A proof theory for a sequential version of POOL

by

Pierre America   Frank S. de Boer

90/12

October, 1990
This is a series of notes of the Computing Science Section of the Department of Mathematics and Computing Science Eindhoven University of Technology. Since many of these notes are preliminary versions or may be published elsewhere, they have a limited distribution only and are not for review. Copies of these notes are available from the author or the editor.

Eindhoven University of Technology
Department of Mathematics and Computing Science
P.O. Box 513
5600 MB EINDHOVEN
The Netherlands
All rights reserved
Editors: prof.dr.M.Rem
         prof.dr.K.M. van Hee
A proof theory for a sequential version of POOL

Pierre America and Frank de Boer
Contents

1 Introduction 2

2 The language SPOOL 4
   2.1 An informal introduction 4
   2.2 The syntax 5

3 Semantics 10
   3.1 Domain definitions 10
   3.2 The semantic functions 13
   3.3 Remarks on the semantics 19

4 The assertion language and its semantics 23
   4.1 The assertion language 23
   4.2 Semantics of assertions and correctness formulae 25

5 The proof system 30
   5.1 Simple assignments 30
   5.2 Creating new objects 35
   5.3 Sending messages 43
   5.4 Other axioms and rules 51

6 Completeness 54
   6.1 Introduction 54
   6.2 The strongest postcondition 61
6.3 Freezing the initial state ........................................ 64
6.4 Invariance ......................................................... 68
6.5 Most general correctness formulae ......................... 71
6.6 The context switch ............................................... 81

7 Conclusions .......................................................... 90

References .............................................................. 91

A A generalisation of the rule (MR) .............................. 92

B Expressibility .......................................................... 95
   B.1 Coding mappings ............................................... 95
   B.2 Arithmetizing Truth ............................................ 96
   B.3 Expressing the coding relationship ....................... 100
   B.4 Expressing the strongest postcodition .................. 101

C A closure property of the semantics ......................... 104
1 Introduction

This document explores the possibilities of giving a Hoare-style proof system for a language, called SPOOL, which is a sequential version of the language POOL [1]. SPOOL is an object-oriented language, just like POOL, but it is sequential, so that we do not have to deal with the specific problems connected with parallelism (it turns out that the other problems are already difficult enough).

The main aspect of SPOOL that is dealt with is the problem of how to reason about pointer structures. In SPOOL, objects can be created at arbitrary points in a program, references to them can be stored in variables and passed around as parameters in messages. This implies that complicated and dynamically evolving structures of references between objects can occur. We want to reason about these structures on an abstraction level that is at least as high as that of the programming language. In more detail, this means the following:

- The only operations on "pointers" (references to objects) are
  - testing for equality
  - dereferencing (looking at the value of an instance variable of the referenced object)
- In a given state of the system, it is only possible to mention the objects that exist in that state. Objects that do not (yet) exist never play a role.

Strictly speaking, direct dereferencing is not even allowed in the programming language, because each object only has access to its own instance variables. However, for the time being we allow it in the assertion language. Otherwise, even more advanced techniques would be necessary to reason about the correctness of a program.

The above restrictions have quite severe consequences for the proof system. The limited set of operations on pointers implies that first-order logic is too weak to express some interesting properties of pointer structures (for example, the fact that it is possible to go from $w$ to $z$ by following a finite number of $x$-links). It is surely too weak to apply the standard techniques in proofs of completeness of a proof system, where arbitrarily long computation sequences are coded into a finite set of variables.

Therefore we have to extend our assertion language to make it more expressive. We considered two approaches:

- Using recursively defined predicates, by which the above "interesting" properties of pointer structures can be expressed quite easily. This approach is worked out in [2].
• Allowing the assertion language to reason about finite sequences of objects. In this way the above properties can also be expressed (but not quite so elegantly). This approach is studied in this report.

In section 2 we shall present the syntax of this language SPOOL. Then, in section 3 we shall give a denotational semantics for it. In section 4 we introduce an assertion language, using quantification over finite sequences of objects, in which properties of states in a computation can be formulated, and we formally define its semantics. After that, in section 5, we present a Hoare-style proof system for SPOOL using this assertion language. This proof system is proved to be sound with respect to the denotational semantics. In section 6 we prove the completeness of the system. Finally, in section 7, some conclusions are drawn from the present work.
2 The language SPOOL

2.1 An informal introduction

The shortest description of the language SPOOL would be that it results from omitting the body of each class in POOL-T [1]. The most important consequence of this is that the parallelism, present in POOL-T, disappears. But let us try to give a short, independent description of SPOOL.

The most important concept is the concept of an object. This is an entity containing data and procedures (methods) acting on these data. The data are stored in variables, which come in two kinds: instance variables, whose lifetime is the same as that of the object they belong to, and temporary variables, which are local to a method and last as long as the method is active. Variables can contain references to other objects in the system (or even the object under consideration itself). The object a variable refers to (its value) can be changed by an assignment. The value of a variable can also be nil, which means that it refers to no object at all.

The variables of an object cannot be accessed directly by other objects. The only way for objects to interact is by sending messages to each other. If an object sends a message, it specifies the receiver, a method name, and possibly some parameter objects. Then control is transferred from the sender object to the receiver. This receiver then executes the specified method, using the parameters in the message. Note that this method can, of course, access the instance variables of the receiver. The method returns a result, an object, which is sent back to the sender. Then control is transferred back to the sender which resumes its activities, possibly using this result object.

The sender of a message is blocked until the result comes back, that is, it cannot answer any message while it still has an outstanding message of its own. Therefore, when an object sends a message to itself (directly or indirectly) this will lead to abnormal termination of the program. This is an important difference with some other object-oriented languages, like Smalltalk-80 [6].

Objects are grouped into classes. Objects in one class (the instances of the class) share the same methods, so in a certain sense they share the same behaviour. New instances of a given class can be created at any time. There are two standard classes, Int and Bool, of integers and booleans, respectively. They differ from the other classes in that their instances already exist at the beginning of the execution of the program and no new ones can be created. Moreover, some standard operations on these classes are defined.

A program essentially consists of a number of class definitions, together with a statement to be executed by an instance of a specific class. Usually, but not necessarily, this
instance is the only non-standard object that exists at the beginning of the program: the others still have to be created.

2.2 The syntax

In order to describe the language SPOOL, which is strongly typed, we use typed versions of all variables, expressions, etc. These types are indicated by subscripts or superscripts in this language description. Often, when this typing information is redundant, it is omitted. Of course, for a practical version of the language, a syntactical variant, in which the type of each variable is indicated by a declaration, is easier to use.

Assumption 2.1
We assume the following sets to be given:

- A set $C$ of class names, with typical element $c$ (this means that metavariables like $c, c', c_1, \ldots$ range over elements of the set $C$. We assume that Int, Bool \notin C and define the set $C^+ = C \cup \{\text{Int}, \text{Bool}\}$ with typical element $d$.

- For each $c \in C$ and $d \in C^+$ we assume a set $IVar_c^d$ of instance variables of type $d$ in class $c$. By this we mean that such a variable may occur in the definition of class $c$ and that its contents will be an object of type $d$. The set $IVar_c^d$ will have as a typical element $x_d^c$.

- For each $d \in C$ we assume a set $TVar_d$ of temporary variables of type $d$, with typical element $u_d$.

- We shall let the metavariable $n$ range over elements of $\mathbb{Z}$, the set of whole numbers.

- For each $c \in C$ and $d_0, \ldots, d_n \in C^+$ ($n \geq 0$) we assume a set $MName_{d_0, \ldots, d_n}^c$ of method names of class $c$ with result type $d_0$ and parameter types $d_1, \ldots, d_n$. The set $MName_{d_0, \ldots, d_n}^c$ will have $m_{d_0, \ldots, d_n}^c$ as a typical element.

Now we can specify the syntax of our language. We start with the expressions:

Definition 2.2
For any $c \in C$ and $d \in C^+$ we define the set $Exp_d^c$ of expressions of type $d$ in class $c$, with typical element $e_d^c$, as follows:
\[
e_d^e ::= \begin{array}{l}
x_d^e \\
u_d \\
il_d \\
sel_d \quad \text{if } c = d \\
true | false \quad \text{if } d = \text{Bool} \\
n \quad \text{if } d = \text{Int} \\
e_1^d \equiv e_2^d \quad \text{if } d = \text{Bool} \\
e_1^d + e_2^d \quad \text{if } d = \text{Int} \\
\vdots \\
e_1^d < e_2^d \quad \text{if } d = \text{Bool} \\
\vdots
\end{array}
\]

The intuitive meaning of these expressions will probably be clear from section 2.1. Note that in the language we put a dot over the equal sign (\(\equiv\)) to distinguish it from the equality sign we use in the meta-language.

**Definition 2.3**

The set \(SExp_d^c\) of expressions with possible side effect of type \(d\) in class \(c\), with typical element \(s_d^e\), is defined as follows:

\[
s_d^e ::= \begin{array}{l}
e_d^e \\
\text{new}_d \quad \text{if } d \in C \ (d \neq \text{Int, Bool}) \\
e_0^c ! m_{d_1,d_2,\ldots,d_n}(e_1^c,\ldots,e_n^c) \ (n \geq 0)
\end{array}
\]

The first kind of side effect expression is a normal expression, which has no actual side effect, of course. The second kind is the creation of a new object. This new object will also be the value of the side effect expression. The third kind of side effect expression specifies that a message is to be sent to the object that results from \(e_0\), with method name \(m\) and with arguments (the objects resulting from) \(e_1, \ldots, e_n\).

**Definition 2.4**

The set \(Stat_c^c\) of statements in class \(c\), with typical element \(S_d^c\), is defined by:

\[
S_d^c ::= \begin{array}{l}
x_d^e \\
u_d^e \\
s_d^e \\
S_1^e ; S_2^e \\
\text{if } e^c \text{ then } S_1^e \text{ [else } S_2^e \text{]} \text{ fi} \\
\text{while } e^c \text{ do } S_c^c \text{ od}
\end{array}
\]

Again, the intuitive meaning of these statements will probably be clear. Note that a side effect expression \(s\) may occur in the place of a statement. This means that \(s\) is
evaluated and then its value is discarded, so that only the side effect remains. If in
a conditional statement the else-part is absent, the statement is interpreted as if it
contained else nil.

**Definition 2.5**
The set $\text{MethDef}_{d_0, \ldots, d_n}$ of method definitions of class $c$ with result type $d_0$ and
parameter types $d_1, \ldots, d_n$ (with typical element $\mu_{d_0, \ldots, d_n}$) is defined by:

$$\mu_{d_0, \ldots, d_n} ::= (u_{1d_1}, \ldots, u_{nd_n}) : S^c \uparrow e^c_{d_0}$$

Here we require that the $u_{id_i}$ are all different and that none of them occurs at the left
hand side of an assignment in $S^c$ (and, of course, that $n \geq 0$).

When an object is sent a message, the method named in the message is invoked as
follows: The variables $u_1, \ldots, u_n$ (the parameters of the methods) are given the values
specified in the message, all other temporary variables are initialized to nil, and then
the statement $S$ is executed. After that the expression $e$ is evaluated and its value,
the result of the method, is sent back to the sender of the message, where it will be
the value of the send-expression that sent the message.

**Definition 2.6**
The set $\text{ClassDef}_{c_1, \ldots, c_m}$ of class definitions of class $c$ defining methods $m_1, \ldots, m_n$, with typical element $D_{c_1, \ldots, c_m}$, is defined by:

$$D_{c_1, \ldots, c_m} ::= c : (m_1^c \leftarrow \mu_1^c, \ldots, m_n^c \leftarrow \mu_n^c)$$

where we require that all the method names are different (and $n \geq 0$).

**Definition 2.7**
The set $\text{Unit}_{c_1, \ldots, c_m}$ of units with classes $c_1, \ldots, c_n$ defining methods $m_1, \ldots, m_k$, with typical element $U_{c_1, \ldots, c_m}$, is defined by:

$$U_{c_1, \ldots, c_m} ::= D_{c_1} \ldots D_{c_m}$$

where $m_1, \ldots, m_k = m_1, \ldots, m_n$. We require that all the class names are different.

**Definition 2.8**
Finally, the set $\text{Prog}^c$ of programs in class $c$, with typical element $\rho^c$, is defined by:

$$\rho^c ::= (U_{c_1, \ldots, c_m} : S^c)$$

Here we require that $c$ occurs in $c_1, \ldots, c_n$. (The symbol ‘|’ is part of the syntax, not
of the meta-syntax.)

The interpretation of such a program is that the statement $S$ is executed by some
object of class $c$ (the root object) in the context of the declarations contained in the
unit $U$. In many cases (including the following example) we shall assume that at the
beginning of the execution this root object is the only existing non-standard object.
Example 2.9
The following program generates prime numbers using the sieve method of Eratosthenes. We assume the following symbols:

- The class name Sieve ∈ C (abbreviated sometimes by c₁) with instance variables p ∈ IVar^{c₁} and next ∈ IVar^{c₁}, temporary variable q ∈ TVar and method name input ∈ MName^{c₁}.

- The class name Driver ∈ C (abbreviated by c₂) with instance variables i, bound ∈ IVar^{c₂} and first ∈ IVar^{c₂}.

Then this is the program:

```plaintext
(Sieve: (input ⇔ (q) : if next = nil
   then next ← new;
   p ← q
   else if q mod p ≠ 0
       then next ! input(q)
   fi
  fi
  † self
),
Driver: ⟨⟩
| Driver : i ← 2;
   first ← new;
   while i < bound
   do first ! input(i);
       i ← i + 1
   od
)
```

Figure 1 represents the system in a certain stage of the execution of the program.
Figure 1: Objects in the sieve program in a certain stage of the execution
3 Semantics

3.1 Domain definitions

Definition 3.1
We assume for every \( c \in C \) an infinite set \( O^c \) of object names of class \( c \), with typical element \( \beta^c \). We define \( P^c \) to be the set of all finite subsets of \( O^c \), with typical element \( \pi^c \). Furthermore we assume a function \( \text{pick}^c : P^c \to O^c \) which satisfies
\[
\forall \pi^c \in P^c : \text{pick}^c(\pi^c) \notin \pi^c.
\]
This function will be used to generate the name of a new object, whenever one is created.

For the standard classes \( \text{Int} \) and \( \text{Bool} \) we define the sets of object names as follows:
\[
O = \mathbb{Z} \\
O = B = \{t, f\}
\]
(We shall not need functions \( \text{pick} \) or \( \text{pick} \).)

Definition 3.2
For every set \( X \) we define the corresponding flat domain \( X_\perp \) to be the set \( X \cup \{\bot\} \), equipped with an ordering \( \sqsubseteq \) defined by
\[
x \sqsubseteq y \iff x = \bot \lor x = y.
\]
Note that for every set \( X \), \( X_\perp \) is a complete partial order (cpo). Sometimes we shall only consider the underlying set of this ordering, for example in definition 3.4.

Definition 3.3
We shall often use generalized Cartesian products of the form
\[
\prod_{i \in A} B(i).
\]
As usual, each element of this set is a function \( f \) with domain \( A \) such that \( f(i) \in B(i) \) for each \( i \in A \). We shall sometimes write \( f[i] \) for \( f(i) \) if \( i \in A \) and \( f \in \prod_{i \in A} B(i) \), and also we sometimes write \( (f(i))_{i \in A} \) for \( \lambda(i \in A).f(i) \). Finite products are special cases: If \( A \) is of the form \( \{1, \ldots, n\} \) we sometimes write \( B(1) \times \cdots \times B(n) \).

Definition 3.4
We define the set \( \Sigma \) of states, with typical element \( \sigma \), as follows:
\[
\Sigma = \prod_c P^c \times \prod_d \left( O^c \to IVar_d^c \to O_1^d \right) \times \prod_d \left( TVar_d \to O_1^d \right)
\]
A little explanation is surely required here. A state \( \sigma \in \Sigma \) records the values of the variables in the whole system at a certain point in the computation:
• Its first component $\sigma_{(1)}$ gives for every class $c \in C$ a finite set of objects $\sigma_{(1)(c)} \in \mathbb{P}^c$. This set represents the objects that exist in this state (i.e., they have already been created).

• The second component $\sigma_{(2)}$ records the values of the instance variables. More concretely, if $c \in C$ and $d \in C^+$ are class names, $\beta^c \in \mathcal{O}^c$ is an object of class $c$, and $x^c_d \in IVar^c_d$ is an instance variable of type $d$ in class $c$, then $\sigma_{(2)(c,d)}(\beta^c)(x^c_d) \in \mathcal{O}^d_\bot$ is the value of the instance variable $x^c_d$ of object $\beta^c$. If this value is $\bot$, this means that the variable refers to no object. This is the situation for a variable that has not been initialized, but it can also be achieved by assigning nil to it.

• The third component $\sigma_{(3)}$ records the values of the temporary variables. More concretely again, if $d \in C^+$ is a class name and $u_d \in TVar_d$ is a temporary variable of type $d$, then $\sigma_{(3)(d)}(u_d) \in \mathcal{O}^d_\bot$ is the value of the variable $u_d$. Here again, it is possible that the value of the variable is nil.

For any state $\sigma$ we introduce by convention that $\sigma_{(1)(c)} = \mathbb{Z}$ and $\sigma_{(3)(c)} = \mathbb{B}$. Furthermore we write $\sigma^{(c)}$ for $\sigma_{(1)(d)}$.

**Definition 3.5**
Note that in general it is possible that in a state the variables of an existing object refer to an object that does not exist. If this is not the case and, additionally, the variables of the non-existing objects are not initialized, we say that the state is consistent. More precisely, we call a state $\sigma$ consistent if

- $\forall c \in C \forall \beta^c \in \sigma^{(c)} \forall c' \in C \forall x_{c'}^c \in IVar^c_{c'} \sigma_{(2)(c,c')}(\beta^c)(x_{c'}^c) \in \sigma^{(c')}_{\bot}$
- $\forall c \in C \forall u_c \in TVar_c \sigma_{(3)(c)}(u_c) \in \sigma^{(c)}_{\bot}$
- $\forall c \in C \forall \beta^c \in \mathcal{O}^c \setminus \sigma^{(c)} \forall d \in C^+ \forall x_{c'}^d \in IVar_{c'}^d \sigma_{(2)(c,d)}(\beta^c)(x_{c'}^d) = \bot$

(Note that it would not make sense for either $c$ or $c'$ to be Int or Bool). We shall occasionally use the shorthand $OK(\sigma)$ to indicate that $\sigma$ is consistent.

**Definition 3.6**
We say that a state $\sigma'$ extends a state $\sigma$ (notation $\sigma \preceq \sigma'$) if $\forall c \in C \ \sigma^{(c)} \subseteq \sigma'^{(c)}$.

**Definition 3.7**
We shall make flexible use of the so-called variant notation, especially in connection with states. The variant notation is a short way to express a new state that arises when some component of an old state is modified. For example, if we write

$$\sigma' = \sigma\{\beta_1^d / \beta_2^c, x_{c'}^d\}$$
this means the following:

\[
\begin{align*}
\sigma'(1) &= \sigma(1) \\
\sigma'(2)(c,d)(\beta_2)(x) &= \beta_1 \\
\sigma'(2)(c,d)(\beta_2)(x') &= \sigma(2)(c,d)(\beta_2)(x') \quad \text{if } x' \neq x \\
\sigma'(2)(c,d)(\beta') &= \sigma(2)(c,d)(\beta') \quad \text{if } \beta' \neq \beta_2 \\
\sigma'(2)(c',d') &= \sigma(2)(c',d') \\
\sigma'(3) &= \sigma(3)
\end{align*}
\]

(This example also illustrates the usefulness of this notation.)

**Definition 3.8**

The set \( \Delta^c \) of contexts of class \( c \), with typical element \( \delta^c \), is defined as follows:

\[
\Delta^c = O^c \times \prod_{c'} P^c
\]

The meaning of a context \( \delta^c \) is as follows:

- The first component \( \delta^c(1) \in O^c \) indicates the object that is currently executing (the object denoted by self).
- The second component \( \delta^c(2) \) represents all the objects that are waiting for the result of a message they have sent. This is because these objects become blocked, that is, they cannot answer any message before they have received the result of their outstanding message. If \( c' \in C \) is a class name, then \( \delta^c(2)(c') \in P^c \) is the set of blocked objects of class \( c' \).

**Definition 3.9**

We say that a context \( \delta^c \) agrees with a state \( \sigma \) if

- \( \delta^c(1) \in \sigma(c) \)
- \( \forall c' \in C \quad \delta^c(2)(c') \subseteq \sigma(c') \)

We shall write the shorthand \( OK(\sigma, \delta) \) to indicate that \( \sigma \) is consistent and \( \delta \) agrees with \( \sigma \).

**Definition 3.10**

The domain \( \Gamma \) of environments, with typical element \( \gamma \), is defined as follows:

\[
\Gamma = \prod_{c,d_0,\ldots,d_n} \left( MName_{c_0,\ldots,c_n} \rightarrow \left( \prod_{i=1}^n O^i \right) \rightarrow \Delta^c \rightarrow \Sigma \rightarrow \left( \Sigma^c \times O^\Sigma \right) \right)
\]
An environment $\gamma$ records the meaning of the methods. More concretely, if $c \in C$ and $d_0, \ldots, d_n \in C^+$ are classes, $m \in M$Name$^c_{d_0, \ldots, d_n}$ is a method name, $\bar{\beta} = (\beta_1^{d_1}, \ldots, \beta_n^{d_n}) \in \prod_{i=1}^n \text{O}_{d_i}$ a row of objects (each possibly $\bot$), $\delta \in \Delta^c$ a context, $\sigma \in \Sigma^c$ a state (again possibly $\bot$), then $\gamma_{(c,d)}(m)(\bar{\beta})(\delta)(\sigma)$ is a pair $\langle \sigma', \delta_0 \rangle \in \Sigma^c \times \text{O}_{\delta_0}$, with the intended meaning that if the method named by $m$ is invoked with parameters $\bar{\beta}$, in the context $\delta$ (which indicates among others the object that executes the method), and starting in the state $\sigma$, then after the execution $\sigma'$ will be the new state and $\delta_0$ is the result of the message. Here $\langle \sigma', \delta_0 \rangle = \langle \bot, \bot \rangle$ indicates abnormal termination or divergence.

**Definition 3.11**
We call an environment $\gamma$ agreement-preserving if for every $c, d_0, \ldots, d_n$, for every $m_{c,d}$, for every $\delta^c$, for every $\sigma \in \Sigma$, and for every $\bar{\beta} = (\beta_1^{d_1}, \ldots, \beta_n^{d_n}) \in \prod_{i=1}^n \sigma^{(d_i)}$ (note that we consider only existing objects) we have that if $\text{OK}(\sigma, \delta)$ and $\langle \sigma', \delta_0 \rangle = \gamma_{(c,d)}(m)(\bar{\beta})(\delta)(\sigma)$ and $\sigma' \neq \bot$ then $\text{OK}(\sigma')$, $\sigma \leq \sigma'$, and $\delta_0 \in \sigma^{(d_0)}$.

Note that the requirement is somewhat stronger than preservation of the agreement between state and context. We require that the new state extends the old state and that it is consistent. This automatically implies that the context $\delta$ agrees with the new state.

### 3.2 The semantic functions

**Definition 3.12**

The semantics of expressions is given by a function $E^c_d : \text{Exp}^c_d \rightarrow \Delta^c \rightarrow \Sigma_c \rightarrow \text{O}_{\delta}^d$, which is defined as follows:

- $E^c_d[\text{true}](\delta)(\sigma) = t$ (only if $d = \text{Bool}$)
- $E^c_d[\text{false}](\delta)(\sigma) = f$ (only if $d = \text{Bool}$)
- $E^c_d[n](\delta)(\sigma) = n$ (only if $d = \text{Int}$)

$$E^c_d[e_1_d \equiv e_2_d](\delta)(\sigma) = t$$ if $E^c_d[e_1](\delta)(\sigma) = E^c_d[e_2](\delta)(\sigma)$ otherwise (only if $d = \text{Bool}$)
Although most of these equations speak for themselves, we shall give some informal explanation.

- The function $\mathcal{E}_d[e](\delta)$ is strict; that is, it will always yield $\bot$ if it is applied to a state $\sigma$ that is equal to $\bot$.

- The value of an instance variable is looked up in the second component of the state $\sigma$. The first component of the context $\delta$ indicates the currently active object.

- The value of a temporary variable is looked up in the third component of the state $\sigma$.

- The value of the expression nil is always $\bot$.

- The value of the expression self is the first component of the context $\delta$.

- The Boolean constants true and false get the corresponding truth-values as their value.

- Integer numbers are mapped to themselves. Note that at this point we are confusing syntactic and semantic entities a little, but here this is harmless.

- The equal sign between expressions means that we test whether their values are really the same objects. Note that this is a kind of non-strict predicate, because if both sides yield $\bot$, the result of the equality is nevertheless $t$.

- Addition is only defined for genuine integers: If one of the two sides yields $\bot$ the result is also $\bot$.

- The same is true for the relation $<$. 

Doc. No.
where
\[ F_i' = \{ \text{init} \} p_i \{ S_P^c (\rho_i, \text{init}) \}. \]

Now by lemma 6.46 and lemma 6.47 an application of the consequence rule gives us
\[ F_i \vdash F_i' \] where
\[ F_i = \{ P_i[e^i/\text{self}, u^i][f/\text{id}][b_{c_i} \circ \langle \text{self} \rangle /b_{c_i}]\} p_i \{ S_P^c (\rho_i, \text{init}) \}. \]

So we have
\[ F_1, \ldots, F_k \vdash \{ P_i \land \bigwedge_j v^i_j \neq \text{nil} \land \text{self} \notin b_{c_i} \} \langle U|c'_i : S_i \rangle \{ Q_i^c[e_i/r_i] \}. \]

By theorem 6.33 we have
\[ \vdash \{ \text{Subs}(\text{ire}, s\text{f}1, \text{cr}) \} \langle U|c'_i : S_i \rangle \{ \text{Subs}(\text{ire}, s\text{f}1, \text{cr}) \}. \]

So by the conjunction rule we infer
\[ \{ P_i \land \bigwedge_j v^i_j \neq \text{nil} \land \text{self} \notin b_{c_i} \} \langle U|c'_i : S_i \rangle \{ Q_i^c[e_i/r_i] \} \]

By proposition 6.50 an application of the consequence rule gives us
\[ F_1, \ldots, F_m \vdash \{ P_i \land \bigwedge_j v^i_j \neq \text{nil} \land \text{self} \notin b_{c_i} \} \langle U|c'_i : S_i \rangle \{ Q_i^c[e_i/r_i] \}. \]

We now can apply rule (NMR), making use of lemma 6.46, yielding the derivability of the correctness formula:
\[ \{ P_i \land \bigwedge_j v^i_j \neq \text{nil} \land \text{self} \notin b_{c_i} \} \langle U|c'_i : S_i \rangle \{ Q_i^c[e_i/r_i] \}. \]

Applying next (MI) or (MT) gives us the derivability of
\[ \{ P_i[e^i/\text{self}, u^i][f/\text{id}][b_{c_i} \circ \langle \text{self} \rangle /b_{c_i}]\} p_i \{ S_P^c (\rho_i, \text{init}) \}. \]

So an application of the consequence rule (the assertion \( \text{init} \) by lemma 6.46 implies the precondition, and \( \vdash S_P^c (\rho_1, \text{init}) \rightarrow S_P^c (\rho_1, \text{init}) \)) gives us the desired result (note that \( \rho_1 = \rho \) by definition)
\[ \vdash \{ \text{init} \} p \{ S_P^c (\rho, \text{init}) \}. \]

We conclude with the completeness theorem:

Doc. No.
In order to evaluate a send-expression, first the destination object $\beta_0$ and the parameters $\beta_1, \ldots, \beta_n$ are computed (in the old state). Note that if the destination is $\perp$ (i.e., nil), then the program will fail, which is represented by setting $(\sigma', \beta^d)$ to $(\perp, \perp)$. Otherwise a new context is created, in which the executing object is the destination of the message, and in which the sending object is added to the set of blocked objects (of the appropriate class). Then the meaning of the method $m$ is looked up in the environment $\gamma$ and, provided with the parameters, the new context and the old state, it gives us the new state and the result of the send-expression.

