BOOL_EXP).synthesize());
365
366     System.err.println(StringUtil.repeat("\t", _nestDepth) + "checking␣" +
        preCondition + "->" + postCondition + "␣at␣" + _node);
367
368     _wlp_nestDepth = 0;
369     _wlp_printDepth = 0;
370
371     wlp(_node._actualNode, postCondition, new wlp_callback() {
372       @Override
373       public void result(HoareCond finalPreCondition) throws IOException,
        HoareException, LexerException, ParserException {
374         System.out.println("final␣preCondition:␣" + finalPreCondition);
375
376         try {
377           implicates(preCondition, finalPreCondition, new ImplicationInterface() {
378             @Override
379             public void result(boolean yes) throws HoareException, LexerException,
         IOException, ParserException {
380               if (yes) {
381                 System.out.println(preCondition + "->" + postCondition + "␣holds␣
        true␣(wlp:␣" + finalPreCondition + ")");
382               } else {
383                 System.out.println(preCondition + "->" + postCondition + "␣failed␣
        (wlp:␣" + finalPreCondition + ")");
384               }
385
386               _callback.finished();
387             }
388           });
389         } catch (ScriptException e) {
390           e.printStackTrace();
391         }
392       }
393     });
394   }
395
396   public void start() throws IOException, HoareException, LexerException,
        ParserException {
397     _execChainIt.next().exec();
398   }
399
400   public Executer(HoareNode node, int nestDepth, HoareWhileGrammar grammar,
        ObservableMap<SyntaxTreeNode, HoareCond> preCondMap, ObservableMap<
        SyntaxTreeNode, HoareCond> postCondMap, ExecInterface callback) throws
        IOException, HoareException, NoRuleException, LexerException {
401     _node = node;
402     _nestDepth = nestDepth;
403     _grammar = grammar;
404     _preCondMap = preCondMap;
```

```
405     _postCondMap = postCondMap;
406     _callback = callback;
407 
408     ExecInterface childCallback = new ExecInterface() {
409       @Override
410       public void finished() throws HoareException, LexerException, IOException,
    ParserException {
411         Executer next = _execChainIt.next();
412 
413         next.exec();
414       }
415     };
416 
417     for (HoareNode child : node.getChildren()) {
418       _execChain.add(new Executer(child, nestDepth + 1, _grammar, preCondMap,
    postCondMap, childCallback));
419     }
420 
421     _execChain.add(this);
422 
423     _execChainIt = _execChain.iterator();
424   }
425 }
426 
427 private Vector<Executer> _execChain;
428 private Iterator<Executer> _execChainIt;
429 
430 public void exec() throws HoareException, LexerException, IOException,
    ParserException {
431   System.err.println("hoaring...");
432 
433   Vector<HoareNode> children = collectChildren(_tree.getRoot());
434 
435   if (children.isEmpty()) {
436     System.err.println("no␣hoareBlocks");
437   } else {
438     _execChain = new Vector<>();
439 
440     for (HoareNode child : children) {
441       if (children.lastElement().equals(child)) {
442         _execChain.add(new Executer(child, 0, _grammar, _preCondMap, _postCondMap,
     new ExecInterface() {
443           @Override
444           public void finished() throws HoareException, NoRuleException,
    LexerException, IOException {