Definition 3.14
The semantics of statements is given by a function

$$\mathcal{S}^e : \text{Stat}^e \rightarrow \Gamma \rightarrow \Delta^e \rightarrow \Sigma_\perp \rightarrow \Sigma_\perp,$$

which is defined as follows:

$$\mathcal{S}^e[\mathcal{S}^e]\gamma(\delta)(\perp) = \perp \quad \text{from now on we assume } \sigma \neq \perp$$

$$\mathcal{S}^e[x_{\delta} \leftarrow s_{\delta}](\gamma)(\delta)(\sigma) = \sigma''$$

where

$$\langle \sigma', \beta \rangle = \mathcal{Z}_e^e[x_{\delta}](\gamma)(\delta)(\sigma)$$

$$\sigma'' = \sigma'\{\beta/\delta(1), \pi\}$$

$$\mathcal{S}^e[u_{e} \leftarrow s_{\delta}](\gamma)(\delta)(\sigma) = \sigma''$$

where

$$\langle \sigma', \beta \rangle = \mathcal{Z}_e^e[u_{e}](\gamma)(\delta)(\sigma)$$

$$\sigma'' = \sigma'\{\beta/u\}$$

$$\mathcal{S}^e[s_{\delta}](\gamma)(\delta)(\sigma) = (\mathcal{Z}_e^e[s_{\delta}](\gamma)(\delta)(\sigma))_{(1)}$$

$$\mathcal{S}^e[S_1; S_2](\gamma)(\delta)(\sigma) = \mathcal{S}^e[S_2](\gamma)(\delta)(\mathcal{S}^e[S_1](\gamma)(\delta)(\sigma))$$

$$\mathcal{S}^e[\text{if } e \text{ then } S_1 \text{ else } S_2 \text{ fi}](\gamma)(\delta)(\sigma) = \begin{cases} \perp & \text{if } \beta = \perp \\ \mathcal{S}^e[S_1](\gamma)(\delta)(\sigma) & \text{if } \beta = t \\ \mathcal{S}^e[S_2](\gamma)(\delta)(\sigma) & \text{if } \beta = f \end{cases}$$

where $\beta = \mathcal{E}[e](\delta)(\sigma)$

$$\mathcal{S}^e[\text{while } e \text{ do } S \text{ od}](\gamma) = \mu \Phi$$

where $\Phi : (\Delta^e \rightarrow (\Sigma_\perp \rightarrow \Sigma_\perp)) \rightarrow (\Delta^e \rightarrow (\Sigma_\perp \rightarrow \Sigma_\perp))$ is defined as follows:

$$\Phi(\phi)(\delta)(\sigma) = \begin{cases} \perp & \text{if } \beta = \perp \\ \phi(\delta, \mathcal{S}^e[S](\gamma)(\delta)(\sigma)) & \text{if } \beta = t \\ \sigma & \text{if } \beta = f \end{cases}$$

where $\beta = \mathcal{E}[e](\delta)(\sigma)$
Here is some informal explanation:

- For any $S$, $\gamma$, and $\delta$, $S[\gamma](\delta)$ is a strict function from $\Sigma_\bot$ to $\Sigma_\bot$.

- If an assignment to an instance variable $x$ is done, first the right hand side is evaluated, resulting in a new state $\sigma'$ (because of possible side effects), and an object $\beta$. Now the final state $\sigma''$ is constructed from $\sigma'$ by modifying its second component in such a way that the object $\beta$ becomes the value of the variable $x$.

- For an assignment to a temporary variable, essentially the same thing is done, except that the new value is stored away in the third component of the resulting state $\sigma''$.

- If a side effect expression occurs at the place of a statement, it is evaluated and its resulting object is ignored. Only the new state is kept (this is the first component of the result of the evaluation).

- Sequential composition of statements is modelled by letting the second statement act on the state that results from the first statement.

- For a conditional statement first the condition is evaluated. Depending on that the first or the second clause is executed (or a failure is signalled).

- A while statement is modelled by taking the least fixed point of the operator $\Phi$. This operator takes its argument $\varphi$ as an approximation of the meaning of the while statement and maps it to a better approximation, obtained by unwinding the loop one more time.

**Definition 3.15**

The semantics of method definitions is given by a function

$$
\mathcal{M}_{d_0, \ldots, d_n} : \text{MethDef}_{d_0, \ldots, d_n} \rightarrow \Gamma \rightarrow \left( \prod_{i=1}^{n} \mathcal{O}_{d_i} \right) \rightarrow \Delta^c \rightarrow \Sigma_\bot \rightarrow (\Sigma_\bot \times \mathcal{O}^d_\bot)
$$

which is defined by:

Doc. No.
\[ M_{d_0, \ldots, d_n}^\varepsilon [u_{1d_1}, \ldots, u_{nd_n}] : S^\varepsilon \uparrow e_{d_0}^\varepsilon (\beta_1^{d_1}, \ldots, \beta_n^{d_n})(\delta^\varepsilon)(\sigma) = (\sigma''', \beta^{d_0}) \]

where \( \sigma' = \perp \) if \( \delta_{(1)} \in \delta_{(2)}(c) \) or \( \sigma = \perp \)

\[
\begin{align*}
\sigma'_{(3)}(u_d) &= \beta_i^{d_i} & \text{if } d = d_i \text{ and } u_d = u_{i d_i} \\
\sigma'' &= \mathcal{S}^{\varepsilon \Sigma}[S^\varepsilon](\gamma)(\delta^\varepsilon)(\sigma') \\
\beta^{d_0} &= \mathcal{E}^{\varepsilon \Sigma}[e_{d_0}^\varepsilon](\delta^\varepsilon)(\sigma'') \\
\sigma''' &= \perp \quad \text{if } \sigma'' = \perp \\
&= (\sigma''_{(1)}, \sigma''_{(2)}, \sigma''_{(3)}) \quad \text{if } \sigma''' \neq \perp
\end{align*}
\]

Again we give an informal explanation: The first thing to be checked when a method is to be executed is whether the executing object is blocked, that is whether \( \delta_{(1)} \in \delta_{(2)}(c) \) or whether the starting state \( \sigma \) is \( \perp \). If this is the case the result of the method will be the pair \( \langle \perp, \perp \rangle \) (this will come out automatically if we set \( \sigma' \) to \( \perp \)). Next we construct a state \( \sigma' \) by initializing all temporary variables to \( \perp \), except the formal parameters, which are bound to the corresponding actual ones (that is, the variable \( u_{i d_i} \) is set to \( \beta_i^{d_i} \)). In this modified state \( \sigma' \) we execute the statement \( S^\varepsilon \) of the method, which results in a new state \( \sigma'' \). In this state we can evaluate the result expression \( e_{d_0}^\varepsilon \), which gives us the object \( \beta^{d_0} \). The state \( \sigma''' \) after the method execution is obtained by restoring the temporary variables to their values before the method execution.

**Definition 3.16**

The semantics of class definitions is given by a function

\[ C_{m_1, \ldots, m_n}^\varepsilon : \text{ClassDef}^\varepsilon_{m_1, \ldots, m_n} \rightarrow \Gamma \rightarrow \Gamma \]

which is defined as follows:

\[
C_{m_1, \ldots, m_n}^\varepsilon [c : (m_1^\varepsilon_1 \triangleq \mu_1^\varepsilon_{d_1}, \ldots, m_n^\varepsilon_n \triangleq \mu_n^\varepsilon_{d_n})](\gamma) = \gamma\left\{ M[\mu_1^\varepsilon_{d_1}][\gamma] / m_1^\varepsilon_{d_1} \right\} \ldots \left\{ M[\mu_n^\varepsilon_{d_n}][\gamma] / m_n^\varepsilon_{d_n} \right\}
\]

This means that in the environment \( \gamma \) the value associated with each method \( m \) in the class definition is replaced by the value obtained from the corresponding method definition. However, this method definition is still evaluated with respect to the old environment \( \gamma \). Note that the order of the replacements does not matter, because it is required that all method names must be different.

**Definition 3.17**

The semantics of units is given by a function

\[ U_{m_1, \ldots, m_k}^\varepsilon : \text{Unit}^\varepsilon_{m_1, \ldots, m_k} \rightarrow \Gamma \rightarrow \Gamma \]

Doc. No.
which is defined by:

$$U_{m_1;...,m_k}^c[D_1^c;...,D_n^c](\gamma) = \gamma'$$

where $$\gamma' = \gamma(\zeta_j/m_j)_{j=1}^k$$

$$\langle \zeta_1, ..., \zeta_k \rangle = \mu \Psi$$

$$\Psi(\zeta_1', ..., \zeta_k') = (\gamma''(c_{i_j}, d_{j})(m_j))_{j=1}^k$$

$$\gamma'' = C[D_1] \circ \cdots \circ C[D_n](\gamma(\zeta_j'/m_j)_{j=1}^k)$$

(we suppose that $$m_j = m_{j_{i_j}}$$).

The main point in this definition is the construction of an environment $$\gamma'$$ from the least fixed point of the operator $$\Psi$$. This operator $$\Psi$$ takes as its argument a row $$\zeta_1', ..., \zeta_k'$$ of possible meanings of the methods defined in the unit. Assuming these meanings for the corresponding methods, a new environment $$\gamma''$$ is determined from the class definitions in the unit and from this environment the new meanings for the previous methods are extracted, yielding the output of $$\Psi$$. The least fixed point of $$\Psi$$ therefore consists of the meanings of the methods defined in the unit, where for the other methods the meanings recorded in $$\gamma$$ are assumed.

Because we require that all the class names (the $$c_i$$) are different, each $$C[D_i]^c$$ modifies a different part of the environment $$\gamma(\zeta_j'/m_j)_{j=1}^k$$. Therefore the order in which they are composed does not matter.

**Definition 3.18**

Finally we give the semantics of programs by defining a function

$$P^c : Prog^c \rightarrow \Gamma \rightarrow \Delta^c \rightarrow \Sigma_\perp \rightarrow \Sigma_\perp$$

as follows:

$$P[U^c]((U^c_1;...,c^c_k)lc : S^c)E(\gamma) = S^c[S](\gamma')$$

where $$\gamma' = U[U](\gamma)$$

If every method used in the program is defined in the unit then the meaning is independent of the environment $$\gamma$$. One could take the “empty” environment $$\gamma_0$$, defined by

$$\gamma_0(c, d)(m^c_\alpha)(\bar{\delta})(\delta^c)(\sigma) = (\perp, \perp)$$

(this is certainly agreement-preserving).

**3.3 Remarks on the semantics**

In the foregoing definition of the semantic functions that play a role in our language, we have omitted some details. One of these details is the fact that all the functions of which we need the least fixed point are indeed continuous.
Lemma 3.19
The function $\Phi$, used in the semantics of while statements in definition 3.14, is continuous.

Proof
First of all it is easy to see that

- For every expression $e$ and for every context $\delta$, the function $E[e](\delta)$ is strict, i.e., that $E[e](\delta)(\perp) = \perp$.

- For every statement $S$, for every environment $\gamma$, and for every context $\delta$, the function $S[S](\gamma)(\delta)$ is also strict, i.e., $S[S](\gamma)(\delta)(\perp) = \perp$.

Now after a little calculation it becomes clear that this is all we need to ensure the continuity of $\Phi$, which moreover maps strict functions in $\Sigma \rightarrow \Sigma$ again to strict functions (so its least fixed point will also be a strict function).

Lemma 3.20
The function $\Psi$, used in definition 3.17 to define the semantics of units, is continuous.

Proof
The proof of this lemma is somewhat more involved. It would proceed in the following steps:

- For any side effect expression $s$, $E[s]$ is a continuous function from $\Gamma$ to $\Delta \rightarrow \Sigma \times O^d$.

- For any statement $S$, $S[S]$ is a continuous function from $\Gamma$ to $\Delta \rightarrow \Sigma \rightarrow \Sigma$.

- For any method definition $\mu_{\delta_0, \ldots, \delta_n}$, $M[\mu]$ is a continuous function from $\Gamma$ to $(\Pi_{i=1}^n O^d_i) \rightarrow \Delta \rightarrow \Sigma \rightarrow \Sigma \times O^d_\perp$.

- For any class definition $D$, $C[D]$ is a continuous function from $\Gamma$ to $\Gamma$.

- Now we can prove that $\Psi$ is a continuous function.

In retrospect we can change the domain assignments of several entities as follows (where $\triangleleft$ stands for continuous functions and $\downarrow$ for strict functions):

Doc. No.
Lemma 3.21
Now we come to the issues of consistent states and agreement between context and state. We can make the following observations:

• For any expression $e'_d$, for any state $\sigma \in \Sigma$, and for any context $\delta \in \Delta^c$ such that $OK(\sigma, \delta)$, we have that $E[e](\delta)(\sigma) \in \sigma_\perp^{(d)}$.

• For any side effect expression $s'_d$, for any agreement-preserving environment $\gamma$, for any state $\sigma \in \Sigma$, and for any context $\delta \in \Delta^c$ such that $OK(\sigma, \delta)$, we have that if $\langle \sigma', \beta^d \rangle = S[s](\gamma)(\delta)(\sigma)$ and $\sigma' \neq \perp$ then $OK(\sigma')$, $\sigma \preceq \sigma'$ (therefore also $OK(\sigma', \delta)$), and $\beta^d \in \sigma'_{\perp^{(d)}}$.

• For any statement $S^c$, for any agreement-preserving environment $\gamma$, for any state $\sigma \in \Sigma$, and for any context $\delta \in \Delta^c$ such that $OK(\sigma, \delta)$, if $\sigma' = S[S](\gamma)(\delta)(\sigma)$ and $\sigma' \neq \perp$ then $OK(\sigma')$, $\sigma \preceq \sigma'$ (therefore also $OK(\sigma', \delta)$).

• For any method definition $\mu_{d_0, \ldots, d_n}$, for any agreement-preserving environment $\gamma$, for any state $\sigma \in \Sigma$, for any context $\delta \in \Delta^c$ such that $OK(\sigma, \delta)$, and for any row of (existing) objects $\bar{\beta} = (\beta_1^{d_1}, \ldots, \beta_n^{d_n}) \in \prod_{i=1}^n \sigma_\perp^{(d_i)}$ we have if $\langle \sigma', \beta^d_0 \rangle = M[\mu](\gamma)(\bar{\beta})(\delta)(\sigma)$ and $\sigma' \neq \perp$ then $OK(\sigma')$, $\sigma \preceq \sigma'$ (so also $OK(\sigma', \delta)$), and $\beta^d_0 \in \sigma'_{\perp^{(d_0)}}$.

• For any class definition $D$ and for any agreement-preserving environment $\gamma$ we have that $C[D](\gamma)$ is again an agreement-preserving environment.

• For any unit $U$ and for any agreement-preserving environment $\gamma$ we have that $U[U](\gamma)$ is again an agreement-preserving environment.

• For any program $P^c$, for any agreement-preserving environment $\gamma$, for any state $\sigma \in \Sigma$, and for any context $\delta^c$ such that $OK(\sigma, \delta)$, if $\sigma' = P[P](\gamma)(\delta)(\sigma)$ and $\sigma' \neq \perp$ then $OK(\sigma')$ and $\sigma \preceq \sigma'$ (therefore also $OK(\sigma', \delta)$).
Proof
The proof consists of an easy induction on the structure of the syntactical object under consideration.
4 The assertion language and its semantics

In this section we shall develop a formalism for expressing certain properties of states, and we shall give a semantics for it.

One element of this assertion language will be the introduction of logical variables. These variables may not occur in the program, but only in the assertion language. Therefore we are always sure that the value of a logical variable can never be changed by a statement. Apart from a certain degree of cleanliness, this has the additional advantage that we can use logical variables to express the constancy of certain expressions (for example in the proof rule (MI) for message passing in definition 5.24). Logical variables also serve as bound variables for quantifiers.

The set of expressions in the assertion language is larger than the set of programming language expressions not only because it contains logical variables, but also because it is allowed to refer to instance variables of other objects. Furthermore we include conditional expressions in the assertion language because they are very convenient (e.g., in the axiom (SAI), see definitions 5.6 and 5.7).

In two respects our assertion language differs from the usual first-order predicate logic: Firstly, the range of quantifiers is limited to the existing, non-nil objects in the current state. With respect to the classes Int and Bool this only means that the range does not include \( \perp \). This does not affect essentially the expressive power of the assertion language, but in most practical cases one wants to exclude \( \perp \) from the quantification, so in these cases the assertions become shorter. For the other classes this restriction means that we cannot talk about objects that have not yet been created, even if they could be created in the future. This is done in order to satisfy the requirements on the proof system stated in the introduction. Because of this the range of the quantifiers can be different for different states. More in particular, a statement can change the truth of an assertion even if none of the program variables accessed by the statement occurs in the assertion, simply by creating an object and thereby changing the range of a quantifier. (The idea of restricting the range of quantifiers was inspired by [8].)

Secondly, in order to strengthen the expressiveness of the logic, it is augmented with quantification over finite sequences of objects. It is quite clear that this is necessary, because simple first-order logic is not able to express certain interesting properties.

4.1 The assertion language

Definition 4.1
For each \( d \in C^+ \) we introduce the symbol \( d^* \) for the type of all finite sequences with
elements from $d$, we let $C^*$ stand for the set $\{d^* \mid d \in C^+\}$, and we use $C^+$, with typical element $a$, for the union $C^+ \cup C^*$. We define $O^{d'}$ to be the set of finite sequences with elements from $O^d_1$ (note that the elements can also be $1$). The empty sequence $e^d$ is also included in $O^{d'}$. The elements in a sequence are always numbered starting from 1. In order to simplify some formulae we define $O^{d''}_1$ to be the same as $O^{d'}$, in deviation from definition 3.2. In addition to $\beta^{d''}$, we shall sometimes use $\alpha^{d''}$ to range over elements of $O^{d''}$.

We have the following functions:

- $\text{len}^d : O^{d''} \to \mathbb{Z}$ returns the number of elements in the sequence.
- $\text{elt}^d : O^{d''} \times \mathbb{Z} \to O^d_1$ extracts from the first argument the element numbered by the second argument. If the second argument is "out of bounds" (less than 1 or greater than the length of the first argument) then the result is $\bot$.

Assumption 4.2
We assume that for every $a$ in $C^+$ we have a set $LVar_a$ of logical variables of type $a$, with typical element $z_a$.

Definition 4.3
We the set $LExp^c_a$ of logical expressions of type $a$ in class $c$, with typical element $l_a^c$, as follows:

$$ l_a^c ::= e_a^c \quad \text{if } a \in C^+ $$
$$ l_a^c \cdot x_a^c \quad \text{if } a \in C^+ $$
$$ \text{if } l_0^c \text{ then } l_1^c \text{ else } l_2^c \quad \text{if } a \in C^+ $$
$$ l_1^c \cdot l_2^c \quad \text{if } a = \text{Bool} $$
$$ l_1^c + l_2^c \quad \text{if } a = \text{Int} $$
$$ \vdots $$
$$ l_1^c < l_2^c \quad \text{if } a = \text{Bool} $$
$$ \vdots $$
$$ |l_0^c| \quad \text{if } a = \text{Int} \text{ and } d \in C^+ $$
$$ l_1^c \cdot l_2^c \quad \text{if } a \in C^+ $$

Note that the difference with the set $Exp^c_d$ of expressions in the programming language is that in logical expressions we can use logical variables, refer to the instance variables of other objects, and write conditional expressions. Furthermore, we extended the domain of discourse by means of logical variables ranging over sequences and notations.
to express the length of a sequence and the selection of an element from a sequence. The selection operator \( \cdot \) can be distinguished from the dereferencing operator \( . \) by its higher vertical position on the line and by the type of its first argument.

**Definition 4.4**
The set \( \text{Ass}_c \) of assertions in class \( c \), with typical elements \( P^c \) and \( Q^c \), is defined by:

\[
\begin{align*}
P^c & ::= l^c \\
& \quad \mid P^c \rightarrow Q^c \\
& \quad \mid \neg P^c \\
& \quad \mid \forall z_a P^c \\
& \quad \mid \exists z_a P^c
\end{align*}
\]

This definition is rather conventional.

**Definition 4.5**
Of course, we shall freely use the logical connectives \( \wedge, \vee, \) and \( \leftrightarrow \), which we consider as abbreviations of appropriate constructions with \( \rightarrow \) and \( \neg \). Furthermore we shall use \( l^c \uparrow \) as an abbreviation for \( l^c_d = \text{nil}_d \) and \( l^c \downarrow \) for \( \neg l^c_d = \text{nil}_d \).

**Definition 4.6**
Finally we define the set \( \text{Corr}_c \) of correctness formulae in class \( c \), with typical element \( F^c \), as follows:

\[
\begin{align*}
F^c & ::= P^c \\
& \quad \mid \{P^c\}^c\{Q^c\}
\end{align*}
\]

### 4.2 Semantics of assertions and correctness formulae

**Definition 4.7**
In order to be able to assign a semantics to logical expressions we first define the set \( \Omega \) of valuations, with typical element \( \omega \), as follows:

\[
\Omega = \prod_a (L\text{Var}_a \rightarrow O^a_a).
\]

(Remember that \( O^a_\perp = O^a_\top \) if \( a \in C^* \).) A valuation assigns a value to each logical variable.

**Definition 4.8**
We call a valuation \( \omega \) compatible with a state \( \sigma \) if

- \( \forall e \in C \forall z_e \in L\text{Var}_e \quad \omega_{[e]}(z) \in \sigma_{[e]}^\perp \)

Doc. No.
\[ \forall c \in C \forall z_c^\ast \in LVar_z \forall n \in \mathbb{Z} \ \text{el}t^c(\omega(z')^1(n)) \in \sigma_1^c \]

Again an abbreviation is useful: we shall write \(OK(\sigma, \delta, \omega)\) meaning that \(\sigma\) is consistent, \(\delta\) agrees with \(\sigma\), and \(\omega\) is compatible with \(\sigma\).

**Lemma 4.9**
Concerning the preservation of compatibility by statements and programs we have the following properties:

- For any statement \(S^c\), for any agreement-preserving environment \(\gamma\), for any state \(\sigma \in \Sigma\), for any context \(\delta^c\) and for any valuation \(\omega\) such that \(OK(\sigma, \delta, \omega)\) we have if \(\sigma' = S[\delta]((\gamma)(\delta)(\sigma))\) and \(\sigma' \neq \bot\) then \(OK(\sigma', \delta, \omega)\).

- For any program \(P^c\), for any agreement-preserving environment \(\gamma\), for any state \(\sigma \in \Sigma\), for any context \(\delta^c\) and for any valuation \(\omega\) such that \(OK(\sigma, \delta, \omega)\) we have if \(\sigma' = P[\rho]((\gamma)(\delta)(\sigma))\) and \(\sigma' \neq \bot\) then \(OK(\sigma', \delta, \omega)\).

**Proof**
This is an easy consequence of lemma 3.21.

**Definition 4.10**
We define the semantics of logical expressions by specifying the function
\[ \mathcal{L}^c_a : LExpr^c_a \to \Omega \to \Delta^c \to \Sigma \to O_\bot^a \]
as follows:

\[
\begin{align*}
\mathcal{L}^c_a[\text{if } a \text{ then } b \text{ else } c](\omega)(\delta)(\sigma) &= \mathcal{L}^c_a[b](\omega)(\delta)(\sigma) \quad \text{if } \beta = \bot \\
&= \mathcal{L}^c_a[c](\omega)(\delta)(\sigma) \quad \text{otherwise}
\end{align*}
\]
where \(\beta^c = \mathcal{L}^c_a[l](\omega)(\delta)(\sigma)\)

\[
\begin{align*}
\mathcal{L}^c_a[l_0\text{Bool}] \text{ if } l_1 \text{ else } l_2(\omega)(\delta)(\sigma) &= \bot \quad \text{if } \beta = \bot \\
&= \mathcal{L}^c_a[l_1](\omega)(\delta)(\sigma) \quad \text{if } \beta = \text{t} \\
&= \mathcal{L}^c_a[l_2](\omega)(\delta)(\sigma) \quad \text{if } \beta = \text{f}
\end{align*}
\]

(only if \(d = \text{Bool}\))
\[ L^c_{\omega}[(l_1 + l_2)](\delta)(\sigma) = \top \quad \text{if } L^c_{\omega}[(l_1)](\delta)(\sigma) = \top \\
\quad \quad \text{or } L^c_{\omega}[(l_2)](\delta)(\sigma) = \top \\
= L^c_{\omega}[(l_1)](\delta)(\sigma) + L^c_{\omega}[(l_2)](\delta)(\sigma) \\
\quad \text{otherwise} \]

(only if \( d = \text{Int} \))

\[ L^c_{\omega}[(l_1 \cdot l_2)](\delta)(\sigma) = \top \quad \text{if } L^c_{\omega}[(l_1)](\delta)(\sigma) = \top \\
\quad \quad \text{or } L^c_{\omega}[(l_2)](\delta)(\sigma) = \top \\
= t \quad \text{if } L^c_{\omega}[(l_1)](\delta)(\sigma) < L^c_{\omega}[(l_2)](\delta)(\sigma) \\
= f \quad \text{otherwise} \]

(only if \( d = \text{Bool} \) and \( d' = \text{Int} \))

These equations are just what one would expect, especially after having seen definition 3.12.

**Lemma 4.11**

If \( \sigma \in \Sigma, \delta \in \Delta^c, \) and \( \omega \in \Omega \) are such that \( OK(\sigma, \delta, \omega) \), then for every logical expression \( l \in LExpr^c_\omega \) we have \( L^c_{\omega}[(l)](\delta)(\sigma) \in \sigma_{(d)}^{(c)} \), and for every expression \( l \in LExpr^c_\omega \) we have \( elt^c(L^c_{\omega}[(l)](\delta)(\sigma), n) \in \sigma_{(d)}^{(c)} \), for every \( n \).

**Proof**

Induction on the complexity of \( l \).

**Definition 4.12**

Now we can define the semantics of assertions in terms of the function

\[ A^c : Ass^c \rightarrow \Omega \rightarrow \Delta^c \rightarrow \Sigma \rightarrow B \]

as follows:

\[ A^c[\{ l \}](v)(\omega)(\delta)(\sigma) = t \quad \text{if } L^c_{\omega}[(l)](\delta)(\sigma) = t \\
= f \quad \text{otherwise} \]

\[ A^c[\neg P^c](v)(\omega)(\delta)(\sigma) = f \quad \text{if } A^c[P^c](v)(\omega)(\delta)(\sigma) = t \\
= t \quad \text{otherwise} \]

\[ A^c[\forall z_d P^c](v)(\omega)(\delta)(\sigma) = t \quad \text{if for all } \beta \in \sigma^{(d)} \text{ we have} \\
A^c[P^c](v)(\omega\{\beta/z\})(\delta)(\sigma) = t \\
= f \quad \text{otherwise} \]

Doc. No.
\[ \mathcal{A}^c[\exists z_d \ P^c](v)(\delta)(\sigma) = \begin{cases} t & \text{if there is a } \beta \in \sigma^{(d)} \text{ such that } \\ \mathcal{A}^c[P^c](v)(\beta/z)(\delta)(\sigma) = t \\ f & \text{otherwise} \end{cases} \]

\[ \mathcal{A}^c[\forall z_d \ P^c](\omega)(\delta)(\sigma) = \begin{cases} t & \text{if for all } \alpha \in \mathcal{O}^d* \text{ such that } \\ \forall n \in \mathbb{Z} \ e\ellt(\alpha, n) \in \sigma^{(d)}_1 \text{ we have } \\ \mathcal{A}^c[P^c](\omega{\alpha/z})(\delta)(\sigma) = t \\ f & \text{otherwise} \end{cases} \]

\[ \mathcal{A}^c[\exists z_d \ P^c](\omega)(\delta)(\sigma) = \begin{cases} t & \text{if there is an } \alpha \in \mathcal{O}^d* \text{ such that } \\ \forall n \in \mathbb{Z} \ e\ellt(\alpha, n) \in \sigma^{(d)}_1 \text{ and } \\ \mathcal{A}^c[P^c](\omega{\alpha/z})(\delta)(\sigma) = t \\ f & \text{otherwise} \end{cases} \]

A few remarks should be made here.

- Note that the possible values of a boolean logical expression are \( t, f, \) and \( \bot. \) If such an expression is viewed as an assertion, only \( t \) and \( f \) remain. If viewed as an expression it yields \( \bot, \) as an assertion it delivers \( f. \)

- It is very important to note that in assertions of the form \( \forall z \ P \) and \( \exists z \ P \) the quantification ranges only over the existing, non-nil objects of the appropriate type.

Example 4.13

The formula

\[ v \xrightarrow{x} w \]

from [7] can be expressed in our new assertion language in the following way:

\[ \exists z_d^* (z \cdot 1 \triangleq v \land z \cdot |z| \triangleq w \land \forall n (0 < n \land n < |z|) \rightarrow (z \cdot n).x \triangleq z \cdot (n + 1)) \]

Example 4.14

There are no logical expressions in the language to construct a sequence with one specific element (a singleton). However, if we want to say that property \( P \) holds for the singleton whose element is given by the logical expression \( l, \) we can do this as follows:

\[ \exists z_d^* |z| \triangleq 1 \land z \cdot 1 \triangleq l \land P(z) \]
or equivalently:
\[ \forall z \in A^* \ (|z| = 1 \land z \cdot 1 \equiv l) \rightarrow P(z). \]
A similar procedure is possible for the empty sequence and for the concatenation of two sequences. Furthermore we can see whether two sequences are equal by checking if they have the same lengths and whether their corresponding elements are equal. (Direct ways of expressing the above things could be included in the assertion lan­guage, but they would make the substitution operation \([\text{new}/u]\) in definitions 5.13 and 5.15 much more complicated.)

**Definition 4.15**
Finally we define the notion of **truth** and **validity** of correctness formulae.

- We say that a correctness formula of the form \(P^c\) is **true** with respect to a valuation \(\omega\), a context \(\delta^c\), and a state \(\sigma\), written as \(\omega, \delta, \sigma \models P\), if \(OK(\sigma, \delta, \omega)\) and
  \[ A^c[P](\omega)(\delta)(\sigma) = t \]
- We call a correctness formula of the form \(P^c\) **valid**, written as \(\models P\), if it is true with respect to every \(\omega, \delta^c, \) and \(\sigma\) such that \(OK(\sigma, \delta, \omega)\).
- A correctness formula of the form \(\{P^c\} \rho^c \{Q^c\}\) is called **true** with respect to an environment \(\gamma\), a valuation \(\omega\), a context \(\delta^c\), and a state \(\sigma\), written as \(\gamma, \omega, \delta, \sigma \models \{P\} \rho\{Q\}\), if \(\omega, \delta, \sigma \models P\) implies that for the state \(\sigma' = P^c[\rho](\gamma)(\delta)(\sigma)\) we have
  \[ \sigma' \neq 1 \Rightarrow \omega, \delta, \sigma' \models Q. \]
- We define a correctness formula of the form \(\{P^c\} \rho^c \{Q^c\}\) to be **valid** with respect to an environment \(\gamma\), written as \(\gamma \models \{P\} \rho\{Q\}\), if we have \(\gamma, \omega, \delta, \sigma \models \{P\} \rho\{Q\}\) for every \(\omega, \delta^c, \) and \(\sigma\). We call such a correctness formula simply **valid** if it is valid with respect to every environment.
5 The proof system

In this section we shall present a number of axioms and rules that can be used to derive correctness formulae. For each axiom and rule we shall give its justification by proving that it is valid. Note that axioms are correctness formulae so we have already defined what validity means for them. We call a proof rule valid if for every environment $\gamma$ the validity of the premisses of the rule with respect to $\gamma$ implies the validity of the conclusion with respect to $\gamma$. The consequence of the validity of all the axioms and rules will be that our proof system is sound, i.e., that if we can derive a correctness formula (without any further assumptions), this correctness formula will be valid. (There is one rule in the system that cannot be proved valid in isolation: the recursion rule (MR) in definition 5.33. It will get a special treatment in the soundness proof of the whole proof system (see theorem 5.40).)

5.1 Simple assignments

Definition 5.1
We shall call a statement a simple assignment if it is of the form $x \leftarrow e$ or $u \leftarrow e$ (that is, it uses the first form of a side effect expression: the one without a side effect).

5.1.1 Simple assignment to a temporary variable

Definition 5.2
Our first axiom deals with the case that the target variable is a temporary variable:

$\{P[e_2/u_2]\} \langle U | c : u_d \leftarrow e_2 \rangle \{P_c\}$  

(SAT)

Here the notation $P[e/u]$ means: $P$ in which $e$ is substituted for $x$. We shall formalize that notion in the next definition. (Note that this definition merely asserts that the name (SAT) refers to the class of formulae of the form listed above.)

Definition 5.3
We shall define the substitution operation $[e/u]$ first for logical expressions:

$\begin{align*}
  x \ [e/u] &= x \\
  u \ [e/u] &= e \\
  u' \ [e/u] &= u' \quad \text{if } u' \neq u \\
  z \ [e/u] &= z \\
  l \ [e/u] &= l \quad \text{if } l = \text{nil, self, true, false} \\
  n \ [e/u] &= n \\
  l.x \ [e/u] &= (l[e/u]).x
\end{align*}$
if $l_0$ then $l_1$ else $l_2$ fi\[e/uJ = \text{if } l_0[e/u] \text{ then } l_1[e/u] \text{ else } l_2[e/u] \text{ fi}

(l_1 \equiv l_2)[e/u] = (l_1[e/u]) \equiv (l_2[e/u])

(l_1 + l_2)[e/u] = (l_1[e/u]) + (l_2[e/u])

::

(l_1 < l_2)[e/u] = (l_1[e/u]) < (l_2[e/u])

::

$|l| [e/u] = |l[e/u]|

(l_1 \cdot l_2)[e/u] = (l_1[e/u] \cdot l_2[e/u])

Now we define this substitution for assertions other than logical expressions:

$(P \rightarrow Q)[e/u] = (P[e/u]) \rightarrow (Q[e/u])$

$(\neg P) [e/u] = \neg (P[e/u])$

$(\forall z P) [c/u] = \forall z (P[c/u])$

$(\exists z P) [c/u] = \exists z (P[c/u])$

This definition can be summarized by saying that we can perform the substitution $[e/u]$ by replacing $u$ by $e$ everywhere in the expression or assertion at hand. However, this will not be true for the notions of substitution that we will define in the sequel, despite the fact that we use a very similar notation to indicate those substitutions.

In the following lemma we express the most important characteristic of the substitution $[e/u]$. Informally spoken, for any logical expression or assertion, the substituted form has the same value in the state before the assignment as the unsubstituted form has in the state after the assignment.

Lemma 5.4
Consider the assignment statement $u_d \leftarrow e_d'$. Let $\gamma \in \Gamma$, $\sigma \in \Sigma$ and $\delta \in \Delta^c$ be arbitrary, and let

$\sigma' = \mathcal{S}(u \leftarrow e)(\gamma)(\delta)(\sigma)$.

Then we have the following facts:

1. For every logical expression $l_{\omega_d}^c$ and every valuation $\omega$

$\mathcal{L}[l[e/u]](\omega)(\delta)(\sigma) = \mathcal{L}[l](\omega)(\delta)(\sigma')$.

2. For every assertion $P^c$, every valuation $\omega$

$\mathcal{A}[P[e/u]](\omega)(\delta)(\sigma) = \mathcal{A}[P](\omega)(\delta)(\sigma')$. 

Doc. No.
Proof
First we observe that $\sigma' = S[u \leftarrow e](\gamma)(\delta)(\sigma)$ means that $\sigma' = \sigma(\beta/u)$, where $\beta = E[e](\delta)(\sigma)$.

Now we can prove the first part of the lemma by induction with respect to the structure of $I$. The only interesting case occurs when $I = u$ so that $I[e/u] = e$:

$$L[e](\omega)(\delta)(\sigma) = E[e](\delta)(\sigma)$$
$$= \beta$$
$$= \sigma'(\delta)(u)$$
$$= E[u](\delta)(\sigma')$$
$$= \omega\langle e \rangle(\delta)(\sigma')$$

After that we can prove the second part of the lemma by a straightforward induction on the structure of $P$.

Of course, this lemma is easily extended to the case where instead of an assignment statement we take a program in which the statement is a simple assignment to a temporary variable:

Corollary 5.5
The axiom (SAT) is valid, that is, for every environment $\gamma$ we have

$$\gamma \models \{P[e/u]\} \langle U|c : u \leftarrow e \rangle \{P\}.$$

Note that the corollary uses only one direction of the lemma. The two directions together say that $P[e/u]$ is the weakest precondition of the statement $u \leftarrow e$ with respect to the postcondition $P$.

5.1.2 Simple assignment to an instance variable

Definition 5.6
In the case that the target variable of an assignment statement is an instance variable, we use the following axiom:

$$\{P^c[e_2^2/x_2^2]\} \langle U|c : x_2^2 \leftarrow e_2^2 \rangle \{P^c\} \quad (SAI)$$

This looks very similar to our first axiom (SAT), but note that we have not yet defined what substitution means if we substitute an expression for an instance variable instead.
of a temporary variable. We shall do that now, and the difference will become clear immediately:

**Definition 5.7**
The substitution operation \([e/x]\) is defined as follows on logical expressions:

\[
\begin{align*}
x & \quad [e/x] = e \\
x' & \quad [e/x] = x' \quad \text{if } x' \neq x \\
u & \quad [e/x] = u \\
z & \quad [e/x] = z \\
l & \quad [e/x] = l \quad \text{if } l = \text{nil, self, true, false} \\
n & \quad [e/x] = n \\
l.x & \quad [e/x] = \begin{cases} \text{if } (l[e/x]) \doteq \text{self then } e \text{ else } (l[e/x]), x \end{cases} \\
l.x' & \quad [e/x] = (l[e/x]).x' \quad \text{if } x' \neq x \\
\end{align*}
\]

if \(l_0\) then \(l_1\) else \(l_2\) fi\([e/x]\) = if \(l_0[e/x]\) then \(l_1[e/x]\) else \(l_2[e/x]\) fi

\[
\begin{align*}
(l_1 \doteq l_2)[e/x] & = (l_1[e/x]) \doteq (l_2[e/x]) \\
(l_1 + l_2)[e/x] & = (l_1[e/x]) + (l_2[e/x]) \\
\vdots \\
(l_1 < l_2)[e/x] & = (l_1[e/x]) < (l_2[e/x]) \\
\vdots \\
|l| & \quad [e/x] = |l[e/x]| \\
(l_1 \cdot l_2)[e/x] & = (l_1[e/x] \cdot l_2[e/x])
\end{align*}
\]

The definition is extended to assertions other than logical expressions in the same way as before:

\[
\begin{align*}
(P \rightarrow Q)[e/x] & = (P[e/x]) \rightarrow (Q[e/x]) \\
(\neg P) & \quad [e/x] = \neg (P[e/x]) \\
(\forall z \; P) & \quad [e/x] = \forall z (P[e/x]) \\
(\exists z \; P) & \quad [e/x] = \exists z (P[e/x])
\end{align*}
\]

The most important aspect of this definition is certainly the conditional expression that turns up when we are dealing with a logical expression of the form \(l.x\). This is necessary because a certain form of form of aliasing is possible: the situation that different expressions refer to the same variable. In the case of \(l.x\), it is possible that, after substitution, \(l\) refers to the currently active object, so that \(l.x\) is the
same variable as \( x \) and should be substituted by \( e \). It is also possible that, after substitution, \( l \) does not refer to the currently executing object, and in this case no substitution should take place. Since we cannot decide between these possibilities by the form of the expression only, a conditional expression is constructed which decides "dynamically".

**Lemma 5.8**
Consider the assignment statement \( x_d^e \leftarrow e_d^e \). Let \( \gamma \in \Gamma, \sigma \in \Sigma, \) and \( \delta \in \Delta^e \) be arbitrary, and let

\[
\sigma' = S[x \leftarrow e](\gamma)(\delta)(\sigma).
\]

Then we have the following facts:

1. For every logical expression \( l \), and every valuation \( \omega \)
   \[
   \mathcal{L}[l[e/x]](\omega)(\delta)(\sigma) = \mathcal{L}[l](\omega)(\delta)(\sigma').
   \]

2. For every assertion \( P \), and every valuation \( \omega \)
   \[
   \mathcal{A}[P[e/x]](\omega)(\delta)(\sigma) = \mathcal{A}[P](\omega)(\delta)(\sigma').
   \]

**Proof**
Like in lemma 5.4 we first note that \( \sigma' = \sigma[\beta/\delta_1, x] \) where \( \beta = \mathcal{L}[e](\delta)(\sigma) \). The first part of the lemma is now proved by induction on the complexity of \( l \). We shall only deal with the most interesting case: \( l = l' \cdot x \). The induction hypothesis tells us that \( \mathcal{L}[l'[e/x]](\omega)(\delta)(\sigma) = \mathcal{L}[l'](\omega)(\delta)(\sigma') \). Let us call this object \( \beta_0 \). Now if \( \beta_0 = \delta_1 \) then \( \mathcal{L}[l' \cdot x](\omega)(\delta)(\sigma') = \sigma'_2(\delta_1)(x) = \beta = \mathcal{L}[e](\omega)(\delta)(\sigma) \). Otherwise we have \( \mathcal{L}[l' \cdot x](\omega)(\delta)(\sigma') = \sigma'_2(\beta_0)(x) = \mathcal{L}[l'[e/x] \cdot x](\omega)(\delta)(\sigma) \). So \( \mathcal{L}[l'[e/x] \cdot x](\omega)(\delta)(\sigma') \).

The rest of the lemma is proved in a way similar to lemma 5.4.

Again we can extend this to programs instead of statements:

**Corollary 5.9**
The axiom \( \text{SAI} \) is valid, that is, for every environment \( \gamma \) we have

\[
\gamma \models \{ P[e/x] \} (U|c : x \leftarrow e) \{ P \}.
\]

Note that this corollary also uses only one direction of the corresponding lemma. Again the two directions together say that \( P[e/x] \) is the weakest precondition of the statement \( x \leftarrow e \) with respect to the postcondition \( P \).

Doc. No.
5.2 Creating new objects

5.2.1 Assigning a new object to a temporary variable

Definition 5.10
For an assignment of the form $u \leftarrow \text{new}$ we have a axiom similar to the previous two:

\[
\{ P^c[\text{new} / u] \} \ (U : u \leftarrow \text{new}) \ \{ P^c \} \tag{NT}
\]

Again we still have to define what this notion of substitution looks like, but first we shall define the substitution of an expression for a logical variable, because we shall need that later:

Definition 5.11
We define the substitution operation $[e/z]$ on logical expressions by:

\[
\begin{align*}
x \ [e/z] &= x \\
u \ [e/z] &= u \\
z \ [e/z] &= I \\
z' \ [e/z] &= z' \quad \text{if } z' \neq z \\
l' \ [e/z] &= l' \quad \text{if } l' = \text{nil, self, true, false} \\
n \ [e/z] &= n \\
l'.x \ [e/z] &= (l'[e/z]) \cdot x \\
\end{align*}
\]

if $l_0$ then $l_1$ else $l_2$ fi$[e/z] = \text{if } l_0[e/z] \text{ then } l_1[e/z] \text{ else } l_2[e/z] \text{ fi}$

\[
\begin{align*}
(l_1 \equiv l_2)[e/z] &= (l_1[e/z]) \equiv (l_2[e/z]) \\
(l_1 + l_2)[e/z] &= (l_1[e/z]) + (l_2[e/z]) \\
&\vdots \\
(l_1 < l_2)[e/z] &= (l_1[e/z]) < (l_2[e/z]) \\
&\vdots \\
|l| \ [e/z] &= |l[e/z]| \\
(l_1 \cdot l_2)[e/z] &= (l_1[e/z] \cdot l_2[e/z])
\end{align*}
\]

We extend this definition to assertions other than logical expressions as follows:
\[(P \rightarrow Q)[e/z] = (P[e/z]) \rightarrow (Q[e/z])\]
\[\neg P \ [e/z] = \neg (P[e/z])\]
\[\forall z \ P \ [e/z] = \forall z \ P\]
\[\forall z' \ P \ [e/z] = \forall z' (P[e/z]) \text{ if } z' \neq z\]
\[\exists z \ P \ [e/z] = \exists z \ P\]
\[\exists z' \ P \ [e/z] = \exists z' (P[e/z]) \text{ if } z' \neq z\]

This definition can be summarized by observing that the substitution can be carried out by replacing \(z\) by \(e\) everywhere except in the scope of a quantifier where \(z\) is bound.

**Lemma 5.12**
Let \(\sigma \in \Sigma, \delta \in \Delta^\circ, e \in \text{Exp}^\circ_{\sigma},\) and \(z \in \text{LVar}_{\sigma}\) be arbitrary, and let \(\beta = \mathcal{E}[e](\delta)(\sigma).\) Then we have

1. For all \(l \in \text{LExp}^\circ_{\sigma}\) and for all \(\omega \in \Omega:\)
\[\mathcal{L}[l[e/z]](\omega)(\delta)(\sigma) = \mathcal{L}[l][\omega(\beta/z)](\delta)(\sigma)\]

2. For all \(P \in \text{Ass}^\circ,\) for all \(\omega \in \Omega:\)
\[\mathcal{A}[P[e/z]](\omega)(\delta)(\sigma) = \mathcal{A}[P][\omega(\beta/z)](\delta)(\sigma)\]

**Proof**
A rather trivial induction on the complexity of \(l\) and \(P.\)

Now we can define the substitution \([\text{new}_c/u_c].\) We shall do this first for logical expressions. As with the notions of substitution used in the axioms for simple assignments, we want the expression after substitution to have the same meaning in a state before the assignment as the unsubstituted expression has in the state after the assignment. However, in the case of a new-assignment, there are expressions for which this is not possible, because they refer to the new object (in the new state) and there is no expression that could refer to that object in the old state, because it does not exist yet. Therefore the result of the substitution must be left undefined in some cases.

However we will show that we are able to carry out the substitution. The idea behind this is that in such an assertion the variable \(u\) referring to the new object can essentially occur only in a context where either one of its instance variables is referenced, or it is compared for equality with another expression. In both of these cases we can predict the outcome without having to refer to the new object.
Definition 5.13
Here comes the formal definition of the substitution \([\text{new}/u]\) for logical expressions:

\[
x [\text{new}/u] = x
\]
\[
u [\text{new}/u] \text{ is undefined}
\]
\[
u' [\text{new}/u] = u \text{ if } u' \neq u
\]
\[
z [\text{new}/u] = z
\]
\[
l [\text{new}/u] = l \text{ if } l = \text{nil, self, true, false}
\]
\[
n [\text{new}/u] = n
\]

\[
x' . x [\text{new}/u] = x' . x
\]
\[
u . x [\text{new}/u] = \text{nil}
\]
\[
u' . x [\text{new}/u] = u' . x \text{ if } u' \neq u
\]
\[
z . x [\text{new}/u] = z . x
\]
\[
l . x [\text{new}/u] = l . x \text{ if } l = \text{nil, self}
\]
\[
l . x' . x [\text{new}/u] = (l . x' [\text{new}/u]) . x
\]

\[
\left( \text{if } l_0 \text{ then } l_1 \text{ else } l_2 \text{ fi} \right) [\text{new}/u] = \text{if } l_0 [\text{new}/u] \text{ then } (l_1 . x) [\text{new}/u] \text{ else } (l_2 . x) [\text{new}/u] \text{ fi}
\]

if \( l_0 \) then \( l_1 \) else \( l_2 \) \([\text{new}/u]\)

\[
\left( l_1 \equiv l_2 \right) [\text{new}/u] = \left( l_1 [\text{new}/u] \right) \equiv \left( l_2 [\text{new}/u] \right)
\]

if neither \( l_1 \) nor \( l_2 \) is \( u \) or of the form \( \ldots \) fi

\[
\left( l_1 \equiv l_2 \right) [\text{new}/u] = \text{false}
\]

if either \( l_1 = u \) and \( l_2 \) is not \( u \) or of the form \( \ldots \) fi

or \( l_2 = u \) and \( l_1 \) is not \( u \) or of the form \( \ldots \) fi

\[
\left( l_1 \equiv l_2 \right) [\text{new}/u] = \text{true}
\]

if \( l_1 = l_2 = u \)
\[
\left(\text{if } l_0 \text{ then } l_1 \text{ else } l_2 \text{ fi} \right) \left[\text{new/u}\right] =
\begin{cases}
\text{if } l_0 \left[\text{new/u}\right] \uparrow \\
\text{then } \left(l_3 \uparrow\right) \left[\text{new/u}\right] \\
\text{else if } l_0 \left[\text{new/u}\right] \\
\text{then } \left(l_1 \downarrow l_3\right) \left[\text{new/u}\right] \\
\text{else } \left(l_2 \downarrow l_3\right) \left[\text{new/u}\right] \\
\text{fi}
\end{cases}
\]

\[
\left(l_1 \downarrow \text{if } l_0 \text{ then } l_2 \text{ else } l_3 \text{ fi} \right) \left[\text{new/u}\right] =
\begin{cases}
\text{if } l_0 \left[\text{new/u}\right] \uparrow \\
\text{then } \left(l_1 \uparrow\right) \left[\text{new/u}\right] \\
\text{else if } l_0 \left[\text{new/u}\right] \\
\text{then } \left(l_1 \downarrow l_2\right) \left[\text{new/u}\right] \\
\text{else } \left(l_1 \downarrow l_3\right) \left[\text{new/u}\right] \\
\text{fi}
\end{cases}
\]

\text{if } l_1 \text{ is not of the form if } \ldots \text{ fi}

\[
(l_1 + l_2) \left[\text{new/u}\right] = (l_1 \left[\text{new/u}\right]) + (l_2 \left[\text{new/u}\right])
\]

\[
(l_1 < l_2) \left[\text{new/u}\right] = (l_1 \left[\text{new/u}\right]) < (l_2 \left[\text{new/u}\right])
\]

\[
| l | \left[\text{new/u}\right] = |l| \left[\text{new/u}\right]
\]

\[
(l_1 \cdot l_2) \left[\text{new/u}\right] = (l_1 \left[\text{new/u}\right]) \cdot (l_2 \left[\text{new/u}\right])
\]

\text{Lemma 5.14}
\text{Let } u \in TVar_d \text{ with } d \in C \text{ (i.e., } d \neq \text{Int, Bool}).

1. For every logical expression \(l\) we have that \(l[\text{new/u}]\) is defined if and only if \(l\) is \textit{not} of the form indicated by the following BNF definition:

\[
l_0 ::= u
\]

\[
| l | \text{ if } l_0 \text{ then } l \text{ else } l_1 \text{ fi}
\]

\[
| l | \text{ if } l_0 \text{ then } l_1 \text{ else } l // fi
\]

Doc. No.
2. If \( \sigma \in \Sigma, \delta \in \Delta^*, \omega \in \Omega, \) and \( \gamma \in \Gamma \) are such that \( \mathcal{O}(\sigma, \delta, \omega), \) and if \( \sigma' = S[\gamma](\delta)(\sigma) \) then for every logical expression \( l \) such that \( l[\text{new}/u] \) is defined we have

\[
\mathcal{L}[l[\text{new}/u]](\omega)(\delta)(\sigma) = \mathcal{L}[l](\omega)(\delta)(\sigma').
\]

**Proof**

The first part is easily proved by induction on the complexity of \( l \). For the second part we first observe that

\[
\sigma' = \sigma\{\sigma(1)U \downarrow \beta / \downarrow \}
\]

where \( \beta = \text{pick}^d(\sigma(1)U \downarrow) \), so \( \beta \notin \sigma(1)U \downarrow \{ \downarrow \} \) (see definitions 3.13 and 3.14).

Now we can prove our lemma by induction on the complexity of \( l \). In several places we need the information that \( \mathcal{O}(\sigma, \delta, \omega) \) together with lemma 4.11 in order to prove that the result of an intermediate logical expression is not equal to \( \beta \). Let us deal with one representative case: \( l = x'.x \). Then \( l[\text{new}/u] = l = x'.x \). Now the induction hypothesis tells us that \( \mathcal{L}[x'.x](\omega)(\delta)(\sigma) = \mathcal{L}[x'.x](\omega)(\delta)(\sigma') \). If we put this equal to \( \beta' \) then we know \( \beta' \neq \beta \) because lemma 4.11 tells us that \( \beta' \in \sigma(1)U \downarrow \{ \downarrow \} \). Therefore we have \( \mathcal{L}[x'.x](\omega)(\delta)(\sigma) = \sigma(2)(\beta')(x) = \sigma'(2)(\beta')(x) = \mathcal{L}[x'.x](\omega)(\delta)(\sigma') \). \( \square \)

**Definition 5.15**

We extend the substitution operation \( [\text{new}/u] \) to assertions other than logical expressions as follows (we assume that the type of \( u \) is \( d \in C)\):

\[
(P \rightarrow Q)[\text{new}/u] = (P[\text{new}/u]) \rightarrow (Q[\text{new}/u])
\]

\[
(\neg P)[\text{new}/u] = \neg(P[\text{new}/u])
\]

\[
(\forall z_d P)[\text{new}/u] = (\forall z(P[\text{new}/u])) \wedge (P[u/z][\text{new}/u])
\]

\[
(\forall z_d P)[\text{new}/u] = (\forall z \forall z' [z] = [z'] \rightarrow (P[z', u/z][\text{new}/u]))
\]

\[
(\forall z_a P)[\text{new}/u] = (\forall z(P[\text{new}/u])) \quad \text{if } a \neq d, d^*
\]

\[
(\exists z_d P)[\text{new}/u] = (\exists z(P[\text{new}/u])) \lor (P[u/z][\text{new}/u])
\]

\[
(\exists z_d P)[\text{new}/u] = (\exists z \exists z' [z] = [z'] \land (P[z', u/z][\text{new}/u]))
\]

\[
(\exists z_a P)[\text{new}/u] = (\exists z(P[\text{new}/u])) \quad \text{if } a \neq d, d^*
\]

Here we choose for \( z' \) the first variable from \( L\text{Var}^* \) that does not occur in \( P \). The idea is that \( z \) and \( z' \) together code a sequence of objects in the state after the new-statement. At the places where \( z' \) yields t the value of the coded sequence is the newly created object. Where \( z' \) yields f the value of the coded sequence is the same as the value of \( z \) and where \( z' \) delivers 1. the coded sequences also yields 1.