445             System.err.println("hoaring␣finished");
446           }
447         }));
448       } else {
449         _execChain.add(new Executer(child, 0, _grammar, _preCondMap, _postCondMap,
     new ExecInterface() {
450           @Override
451           public void finished() throws IOException, HoareException,
    LexerException, ParserException {
452             _execChainIt.next().exec();
453           }
454         }));
455       }
456     }
457 
458     Iterator<Executer> execChainIt = _execChain.iterator();
```

```
459
460       execChainIt.next().exec();
461     }
462 }
```

Listing L27: ***Hoare*** (Java)

Appendix E

Grammar for Hoare-decorated while programs

$$
\begin{array}{lll}
\langle exp \rangle & ::= & \langle sum \rangle \\
\langle sum \rangle & ::= & \langle prod \rangle\ \langle sum' \rangle \\
\langle sum' \rangle & ::= & \text{`+'}\ \langle prod \rangle\ \langle sum' \rangle \\
 & | & \text{`-'}\ \langle prod \rangle\ \langle sum' \rangle \\
 & | & \epsilon \\
\langle prod \rangle & ::= & \langle pow \rangle\ \langle prod' \rangle \\
\langle prod' \rangle & ::= & \text{`*'}\ \langle pow \rangle\ \langle prod' \rangle \\
 & | & \text{`/'}\ \langle pow \rangle\ \langle prod' \rangle \\
 & | & \epsilon \\
\langle pow \rangle & ::= & \langle factorial \rangle\ \langle pow' \rangle \\
\langle pow' \rangle & ::= & \text{`\^{}'}\ \langle pow \rangle \\
 & | & \epsilon \\
\langle factorial \rangle & ::= & \langle exp\_elem \rangle\ \langle factorial' \rangle \\
\langle factorial' \rangle & ::= & \text{`!'} \\
 & | & \epsilon \\
\langle exp\_elem \rangle & ::= & \langle id \rangle\ \langle param\_list \rangle \\
 & | & \langle exp\_lit \rangle \\
 & | & \text{`('}\ \langle exp \rangle\ \text{`)'} \\
\langle param\_list \rangle & ::= & \text{`('}\ \langle param \rangle\ \langle param\_list' \rangle\ \text{`)'} \\
 & | & \epsilon \\
\langle param\_list' \rangle & ::= & \text{`;'}\ \langle param \rangle\ \langle param\_list' \rangle \\
 & | & \epsilon \\
\langle param \rangle & ::= & \langle exp \rangle \\
\langle exp\_lit \rangle & ::= & \text{[1-9][0-9]*} \\
 & | & \text{`0'}
\end{array}
$$

⟨*id*⟩ ::= [a-zA-Z][a-zA-Z0-9]*

⟨*bool_exp*⟩ ::= ⟨*bool_or*⟩

⟨*bool_or*⟩ ::= ⟨*bool_and*⟩ ⟨*bool_or'*⟩

⟨*bool_or'*⟩ ::= '|' ⟨*bool_and*⟩ ⟨*bool_or'*⟩
| ϵ

⟨*bool_and*⟩ ::= ⟨*bool_neg*⟩ ⟨*bool_and'*⟩

⟨*bool_and'*⟩ ::= '&' ⟨*bool_neg*⟩ ⟨*bool_and'*⟩
| ϵ

⟨*bool_neg*⟩ ::= ⟨*bool_elem*⟩
| '~' ⟨*bool_elem*⟩

⟨*bool_elem*⟩ ::= ⟨*exp*⟩ '<' ⟨*exp*⟩
| 'true'
| '[' ⟨*bool_exp*⟩ ']'

⟨**prog*⟩ ::= ⟨*cmd*⟩ ⟨*prog'*⟩

⟨*prog'*⟩ ::= ';' ⟨*cmd*⟩ ⟨*prog'*⟩
| ϵ

⟨*cmd*⟩ ::= ⟨*skip*⟩
| ⟨*assign*⟩
| ⟨*alt*⟩
| ⟨*while*⟩

⟨*skip*⟩ ::= 'SKIP'

⟨*assign*⟩ ::= ⟨*id*⟩ ':=' ⟨*exp*⟩

⟨*alt*⟩ ::= 'IF' ⟨*bool_exp*⟩ 'THEN' ⟨*prog*⟩ ⟨*alt_else*⟩ 'FI'

⟨*alt_else*⟩ ::= 'ELSE' ⟨*prog*⟩
| ϵ

⟨*while*⟩ ::= 'WHILE' ⟨*bool_exp*⟩ 'DO' ⟨*prog*⟩ 'OD'

⟨*hoare_block*⟩ ::= ⟨*hoare_pre*⟩ ⟨*prog*⟩ ⟨*hoare_post*⟩

⟨*hoare_pre*⟩ ::= 'PRE' '{' ⟨*bool_exp*⟩ '}'

⟨*hoare_post*⟩ ::= 'POST' '{' ⟨*bool_exp*⟩ '}'

Declaration of Originality

I hereby confirm that I have written the accompanying thesis by myself, without contributions from any sources other than those cited in the text and acknowledgements. This applies also to all graphics, drawings, maps and images included in the thesis.

Merseburg, November 1, 2017

.....	.....
Place and date	*Signature*