We still have to define the substitution operation \( [z', u/z] \) and we shall do that now:
Definition 5.16
Let \( d \in C \), \( u \in TVard_d \), \( z \in LVar_d^* \), and \( z' \in LVar^* \). For logical expressions we define the operation \([z', u/z]\) as follows:

\[
\begin{align*}
e [z', u/z] &= e, \\
z [z', u/z] &\text{ is undefined,} \\
z'' [z', u/z] &= z'' \quad \text{if } z'' \neq z, \\
l \cdot x [z', u/z] &= (l[z', u/z]) \cdot x, \\
|z| [z', u/z] &= |z|, \\
[l] [z', u/z] &= l[z', u/z] \quad \text{if } l \neq z, \\
(z \cdot l_2) [z', u/z] &= \begin{cases} 
z' \cdot (l_2[z', u/z]) & \text{if } \text{true} \\
0 & \text{if } \text{false}
\end{cases} \\
(l_1 \cdot l_2)[z', u/z] &= (l_1[z', u/z]) \cdot (l_2[z', u/z]) \quad \text{if } l_1 \neq z,
\end{align*}
\]

If \( l_0 \) then \( l_1 \) else \( l_2 \) \( [z', u/z] =
\begin{cases} 
( (l_0[z', u/z]) & \text{if } (l_0[z', u/z]) \text{ true} \\
(l_1[z', u/z]) & \text{if } (l_0[z', u/z]) \text{ false}
\end{cases}
\]

\[
\begin{align*}
(l_1 \vee l_2)[z', u/z] &= (l_1[z', u/z]) \vee (l_2[z', u/z]) \\
(l_1 \mathbf{+} l_2)[z', u/z] &= (l_1[z', u/z]) + (l_2[z', u/z]) \\
\cdots
\end{align*}
\]

\[
\begin{align*}
|l| [z', u/z] &= |l[z', u/z]|, \\
(l_1 \cdot l_2)[z', u/z] &= (l_1[z', u/z] \cdot l_2[z', u/z])
\end{align*}
\]

We extend this definition to assertions other than logical expressions as follows:

\[
\begin{align*}
(P \to Q)[z', u/z] &= (P[z', u/z]) \to (Q[z', u/z]), \\
(-P) [z', u/z] &= \neg (P[z', u/z]), \\
(\forall z \, P) [z', u/z] &= (\forall z \, P) \\
(\forall z'' \, P) [z', u/z] &= (\forall z'' \, (P[z', u/z])) \quad \text{if } z'' \neq z, \\
(\exists z \, P) [z', u/z] &= (\exists z \, P) \\
(\exists z'' \, P) [z', u/z] &= (\exists z'' \, (P[z', u/z])) \quad \text{if } z'' \neq z
\end{align*}
\]

Lemma 5.17
Let \( u, z, z' \) be as in definition 5.16. Let \( \sigma \in \Sigma \), \( \delta \in \Delta^c \), \( \omega \in \Omega \), and take \( \alpha = \omega_{(d^c)}(z) \), \( \alpha' = \omega_{(d)}(z') \), \( \beta = \sigma_{(d)}(u) \). Suppose that \( \text{len}^d(\alpha) = \text{len}(\alpha') \). Define \( \alpha'' \in O^d \) to be the sequence that satisfies (for all \( n \in Z \)):

Doc. No.
\[
\text{len}(\alpha'') = \text{len}(\alpha) \\
\text{elt}(\alpha'', n) = \beta \quad \text{if} \ \text{elt}(\alpha', n) = \top \\
\text{elt}(\alpha'', n) = \text{elt}(\alpha, n) \quad \text{if} \ \text{elt}(\alpha', n) = \bot \\
\text{elt}(\alpha'', n) = \bot \quad \text{if} \ \text{elt}(\alpha', n) = \bot
\]

and take \( \omega' = \omega\{\alpha''/z\} \).

Then we have:

1. For every \( l \in LExpr_{\alpha}^\circ \) such that \( l \neq z \):
   \[
   L_{\alpha}^\circ [l[z', u/z]](\omega)(\delta)(\sigma) = L_{\alpha}^\circ [l](\omega')(\delta)(\sigma).
   \]

2. For every \( P \in Ass_{\alpha}^\circ \) such that \( z' \) does not occur in \( P \):
   \[
   A_{\alpha}^\circ [P[z', u/z]](\omega)(\delta)(\sigma) = A_{\alpha}^\circ [P](\omega')(\delta)(\sigma).
   \]

**Proof**

The proof consists of a quite easy induction on the complexity of \( l \) and \( P \) respectively. Of course, the only interesting case is when \( l \) is of the form \( z \cdot l_2 \). Note that the condition on \( z' \) is necessary to exclude assertions of the form \( \forall z' P \) or \( \exists z' P \).

**Lemma 5.18**

Let \( \sigma \in \Sigma, \delta \in \Delta^\circ, \omega \in \Omega \) such that \( OK(\sigma, \delta, \omega) \). Let \( d \in C, u \in TVar_d, \gamma \in \Gamma \) and define \( \sigma' = S^\circ[u \leftarrow \text{new}](\gamma)(\delta)(\sigma) \). Then for every assertion \( P \in Ass_{\alpha}^\circ \) we have
\[
A_{\alpha}^\circ [P[\text{new}/u]](\omega)(\delta)(\sigma) = A_{\alpha}^\circ [P](\omega)(\delta)(\sigma').
\]

**Proof**

Again we use induction on the complexity of \( P \). The only case which is not yet clear from the first approach is quantification over sequences, so let us consider the case where \( P = \forall z_{d^*} Q \). Take \( \beta = f^d(\sigma(d)) \), so that \( \sigma'(d) = \sigma(d) \cup \{\beta\} \) and \( \beta = \sigma'(3)(d)(u) \), and let \( z' \) be the first variable from \( LVar_{d^*} \) that does not occur in \( Q \).

Now suppose that
\[
A[[\forall z_{d^*} Q][\text{new}/u]](\omega)(\delta)(\sigma) = \top.
\]

We shall prove that
\[
A[[\forall z_{d^*} Q]](\omega)(\delta)(\sigma') = \top
\]
so we have to show that for every \( \alpha'' \in O_{d^*}^{\circ} \) such that \( \text{elt}(\alpha'', n) \in \sigma'(d) \) for all \( n \in Z \), it is the case that \( A[[Q]](\omega\{\alpha''/z\})(\delta)(\sigma') = \top \). If we have such an \( \alpha'' \), we can define \( \alpha \in O_{d^*}^{\circ} \) and \( \alpha' \in O^\circ \) as follows:

Doc. No.
\[ \text{len}(\alpha) = \text{len}(\alpha') = \text{len}(\alpha'') \]

\[
\text{elt}(\alpha, n) = 1, \quad \text{elt}(\alpha', n) = t \quad \text{if} \quad \text{elt}(\alpha'', n) = \beta \\
\text{elt}(\alpha, n) = \text{elt}(\alpha'', n), \quad \text{elt}(\alpha', n) = f \quad \text{if} \quad 1 \leq n \leq \text{len}(\alpha'') \\
\] and \( \text{elt}(\alpha'', n) \neq \beta \)

Now because

\[
A[\forall z:\forall z'.z | z' \rightarrow Q[z', u/z][\text{new}/u]](\omega)(\delta)(\sigma) = t
\]

and because \( \alpha \) and \( \alpha' \) have equal length and do not have elements outside \( \sigma_1^{(d)} \) and \( \sigma_1^{(t)} \) respectively, we know that

\[
A[Q[z', u/z][\text{new}/u]](\omega(\alpha/z)(\alpha'/z'))(\delta)(\sigma) = t.
\]

The induction hypothesis then tells us that

\[
A[Q[z', u/z]](\omega(\alpha/z)(\alpha'/z'))(\delta)(\sigma') = t.
\]

Finally we can apply lemma 5.17 and use the fact that \( z' \) does not occur in \( Q \), to see that

\[
A[Q](\omega(\alpha''/z))(\delta)(\sigma') = t.
\]

To prove that \( A[\forall z:\forall z'.z | z' \rightarrow Q[z', u/z][\text{new}/u]](\omega)(\delta)(\sigma) = t \) implies \( A[\forall z:\forall z'. Q][\text{new}/u]](\omega)(\delta)(\sigma) = t \) involves reasoning in the other direction, in particular to find a suitable \( \alpha'' \) for each pair \( \alpha, \alpha' \) that satisfies certain conditions. We omit further details. \( \square \)

Again we extend this result to the case of programs:

**Corollary 5.19**

The axiom (NT) is valid, that is, for every environment \( \gamma \) we have

\[
\gamma = \{ P[\text{new}/u] \} \langle U \mid c : u \leftarrow \text{new} \rangle \{ P \}.
\]

\( \square \)

### 5.2.2 Assigning a new object to an instance variable

**Definition 5.20**

If our assignment is of the form \( z \leftarrow \text{new} \) we have the following axiom:

\[
\{ P[\text{new}_c/z_{\gamma}] \} \langle U \mid c : x_{\gamma} \leftarrow \text{new}_c \rangle \{ P \} \tag{NI}
\]

Fortunately, after having worked through the previous subsection, this new axiom is simple to define and to prove valid.
Definition 5.21
The substitution operation \([\text{new}e / x]_{\sigma}\) is defined by:

\[ P[\text{new}e / x]_{\sigma} = P[u.e / x]_{\sigma} \] 

where \(u.e\) is a temporary variable that does not occur in \(P\). (It is easy to see that this definition does not depend on the actual \(u\) used.)

Lemma 5.22
Let \(\sigma, \delta \in \Delta^c\) and \(\omega \in \Omega\) be such that \(\text{OK}(\sigma, \delta, \omega)\). Let \(\gamma \in \Gamma, d \in C, x \in \text{IVar}_d^c\), and define \(\sigma' = S[x \leftarrow \text{new}] (\gamma)(\delta)(\sigma)\). Then for every assertion \(P^c\) we have

\[ \omega, \delta, \sigma\models P[\text{new} / x] \iff \omega, \delta, \sigma'\models P. \]

Proof
Choose some \(u \in TVar_d\) which does not occur in \(P\), so that we have \(P[\text{new} / x] = P[u / x][\text{new} / u]\). Let \(\sigma'' = S[u \leftarrow \text{new}; x \leftarrow u] (\gamma)(\delta)(\sigma)\). We have by lemma 5.8 and lemma 5.18 that \(\omega, \delta, \sigma\models P[u / x][\text{new} / u] \iff \omega, \delta, \sigma''\models P\).

Now if \(\beta = \text{pick}^d(\sigma(d))\) then we have \(\sigma' = \sigma\{\beta / (1, x)\}\) and \(\sigma'' = \sigma\{\beta / u\}\{\beta / (1, x)\}\), so that \(\sigma'' = \sigma'\{\beta / u\}\). Because \(u\) does not occur in \(P\) we have \(\omega, \delta, \sigma'\models P \iff \omega, \delta, \sigma''\models P\), and the result of the lemma follows.

Corollary 5.23
The axiom (NI) is valid, that is, for every environment \(\gamma\) we have

\[ \gamma \models \{ P[\text{new} / x] \} \langle U | c : x \leftarrow \text{new} \} \{P\}. \]

5.3 Sending messages

In this subsection we present some proof rules for verifying the third kind of assignments: the ones where a message is sent and the result stored in the variable on the left hand side. We start with a rule for a non-recursive method and later on we show how to deal with recursion.

Definition 5.24
For the statement \(x \leftarrow e_0!m(e_1, \ldots, e_n)\), where \(x \in \text{IVar}_{d_0}^c\), \(m \in \text{Name}_{d_0}^c, \ldots, d_n\), \(e_0 \in \text{Exp}_{d_0}^c\) and \(e_i \in \text{Exp}_{d_i}^c\) for \(i = 1, \ldots, n\), we have the following proof rule:

\[
\frac{\text{MI}}{
\begin{array}{c}
P \wedge \land_{i=1}^k v_i \equiv \text{nil} \\
Q[e'] S \\
Q[e'/\text{self}, \bar{u}][f/\bar{x}] \rightarrow R[e/x]
\end{array}
\}
\]

\[
\{P[\bar{e}/\text{self}, \bar{u}][f/\bar{x}]\} \langle U | c : x \leftarrow e_0!m(e_1, \ldots, e_n) \} \{R\}
\]
where $S \in \text{Stat}^c$ and $e \in \text{Exp}_{d_0}^c$ are the statement and expression occurring in the definition of the method $m$ in the unit $U$, $u_1, \ldots, u_n$ are its formal parameters, $v_1, \ldots, v_k$ is a row of temporary variables that are not formal parameters ($k \geq 0$), $r$ is a logical variable of type $d_0$ that does not occur in $R$, $f_j$ is an arbitrary row of expressions (not logical expressions) in class $c$, and $\bar{z}$ is a row of logical variables, mutually different and different from $r$, such that the type of each $z_i$ is the same as the type of the corresponding $f_j$. Furthermore, $[\bar{e}/\text{self}, \bar{u}]$ stands for a \emph{simultaneous} substitution having the “components” $[e_0/\text{self}], [e_1/u_1], \ldots, [e_n/u_n]$ (a formal definition will follow). We require that no temporary variables other than the formal parameters $u_1, \ldots, u_n$ occur in $P$ or $Q$.

We still have to define precisely what $[\bar{e}/\text{self}, \bar{u}]$ means, but before doing that let us give some informal explanation of the above rule. When a statement as above is executed, several things happen. First, control is transferred from the sender of the message to the receiver (context switching). The formal parameters of the receiver are initialized with the values of the expressions that form the actual parameters of the message and the other temporary variables are initialized to nil. Then the body $S$ of the method is executed. After that the result expression $e$ is evaluated, control is returned to the sender, the temporary variables are restored, and the result object is assigned to the variable $x$.

The first thing, the context switching, is represented by the substitution $[e_0/\text{self}]$. A little more precisely, an assertion $P$ as seen from the receiver’s viewpoint is equivalent to $P[e_0/\text{self}]$ from the viewpoint of the sender. Note that this substitution also changes the class of the assertion: $P[e_0/\text{self}] \in \text{Ass}^c$ whereas $P \in \text{Ass}^c$. Now the passing of the parameters is simply represented by the substitution $[e_1, \ldots, e_n/u_1, \ldots, u_n]$. Therefore after the parameters have been transferred to the receiver, $P$ from the receiver’s viewpoint corresponds to $P[e/\text{self}, \bar{u}]$ as seen by the sender. (Note that we really need \emph{simultaneous} substitution here, because $u_i$ might occur in an $e_j$ with $j < i$, but it should not be substituted again.) In reasoning about the body of the method we may also use the information that temporary variables that are not parameters are initialized to nil.

The second thing to note is the way the result is passed back. Here the logical variable $r$ plays an important role. This is best understood by imagining after the body $S$ of the method the statement $r \leftarrow e$ (which is syntactically illegal, however, because $r$ is a \emph{logical} variable). In the sending object one could imagine the (equally illegal) statement $x \leftarrow r$. Now if the body $S$ terminates in a state where $Q[e/r]$ holds (a premiss of the rule) then after this “virtual” statement $r \leftarrow e$ we would have a situation in which $Q$ holds. Otherwise stated, the assertion $Q$ describes the situation after executing the method body, in which the result is represented by the logical variable $r$, everything seen from the viewpoint of the receiver. Now if we context-switch this $Q$ to the sender’s side, and if it implies $R[r/x]$, then we know that after assigning the result to the variable $x$ (our second imaginary assignment $x \leftarrow r$), the
assertion \( R \) will hold.

Now we come to the role of \( f \) and \( z \). We know that during the evaluation of the method the sending object becomes blocked, that is, it cannot answer any incoming messages. Therefore its instance variables will not change in the meantime. The temporary variables will be restored after the method is executed, so these will also be unchanged and finally the symbol self will retain its meaning over the call. All the expressions in class c (and in particular the \( f_i \)) are built from these expressions plus some inherently constant expressions and therefore their value will not change during the call. However, the method can change the variables of other objects and new objects can be created, so that the properties of these unchanged expressions can change. In order to be able to make use of the fact that the expressions \( f \) are constant during the call, the rule offers the possibility to replace them temporarily by the logical variables \( z \), which are automatically constant. So, in reasoning from the receiver's viewpoint (in the rule this applies to the assertions \( P \) and \( Q \)) the value of the expression \( f_i \) is represented by \( z_i \), and in context switching \( f_i \) comes in again by the substitution \([f/z]\). Note that the constancy of \( f \) is guaranteed up to the point where the result of the method is assigned to \( x \), and that \( x \) may occur in \( f_i \), so that it is possible to make use of the fact that \( x \) remains unchanged right up to the assignment of the result.

**Definition 5.25**

Now we define formally the substitution operation \([e/self]\). First we do this for logical expressions:

\[
\begin{align*}
  x \ [e/self] & = e . x \\
  u \ [e/self] & = u \\
  z \ [e/self] & = z \\
  self\ [e/self] & = e \\
  l \ [e/self] & = l \quad \text{if } l = \text{nil, true, false, } n \\
  l \cdot z\ [e/self] & = (l\ [e/self]) \cdot x \\
  \text{if } l_0 \text{ then } l_1 \text{ else } l_2 \ fi\ [e/self] & = \text{if } l_0\ [e/self] \text{ then } l_1\ [e/self] \text{ else } l_2\ [e/self] \ fi \\
  (l_1 \ =\ l_2)\ [e/self] & = (l_1\ [e/self]) \ =\ (l_2\ [e/self]) \\
  (l_1 \ +\ l_2)\ [e/self] & = (l_1\ [e/self]) \ +\ (l_2\ [e/self]) \\
  \vdots \\
  (l_1 \ <\ l_2)\ [e/self] & = (l_1\ [e/self]) \ <\ (l_2\ [e/self]) \\
  \vdots \\
  l[l\ [e/self]] & = l[l\ [e/self]] \\
  (l_1 \cdot l_2)\ [e/self] & = (l_1\ [e/self] \cdot l_2\ [e/self])
\end{align*}
\]
Now we extend this to assertions other than logical expressions:
\[(P \rightarrow Q)[e/self] = (P[e/self]) \rightarrow (Q[e/self])\]
\[\neg P[ e/self] = \neg (P[e/self])\]
\[(\forall z P)[ e/self] = \forall z(P[e/self])\]
\[(\exists z P)[ e/self] = \exists z(P[e/self])\]

Lemma 5.26
Let \(\sigma \in \Sigma, \delta \in \Delta^e, e \in \text{Exp}_e^\omega,\) and define \(\beta' = \mathcal{E}[e](\delta)(\sigma)\). Let \(\delta' \in \Delta^e\) be such that \(\delta'|_1 = \beta\). Then we have

1. For every logical expression \(I^e\) and every valuation \(\omega\)
   \[\mathcal{L}[I](\omega)(\delta')(\sigma) = \mathcal{L}[I[e/e]](\omega)(\delta)(\sigma)\]
2. For every assertion \(P^e\) and every valuation \(\omega\)
   \[\mathcal{A}[P](\omega)(\delta')(\sigma) = \mathcal{A}[P[e/e]](\omega)(\delta)(\sigma)\]

Proof
An easy induction on the complexity of \(I\) and \(P\).

Definition 5.27
Although the intention of simultaneous substitution is probably clear to the reader, we give its definition for the case in which we really need it here, for completeness' sake. Let \(\bar{e} = e_0, \ldots, e_n\) and \(\bar{u} = u_1, \ldots, u_n\). Then we define:
\[x[e/self, \bar{u}] = e_0 \cdot x\]
\[u_i[e/self, \bar{u}] = e_i \quad \text{for } i = 1, \ldots, n\]
\[u[e/self, \bar{u}] = u \quad \text{if } u \notin \{u_1, \ldots, u_n\}\]
\[z[e/self, \bar{u}] = z\]
\[\text{self}[e/self, \bar{u}] = e_0\]
\[l[e/self, \bar{u}] = l \quad \text{if } l = \text{nil, true, false, } n\]
\[l \cdot x[e/self, \bar{u}] = (l[e/e, \bar{u}]).x\]
\[\text{if } l_0 \text{ then } l_1 \text{ else } l_2 [e/self, \bar{u}] = \text{if } l_0[e/self, \bar{u}] \text{ then } l_1[e/self, \bar{u}] \text{ else } l_2[e/self, \bar{u}] \text{ fi}\]
\[(l_1 \doteq l_2)[e/self, \bar{u}] = (l_1[e/self, \bar{u}]) \doteq (l_2[e/self, \bar{u}])\]
\[(l_1 + l_2)[e/self, \bar{u}] = (l_1[e/self, \bar{u}]) + (l_2[e/self, \bar{u}])\]
\[
\vdots
\]
\[(l_1 < l_2)[e/self, \bar{u}] = (l_1[e/self, \bar{u}]) < (l_2[e/self, \bar{u}])\]
\[
\vdots
\]
\[
|I|_{\bar{e}/self, \bar{u}} = |I|_{\bar{e}/self, \bar{u}} \\
(l_1 \cdot l_2)_{\bar{e}/self, \bar{u}} = (l_1_{\bar{e}/self, \bar{u}} \cdot l_2_{\bar{e}/self, \bar{u}})
\]

Now we extend this to assertions other than logical expressions:

\[
(P \rightarrow Q)_{\bar{e}/self, \bar{u}} = (P_{\bar{e}/self, \bar{u}}) \rightarrow (Q_{\bar{e}/self, \bar{u}}) \\
(\neg P)_{\bar{e}/self, \bar{u}} = \neg (P_{\bar{e}/self, \bar{u}}) \\
(\forall z P)_{\bar{e}/self, \bar{u}} = \forall z (P_{\bar{e}/self, \bar{u}}) \\
(\exists z P)_{\bar{e}/self, \bar{u}} = \exists z (P_{\bar{e}/self, \bar{u}})
\]

Of course we also have a corresponding lemma:

**Lemma 5.28**

Let \( \sigma \in \Sigma \), \( \delta \in \Delta^e \) and \( e_i \in \text{Exp}_{\delta_i} \) for \( i = 0, \ldots, n \) (with \( d_0 \in C \)). Define \( \beta_i = \mathcal{L}[e_i](\delta)(\sigma) \). Let \( \delta' \in \Delta^{d_0} \) be such that \( \delta'_{(1)} = \beta_0 \) and let \( \sigma' = \sigma_{\{\beta_i/u_i\}_{i=1}^k} \). Then we have

1. For every logical expression \( l^{d_0}_e \) and every valuation \( \omega \)
   \[
   \mathcal{L}[l](\omega)(\delta')(\sigma') = \mathcal{L}[l_{\bar{e}/self, \bar{u}}](\omega)(\delta)(\sigma).
   \]

2. For every assertion \( P^{d_0} \) and every valuation \( \omega \)
   \[
   \mathcal{A}[P](\omega)(\delta')(\sigma') = \mathcal{A}[P_{\bar{e}/self, \bar{u}}](\omega)(\delta)(\sigma).
   \]

**Proof**

Again a quite simple induction on the complexity of \( l \) and \( P \).

**Example 5.29**

Let us illustrate the use of the rule (MI) by a small example. Consider the unit \( U = c : (m : u_0) : x_1 \leftarrow u_0 \uparrow x_2 \) and the program \( \rho = (U[c : x_1 \leftarrow u_1!m(x_2)]) \). We want to show

\[
\{ u_1 . x_1 \triangleq x_1 \land \neg u_1 \triangleq \text{self} \} \rho \{ u_1 . x_1 \triangleq x_2 \land x_1 \triangleq u_1 . x_2 \}.
\]

So let us apply the rule (MI) with the following choices:

\[
\begin{align*}
P &= x_1 \triangleq x_1 \land \neg \text{self} \triangleq x_2 \\
Q &= x_1 \triangleq u_0 \land \neg x_2 \land \neg \text{self} \triangleq x_2 \\
R &= u_1 . x_1 \triangleq x_2 \land x_1 \triangleq u_1 . x_2 \\
k &= 0 \quad \text{(we shall use no } u_i) \\
f_1 &= x_1 \quad \text{(represented by } z_1 \text{ in } P \text{ and } Q) \\
f_2 &= \text{self} \quad \text{(represented by } z_2 \text{ in } P \text{ and } Q)
\end{align*}
\]

Doc. No.
First notice that $P[u_1, x_2 / self, u_0][x_1, self / z_1, z_2] = u_1 . x_1 = z_1 \land \neg u_1 = self$ so that the result of the rule is precisely what we want.

For the first premiss we have to prove

$$\{x_1 = z_1 \land \neg self = z_2\} \{u_1 . x_1 = u_0 . x_2 = z_2 \land \neg self = z_2\}.$$ 

This is easily done with the axiom (SAI) and the rule of consequence (which will be introduced in definition 5.39).

With respect to the second premiss, we have

$$Q[u_1, x_2 / self, u_0][x_1, self / z_1, z_2] = u_1 . x_1 = z_2 \land \neg u_1 . x_2 = z_2 \land \neg self = z_2.\]

$$R[r/x_1] = \begin{cases} u_1 \text{ if } u_1 = self \text{ then } r \text{ else } u_1 . x_1 \text{ if } z_2 \land \neg u_1 = z_2.\end{cases}$$

It is quite clear that the first implies the second, and we can use this implication as an axiom (see definition 5.38).

**Lemma 5.30**

The proof rule (MI) is valid.

**Proof**

Consider the rule as listed in definition 5.24. Let $\gamma \in \Gamma$ and suppose that the premisses are valid with respect to $\gamma$. We shall prove that the conclusion is valid with respect to $\gamma$. So let $\sigma, \delta, \omega \in \Delta^e$, and $\omega \in \Omega$ be such that $\sigma, \delta, \omega \models P[\bar{e} / self, \bar{u}][\bar{i} / \bar{z}]$. Let $\gamma' = \mathcal{U}[\mathcal{U}](\gamma)$ and let $\sigma' = \mathcal{P}[\mathcal{U}[c : x \leftarrow e_0.m(e_1, \ldots, e_n)](\gamma)(\delta)(\sigma)$. So $\sigma' = S[x \leftarrow e_0.m(e_1, \ldots, e_n)](\gamma)(\delta)(\sigma)$. We have to prove $\sigma', \delta, \omega \models R$.

Let $\omega' = \omega[\mathcal{F}[\bar{f}](\delta)(\sigma)/z_i]_{i=1}^{\bar{i}}$. Then lemma 5.12 gives us $\sigma, \delta, \omega' \models P[\bar{e} / self, \bar{u}]$. Let $\beta_i = \mathcal{E}[e_i](\delta)(\sigma)$ for $i = 0, \ldots, n$ and suppose that $\beta_0 \neq \bot$ and $\beta_0 \notin \delta(2)(\sigma)$ (otherwise we would have that $\sigma' = \bot$ and the result would be trivial). Define $\delta' = \langle \beta_0, \delta(2) \cup \{\delta(1) / c\}\rangle$ and $\sigma_1 = \langle \sigma(1), \sigma(2), \sigma(3) \rangle$ where $\sigma_1(3)(u_i) = \beta_i$ and $\sigma_1(3)(u_d) = \bot$ if $u \notin \{u_1, \ldots, u_n\}$. Now because of lemma 5.28 and the fact
\[
\begin{align*}
\sigma, \delta, \omega \models P[\bar{e}/\text{self}, \bar{u}][\bar{f}/\bar{z}] & \Rightarrow \sigma, \delta, \omega' \models P[\bar{e}/\text{self}, \bar{u}] \Rightarrow \sigma_1, \delta', \omega' \models P \\
& \downarrow \\
& \sigma_2, \delta', \omega' \models Q[e/r] \\
\sigma'', \delta, \omega_1 \models Q[\bar{e}/\text{self}, \bar{u}][\bar{f}/\bar{z}] & \Leftarrow \sigma'', \delta, \omega'_1 \models Q[\bar{e}/\text{self}, \bar{u}] \Leftarrow \sigma_2, \delta', \omega'_1 \models Q \\
& \downarrow \\
& \sigma'', \delta, \omega_1 \models R[r/x] \\
& \downarrow \\
& \sigma', \delta, \omega_1 \models R \\
& \downarrow \\
& \sigma', \delta, \omega \models R
\end{align*}
\]

Figure 3: The structure of the proof of lemma 5.30.

that temporary variables other than the \(u_i\) may not occur in \(P\), we have \(\sigma_1, \delta', \omega' \models P\). We also know that \(\sigma_1, \delta', \omega' \models v_i \neq \text{nil} \) for \(i = 1, \ldots, k\) so \(\sigma_1, \delta', \omega' \models P \wedge \bigwedge_{i=1}^{k} v_i \neq \text{nil}\).

Now because of the construction of \(\gamma'\) in definition 3.17 we know that \(\gamma'(c', \bar{d})(m) = M[\bar{u}] : S \uparrow e[\gamma']\) so we can refer directly to the method definition of \(m\) in \(U\) to see what \(\gamma'(c', \bar{d})(m)\) does. So let us take \(\sigma_2 = P[\bar{u}] : S[\gamma'(c', \bar{d})(\sigma_1)], \) then \(\sigma_2 = S[S][\gamma')(\sigma_1)\). Assume that \(\sigma_2 \neq \bot\), otherwise we have \(\sigma' = \bot\) and we are ready. The validity of the first premiss with respect to \(\gamma\) tells us that \(\sigma_2, \delta', \omega' \models Q[e/r]\). Let \(\beta = E[e][\gamma')(\sigma_2), \omega_1 = \omega(\beta/r)\), and \(\omega'_1 = \omega'(\beta/r)\). Then because of lemma 5.12 we have \(\sigma_2, \delta', \omega'_1 \models Q\).

Let \(\sigma'' = (\sigma_2(1), \sigma_2(2), \sigma_3)\) (we restore the temporary variables). Now we appeal to the reader's understanding of the semantics of the language to see that the method destination \(e_0\), the actual parameters \(e_1, \ldots, e_n\) and the expressions \(f\) are unchanged in \(\sigma''\) in comparison with \(\sigma\). Otherwise stated, \(E[e_1][\gamma')(\sigma_2)] = E[e_1][\gamma')(\sigma'')\) and the same for \(f_i\). (Of course, this can also be proved formally.) Then we know from lemma 5.28 that \(\sigma'', \delta, \omega'_1 \models Q[\bar{e}/\text{self}, \bar{u}]\) and from lemma 5.12 together with the observation that \(\omega'_1 = \omega_1(E[f_i[\gamma')(\sigma)/z_i])_{i=1}^{n}\) we get \(\sigma'', \delta, \omega_1 \models Q[\bar{e}/\text{self}, \bar{u}][\bar{f}/\bar{z}]\).

From the second premiss we can conclude that \(\sigma'', \delta, \omega_1 \models R[r/x]\). Now for the final state \(\sigma'\) we know that \(\sigma' = \sigma''\{\beta/\delta(1), x\}\), so lemma 5.8 tells us that \(\sigma', \delta, \omega_1 \models R\). Finally, because \(\gamma\) does not occur in \(R\), we have \(\sigma', \delta, \omega \models R\).

\[\square\]

Definition 5.31
For the statement \(u \leftarrow e_0!m(e_1, \ldots, e_n), \) where \(u \in TVar_{d_0}, m \in MName_{d_0, \ldots, d_n}\).
Lemma 5.32
The proof rule (MT) is valid.

Proof
This can be proved by a slight adaptation of the proof of lemma 5.30.

Now we come to the issues of how to handle recursive and even mutually recursive methods. For this we use an adapted version of the classical recursion rule (see for example [3]). The classical rule goes as follows (in the notation of [3]):

\[
\{p\} P \{q\} \vdash \{p\} S_0 \{q\} \\
\{p\} P \{q\}
\]

The idea is to prove (the operator \( \vdash \) expresses provability) the correctness of the body \( (S_0) \) from the assumption that the procedure call \( (P) \) itself satisfies its specification. If that has been done we can conclude the correctness of the procedure call without assumptions. The validity of this rule can be proved as follows: the meaning of the procedure call is the limit of a increasing sequence starting with \( \bot \), in which every element is obtained from the previous one by assuming the previous as the meaning of the procedure call and calculating the meaning of the body from that. From the premiss of the rule we can prove that every element in the sequence satisfies the specification and by a continuity argument we conclude that the procedure call itself satisfies the specification.

There are several remarks to be made. One is that in proving the premiss of the rule we may not make use of the declaration of \( P \), because otherwise we are not sure that the implication also holds for the intermediate elements in the approximating sequence. The second remark is that if we have a non-recursive rule like our rules (MI) and (MT), then we could change the conclusion of the recursion rule into \( \{p\} S \{q\} \), from which we could infer \( \{p\} P \{q\} \) by the non-recursive rule. We do that in our proof system to be able to use the outcome of the recursion rule for different values of the parameters. Finally it is clear how to extend the rule to several, mutually recursive procedures.

Definition 5.33
For mutually recursive methods \( m_1, \ldots, m_n \) we have the following rule:

\[
\frac{\bar{F}_1, \ldots, \bar{F}_n}{\bar{F}}
\]

where

\( \bar{F}_1, \ldots, \bar{F}_n \)

\( F_1, \ldots, F_n \sim F'_1, \ldots, F'_n \) (MR)
\[ F_i = \{ P_i^c[e_i^i/x_i] \} \langle U^-|c_i : x_i \leftarrow e_i^0 : m_i(e_i^1, \ldots, e_i^m) \} \{ R_i^c \} \]

\[ F'_i = \{ P_i^c \land \bigwedge_{j=1}^{K_i} v_j ^i \equiv \text{nil} \} \langle U^-|c_i' : S_i \} \{ Q_i^c[e_i'/r_i] \} \]

\[ F_i = \{ P_i[e^i/x_i',u_i^i] \langle \bar{f}^i / \bar{z}^i \rangle \rightarrow R_i[r_i/x_i] \}

\[ F = \{ P_i \land \bigwedge_{j=1}^{K_i} v_j ^i \equiv \text{nil} \} \langle U|e_i' : S_i \} \{ Q_i^c[e_i'/r_i] \} \]

\( \bar{u}^i, S_i, \text{and } e_i \) are as they occur in the definition of \( m_i \) in \( U \)

\( x_i \) are instance or temporary variables

\( U^- \) results from \( U \) by deleting the definitions of \( m_1, \ldots, m_n \)

\( P_i, Q_i, R_i, f^i, \bar{z}^i, \bar{v}^i, k_i, \) and \( r_i \) are just like in definition 5.24

We cannot prove the validity of this proof rule on its own, because it depends on what the other rules can prove (the operator \( \vdash \) occurs in the premiss).

### 5.4 Other axioms and rules

Finally in this subsection we shall list the remaining axioms and rules of our proof system. They will deal with the more ordinary statements and therefore they are not very new (most of them can already be found in [4]).

**Definition 5.34**

For a side effect expression \( s^e_d \) functioning as a statement we have the following rule:

\[
\begin{align*}
\{ P^c \} \langle U|c : u_d \leftarrow s^e_d \} \{ Q^c \} \\
\{ P \} \langle U|c : s \} \{ Q \}
\end{align*}
\]

where \( u_d \) is a temporary variable not occurring in \( P \) or \( Q \).

**Definition 5.35**

For the sequential composition of statements we have the following proof rule:

\[
\begin{align*}
\{ P^c \} \langle U|S_1 \} \{ Q^c \} \quad \{ Q^c \} \langle U|S_2 \} \{ R^c \}
\end{align*}
\]

\[
\{ P \} \langle U|S_1; S_2 \} \{ R \}
\]

**Definition 5.36**

For the conditional statement we have this rule:

\[
\begin{align*}
\{ P^c \land e \} \langle U|S_1 \} \{ Q^c \} \\
\{ P^c \land \neg e \} \langle U|S_2 \} \{ Q^c \}
\end{align*}
\]

\[
\{ P \} \langle U|if \ e \ then \ S_1 \ else \ S_2 \ fi \} \{ Q \}
\]

Doc. No.
Definition 5.37
For the while loop we have the following rule:
\[
\frac{\{ P^c \land e^c \} \langle U | S^c \rangle \{ P^c \}}{\{ P \} \langle U | \text{while } e \text{ do } S \text{ od} \} \{ P \land \neg e \}} \quad (W)
\]

Definition 5.38
For every valid (see definition 4.15) assertion \( P^c \) we have the axiom:
\[
P \quad \text{(TR)}
\]

Definition 5.39
Finally, we have the so-called rule of consequence:
\[
P_1^c \rightarrow P_2^c \quad \{ P_2 \} \langle U | c \cdot S \rangle \{ Q_2 \} \quad Q_2^c \rightarrow Q_1^c
\[
\frac{\{ P_1 \} \langle U | c \cdot S \rangle \{ Q_1 \}}{(RC)}
\]

Theorem 5.40
The proof system consisting of the axioms (SAT), (SAI), (NT), (NI), and (TR), plus the rules (MI), (MT), (MR), (ES), (SC), (C), (W), and (RC) is sound, that is, for every row of correctness formulae \( F_0, \ldots, F_n \) and for every environment \( \gamma \) we have if \( F_1, \ldots, F_n \vdash F_0 \) and \( \gamma \models F_i \) for \( i = 1, \ldots, n \) then \( \gamma \models F_0 \).

Proof
For all rules except (MR) the validity can be proved individually. For some we have already done that, for the others it is very easy. The rest of the proof runs by induction on the length of the proof of \( F_0 \) from \( F_1, \ldots, F_n \). The only interesting case occurs if the last rule applied is (MR). From now on let us use the notation of definition 5.33 and forget about the old \( F_0, \ldots, F_n \).

In the premiss of the rule (MR) we first have \( F_1, \ldots, F_n \), and these are valid because the only way to get them is by using the axiom (TR). The second premiss says that \( F_1, \ldots, F_n \vdash F'_1, \ldots, F'_n \). This must be provable by a shorter proof than our current one so the induction hypothesis says that for every environment \( \gamma \) such that \( \gamma \models F_1, \ldots, F_n \) we also have that \( \gamma \models F'_1, \ldots, F'_n \). Let us take a particular \( \gamma \) and define \( \gamma' = U[U](\gamma) \). Now \( \gamma' \) is the limit of an increasing sequence \( \gamma_0, \gamma_1, \ldots \) where \( \gamma_0 = \gamma' \langle \lambda \beta \cdot \lambda \delta \cdot \lambda \sigma \cdot (1, 1) / m_i \rangle_{i=1}^n \) and \( \gamma_{i+1}' \) is obtained from \( \gamma_i' \) by calculating and filling...
in the meanings of the method definitions of \(m_1, \ldots, m_n\). Furthermore we observe that for every \(i\) and for every \(m \in \{m_1, \ldots, m_n\}\) we have that \(\mathcal{U}[U^-](\gamma'_i)(m) = \gamma'_i(m)\) because \(m\) is not defined in \(U^-\).

Now for \(\gamma'_0\) we have quite trivially that \(\gamma'_0 \models F'_1, \ldots, F'_n\) (the send-expression never terminates). Furthermore from \(\gamma'_i \models F'_j\) we can get to \(\gamma'_{i+1} \models F_j\) by an argument analogous to that in lemma 5.30. From the validity of the second premiss we can then conclude that \(\gamma'_{i+1} \models F_j\) for \(j = 1, \ldots, n\). By induction we get \(\gamma'_i \models F'_1, \ldots, F'_n\) for every \(i\), so by continuity we get in particular \(\gamma' \models F'_1\). And this in turn implies \(\gamma \models F\). \(\Box\)
6 Completeness

6.1 Introduction

We prove in this section that every valid correctness formula about an arbitrary closed program is derivable from the proof system based on the assertion language with quantification over finite sequences of objects. To this end we use enhanced versions of the standard techniques for proving completeness. These techniques are based on the expressibility of the strongest postcondition, or, alternatively, the weakest precondition. Using the assertion language with quantification over finite sequences of objects we know how to express the strongest postcondition. However, we conjecture that we cannot in general express the strongest postcondition or the weakest precondition within the assertion language with recursive predicates. We think this is due to the inexpressibility within this assertion language of the notion of finiteness.

In order to get a complete proof system, however, we have to modify the rules (MI), (MT), and (MR) so that we can reason about deadlock behaviour. Regardless of the assertion language we use these rules are incomplete. Consider the following example:

Example 6.1
Let \( \rho = (U | c : x \leftarrow \text{self!m}()) \) be closed and \( m() \leftarrow \text{nil} \) nil occur in \( U \). We obviously have \( \models \{ \text{true} \}\rho \{ \text{false} \} \). But we do not have the derivability of this correctness formula. For otherwise there would exist assertions \( P, Q \) and \( R \) such that:

1. \( \models \{ P \land \forall i v_i \leftarrow \text{nil} \}\{ U | c : \text{nil} \}\{ Q[\text{nil}/r] \} \)
2. \( \models Q[\text{self}/\text{self}][\tilde{f}/\tilde{z}] \rightarrow R[r/x] \)
3. \( \models \text{true} \rightarrow P[\text{self}/\text{self}][\tilde{f}/\tilde{z}] \) and \( \models R \rightarrow \text{false} \)

for some sequence of expressions \( \tilde{f} \), sequence of corresponding logical variables \( \tilde{z} \) and logical variable \( r \) of the same type as the instance variable \( x \). Now, as \( \models R \rightarrow \text{false} \), we have \( \models R[r/x] \rightarrow \text{false} \). So from clause 2 it then follows that \( \models Q[\text{self}/\text{self}][\tilde{f}/\tilde{z}] \rightarrow \text{false} \). Furthermore we have \( \models Q[\text{self}/\text{self}] \leftrightarrow Q \) so we infer \( \models Q[\tilde{f}/\tilde{z}] \rightarrow \text{false} \). From clause 1 in turn it is not difficult to deduce that \( \models P \rightarrow Q[\text{nil}/r] \) (use \( \forall_i TVar(P, Q) = \emptyset \) and the truth of the correctness formula of clause 1). So we have \( \models P[\tilde{f}/\tilde{z}] \rightarrow Q[\text{nil}/r][\tilde{f}/\tilde{z}] \). Note next that \( \models Q[\tilde{f}/\tilde{z}] \rightarrow \text{false} \) implies \( \models Q[\text{nil}/r][\tilde{f}/\tilde{z}] \rightarrow \text{false} \), from which we infer that \( \models P[\tilde{f}/\tilde{z}] \rightarrow \text{false} \), which in turn, using \( \models P[\text{self}/\text{self}] \leftrightarrow P \), would imply by clause 3 \( \models \text{true} \rightarrow \text{false} \). We thus have reached a contradiction. So we conclude that \( \forall \{ \text{true} \}\rho \{ \text{false} \} \).
Note that adding the conjunct \( \neg (\text{self} = e_0) \) to the precondition of the conclusion of the rules (MI) and (MT) does not solve the general case of longer cycles in the calling chain.

To reason about deadlock in the proof system based on the assertion language containing quantification over finite sequences we introduce a collection of logical variables with special roles.

**Definition 6.2**

We fix for each class name \( c \) a logical variable \( b_c \in \mathit{LVar}_c \). Furthermore we define \( \mathit{BVar} = \{ b_c : c \in C \} \).

We will interpret the variable \( b_c \) as denoting a sequence of all the blocked objects of class \( c \). Formally, we redefine the notion \( OK(\sigma, \delta, \omega) \) as follows:

**Definition 6.3**

For arbitrary \( \sigma, \delta, \omega \) we define \( OK(\sigma, \delta, \omega) \) iff \( \sigma \) is consistent, \( \delta \) agrees with \( \sigma \), \( \omega \) is compatible with \( \sigma \) and for an arbitrary \( c \) we have

\[
\delta_{(2)}(c) = \{ \alpha : \exists n \in \mathbb{N}(\mathit{elt}(b_c, n) = \alpha \neq \bot) \}.
\]

So we have \( OK(\sigma, \delta, \omega) \) if additionally \( b_c \), for an arbitrary \( c \), consists precisely of all the blocked objects of class \( c \). Note that we have thus introduced in the assertion language a means to refer to the second component of a context. Given this fixed interpretation we do not allow the variable \( b_c \) to be quantified. It is a straightforward exercise to check that under this definition of \( OK(\sigma, \delta, \omega) \) the soundness proofs given still hold.

Next we modify the rule (MI) as follows:

**Definition 6.4**

For the statement \( x \leftarrow e_0!m(e_1, \ldots, e_n) \), where \( x \in \mathit{IVar}_{d_0} \), \( m \in \mathit{MName}_{d_0, \ldots, d_n} \), \( e_0 \in \mathit{Exp}_d \) and \( e_i \in \mathit{Exp}_d \), for \( i = 1, \ldots, n \), we have the following proof rule:

\[
\frac{P' \land \bigwedge_{i=1}^k v_i = \mathit{nil} \land \neg (\text{self} \in b_c)}{(U|x') : S}\{Q'[e/r]\} \quad Q' \rightarrow R[\tau/x]}
\]

where \( P' = P[e/\text{self}, \bar{u}][\bar{f}/\bar{z}][b_c \circ (\text{self})/b_c], Q' = Q[e/\text{self}, \bar{u}][\bar{f}/\bar{z}][b_c \circ (\text{self})/b_c], S \in \mathit{Stat}^d \) and \( e \in \mathit{Exp}_{d_0} \) are the statement and expression occurring in the definition of the method \( m \) in the unit \( U \), \( u_1, \ldots, u_n \) are its formal parameters, \( v_1, \ldots, v_k \) is a row of temporary variables that are not formal parameters \( (k \geq 0) \), \( \tau \) is a logical variable of type \( d_0 \) that does not occur in \( R \), \( \bar{f} \) is an arbitrary row of expressions \( (\text{not}
logical expressions) in class $c$, and $\bar{z}$ is a row of logical variables, mutually different and different from $\bar{r}$, such that the type of each $z_i$ is the same as the type of the corresponding $f_i$. We require that no temporary variables other than the formal parameters $u_1, \ldots, u_n$ occur in $P$ or $Q$. The boolean expression $l_1 \leq l_2$ abbreviates $\exists i (l_1 = l_2 \cdot i)$, where $i$ is some fresh logical integer variable. $P[b_c \circ (\text{self})/b_c]$, for an arbitrary assertion $P$, equals the assertion

$$\exists z (P[z/b_c] \land |z| = |b_c| + 1 \land \forall i (i \leq |b_c| \rightarrow z \cdot i \equiv b_c \cdot i) \land (z \cdot |z| \equiv \text{self})$$

where $z \in LVar_{c^+}, i \in LVar$ are some fresh variables.

The idea of this substitution $[b_c \circ (\text{self})/b_c]$ can be explained roughly as follows: Occurrences of the variable $b_c$ in the assertions $P^{c'}$ and $Q^{c'}$, which describe the input state and the output state of the receiver of the method call, denote the set of blocked objects of class $c$ belonging to those states. When we want to describe the input state and the output state of the receiver from the point of view of the sender we have to take into account that this set of blocked objects can now be viewed as the set of blocked objects of class $c$ belonging to the input state and the output state of the sender of the method call plus the sender itself.

The rules (MT) and (MR) are modified accordingly. The soundness proofs of these new versions of (MI) and (MT) are straightforward modifications of the proofs of the soundness of the original ones (in the proof of 5.30 the substitution $[b_c \circ (\text{self})/b_c]$ can be considered simply as part of the simultaneous substitution $[f/z]$). The proof of the soundness of the new version of (MR), assuming the soundness of the new versions of (MI) and (MT), does not need to be modified.

We note that with respect to the proof system based on the assertion language containing recursive predicates this proof method does not apply. To incorporate some reasoning mechanism about deadlock behaviour in this system one could add to it some notion of auxiliary variables, which can be used to code the relevant control information.

It will appear to be technically convenient to introduce another modification of the rule (MR). This modification consists simply of replacing every occurrence of $U^-$ in this rule by $U$ itself. We denote the resulting rule by (NMR). The main difference between the rules (NMR) and (MR) is that the rule (NMR) allows nested applications to some method name. However, in appendix A it is shown that a proof using the rule (NMR) can be transformed into a proof using (MR), and vice versa.

To be able to prove completeness we have to add the following rules to the proof system (based on the assertion language containing quantification over finite sequences).

**Definition 6.5**

Doc. No.
Conjunction rule:
\[
\{P_1^c\} \rho^c\{Q_1^c\} \quad \{P_2^c\} \rho^c\{Q_2^c\} \\
\{P_1^c \land P_2^c\} \rho^c\{Q_1^c \land Q_2^c\}
\]  \hspace{1cm} (CR)

**Definition 6.6**
Elimination rule 1:
\[
\{P^c\} \rho^c\{Q^c\} \quad \exists z_d P^c \lor P[nil/z_d] \rho^c\{Q^c\}
\]  \hspace{1cm} (ER1)

where \(z_d \not\in LVar(Q^c) \cup BVar\). Due to the interpretation of the quantifiers as ranging only over existing objects we have to express explicitly that the precondition also holds when the value of the quantified variable is undefined (nil).

**Definition 6.7**
Elimination rule 2:
\[
\{P^c\} \rho^c\{Q^c\} \quad \exists z_d P^c \lor P[nil/z_d] \rho^c\{Q^c\}
\]  \hspace{1cm} (ER2)

where \(a = d^*, \) for some \(d,\) and \(z_a \not\in LVar(Q^c) \cup BVar\).

**Definition 6.8**
Initialization rule 1:
\[
\{P^c\} \rho^c\{Q^c\} \quad \{P^c[l/z]\} \rho^c\{Q^c\}
\]  \hspace{1cm} (IR1)

where \(z\) and \(l\) are of the same type, and \(z \not\in LVar(Q^c) \cup BVar\).

**Definition 6.9**
Initialization rule 2:
\[
\{P^c\} \rho^c\{Q^c\} \quad \{P^c[l/u]\} \rho^c\{Q^c\}
\]  \hspace{1cm} (IR2)

where \(u\) and \(l\) are of the same type and \(u \not\in TVar(\rho, Q)\).

**Definition 6.10**
Substitution rule:
\[
\{P^c\} \rho^c\{Q^c\} \quad \{P^c[z'/z]\} \rho^c\{Q^c[z'/z]\}
\]  \hspace{1cm} (SR)

where \(z', z\) are logical variables of the same type, and \(z \not\in BVar\).

The soundness of these new rules is a straightforward exercise. We illustrate the necessity of the condition \(z \not\in BVar\) by the following example:

Doc. No.
Example 6.11
Let $\rho = \langle U, c : y \leftarrow x \cdot m() \rangle$. By the new definition of $OK(\sigma, \delta, \omega)$ we have, assuming the type of the variable $x$ to be $c$,

$$\models \{x \in b_c\} \rho \{\text{false}\},$$

where $x \in b_c$ abbreviates the assertion $\exists i (x = b_c \cdot i)$. If we would allow the initialization of the variable $b_c$, or allow it to be substituted, we could derive from this formula by an application of the rule (SR) or (IR1) the following:

$$\{x \in z\} \rho \{\text{false}\}.$$

Applying next the elimination rule (ER2), assuming $z \not\in BVar$, then gives us the derivability of the formula:

$$\{\exists z (x \in z)\} \rho \{\text{false}\}.$$

Finally, we apply the consequence rule:

$$\{\text{true}\} \rho \{\text{false}\}.$$

But this last formula is not valid in general!

Finally, for technical convenience we would like to assume that the sets $C$, $IVar$, and $TVar$ are finite. This assumption can be justified as follows: Let $C'$ be a finite subset of $C$, and $IVar'$ be a finite subset of $\bigcup_{c,d} IVar'_d$, where $c$ ranges over $C'$, and $d$ ranges over the set $C'^* = C' \cup \{\text{Int, Bool}\}$. Next we fix the temporary integer variables $u, u'$, and for every $d \in C'^*$ the temporary variables $re_d, re'_d$. Let $r \in$ denote a sequence of these variables. Now let $TVar'$ be a finite subset of $\bigcup_d TVar_d$ (again, $d$ ranging over $C'^*$), such that $re \not\subseteq TVar'$. Given these sets $C'$, $IVar'$, and $TVar'$ we have the following definition.

Definition 6.12
We define an expression $l^*_a$ to be restricted iff $c \in C'$, $a = d, d^*$, with $d \in C'^*$, $IVar(l^*_a) \subseteq IVar'$, and $TVar(l^*_a) \subseteq TVar'$. We define an assertion $P^c$ to be restricted iff $c \in C'$ and every expression occurring in $P^c$ is restricted. We call a program $\rho = \langle U, c : S \rangle$ restricted iff $c \in C'$, every expression occurring in $\rho$ is restricted, $u, u' \not\in TVar(\rho)$, and, finally, the temporary variables $re_d, re'_d$ are only allowed in the main statement $S$ itself, where $S = re_d \leftarrow s_d$ or $S = re'_d \leftarrow s_d$, with $TVar(s) \cap r_e = \emptyset$.

A correctness formula $\{P\} \rho \{Q\}$ is called restricted iff $P, Q$, and $\rho$ are restricted.

We will prove that an arbitrary valid restricted correctness formula is derivable by a derivation in which there occur only restricted correctness formulae. Such a derivation we call restricted too. The extra variables $r_e$ are used in applications of the rules (W) and (ES): The variables $re_d, re'_d$ are used to store temporarily the result of the execution of a statement $s_d$; the variables $u, u'$ are needed to express the invariant
of a while statement. However applications of the consequence rule in a restricted
derivation are based on a different notion of validity of assertions and correctness
formulae. This new notion of validity consists of restricting all the semantic entities
to the sets \( C', IVar', \) and \( TVar' \). As an example of the restriction of a semantic entity
we define that of a state.

**Definition 6.13**

We define the restriction of a state \( \sigma \), which we denote by \( \sigma \downarrow \), to be an element of

\[
\Sigma \downarrow = \prod_{c \in C'} P_c \times \prod_{c \in C', d \in C'^+} (O_c \rightarrow IVar_d'^c \rightarrow O_d'^1) \times \prod_{d \in C'^+} (TVar_d'^c \rightarrow O_d'^1)
\]

such that

- \( \sigma \downarrow (c) = \sigma(c), \ c \in C' \).
- \( \sigma \downarrow (\alpha)(x) = \sigma(\alpha)(x), \ \alpha \in O_c, \ \text{for} \ c \in C', \ \text{and} \ x \in IVar' \).
- \( \sigma \downarrow (u) = \sigma(u), \ u \in TVar' \).

In a similar way we have corresponding restricted versions of all our semantic entities.
We have the following lemma, which states that the meaning of a restricted program
depends only on those parts of a state specified by the sets \( C', IVar', \) and \( TVar' \).

**Lemma 6.14**

For an arbitrary restricted program \( \rho \), and \( \sigma, \sigma', \delta, \gamma \) such that

1. \( \sigma(c) = \sigma'(c), \ c \notin C' \).
2. \( \sigma(\alpha) = \sigma'(\alpha), \ \text{for} \ \alpha \in O_c, \ c \notin C' \).
3. \( \sigma(\alpha) = \sigma'(\alpha), \ \text{for} \ \alpha \in O_c \setminus \sigma(c), \ c \in C' \).
4. \( \sigma(\alpha)(x) = \sigma'(\alpha)(x), \ \text{for} \ \alpha \in \sigma(c), \ c \in C', \ x \notin IVar' \).
5. \( \sigma'(\alpha)(x) = \bot, \ \text{for} \ \alpha \in \sigma(c) \setminus \sigma(c), \ c \in C', \ x \notin IVar' \).
6. \( \sigma(u) = \sigma'(u), \ u \notin TVar' \).

we have

\[
\sigma' = \mathcal{P}[[\rho]](\gamma)(\delta)(\sigma) \text{ iff } \sigma' \downarrow = \mathcal{P}'[[\rho]](\gamma)(\delta)(\sigma \downarrow),
\]

where \( \mathcal{P}', \gamma \downarrow, \) and \( \delta \downarrow \) denote the restricted versions of \( \mathcal{P}, \gamma, \) and \( \delta, \) respectively. (Here
\( \sigma(\alpha) \) denotes the local state of \( \alpha \) and \( \sigma(\alpha)(x), \ x \) an instance variable, denotes the
value of the variable \( x \) of the object \( \alpha \), finally, \( \sigma(u), \ u \) a temporary variable, denotes
the value of \( u \) in state \( \sigma \).)
The first condition above states that $\sigma$ and $\sigma'$ agree with respect to the existing objects of class $c$, $c \notin C'$. The second condition states that $\sigma$ and $\sigma'$ agree with respect to the local states of objects belonging to a class $c$, $c \notin C'$. That the states $\sigma$ and $\sigma'$ agree with respect to the local states of objects belonging to a class $c$, $c \in C'$, which do not exist in $\sigma'$, is expressed by the third clause. The fourth clause states that $\sigma$ and $\sigma'$ agree with respect to the variables not belonging to $IVar'$ of objects of a class $c$, $c \in C'$, which exist in $\sigma$. The fifth clause then states that the value of a variable not belonging to $IVar'$ of an object of a class $c$, $c \in C'$, which exist in $\sigma'$ but does not exist in $\sigma$, is undefined in the state $\sigma'$. The last clause states that $\sigma$ and $\sigma'$ agree with respect to the temporary variables not belonging to $TVar'$. These conditions are necessary to prove that if $\sigma' \models P'[\rho](\gamma \downarrow)(\delta \downarrow)(\sigma \downarrow)$ then $\sigma' = P'[\rho](\gamma)(\delta)(\sigma)$.

**Proof**

Induction on the structure of the program $\rho$.

By the following two lemmas we have that applications of the consequence rule occurring in a restricted derivation also apply with respect to the original notion of validity, thus justifying our assumption of the finiteness of the sets $C, IVar,$ and $TVar$. These lemmas state that the truth of a restricted assertion and that of a correctness formula only depend on those parts of a state specified by the sets $C', IVar'$, and $TVar'$.

**Lemma 6.15**

For an arbitrary restricted assertion $P^c$, and $\sigma, \delta, \omega$ such that $OK(\sigma, \delta, \omega)$ we have

$$\sigma, \delta, \omega \models P^c \iff \sigma \downarrow, \delta \downarrow, \omega \downarrow \models P^c,$$

where $\omega \downarrow \in \prod_d IVar_a \rightarrow O_a^\alpha$, with $\alpha$ ranging over the set $\{d, d^* : d \in C'^r\}$, and $\omega \downarrow (z) = \omega(z)$.

**Proof**

Straightforward induction on the structure of $P^c$.

Furthermore we have

**Lemma 6.16**

Let $\sigma, \delta, \omega$ such that $OK(\sigma, \delta, \omega)$. We have for an arbitrary restricted correctness formula $\{P\} \rho \{Q\}$

$$\sigma, \delta, \omega \models \{P\} \rho \{Q\} \iff \sigma \downarrow, \delta \downarrow, \omega \downarrow \models \{P\} \rho \{Q\}.$$

**Proof**

Straightforward, using lemmas 6.14 and 6.15.
So in the sequel we may assume the sets $C$, $IVar$, and $TVar$ to be finite. Further, we assume given a set of temporary variables $re$ as defined above. A program $\rho$ from now on will denote, when not stated otherwise, a program such that the temporary variables $re, re'$ are allowed to occur in it only in assignments $re \leftarrow s, re' \leftarrow s$, with $re, re' \not\in TVar(s)$, and $u, u' \not\in TVar(\rho)$. This concludes our discussion concerning the justification of the assumption of the finiteness of the sets $C$, $IVar$, and $TVar$.

6.2 The strongest postcondition

To be able to prove completeness we first have to analyze the notion of a strongest postcondition and its expressibility in the assertion language. As noted already in the introduction, the expressibility of the strongest postcondition in the assertion language with recursive predicates is still an open problem and so is the completeness of the proof system based on this assertion language.

For the analysis of the notion of a strongest postcondition we need some definitions and a theorem. We start with the following definition:

Definition 6.17
An object-space isomorphism (osi) is a family of functions $f = (f^d)_{d \in C^+}$, where $f^d : O^d_+ \rightarrow O^d_+$ is a bijection, $f^d(\bot) = \bot$ and $f^d$, for $d = \text{Int, Bool}$, is the identity mapping.

Given an osi $f$ we next define the isomorphic image of an arbitrary state.

Definition 6.18
Given an osi $f$ we define for an arbitrary state $CT$ the state $I(CT)$ as follows:

- For every $c$: $I(CT)(c) = IC(CT(c))$.
- For every $c, d, x^c_d$: $I(CT)(x^c_d) = f^d(ID(CT(x)^c_d))$, where the osi $f^{-1}$ denotes the inverse of $f$: $f^{-1} = ((f^d)^{-1})_d$.
- For every $d, u_d$: $I(CT)(u_d) = f^d(ID(u_d))$.

Here $f^c(X)$, for some $X \subseteq O^c$, denotes the set $\{f^c(\alpha) : \alpha \in X\}$.

The following theorem essentially expresses that states which are isomorphic cannot be distinguished by the assertion language.

Theorem 6.19
Let $f$ be an osi and $\sigma, \delta, \omega$ be such that $OK(\sigma, \delta, \omega)$. Then for every logical expression $l^c$ and assertion $P^c$ we have:

Doc. No.
62

- \( f^\omega(L[l^\omega]\omega(\delta)(\sigma)) = L[l^\omega](f(\omega))(f(\delta))(f(\sigma)), \)
- \( A^\omega[V^\omega](\omega)(\delta)(\sigma) = A^\omega[V^\omega](f(\omega))(f(\delta))(f(\sigma)). \)

where
\[
\begin{align*}
  f(\delta)_1 & = f^c(\delta_1), \\
  f(\delta)_2(c') & = f^c(\delta_2(c')), \text{ for an arbitrary } c', \text{ and} \\
  f(\omega)(x_d) & = f^d(\omega(x_d)), \quad (f^d((\alpha_1, \ldots, \alpha_n)) = (f^d(\alpha_1), \ldots, f^d(\alpha_n))).
\end{align*}
\]

**Proof**
Straightforward induction on the structure of \( l^\omega, P^\omega \). We only treat the case \( l = x^\omega_d \):
\[
L[l^\omega](f(\omega))(f(\delta))(f(\sigma)) = f(\sigma)(f^\omega(\delta_1))(x) = f^d(\sigma(\delta_1)(x)) = f^d(L[l^\omega](\omega)(\delta)(\sigma))
\]
\( \square \)

We are now sufficiently prepared to analyze the notion of a strongest postcondition.

Given a program \( \rho^c \) and an assertion \( P^c \), we denote by \( sp(\rho^c, P^c) \) the set of final states of executions of \( \rho^c \) starting from a state satisfying \( P^c \). An assertion, defining this set of states \( sp(\rho^c, P^c) \) is called the strongest postcondition of \( \rho^c \) with respect to \( P^c \). As established by the previous theorem, the set of states defined by an arbitrary assertion is closed under isomorphism. However, in general, given a program \( \rho^c \) and an assertion \( P^c \), the set of states \( sp(\rho^c, P^c) \) is not closed under isomorphism. Consider the following example:

**Example 6.20**
Take \( \rho^c = (U|x : x \leftarrow \text{new}), \) with \( \rho^c \) closed, and \( \sigma, \sigma', \delta \) such that \( \sigma' = \{\alpha, \beta\}, \)
\( \sigma(\alpha) = \delta_1 = \alpha \) and \( \sigma' = P[\rho^c][\gamma](\delta)(\sigma) \). Let \( P^c = \text{true} \). So we have that \( \text{pick}^c(\{\alpha\}) = \beta \). Let \( f \) be an arbitrary osi such that \( \text{pick}^c(\{f^c(\alpha)\}) \neq f^c(\beta) \) and \( \text{pick}^c(\{f^c(\beta)\}) \neq f^c(\alpha) \). So we have that \( f(\sigma') = \{f^c(\alpha), f^c(\beta)\} \). Now suppose that there is a \( \sigma_0 \) such that \( f(\sigma') = P[\rho^c][\gamma](\delta)(\sigma(\sigma_0)) \). Then we would have \( \sigma_0^{(c)} = \{f^c(\alpha)\} \) or \( \sigma_0^{(c)} = \{f^c(\beta)\}, \) but both cases lead to a contradiction. Therefore such a \( \sigma_0 \) does not exist and \( f(\sigma') \notin sp(\rho^c, \text{true}) \).

This discrepancy between the assertion language and the semantics of the programming language is solved by closing this set \( sp(\rho^c, P^c) \) under isomorphism. Of course it is not immediately clear that this will work! We will see later that we indeed encounter some difficulties in the completeness proof due to this. These difficulties require some additional reasoning not present in the standard completeness proofs.

The following theorem states the existence of an assertion defining the closure under isomorphism of the set \( sp(\rho^c, P^c) \).

**Theorem 6.21**
Let \( \rho^c \) be closed (not necessarily restricted), \( BVar \subseteq L \subseteq LVar \) (\( L \) finite), \( P^c \)

Doc. No.
such that $LVar(P^c) \subseteq L$. Then there exists an assertion $SP^c_L(\rho, P^c)$ such that $LVar(SP^c_L(\rho, P^c)) \subseteq L$ and for $\sigma, \delta, \omega$ such that $OK(\sigma, \delta, \omega)$ we have:

$$\sigma, \delta, \omega \models SP^c_L(\rho, P^c)$$

iff there exist an osi $f$ and a state $\sigma_0$ such that:

- $f(\sigma) = P[\rho](\gamma)(\delta')(\sigma_0), \gamma$ arbitrary,
- $\sigma_0, \delta', \omega' \models P^c$,

where $\delta' = f(\delta)$ and $\omega' = f(\omega) \downarrow L$. Here we define

$$((f(\omega) \downarrow L)(z) = f(\omega(z)) \quad z \in L$$

$$= \perp \quad z \in (LVar \cap \bigcup_d LVar_d) \setminus L$$

$$= \epsilon \quad z \in (LVar \cap \bigcup_d LVar_{d^*}) \setminus L.$$ 

Note that in the above theorem we cannot take $f(\omega)$, where $f(\omega)(z) = f(\omega(z))$, for $\omega'$. This would require that $f(\omega)$ and $\sigma_0$ are compatible, which cannot be expressed by our assertion language. For suppose there exists an $\alpha \in \sigma(\delta')$, for some $\delta'$, such that $j^{\delta'}(\alpha) \not\in \sigma_0^{\delta'}$. Let $z_{\delta'} \not\in L$, it then follows that $\sigma, \delta, \omega\{\alpha/z_{\delta'}\} \models SP^c_L(\rho, P^c)$, but on the other hand it is not the case that $f(\omega(\alpha/z_{\delta'}))$ and $\sigma_0$ are compatible, so we do not have $\sigma_0, \delta', f(\omega(\alpha/z_{\delta'})) \models P^c$. Note that the above argument essentially boils down to the fact that we cannot describe by one assertion the values of infinitely many logical variables. Thus we have to specify a finite set of logical variables $L$ such that the restriction of $f(\omega)$ to this set $L$ is compatible with $\sigma_0$.

**Proof**

See appendix B. \(\square\)

The following two lemmas together state the correctness of our definition of the notion of strongest postcondition.

**Lemma 6.22**

For an arbitrary $BVar \subseteq L \subseteq LVar$ ($L$ finite), closed program $\rho^c$ and assertion $P^c$ such that $LVar(P^c) \subseteq L$, we have

$$\models \{P^c\} \rho\{SP^c_L(\rho, P^c)\}.$$ 

**Proof**

Let $\sigma, \sigma', \delta, \omega$ ($\sigma, \sigma' \neq \perp$) be such that $OK(\sigma, \delta, \omega), \sigma' = P^c[\rho^c](\gamma)(\delta)(\sigma)$ ($\gamma$ arbitrary),

Doc. No.
and \( \sigma, \delta, \omega \models P^c \). We have that \( \sigma', \delta, \omega \models SP^c_\omega (\rho, P^c) \), for take for the osi \( f \) the family of identity mappings, for \( \sigma_0 \) the state \( \sigma \), and note that because \( LVar(P^c) \subseteq L \) we have \( \sigma, \delta, \omega' \models P^c \), where \( \omega' = \omega \upharpoonright L \).

**Lemma 6.23**

For an arbitrary closed program \( \rho^c \), assertions \( P^c, Q^c \), \( BVar \subseteq L \subseteq LVar \) (\( L \) finite) such that \( LVar(P^c, Q^c) \subseteq L \) we have

\[
\models \{ P^c \} \rho^c \{ Q^c \} \text{ implies } \models SP^c_\omega (\rho^c, P^c) \rightarrow Q^c.
\]

**Proof**

Assume \( \models \{ P \} \rho \{ Q \} \) and let \( \sigma, \delta, \omega \) such that \( OK(\sigma, \delta, \omega) \) and \( \sigma, \delta, \omega \models SP^c_\omega (\rho^c, P^c) \). So there exist an osi \( f \) and a state \( \sigma_0 \) such that:

- \( f(\sigma) = P[\rho](\gamma)(\delta')(\sigma_0), \gamma \) arbitrary.

- \( \sigma_0, \delta', \omega' \models P^c \).

where \( \delta' = f(\delta) \) and \( \omega' = f(\omega) \downarrow L \). From \( \models \{ P^c \} \rho^c \{ Q^c \} \) we then infer that \( f(\sigma), \delta', \omega' \models Q^c \). By \( LVar(Q^c) \subseteq L \) we have \( f(\sigma), \delta', f(\omega) \models Q^c \). So by theorem 6.19 we conclude \( \sigma, \delta, \omega \models Q^c \).

6.3 Freezing the initial state

An essential notion of the standard technique for proving completeness consists of what is called freezing the initial state. To explain this notion, let, only in this paragraph, \( \rho \) denote a program of some simple procedural language (like the ones treated in [3] or [10]) and \( \sigma, \sigma' \) denote some simple functions assigning values to program variables. Let \( \bar{z} \) denote the set of program variables occurring in \( \rho \), \( \bar{z} \) denote a corresponding sequence of logical variables and \( \bar{z} \cong \bar{z} \) abbreviate \( \land_i (x_i \cong z_i) \). Furthermore let \( SP(\rho, \bar{z} \cong \bar{z}) \) be an assertion describing the set of final states resulting from executions of \( \rho \) starting in a state satisfying \( \bar{z} \cong \bar{z} \). In the standard completeness proof an important consequence of the definition of the notion of strongest postcondition is that the assertion \( SP(\rho, \bar{z} \cong \bar{z}) \) in the following sense describes the graph of \( \rho \):

- If the execution of \( \rho \) starting from the state \( \sigma \) results in the state \( \sigma' \) then \( SP(\rho, \bar{z} \cong \bar{z}) \) holds in \( \sigma' \) when the logical variable \( z_i \) is interpreted as \( \sigma(x_i) \), the value of \( x_i \) in \( \sigma \).

Doc. No.
If $SP(\rho, \bar{z} = \bar{z})$ holds in a state $\sigma'$, assuming the logical variable $z_i$ to be interpreted as some value $d_i$, then there exists an execution of $\rho$ starting from the state $\sigma'\{d_i/z_i\}_i$ which results in $\sigma'$.

Note that the logical variables $\bar{z}$ are used to "freeze" the initial state.

Now one of the problems in applying the standard techniques for proving completeness to our proof system consists of how to store a state in a finite set of logical variables. A simple assertion like $\bar{x} = \bar{z}$ does not make sense, because a variable $x$ can be evaluated only with respect to some object. To be able to construct an assertion which expresses how a state is stored in the logical environment we introduce some special logical variables. First we fix for each class name $c$ the logical variables $cr_c , bl_c \in LVar_c$. Every existing object belonging to class $c$ is supposed to be a member of the sequence denoted by $cr_c$. For convenience, we also include $\text{nil}$ in $cr_c$. The sequence denoted by $bl_c$ on the other hand is supposed to contain all the blocked objects belonging to class $c$. Furthermore for each instance variable $x_d$ we fix a logical variable $iv_x \in LVar_d$ and, finally, for each temporary variable $u_d$ we fix a logical variable $tv_u \in LVar_d$. The sequence denoted by $iv_x$, $x \in IVar_c$, will store the value of the variable $x$ for every existing object belonging to class $c$ in the following way: Every existing object of class $c$ occurs at least once in the sequence denoted by $cr_c$. Now the $i$th element of the sequence $iv_x$ is the value of the variable $x$ in the object that is the $i$th element of the sequence $cr_c$. The value of $tv_u$, $u \in TVar$, just equals that of $u$.

All these newly introduced logical variables we assume to be distinct. We let $\bar{st}$ denote a particular sequence (without repetitions) of these logical variables. Now we are ready to define formally the assertion $\text{init}$, which expresses that the current state is represented by $\bar{st}$. In other words, $\text{init}$ is our analogue of the assertion $\bar{x} = \bar{z}$.

**Definition 6.24**

We define the assertion $\text{init}$ as follows:

$$\text{init} = \ \wedge_c cr_c \cdot 1 = \text{nil} \land \forall z \exists i (z_c = cr_c \cdot i) \land$$

$$\wedge_c \forall i ((\forall x \in IVar_c ((cr_c \cdot i) \cdot x = iv_x \cdot i)) \land$$

$$\wedge_{u \in TVar} (u = tv_u) \land$$

$$\wedge_c (bl_c = bl_c)$$

where $IV_c = \bigcup_d IVar_d$, $TV = \bigcup_d TVar_d$, and the logical variable $i$ is supposed to range over the integers. Note that in our assertion language we do not have equality between logical expressions of type $d^i$, for an arbitrary $d$. However, these equalities can easily be expressed in the assertion language: If $l_1$ and $l_2$ are two logical expressions ranging over sequences, then $l_1 = l_2$ can be expressed as $\forall i (l_1 \cdot i = l_2 \cdot i)$, where $i$ is some logical integer variable. Furthermore we remark that for every class name $c$ we have $\text{init} \in Ass_c$. 

Doc. No.
In the following two definitions we define a transformation of a logical expression and an assertion such that the transformed versions only refer to the logical environment. Expressions referring to the state will be translated into expressions which refer to the corresponding part of the logical environment \( st \) used to reflect the state. The problem such a transformation poses can be best explained by the following example:

**Example 6.25**

Suppose we want to transform the expression consisting of the instance variable \( x \). This expression denotes the value of \( x \) with respect to the object denoted by the expression \( \text{self} \). But to look up this value in the logical environment one has to know where the object denoted by \( \text{self} \) occurs in the sequence denoted by \( \text{ere} \), assuming \( x \in \text{IVar}_c^e \) for some \( d \). However, this cannot be determined statically! Note also that we cannot force the existing objects of a class, say class \( c \), to occur in a particular order in the sequence denoted by \( \text{ere} \). Our solution to this problem consists essentially of using a second logical expression, of type \( \text{Bool} \), to describe under which conditions the first expression correctly translates the original one. We will also need a number of logical variables that range over integers, more precisely, over indices in the sequences \( \text{ere} \).

In our example above, the expression \( x \) is then translated into the triple \( ((i), \text{self} \neq \text{ere} \cdot i, \text{id}_x \cdot i) \), where \( i \) is some logical integer variable. This is interpreted as follows: Whenever the variable \( i \) takes such a value that the Boolean expression \( \text{self} \neq \text{ere} \cdot i \) is true, then the expression \( \text{id}_x \cdot i \) takes the desired value.

The analogue of these transformations in the standard completeness proof is the substitution \( [\bar{z}/\bar{x}] \), where \( \bar{z} \) is the part of the logical environment which is used to store the part of the state as specified by \( \bar{x} \).

**Definition 6.26**

We define \( l_\alpha [s]\bar{t} = (i, l_\alpha, l_\alpha) \) for an arbitrary logical expression \( l_\alpha \) by induction on the structure of \( l_\alpha \). Let \( \epsilon \) denote the empty sequence. We treat the following cases:

- \( x_\alpha \bar{z} [s]\bar{t} = ((i), \text{self} \neq c_r \cdot i, \text{id}_x \cdot i) \)
  where \( i \) is some fresh logical integer variable (it does not occur in \( \bar{t} \)).

- \( u_d[s]\bar{t} = (\epsilon, \text{true}, tv_u) \)

- \( l[s]\bar{t} = (\epsilon, \text{true}, l) \)
  where \( l = \text{nil}, \text{self}, \text{true}, \text{false}, n, \) or \( z \).

- \( (c \cdot x_\alpha)[s]\bar{t} = (i \circ (j), l_1 \land l_2 \neq c_r \cdot j, \text{id}_x \cdot j) \)
  where \( l_\alpha [s]\bar{t} = (i, l_1, l_2) \) and \( j \notin i \).

- \( (l_1 + l_2)[s]\bar{t} = (i, l_1 + l_2, l_2 + l_2) \)
  where \( l_1 [s]\bar{t} = (i_1, l_1 + l_2, l_2), l_2 [s]\bar{t} = (i_2, l_1, l_2), i = i_1 \circ j_1, j_1 \) is some sequence of fresh logical integer variables of the same length as \( i_2, l_2, l_2 \).

Doc. No.
\[ (l_1 \land l_2)[\bar{st}] = (\bar{i}, l_1, \land l_2, \bar{l}_3, \text{if } l_3, \text{then } l'_3, \text{else } l'_3) \]

where \( l_1[\bar{st}] = (i_1, l_1, i_1, l_2), l_2[\bar{st}] = (i_2, l_2, i_2), l_3[\bar{st}] = (i_3, l_3, i_3), \bar{i} = \bar{i}_1 \circ \bar{j}_2 \circ \bar{j}_3, \bar{j}_2 \text{ and } \bar{j}_3 \text{ are mutually disjoint sequences of fresh logical variables of the same length as } i_2 \text{ and } i_3, \text{ respectively}, l'_2 = l_2[j_2/i_2], l'_2 = l_2[j_2/i_2], l'_3 = l_3[j_3/i_3], \text{ and } l'_3 = l_3[j_3/i_3].

\[ (l_1 \cdot l_2)[\bar{st}] = (\bar{i}, l_1, \land l_2, l_2, \bar{l}_2) \]

where \( l_1[\bar{st}] = (i_1, l_1, i_1, l_2), l_2[\bar{st}] = (i_2, l_2, i_2), \bar{i} = \bar{i}_1 \circ \bar{j}, \bar{j} \text{ is some sequence of fresh logical integer variables of the same length as } i_2, l'_2 = l_2[j/i_2], \text{ and } l'_2 = l_2[j/i_2].

\[ (l_1 \equiv l_2)[\bar{st}] = (\bar{i}, l_1, \land l_2, l_1, \equiv l_2) \]

where \( l_1[\bar{st}] = (i_1, l_1, i_1, l_2), l_2[\bar{st}] = (i_2, l_2, l_2), \bar{i} = \bar{i}_1 \circ \bar{j}, \bar{j} \text{ is some sequence of fresh logical integer variables of the same length as } i_2, l'_2 = l_2[j/i_2], \text{ and } l'_2 = l_2[j/i_2].

Note that in \( l_2[\bar{st}] = (i, l_1, l_2) \), the expression \( l_1 \) describes where the relevant existing objects, with respect to the evaluation of \( l_2 \), are stored in that part of the logical environment as specified by \( cr_c, c \in C \). An object is said to be of relevance with respect to the evaluation of an expression if it requires the values of some variables of this object. The expression \( l_2 \) then uses this information to select the relevant values in that part of the logical environment where the values of the variables of the existing objects are stored.

**Example 6.27**

Consider the expression \( \text{x.xy} \), where \( z \in LVar_c, x \in IVar^c \). We have

\[ (\text{x.y})[\bar{st}] = ((i, j), z \equiv cr_c \cdot i \land iv_x \cdot i \equiv cr_d \cdot j, iv_y \cdot j) \]

where \( i \) and \( j \) are distinct logical integer variables.

**Definition 6.28**

Next we define the transformation \( P^c[\bar{st}] \) for an arbitrary assertion \( P^c \) by induction on the structure of \( P^c \). We treat the following cases:

\[ l \land l_2 = \exists i(l_1 \land l_2) \]

where \( l \land l_2 = (\bar{i}, l_1, l_2). \)

\[ (P_1 \land P_2)[\bar{st}] = P_1[\bar{st}] \land P_2[\bar{st}] \]

\[ (\forall z_a P)[\bar{st}] = \forall z_a P[\bar{st}] \]

where \( a = d, d^*, d = \text{Int, Bool}. \)

\[ (\forall z_a P)[\bar{st}] = \forall z(a \in cr_c \rightarrow P[\bar{st}]). \]

Doc. No.
\[
(\forall z_a \cdot P)[\bar{s}\bar{t}] = \forall z_a (z_a \subseteq c_{c} \rightarrow P[\bar{s}\bar{t}]),
\]
where \(a = c^*\).

\[
(\exists z_a \cdot P)[\bar{s}\bar{t}] = \exists z_a P[\bar{s}\bar{t}],
\]
where \(a = d, d^*, d = \text{Int, Bool}\).

\[
(\exists z_c \cdot P)[\bar{s}\bar{t}] = \exists z_c (z_c \in c_{c} \land P[\bar{s}\bar{t}]),
\]
where \(a = c^*\).

Here \(l_1 \subseteq l_2\) abbreviates \(\exists i(l_1 \subseteq l_2 \cdot i)\) and \(l_1 \subseteq l_2\) abbreviates \(\forall i(l_1 \cdot i \in l_2)\). Note that, although \(\text{nil} \in c_{c}\), the quantification in \((\forall z_c \cdot P)[\bar{s}\bar{t}]\) and \((\exists z_c \cdot P)[\bar{s}\bar{t}]\) excludes \(\text{nil}\), because quantification always excludes \(\text{nil}\).

The following theorem states that the above transformation as applied to assertions preserves truth. It can be seen as an analogue of the substitution lemma of first-order predicate logic.

**Theorem 6.29**

Let \(P^c\) be an arbitrary assertion. Furthermore let \(\sigma, \delta, \omega\) such that \(\text{OK}(\sigma, \delta, \omega)\) and \(\sigma, \delta, \omega \models \text{init}\). Then:

\[\sigma, \delta, \omega \models P^c \iff \sigma, \delta, \omega \models P^c[\bar{s}\bar{t}]\]

**Proof**

The proof proceeds by induction on the structure of \(P^c\). The case that \(P^c\) equals \(I^c\) is treated as follows: We prove that for every logical expression \(l^c\) there exists a sequence of integers \(\bar{n}\) such that \(\sigma, \delta, \omega(\vec{n}/\bar{i}) \models l^c\) and that for all such \(\bar{n}\) we have \(L[l^c](\omega(\bar{n}/\bar{i}))(\sigma) = L[l^c](\omega(\bar{n}/\bar{i}))(\sigma)\), where \(l^c[\bar{s}\bar{t}] = (\bar{i}, l_1, l_2)\). This is proved by induction on the structure of \(l^c\).

6.4 Invariance

In this section we formulate a syntactic criterion for an assertion to be invariant over the execution of an arbitrary program. First we note that not allowing program variables to occur in an assertion does not guarantee this invariance property! This is due to the restriction of the range of the quantifiers to existing objects. Consider the following example:

**Example 6.30**

Let \(P\) denote the assertion \(\exists z \forall z'(z = z')\), where \(z, z' \in \text{LVar}_c\) for some class name \(c\).
This assertion $P$ expresses that there exists precisely one object of class $c$. Let $\rho^c = (U|x \leftarrow \text{new}), U$ arbitrary and $x \in IVar^c$. Then it is not the case that $\models \{P\} \rho^c \{P\}$, because there exist two objects of class $c$ in the output state.

However, the standard technique to prove completeness relies heavily on the invariance of assertions in which no program variables occur. To be able to apply this technique we define the notion of quantification-restricted assertions.

**Definition 6.31**
We define an assertion $P^c$ to be quantification-restricted if

$$P^c ::= t^c$$

$$::= \exists z_a P \mid \forall z_a P$$

where $a = d, d^*, d = \text{Int, Bool}$

$$::= \exists z_c (z_c \in z_c^* \land P^c)$$

$$::= \exists z_c^* (z_c^* \subseteq z_c^* \land P^c)$$

$$::= \forall z_c (z_c \in z_c^* \rightarrow P^c)$$

$$::= \forall z_c^* (z_c^* \subseteq z_c^* \rightarrow P^c)$$

Here we assume the variables $z_c^*$ and $z_c^*$ to be distinct and the assertion $P$ at the right-hand side of the symbol $::=$ to be quantification-restricted.

An important property of such a quantification-restricted assertion is that its truth is not affected by the creation of new objects:

**Lemma 6.32**
For every quantification-restricted assertion $P$ and every variable $v$ such that $v \notin IVar(P) \cup TVar(P)$ we have $\models P \leftrightarrow P[\text{new}/v]$.

**Proof**
Induction on the complexity of $P$. We treat the representative case of $P = \exists z_c (z_c \in z_c^* \land Q)$, assuming the type of the variable $v$ to be $c$: Now $P[\text{new}/v] = \exists z_c (z_c \in z_c^* \land Q[\text{new}/v]) \lor (v \in z_c^* \land Q[v/z_c])[\text{new}/v]$. But as $(v \in z_c^*)[\text{new}/v]$ can be easily seen to be equivalent to false the second disjunct will be equivalent to false too. Furthermore we have by the induction hypothesis that $Q[\text{new}/v]$ is equivalent to $Q$. Putting these observations together gives us the equivalence of $P$ and $P[\text{new}/v]$. The case $P = \forall z_c (z_c \in z_c^* \rightarrow Q)$ is treated analogously. The cases of $P = \exists z_c^* (z_c^* \subseteq z_c^* \land Q), \forall z_c^* (z_c^* \subseteq z_c^* \rightarrow Q)$ are slightly more complex due to the complexity of the substitution operations involved, but the reasoning pattern is basically the same. $\square$

Doc. No.
A consequence of this lemma is the following invariance property of quantification-restricted assertions:

**Theorem 6.33**
Let \( \rho^c = \langle U | e : S \rangle \) be closed and \( P^c \) be a quantification-restricted assertion such that \( IVar(P^c) \cap IVar(\rho^c) = \emptyset \) and \( TVar(P^c) \cap TVar(\rho^c) = \emptyset \). Then: \( \vdash \{ P^c \} \rho^c \{ P^c \} \).

**Proof**
The proof proceeds by induction on the complexity of \( S \). We consider the case of \( S = v \leftarrow e_0 | m(e_1, \ldots, e_n) \); Let \( M \) be the smallest set such that

- \( \rho \in M \),
- if \( \rho' = \langle U | e' : v' \leftarrow e_0 | m'(e_1', \ldots, e_n') \rangle \in M \) then \( \rho_i = \langle U | e_i : v_i \leftarrow e_0 | m_i(e_1', \ldots, e_n') \rangle \in M \),

where \( v_i \leftarrow e_0 | m_i(e_1', \ldots, e_n') \) or \( e_0 | m_i(e_1', \ldots, e_n') \) occurs in \( S' \), \( S' \) being the body of the method \( m' \). In the latter case we have \( v_i = \text{red}_i \), assuming \( d_i \) to be the type of the result expression of \( m_i \).

Let \( M = \{ \rho_1, \ldots, \rho_k \}, \rho = \rho_1 \), assuming the following notational conventions: \( \rho_i = \langle U | e_i : v_i \leftarrow e_0 | m_i(e_1', \ldots, e_n') \rangle \in M \) and \( m_i(u_1', \ldots, u_n') \subseteq S_i \upharpoonright e_i \) occurs in \( U \), \( i = 1, \ldots, k \). Furthermore, \( e_i' \) denotes the sequence \( e_i, \ldots, e_{n_i} \) and \( v_i' \) the sequence \( u_1', \ldots, u_{n_i}' \). Next we introduce for every class name \( c \) a new variable \( z_c \). We let \( \bar{z} \) denote a sequence (without repetitions) of these variables and \( \bar{b} \) denote the corresponding sequence of the variables \( b_c \in BVar \). Finally we put for \( i = 1, \ldots, k \):

\[
F_i = \{ P' \} \rho_i \{ P' \}, \text{ where } P' = P^c[\bar{z}/\bar{b}][z_c/self], z_c \text{ being a new variable.}
\]

Now we have that

\[
F_1, \ldots, F_k \vdash \{ P' \} \{ U | e_i : S_i \} \{ P' \}
\]

(\( e_i' \) being the type of \( e_0 \)). This is established by induction on the complexity of \( S_i \). The only slightly less straightforward case of \( S_i = v \leftarrow \text{new} \) is taken care by the previous lemma.

Putting \( P_i, Q_i, R_i = P' \) and introducing some logical variable \( r_i \notin LVar(P') \) (of the same type as the variable \( v_i \) ), \( i = 1, \ldots, k \), and observing that \( P'[\bar{e}_i/self, \bar{u}_i][b_{c_1} \circ \langle \text{self}/b_{c_1} \rangle = P' \) we infer by (NMR) that:

\[
\vdash \{ P' \} \{ U | e_i : S_i \} \{ P' \}.
\]

Next we put \( P_1, Q_1 = P' \) and \( R_1 = P'[\bar{z}/\bar{b}] \). We have that:

\[
\vdash P_1[\bar{e}_1/self, \bar{u}_1][\text{self/}z_{c_1}][b_{c_1} \circ \langle \text{self}/b_{c_1} \rangle \rightarrow P^c[\bar{z}/\bar{b}]
\]
and
\[ \models Q_1[e^1/\text{self}, u^1][\text{self}/x_c] [b_{c_1} \circ (\text{self})/b_{c_1}] \rightarrow R_1[r_1/o_{\text{self}}]. \]

Thus applying (MI) (or (MT)) gives us that:
\[ \models \{ P^c[z/b]\} \rho^c \{ P^c[z/b]\}. \]

Finally an application of the substitution rule gives us the derivability of the correctness formula \( \{ pc \} \rho^c \{ pc \} \).

\[ \square \]

6.5 Most general correctness formulae

Now we are able to prove that for an arbitrary \( \rho^c = \langle U|c : v \leftarrow e_0!m(e_1, \ldots, m_n) \rangle \) the correctness formula \( \{ \text{init} \} \rho^c \{ \text{SP}^c_L(\rho^c, \text{init}) \} \), for some \( L \subseteq L\text{Var} \), is a most general one in the sense that an arbitrary valid correctness formula can be derived from the proof system which results from adding these correctness formulae as additional axioms. Completeness then follows by establishing the derivability of \( \{ \text{init} \} \rho^c \{ \text{SP}^c_L(\rho^c, \text{init}) \} \), for an arbitrary \( \rho^c = \langle U|c : v \leftarrow e_0!m(e_1, \ldots, m_n) \rangle \).

But first we need to introduce some new logical variables corresponding to those of \( \tilde{st} \). This is necessary because the variables of \( \tilde{st} \) have a fixed interpretation as specified by the assertion \( \text{init} \). But every valid correctness formula in which variables of \( \tilde{st} \) occur, implicitly provides these variables with some possibly different interpretation. To avoid a clash between these different interpretations we must temporarily substitute in the correctness formula, of which we want to establish its derivability, every variable of \( \tilde{st} \) by some corresponding new variable.

So we introduce for each \( c \) fresh logical variables \( crf_c, btf_c \in L\text{Var}_{c^e} \). For each instance variable \( x \in I\text{Var}_d \) we introduce the fresh logical variable \( ivf_x \in L\text{Var}_{d^e} \), and with each temporary variable \( u \in T\text{Var}_d \) we associate the fresh logical variable \( tvf_u \in L\text{Var}_d \). We assume again that all these newly introduced logical variables are distinct. We let \( \tilde{st}l \) denote a sequence (without repetitions) of these variables. We can thus assume that \( \tilde{st}l \cap \tilde{st}l = \emptyset \).

Furthermore we introduce for every temporary variable \( re_d \) (defined in the introduction to justify the assumption of the finiteness of the sets \( C, I\text{Var}, \) and \( T\text{Var} \)) a fresh logical variable \( ire_d \). Let \( ire \) denote a sequence of these logical variables. We will use the variable \( ire \) when applying the rule (ES): Applications of this rule will make use of the variable \( re \) to store temporarily the result of the expression \( s \). Therefore we have to substitute occurrences of \( re \) in the precondition and the postcondition by the corresponding variable \( ire \). We will see later how to restore the original precondition and postcondition after such an application of the rule (ES).
We start with the following lemma stating the derivability of valid correctness formulae about simple assignments.

**Lemma 6.34**
For an arbitrary program $P = \langle U \mid c : v \leftarrow e \rangle$ we have

$$\models \{P^c\} \rho \{Q^c\} \implies \{P^c\} \rho \{Q^c\}.$$  

**Proof**
Let $v = u$, $u$ some temporary variable. (The case of $v$ being an instance variable is treated similarly.) By lemma 5.4 (note that we actually mean here the corresponding lemma for the proof system based on the assertion language with quantification over sequences) and the assumption that $\models \{P^c\} \rho \{Q\}$ it follows that $\models P^c \rightarrow Q^c[e/u]$. So an application of the axiom (SAT) and the consequence rule gives us the derivability of the correctness formula $\{P^c\} \rho \{Q\}$. 

We have a similar lemma for the creation of new objects:

**Lemma 6.35**
For an arbitrary program $P = \langle U \mid c : v \leftarrow \text{new}\rangle$ we have

$$\models \{P^c\} \rho \{Q^c\} \implies \{P^c\} \rho \{Q^c\}.$$  

**Proof**
Let $v = u$, $u$ some temporary variable. (The case of $v$ being an instance variable is treated similarly.) By lemma 5.18 and the assumption that $\models \{P^c\} \rho \{Q\}$ it follows that $\models P^c \rightarrow Q^c[\text{new}/v]$. So an application of the axiom (NT) and the consequence rule gives us the derivability of the correctness formula $\{P^c\} \rho \{Q\}$. 

Next we have the following lemma stating the derivability of an arbitrary valid correctness formula about sending messages:

**Lemma 6.36**
Let $P = \langle U \mid c : v \leftarrow e_0!m(e_1, \ldots, e_n) \rangle$ be a closed program. Furthermore let $P^c, Q^c$ and $BVar \subseteq L \subseteq LVar$ ($L$ finite) such that $LVar(P, Q) \subseteq L \setminus stl$, and $stl \cup stl \subseteq L$. Then:

$$\models \{P^c\} \rho \{Q^c\} \implies \{\text{init}\} \rho \{SP^c_L(\rho, \text{init})\} \vdash \{P^c\} \rho \{Q^c\}.$$
Proof
Let \( P' = P[s\bar{t}_1/s\bar{t}] \) and \( Q' = Q[s\bar{t}_1/s\bar{t}] \). Furthermore we introduce the following abbreviation: \( P'' = P'[s\bar{t}] \). We start with the assumption:

\[
\{\text{init}\} \rho \{SP^c_L(\rho, \text{init})\}.
\]

By theorem 6.33 (note that \( P'' \) is quantification-restricted, \( IVar(P'') = \emptyset \), and \( TVar(P'') = \emptyset \)) we have the derivability of the following formula:

\[
\{P''\} \rho \{P''\}.
\]

Applying the conjunction rule gives us:

\[
\{P'' \land \text{init}\} \rho \{P'' \land SP^c_L(\rho, \text{init})\}.
\]

We next prove that \( \models P'' \land SP^c_L(\rho, \text{init}) \rightarrow Q' \):

Let \( \sigma, \delta, \omega \models P'' \land SP^c_L(\rho, \text{init}) \). So there exist a state \( \sigma_0 \) and an osi \( f \) such that

- \( f(\sigma) = P[\rho][\gamma](\delta')(\sigma_0), \gamma \) arbitrary,
- \( \sigma_0, \delta', \omega' \models \text{init} \),

where \( \delta' = f(\delta) \) and \( \omega' = f(\omega) \downarrow L \).

By theorem 6.19 we have that \( f(\sigma), f(\delta), f(\omega) \models P'' \). It is not difficult to check that \( LVar(P'') \subseteq L \), so we have \( f(\sigma), \delta', \omega' \models P'' \). Furthermore we have that \( \models \{\neg P''\} \rho \{\neg P''\} \) (by theorem 6.33 we have \( \models \{\neg P''\} \rho \{\neg P''\} \), so the truth of the above correctness formula follows from the soundness of the proof system). It follows that \( \sigma_0, \delta', \omega' \models P'' \). By theorem 6.29, note that \( \sigma_0, \delta', \omega' \models \text{init} \), we then infer \( \sigma_0, \delta', \omega' \models P' \). By the soundness of the substitution rule (SR) we have that \( \models \{P\} \rho \{Q\} \) implies the truth of the correctness formula \( \{P'\} \rho \{Q'\} \). So we infer that \( f(\sigma), \delta', \omega' \models Q' \).

But as \( LVar(Q') \subseteq L \) we have \( f(\sigma), \delta', f(\omega) \models Q' \). Finally an application of theorem 6.19 gives us the desired result \( \sigma, \delta, \omega \models Q' \).

Now we return to our main argument. By the consequence rule we thus infer:

\[
\{P'' \land \text{init}\} \rho \{Q'\}.
\]

Next we apply the initialization rule (IR1):

\[
\{(P'' \land \text{init})[\bar{u}/\bar{v}]\} \rho \{Q'\},
\]

Doc. No.
where \( \tilde{u} \) is a sequence of all the temporary variables and \( \tilde{tv} \) denotes the corresponding sequence of logical variables \( tv_u, u \in \tilde{u} \). Now we use the elimination rule (ER2):

\[
\left\{ \exists \tilde{z}'(P'' \land \text{init})[\tilde{u}/\tilde{tv}] \right\} \rho \{ Q' \},
\]

where \( \tilde{z}' \) is a sequence of the logical variables \( \{ cr_c, bl_c : c \in C \} \) and \( \{ iv_x : x \in IVar \} \). Note that instead of initializing the variables \( \tilde{tv} \) we could also eliminate them by rule (ER1). However, applying the rule (ER1) would require some additional notational machinery in order to deal with the extra case of nil.

Next we prove \( \models P' \rightarrow \exists \tilde{z}'(P'' \land \text{init})[\tilde{u}/\tilde{tv}] \): Let \( \sigma, \delta, \omega \) be such that \( OK(\sigma, \delta, \omega) \) and \( \sigma, \delta, \omega \models P' \). It is not difficult to see that there exists an \( \omega' \) such that \( \omega' \) differs from \( \omega \) only with respect to the variables of \( \tilde{s}t \) and \( \sigma, \delta, \omega' \models \text{init} \). As \( LVar(P') \cap \tilde{s}t = \emptyset \) we have \( \sigma, \delta, \omega' \models P' \). Applying theorem 6.29 then gives us \( \sigma, \delta, \omega' \models P'[\tilde{s}t] \). For every temporary variable \( u \) we have \( \sigma(\tilde{z})(u) = \omega'(tv_u) \), so we infer \( \sigma, \delta, \omega' \models (P'' \land \text{init})[\tilde{u}/\tilde{tv}] \). So we conclude \( \sigma, \delta, \omega \models \exists \tilde{z}'(P'' \land \text{init})[\tilde{u}/\tilde{tv}] \).

We thus have by the consequence rule:

\[
\left\{ P' \right\} \rho \{ Q \}.
\]

Finally an application of the substitution rule finishes the proof. Note that since \( LVar(P'', Q'' \land s) \cap \tilde{s}t \tilde{l} = \emptyset \), we have that \( P'[\tilde{s}t/\tilde{s}t \tilde{l}] = P'' \) and \( Q'[\tilde{s}t/\tilde{s}t \tilde{l}] = Q'' \), so we get

\[
\left\{ P \right\} \rho \{ Q \}.
\]

We next have lemmas 6.38 and 6.39 stating the derivability of valid correctness formulae about statements \( S = s \), where \( s \) is a side-effect expression. In these two lemmas we make use of the following lemma:

**Lemma 6.37**

Let \( \rho = \langle U | c : s \rangle \) and \( \rho' = \langle U | c : re \leftarrow s \rangle \) be restricted programs (see definition 6.12). We then have for arbitrary assertions \( P \) and \( Q \) that

\[
\models \left\{ P \right\} \rho \{ Q \} \text{ implies } \models \left\{ P' \right\} \rho' \{ Q' \},
\]

where \( P' = P[re/re] \) and \( Q' = Q[re/re] \).

**Proof**

Let \( \sigma, \delta, \omega \models P' \) and \( \sigma' = P[\rho'](\gamma)(\delta)(\sigma) \). We have that \( \sigma' = \sigma''\{\beta/re\} \), with \( \langle \sigma'', \beta \rangle = \mathcal{Z}[s](\gamma)(\delta)(\sigma), \gamma' = U[U] \gamma \). As \( re \notin TVar(s) \) (\( \rho \) being restricted) we have \( \langle \sigma_1, \beta \rangle = \mathcal{Z}[s](\gamma')(\delta)(\sigma_0) \), with \( \sigma_1 = \sigma''\{\omega(re)/re\} \) and \( \sigma_0 = \sigma\{\omega(re)/re\} \). This being intuitively clear we feel justified in stating it without a proof. Now,
as \( \sigma, \delta, \omega \models P' \) we have that \( \sigma_0, \delta, \omega \models P \). So from \( \models \{ P \} \rho \{ Q \} \) we then infer \( \sigma_1, \delta, \omega \models Q \), or, equivalently, \( \sigma'', \delta, \omega \models Q' \). Finally, as \( \text{re} \notin \text{TVar}(Q') \), we conclude that \( \sigma', \delta, \omega \models Q' \).

\[ \square \]

**Lemma 6.38**

Let \( \rho = \langle U|c : s \rangle \), where \( s = e, \text{new} \). Furthermore let \( P, Q \) such that \( \text{LVar}(P, Q) \cap \text{ire} = \emptyset \). Then:

\[ \models \{ P \} \rho \{ Q \} \text{ implies } \vdash \{ P \} \rho \{ Q \}. \]

**Proof**

Let \( P' = P[\text{ire}/\text{re}] \) and \( Q' = Q[\text{ire}/\text{re}] \), where \( \text{ire} \) and \( \text{re} \) are of the same type as the expression \( s \). By lemma 6.37 we have \( \models \{ P' \} \rho' \{ Q' \} \), where \( \rho' = \langle U|c : \text{re} \leftarrow s \rangle \). By lemma 6.34, in case \( s = e \), and lemma 6.35, if \( s = \text{new} \), we then have

\[ \vdash \{ P' \} \rho' \{ Q' \}. \]

So by rule (ES) it follows that

\[ \vdash \{ P \} \rho \{ Q \}. \]

Furthermore we have \( \models \{ \text{ire} \equiv \text{re} \} \langle U|c : \text{re} \leftarrow s \rangle \{ \text{ire} \equiv \text{re} \} \). So again by lemmas 6.34 and 6.35 we have

\[ \vdash \{ \text{ire} \equiv \text{re} \} \langle U|c : \text{re} \leftarrow s \rangle \{ \text{ire} \equiv \text{re} \}. \]

Applying again the rule (ES) then gives

\[ \vdash \{ \text{ire} \equiv \text{re} \} \rho \{ \text{ire} \equiv \text{re} \}. \]

Next we apply the conjunction rule

\[ \vdash \{ \text{ire} \equiv \text{re} \land P' \} \rho \{ \text{ire} \equiv \text{re} \land Q' \}. \]

Now \( \models (\text{ire} \equiv \text{re} \land Q') \rightarrow Q \) and \( \models P \rightarrow (\exists \text{ire} P'' \lor P''[\text{nil}/\text{ire}]) \), where \( P'' = \text{ire} \equiv \text{re} \land P' \). (Note that \( \text{ire} \notin \text{LVar}(P) \).) So applying first the consequence rule for \( Q \), then the elimination rule (ER1) (note that \( \text{ire} \notin \text{LVar}(Q) \)), and finally the consequence rule for \( P \), gives us the derivability of

\[ \vdash \{ P \} \rho \{ Q \}. \]

\[ \square \]

We have a similar lemma for valid correctness formulae about a program \( \rho \) of the form \( \langle U|c : e_0!m(e_1, \ldots, e_n) \rangle \).
Lemma 6.39
Let \( P = (U \mid c : e_0 \downarrow m(e_1, \ldots, e_n)) \) be a closed program. Furthermore let \( P, Q \), and \( BVar \subseteq L \subseteq LVar \) (\( L \) finite) such that \( LVar(P, Q) \subseteq L \setminus (stl \cup \text{IRE}) \). Then we have
\[
\models \{ P \} \rho \{ Q \} \text{ implies } \{ \text{init} \} \rho'(SP_L(\rho', \text{init})) \vdash \{ P \} \rho \{ Q \},
\]
where \( \rho' = (U \mid c : r d \leftarrow e_0 \downarrow m(e_1, \ldots, e_n)) \), assuming the type of the result expression of \( m \) to be \( d \).

Proof
Let \( P' = P[lre_d/rd] \) and \( Q' = Q[lre_d/rd] \). An application of lemma 6.37 gives us \( \models \{ P' \} \rho'(Q') \) (remember that \( \rho \) is assumed to be restricted). By lemma 6.36 we have
\[
\{ \text{init} \} \rho'(SP_L(\rho', \text{init})) \vdash \{ P' \} \rho'(Q').
\]
Applying next the rule (ES) gives us
\[
\{ \text{init} \} \rho'(SP_L(\rho, \text{init})) \vdash \{ P' \} \rho(Q').
\]
By theorem 6.33 (observe that \( rd \notin TVar(\rho) \)) we have the derivability of the formula
\[
\vdash \{ lre_d \doteq rd \} \rho \{ lre_d \doteq rd \}.
\]
So by an application of the conjunction rule we have
\[
\{ \text{init} \} \rho(SP_L(\rho, \text{init})) \vdash \{ P' \wedge lre_d \doteq rd \} \rho(Q' \wedge lre_d \doteq rd).
\]
Now we have \( \models (Q' \wedge lre_d \doteq rd) \rightarrow Q \). Furthermore for \( P'' = P' \wedge lre_d \doteq rd \) we have \( \models P \rightarrow (\exists \text{IRE}_d P'' \lor P''[\text{IRE}_d/\text{IRE}]) \) (note that \( lre_d \notin LVar(P) \)). So first applying the consequence rule for \( Q \), then the elimination rule (ER1) (note that \( lre_d \notin LVar(Q) \)), and finally the consequence rule for \( P \) finishes the proof.

Next we have the following main theorem of this section stating the derivability of an arbitrary valid correctness formula using as additional axioms the correctness formulae of the form \( \{ \text{init} \} \rho(SP_L(\rho, \text{init})) \), where \( \rho = (U \mid c : v \leftarrow e_0 \downarrow m(e_1, \ldots, e_n)) \).

Theorem 6.40
Let \( \rho = (U \mid c : S) \) be a closed program. Furthermore let \( P, Q \), and \( BVar \subseteq L \subseteq LVar \) (\( L \) finite) such that \( LVar(P, Q) \subseteq L \setminus (stl \cup \text{IRE}) \). Then:
\[
\models \{ P \} \rho \{ Q \} \text{ implies } F_1, \ldots, F_n \vdash \{ P \} \rho \{ Q \},
\]
where \( F_i = \{ \text{init} \} \rho_i(SP_L(\rho_i, \text{init})) \), \( \rho_i = (U \mid c_i : v_i \leftarrow s_i) \), with \( s_1, \ldots, s_n \) being all the send-expressions occurring in \( S \) such that \( v_i \leftarrow s_i \) occurs in \( S \) or \( v_i = rd \), and \( s_i \) occurs as a statement in \( S \). Here \( d_i \) is assumed to be the type of \( s_i \).
Proof

The proof proceeds by induction on the complexity of $S$.

$S = v \leftarrow s$: Depending on the structure of $s$, by one of the lemmas 6.34, 6.35, 6.36.

$S = s$: Depending on the structure of $s$, by one of the lemmas 6.38, 6.39.

$S = S_1; S_2$: Let $L^- = L \setminus (sI \cup sR)$. We have by lemma 6.22

$$\vdash \{P^c\}p_1\{SP_L-(\rho_1,P^c)\},$$

and

$$\vdash \{SP_L-(\rho_1,P^c)\}p_2\{SP_L-(\rho_2,SP_L-(\rho_1,P^c))\},$$

where $\rho_i = \{U|c : S_i\}$. By the induction hypothesis we have

$$F_1, \ldots, F_n \vdash \{P^c\}p_1\{SP_L-(\rho_1,P^c)\},$$

and

$$F_1, \ldots, F_n \vdash \{SP_L-(\rho_1,P^c)\}p_2\{SP_L-(\rho_2,SP_L-(\rho_1,P^c))\}.$$

It thus suffices to prove that $\vdash SP_L-(\rho_2,SP_L-(\rho_1,P^c)) \rightarrow Q^c$: An application of the rule for sequential composition (SC) and the consequence rule then gives us the desired result.

So suppose that $\sigma, \delta, \omega \models SP_L-(\rho_2,SP_L-(\rho_1,P^c))$, with $OK(\sigma, \delta, \omega)$. By theorem 6.21 there exist a state $\sigma_0$ and an osi $f$ such that

- $f(\sigma) = P[\rho_2](\gamma)(\delta')(\sigma_0), \gamma$ arbitrary,
- $\sigma_0, \delta', \omega' \models SP_L-(\rho_1,P^c),$

where $\delta' = f(\delta)$ and $\omega' = f(\omega) \downarrow L^-$. Now $\sigma_0, \delta', \omega' \models SP_L-(\rho_1,P^c)$ in turn implies that there exist a state $\sigma_0'$ and an osi $g$ such that

- $g(\sigma_0) = P[\rho_1](\gamma)(\delta'')(\sigma_0'), \gamma$ arbitrary,
- $\sigma_0', \delta'', \omega'' \models P^c,$

Doc. No.
where \( \delta'' = g(\delta') \) and \( \omega'' = g(\omega') \downarrow L^- \).

To relate these computations of \( \rho_1 \) and \( \rho_2 \) we apply corollary C.8 of appendix C: There exists an osi \( h \) such that \( h^c \downarrow \sigma^c_0 = g^c \downarrow \sigma^c_0 \), for every \( c \), and \( h(f(\sigma)) = \mathcal{P}[\rho_2](\gamma)(g(\delta'))(g(\sigma_0)) \), where \( \gamma \) is arbitrary.

Since \( g(\delta') = \delta'' \) it follows that \( h(f(\sigma)) = \mathcal{P}[\rho_1](\gamma)(g(\delta''))(g(\sigma_0)) \), with \( \gamma \) arbitrary. So by \( \sigma'_0, \delta'', \omega'' \models P^c \) and \( \models \{ P^c \} \rho \{ Q^c \} \) we infer \( h(f(\sigma)), \delta'', \omega'' \models Q^c \).

Now note that \( OK(\sigma_0, \delta') \). So we have \( h(\delta'_1) = g^c(\delta'_1) = \delta''_1 \) and \( h(\delta'_2(\gamma)) = g(\delta'_2(\gamma)) \) for every \( c \). Thus we infer that \( \delta'' = h(\delta') = h(f(\delta)) \). Moreover for \( z \in L^- \) we have \( h(f(\omega(z))) = h(\omega'(z)) = g(\omega'(z)) = \omega''(z) \). Note that the second identity is justified by \( OK(\sigma_0, \delta', \omega') \). So by theorem 6.19 and the fact that \( LVar(Q^c) \subseteq L^- \) we conclude \( \sigma, \delta, \omega \models Q^c \).

Next we prove \( \models R \land \neg e \rightarrow Q' \):

Let \( \sigma, \delta, \omega \models R \land \neg e \). So let \( \alpha \in \mathbb{N} \) such that \( \sigma', \delta, \omega \models R' \), where \( \sigma' = \sigma \{ \alpha, \alpha/u, u' \} \). So there exist \( f, \sigma_0 \) such that

- \( f(\sigma') = \mathcal{P}[\rho'](\gamma)(\delta')(\sigma_0), \gamma \) arbitrary,
- \( \sigma_0, \delta', \omega' \models P' \land u = 0 \),

where \( \delta' = f(\delta) \) and \( \omega' = f(\omega) \downarrow L^+ \). Now \( u, u' \notin TVar(e) \) so \( \sigma, \delta, \omega \models \neg e \) implies \( \sigma', \delta, \omega \models \neg e \). By theorem 6.19 we have \( f(\sigma'), \delta', f(\omega) \models \neg e \). So from \( LVar(e) = \emptyset \)
it follows that $f(\sigma'), \delta', \omega' \models \neg e$. From this it is not difficult to derive that $f(\sigma') = \mathcal{P}[\rho(\gamma)(\delta')(\sigma_0)]$, where $\sigma_0 = \sigma_0\{\alpha, \alpha/u, u'\}$. Now as $u, u' \notin TVar(P')$ it follows that $\sigma_0, \delta', \omega' \models P'$. So by $\models \{P'\}\rho\{Q'\}$ we have $f(\sigma'), \delta', \omega' \models Q'$. By $LVar(Q') \subseteq L^+$ and theorem 6.19 we have $\sigma', \delta, \omega \models Q'$. So that from $u, u' \notin TVar(Q')$ we finally conclude $\sigma, \delta, \omega \models Q'$.

Finally, we have $\models \{R \land e\}\rho_1\{R\}$, where $\rho_1 = \langle U|c : S_1\rangle$:

Let $\sigma_0, \delta, \omega \models R \land e$, with $OK(\sigma_0, \delta, \omega)$, and $\sigma_1 = \mathcal{P}[\rho_1(\gamma)(\delta)(\sigma_0)]$, with $\gamma$ arbitrary. Let $\alpha \in \mathbb{N}$ such that $\sigma_0', \delta, \omega \models R'$, where $\sigma_0' = \sigma_0\{\alpha, \alpha/u, u'\}$. So there exist $f, \sigma$ such that

- $f(\sigma_0') = \mathcal{P}[\rho'(\gamma)(\delta')(\sigma), \gamma$ arbitrary,
- $\sigma, \delta', \omega' \models P' \land u \equiv 0$,

where $\delta' = f(\delta)$ and $\omega' = f(\omega) \upharpoonright L^+$. So we have the following situation:

$$
\sigma_0, \delta \xrightarrow{\rho_1} \sigma_1 \\
\vdots \\
\sigma_0' \\
\vdots \\
\sigma, \delta' \xrightarrow{\sigma'} f(\sigma_0')
$$

Here $\sigma, \delta \not\models \sigma'$ should be interpreted as $\sigma' = \mathcal{P}[\rho(\gamma)(\delta')(\sigma), \gamma$ arbitrary. We have $\sigma_0', \delta, \omega \models e$ because $u, u' \notin TVar(e)$. So by theorem 6.19 and $LVar(e) = \emptyset$ we infer $f(\sigma_0'), \delta', \omega' \models e$. Now let $\sigma_1' = \sigma_1\{\alpha, \alpha/u, u'\}$. It then follows that $\sigma_1' = \mathcal{P}[\rho_1(\gamma)(\delta)(\sigma_0)]$. We now have the following situation:

$$
\sigma_0, \delta \xrightarrow{\rho_1} \sigma_1 \\
\vdots \\
\sigma_0', \delta \xrightarrow{\rho_1} \sigma_1' \\
\vdots \\
\sigma, \delta' \xrightarrow{\sigma'} f(\sigma_0')
$$

An application of corollary C.8 then gives us an osi $g$ such that $g^0 \downarrow \sigma_0'(c) = f^e \downarrow \sigma_0'(c)$ for every $c$, and $g(\sigma_1') = \mathcal{P}[\rho_1(\gamma)(g(\delta))(f(\sigma_0'))]$, with $\gamma$ arbitrary. Note that from $OK(\sigma_0', \delta)$ it then follows that $g(\delta) = f(\delta) = \delta'$. Finally, we thus have reached the
following situation:

\[
\begin{array}{c|c|c}
\sigma_0, \delta & \rho & \sigma_1 \\
\hline
\sigma'_0, \delta & \rho & \sigma'_1 \\
\end{array}
\]

\[\sigma, \delta' \xrightarrow{\rho'} f(\sigma'_0), \delta' \xrightarrow{\rho_1} g(\sigma'_1)\]

Now it follows that for \(\sigma_2 = \sigma_1(\alpha + 1/u')\) and \(\sigma_3 = g(\sigma'_1)\{\alpha + 1, \alpha + 1/u, u'\}\) we have \(\sigma_3 = \mathcal{P}[\rho'(\gamma)(\delta')(\sigma_2)]\), with \(\gamma\) arbitrary. (Of course this can be proved formally, but as the intuition behind a formal proof is quite obvious, the main idea being simply that the temporary variable \(u\) counts the number of loops, we think we are justified in omitting such a proof.) Now \(\sigma, \delta', \omega' \models P', u, u' \notin TVar(P')\), so \(\sigma_2, \delta', \omega' \models P'\), from which in turn it follows by lemma 6.22 that \(\sigma_3, \delta', \omega' \models R'\). So we infer \(g(\sigma'_1), \delta', \omega' \models R\). Now \(LVar(R) \subseteq L^+\) and for \(z \in L^+\) we have \(g(\omega(z)) = f(\omega(z)) = \omega'(z)\) (the first identity follows from \(OK(\sigma'_0, \omega)\)) so we have \(g(\sigma'_1), \delta', g(\omega) \models R\). It follows by an application of theorem 6.19 that \(\sigma'_1, \delta, \omega \models R\). Finally, as we have \(u, u' \notin TVar(R)\) we conclude \(\sigma_1, \delta, \omega \models R\).

Now by \(\models \{R \land e\} \rho_1 \{R\}\) it follows that \(\models \{R'' \land e\} \rho_1 \{R''\}\) (note that \(u, u' \notin TVar(\rho_1)\)), where \(R'' = R[u, u'/z_u, z_u]\). As \(LVar(R'') \subseteq L^-\) we can apply the induction hypothesis:

\[F_1, \ldots, F_n \vdash \{R'' \land e\} \rho_1 \{R''\}\]

By theorem 6.33 we have

\[\vdash \{z_u \models u \land z_u' \equiv u'\} \rho_1 \{z_u \models u \land z_u' \equiv u'\}\]

Furthermore we have \(\models (R'' \land z_u \models u \land z_u' \equiv u') \rightarrow R\) and \(R \rightarrow (R'' \land z_u \models u \land z_u' \equiv u')\) (note that \(u, u' \notin TVar(R)\)). So applying the conjunction rule, the consequence rule for the postcondition, the initialization rule (IR2), and the consequence rule for the precondition gives us

\[F_1, \ldots, F_n \vdash \{R \land e\} \rho_1 \{R\}\]

From an application of the rule (W) and the consequence rule, using the truth of the implications \(P' \rightarrow R\) and \(R \land \neg e \rightarrow Q'\), it then follows that:

\[F_1, \ldots, F_n \vdash \{P'\} \rho_1 \{Q'\}\]

Now again by an application of theorem 6.33 and the conjunction rule we have

\[F_1, \ldots, F_n \vdash \{P' \land z_u \models u \land z_u' \equiv u'\} \rho_1 \{Q' \land z_u \models u \land z_u' \equiv u'\}\]

We have \(\models (Q' \land z_u \models u \land z_u' \equiv u') \rightarrow Q\) and \(\models P \rightarrow (P' \land z_u \models u \land z_u' \equiv u')\) (note that \(u, u' \notin TVar(R)\)). So applying first the consequence rule for \(Q\), then the initialization rule (IR1), and finally the consequence rule for \(P\) gives us the desired result. \(\square\)
6.6 The context switch

In this subsection we prove the derivability of the correctness formula \( \{ \text{init} \} \rho \{ \text{SP}'_L(\rho, \text{init}) \} \), for \( \rho = (U|c : v \leftarrow e_0|m(e_1, \ldots, e_n)) \) closed and \( \text{BVar} \subseteq L \subseteq \text{LVar} \) such that \( \text{st} \cup \text{stf} \cup \text{lrc} \subseteq L \). From now on until the end of this section unless stated otherwise we assume \( \rho \) and \( L \) to be fixed. We want to apply the rule (NMR) and theorem 6.40. To apply the rule (NMR) we need the following definition:

**Definition 6.41**

Let \( M \) be the smallest set such that

- \( \rho \in M \),
- if \( \rho' = (U|c : v' \leftarrow e_0'|m'(e_1', \ldots, e_k')) \in M \) then \( \rho_i = (U|c : v_i \leftarrow e_0|m(e_1, \ldots, e_n)) \in M \), where \( v_i \leftarrow e_0|m(e_1, \ldots, e_n) \) or \( e_0|m(e_1, \ldots, e_n) \) occurs in \( S' \) as a statement (in this latter case we have \( v_i = \text{result} \), assuming \( d_i \) to be the type of the result expression of \( m_i \)), \( S' \) being the body of the method \( m' \).

Let \( M = \{ \rho_1, \ldots, \rho_k \}, \rho = \rho_1 \), assuming the following notational conventions: \( \rho_i = (U|c : v_i \leftarrow e_0|m_1(e_1, \ldots, e_n)) \in M \), and \( m_i(u_1, \ldots, u_k) = S_i \), \( e_i \) occurs in \( U_i \), \( i = 1, \ldots, ,k \). We let \( e_i \) denote the sequence \( e_1, \ldots, e_n \). Furthermore let \( \mathcal{u} \) be a sequence of all the temporary variables, and let the formal parameters of the method \( m_i \) be denoted by \( u_i \).

We start with a sketch of the proof strategy. To apply theorem 6.40 and the rule (NMR) we have to define assertions \( P_i, Q_i, i = 1, \ldots, ,k \), such that \( \text{LVar}(P_i, Q_i) \subseteq L \setminus (\text{stf} \cup \text{lrc}) \), and

\[
\vdash \left\{ P_i \land \bigwedge_j v_j = \text{nil} \land \text{self} \not\in c_i \right\}(U|c_i : S_i)\left\{ Q_i[e_i / r_i] \right\}, \tag{6.1}
\]

where \( v_i = \mathcal{u} \setminus \mathcal{v} \) and \( c_i ' \) is the type of \( e_0 \),

\[
\vdash \text{init} \rightarrow P_i[e_i / \text{self}, \mathcal{u}] [\mathcal{g} / \mathcal{z}][b_{c_i} \circ \text{self}] / b_{c_i} \tag{6.2}
\]

and

\[
\vdash Q_i[e_i / \text{self}, \mathcal{u}][\mathcal{g} / \mathcal{z}][b_{c_i} \circ \text{self}] / b_{c_i} \rightarrow \text{SP}'_L(\rho_i, \text{init})[r_i / v_i], \tag{6.3}
\]

for some sequence of expressions \( \mathcal{g} \) and corresponding sequence of logical variables \( \mathcal{z} \). Here \( r_i \) for \( i = 1, \ldots, ,k \) is a logical variable of the same type as \( v_i \). By 6.1 an application of theorem 6.40 then gives us

\[
F_1, \ldots, F_k \vdash \left\{ P_i \land \bigwedge_j v_j = \text{nil} \land \text{self} \not\in c_i \right\}(U|c_i : S_i)\left\{ Q_i[e_i / r_i] \right\}
\]
where
\[ F'_i = \{ \text{init} \} P_i \{ S P_{L}^c (\rho_i, \text{init}) \}. \]
Furthermore by an application of the consequence rule, using (6.2), we have \( F_i \vdash F_i' \) where
\[ F_i = \left\{ P_i [e^i / \text{self}, \bar{u}^i] [g^i / \bar{x}^i] [b_{c_i} \circ (\text{self}) / b_{c_i}] \right\} P_i \{ S P_{L}^c (\rho_i, \text{init}) \}. \]
So we have
\[ F_1, \ldots, F_k \vdash \{ P_i \land \bigwedge_j v_j^i \equiv \text{nil} \land \text{self} \not\in b_{c_i} \} \langle U | c_i' : S_i \rangle \{ Q_i [e_i / r_i] \}. \]
An application of (NMR) plus (MT) and the consequence rule, using (6.2) and (6.3), then concludes the proof.

We start with the considering equations (6.2) and (6.3): We define a substitution which neutralizes the context switch. To do so we first introduce some new logical variables.

**Definition 6.42**
We associate with \( u \in \bar{u} \) a new logical variable \( tv_u^2 \) of the same type and with each \( c \in C \) a new logical variable \( id_c \). We define \( tv^2 \) to be the sequence of logical variables \( tv_u^2 \) corresponding to the sequence \( \bar{u} \). Finally let \( \bar{id}^i \), \( i = 1, \ldots, k \), denote the sequence consisting of the variable \( id_{c_i} \) followed by the elements of \( tv_u^2 \).

We have the following lemma about the neutralizing capacity of the substitution \( [\bar{id}^i / \text{self}, \bar{u}] \) with respect to the context switch:

**Lemma 6.43**
For any \( i \in \{1, \ldots, k\} \) and every assertion \( P \in Ass^c \) we have
\[ P^c [\bar{id}^i / \text{self}, \bar{u}] [e^i / \text{self}, \bar{u}^i] = P^c [\bar{id}^i / \text{self}, \bar{u}]. \]

**Proof**
Straightforward induction on the complexity of \( P^c \). \(\square\)

Note that the substitution \( [\bar{id}^i / \text{self}, \bar{u}] \) transforms the assertion \( P^c \) into an assertion in \( Ass^c \) for arbitrary \( c \). Furthermore it is easy to see that if \( LVar(P) \cap \bar{id}^i = \emptyset \) then \( \models P^c \leftrightarrow P^c [\bar{id}^i / \text{self}, \bar{u}] [f / \bar{id}^i] \), where \( f \) denotes the sequence consisting of the expression \( \text{self} \) followed by the elements of \( \bar{u} \). Note that in general we do not have that \( P^c \) is syntactically equal to \( P^c [\bar{id}^i / \text{self}, \bar{u}] [f / \bar{id}^i] \), as is shown by the following example:

Doc. No.
Example 6.44
Take for $P^ci = z \equiv z.y$, where $z \not\in \tilde{id}^i$. We have $P^ci[\tilde{id}^i/sel, \bar{u}] = \tilde{id}_c, x \equiv z.y$ and $(\tilde{id}_c, x \equiv z.y)[f/\tilde{id}] = sel.x \equiv z.y$.

Next we consider the substitution $[b_{ci} \circ (sel)/b_{ci}]$. It is not difficult to see that for every assertion $P^ci$ we have

$$\models (P^ci[bl_{ci}/b_{ci}] \land b_{ci} = bl_{ci} \circ (sel))[b_{ci} \circ (sel)/b_{ci}] \rightarrow P^ci.$$  

But note that we do not have the other way around! However, as $\models init \rightarrow bl_{ci} = b_{ci}$, we do have

$$\models init \rightarrow ((init[bl_{ci}/b_{ci}] \land b_{ci} = bl_{ci} \circ (sel))[b_{ci} \circ (sel)/b_{ci}]).$$

To summarize the argument above we introduce the following definition:

**Definition 6.45**
For any $i \in \{1, \ldots, k\}$ and any assertion $P \in Ass^ci$ we define its reverse context switch $R(P^ci)$ as follows:

$$R(P^ci) = (P^ci[bl_{ci}/b_{ci}] \land b_{ci} = bl_{ci} \circ (sel))[\tilde{id}^i/sel, \bar{u}]$$

We have the following lemma about this reverse context switch:

**Lemma 6.46**
For any $i \in \{1, \ldots, k\}$ and every assertion $P \in Ass^ci$ we have

$$\models R(P^ci)[\tilde{e}^i/sel, \bar{u}][\bar{f}/\tilde{id}^i][b_{ci} \circ (sel)/b_{ci}] \rightarrow P^ci.$$  

and if $\models P^ci \rightarrow b_{ci} = bl_{ci}$ then

$$\models P^ci \rightarrow R(P^ci)[\tilde{e}^i/sel, \bar{u}][\bar{f}/\tilde{id}^i][b_{ci} \circ (sel)/b_{ci}].$$

Here $\bar{f} = sel, \bar{u}$.

**Proof**
Clear from the above. □

So at this stage candidates for $P_i, Q_i, i = 1, \ldots, k$, satisfying equations (6.2) and (6.3) are the assertions $R(init)$ and $R(SP^2_i(\rho_i, init)[r_i/v_i]), i = 1, \ldots, k$. We now proceed by analyzing equation (6.1). Suppose we are given that for some $P$ and $Q$ we have $\models \{P\} \rho_i\{Q\}$. In general we do not have

$$\models \{R(P) \land \bigwedge_j v_j^i = \text{nil} \land \text{self} \not\in b_{ci}\}\{U|c_i^j : S_i\} \{R(Q)[c_i/r_i]\},$$

Doc. No.
where \( Q' = Q[r_i/v_i] \). This is because it is possible that the object executing \( S_i \) is not the object which is sent the message and furthermore nothing is said about the values of the formal parameters. So we add to \( R(P) \) the information \( \text{self} \uparrow e_i^j[i\bar{d}^i/\text{self}, \bar{u}] \) and \( u_j^i = e_j^i[i\bar{d}^i/\text{self}, \bar{u}], j = 1, \ldots, n_i \). We have the following lemma:

**Lemma 6.47**

\[
\models (f^j_i \uparrow (e_i^j[i\bar{d}^i/\text{self}, \bar{u}])(\bar{f}^j/i\bar{d}^i])
\]

where \( \bar{f}^j = \text{self}, \bar{u}^j \) and \( f = \text{self}, \bar{u} \).

**Proof**

Easy. \( \square \)

Note that from lemma 6.46 and lemma 6.47 it follows that for every \( P^{ci} \) such that \( \models P^{ci} \rightarrow b_{ci} \cong bl_{ci} \) we have

\[
\models P \rightarrow \left( R(P) \land \bigwedge_j f^j_i \uparrow (e_i^j[i\bar{d}^i/\text{self}, \bar{u}])(\bar{f}^j/i\bar{d}^i])\right)[\text{self} \uparrow (\text{self})/b_{ci}].
\]

Now we are ready for the following lemma which shows how to transform a valid correctness formula about sending a message into a valid formula about the execution of the body of the message by the receiver:

**Lemma 6.48**

For any \( i \in \{1, \ldots, k\} \) and every \( P, Q \in \text{Ass}^{ci} \) such that \( \models \{P\} \rho_i \{Q\} \) we have

\[
\models \left( P' \land \bigwedge_j v^j \uparrow \text{nil} \land \text{self} \not\in b_{ci}\right) \{U|e_i^j : S_i\}\{Q'[e_i/r_i]\},
\]

where \( P' = R(P) \land \bigwedge_j f^j_i \uparrow (e_i^j[i\bar{d}^i/\text{self}, \bar{u}])(\bar{f}^j/i\bar{d}^i]) \) and \( Q' = R(Q[r_i/v_i]) \), with \( r_i \) a fresh logical variable of the same type as \( v_i \). Here \( \bar{v}^i = \bar{u} \setminus \bar{u}^i \).

**Proof**

Let \( \sigma, \delta, \omega \models P' \land \bigwedge_j v^j_i \uparrow \text{nil} \land \text{self} \not\in b_{ci} \), for \( \sigma, \delta, \omega \) such that \( OK(\sigma, \delta, \omega) \), and \( \sigma' = P[(U|e_i^j : S_i)](\gamma)(\delta)\omega(\sigma) \), with \( \gamma \) arbitrary and \( \sigma' \not\models \perp \).

We define \( \sigma_1 = \sigma\{\omega tv2_u/u\}_{u \in U} \) and \( \delta'_1 = \omega(id_{ci}) \), \( \delta'_1(c) = \delta_1(c) \) for every \( c \).

It follows from lemma 5.28 that \( \sigma_1, \delta', \omega \models P[\text{bl}_{ci}/b_{ci}] \land b_{ci} = b_{ci} \circ (\text{self}) \).

Next we define \( \delta'' \) as follows: \( \delta''_1 = \delta'_1, \delta''_1(c_i) = \delta''_1(c_i) \setminus \{\omega(id_{ci})\} \), and \( \delta''_1(c) = \delta'_1(c) \) for any \( c \neq c_i \). Furthermore we put \( \omega_1 = \omega(\text{bl}_{ci}/b_{ci}) \). It then follows that \( OK(\sigma_1, \delta'', \omega_1) \) and \( \sigma_1, \delta'', \omega_1 \models P \).
Let on the other hand \( \sigma'' = \sigma'(\omega(tv_{2u})/u) \) if \( v_i \in TVar \)

\[
\sigma_2 = \begin{cases} 
\sigma''(\beta/v_i) & \text{if } v_i \in TVar \\
\sigma''(\beta/\omega(id_{c_i}), v_i) & \text{if } v_i \in IVar,
\end{cases}
\]

where \( \beta = E[\epsilon_i(\delta)(\sigma')] \) (remember that \( \epsilon_i \) is the result expression of the method \( m_i \)). Now from \( \sigma, \delta, \omega \models \bigwedge_j f_j^{(i)} = (e_i^{(j)}[\text{id}/\text{self}, \overline{u}]) \) it follows from lemma 5.28 that \( \delta^{(1)} = L[e_i^{(j)}[\text{id}/\text{self}, \overline{u}]][\omega](\delta)(\sigma) = L[e_i^{(j)}][\omega](\delta'')(\sigma_1) \) and \( \sigma_2^{(2)}(u_j) = L[e_i^{(j)}][\omega](\delta'')(\sigma_1) \).

Furthermore from \( \sigma, \delta, \omega \models \text{self} \not\equiv b_i \) it in turn follows that \( \delta^{(1)} \not\equiv \delta_2^{(2)}(c_i) \). Now putting this together with the assumption that \( \sigma' = P[\epsilon_i(\sigma_1)](\gamma)(\delta)(\sigma) \), using \( \sigma, \delta, \omega \models \text{self} \equiv \text{nil} \), enables one to infer that \( \sigma_2 = P[\epsilon_i(\sigma_1)](\gamma)^{(2)}(\sigma_1) \).

Furthermore we are given that \( \models P[j_1(\epsilon i)] \) so from \( \sigma_1, \delta'', \omega_1 \models P \) and \( \sigma_2 = P[\epsilon_i(\sigma_1)](\gamma)(\delta'')(\sigma_1) \) we infer that \( \sigma_2, \delta'', \omega_1 \models Q \). Now let \( \omega_2 = \omega(\beta/r_1) \). It then follows by lemma 5.8 that \( \sigma'', \delta'', \omega_2 \models Q[r_1/v_i] \).

Next we note that as \( \omega_2(b_{c_i}) = \omega(b_{c_i}) \) we have \( \sigma_2, \delta'', \omega_3 \models Q[r_1, b_{c_i}/v_i, b_{c_i}] \), where \( \omega_3 = \omega(\beta/r_1) \).

From \( \sigma, \delta, \omega \models R(P) \) we infer that \( \omega(b_{c_i}) = \omega(b_{c_i}) \circ (\omega(id_{c_i})) \). But \( \omega(id_{c_i}) = \delta^{(1)} \) so we have \( \sigma'', \delta'', \omega_3 \models Q[r_1, b_{c_i}/v_i, b_{c_i}] \land b_{c_i} = b_{c_i} \circ (\omega(id_{c_i})) \).

Now an application of lemma 5.28 gives us \( \sigma', \delta, \omega_3 \models R(Q[r_1/v_i]) \). From this in turn it follows that \( \sigma', \delta, \omega \models Q'[\epsilon_i/r_1] \).

Now we want to apply lesson 6.48 taking init for \( P \) and \( SP^{L^+}(\rho_i, \text{init}) \) for \( Q \). Note that by lemma 6.22 we have \( \models \{ \text{init} \} \rho_i \{ SP^{L^+}(\rho_i, \text{init}) \} \).

Now taking for \( P_i \) the assertion \( R(\text{init}) \land \bigwedge_j f_j^{(i)} = (e_i^{(j)}[\text{id}/\text{self}, \overline{u}]) \) for \( Q_i \) the assertion \( R(SP^{L^+}(\rho_i, \text{init})[r_1/v_i]) \) we have by lemma 6.46 and lemma 6.47 that equations (6.2) and (6.3) are satisfied. However since in the assertions \( P_i \) and \( Q_i \), new logical variables occur which are not contained in \( L \), we must apply theorem 6.40 for \( F_i = \{ \text{init} \} \rho_i \{ SP^{L^+}(\rho_i, \text{init}) \} \), where \( L^+ = L \cup \{ id : c \in C \} \cup \{ tv_{2u} : u \in \overline{u} \} \). But to apply the rule (NMR) we then have to take for \( Q_i \) the assertion \( R(SP^{L^+}(\rho_i, \text{init})[r_1/v_i]) \). An application
of (NMR) and (MI) or (MT) would then give us the derivability of the correctness formula \( \{ \text{init} \} \rho \{ SP_{L+}^\rho (\text{init}) \} \). However, as \( L \models \text{init} \) \( \Rightarrow SP_{L+}^\rho (\text{init}) \) (use \( L \text{Var}(\text{init}) \subseteq L \subseteq L^+ \)), we have by an application of the consequence rule the derivability of \( \{ \text{init} \} \rho \{ SP_{L}^\rho (\text{init}) \} \).

But there is one problem we did not discuss yet. As \( \text{stl} \cup \text{ire} \subseteq \text{LVar}(SP_{L+}^\rho (\rho_i, \text{init})) \) we cannot apply theorem 6.40! This problem is solved as follows: First we define \( L^+ = L^+ \setminus (\text{stl} \cup \text{ire}) \). Next we define the following abbreviation:

**Definition 6.49**
Let \( \text{Subs}(\text{ire}, \text{stl}, \text{cr}) \) abbreviate the assertion:

\[
\bigwedge_c (\text{cr}_c \subseteq \text{cr} \land \text{bl}_c \subseteq \text{cr} \land \text{ire}_c \in \text{cr} \land \bigwedge_{d \in c} \bigwedge (\text{iv}_1 x \subseteq \text{cr}_d \land \bigwedge_{u \in \text{TVar}_c} \text{tv}_1 u \in \text{cr}_d).
\]

The assertion \( \text{Subs}(\text{ire}, \text{stl}, \text{cr}) \) states that all the objects which are denoted by a variable of \( \text{ire} \) or \( \text{stl} \), or which occur in a sequence denoted by some variable of \( \text{stl} \), are stored in the corresponding variable of \( \text{cr} \). We have the following proposition:

**Proposition 6.50**
Let \( \Pi = R(\text{init}) \land \bigwedge f_j = (e_j [i d^j / \text{self}, \bar{u}]), Q_i^- = R(SP_{L^-}^\rho (\rho_i, \text{init})[r_i/v_i]) \) and \( Q_i^+ = R(SP_{L+}^\rho (\rho_i, \text{init})[r_i/v_i]) \). We have

\[
\models \Pi \land \text{Subs}(\text{ire}, \text{stl}, \text{cr}) \iff \Pi
\]

and

\[
\models Q_i^- [e_i/r_i] \land \text{Subs}(\text{ire}, \text{stl}, \text{cr}) \rightarrow Q_i^+[e_i/r_i].
\]

**Proof**
The first assertion follows immediately from the fact that the assertion \( \text{init} \) (and so the assertion \( R(\text{init}) \)) implies the assertion \( \forall z_c (z_c \in \text{cr}_c) \), for every \( c \).

Now we prove the second assertion. Let \( \sigma, \delta, \omega \models Q_i^- [e_i/r_i] \land \text{Subs}(\text{ire}, \text{stl}, \text{cr}) \). For \( \omega_1 = \omega \{ \Upsilon [e_i] \mid (\Delta)(\sigma) / r_i \} \), we then have \( \sigma, \delta, \omega_1 \models Q_i^- \land \text{Subs}(\text{ire}, \text{stl}, \text{cr}) \).

Next we define \( \sigma' = \sigma \{ \omega_1 (tv2_u) / u \} u \in u \), and \( \delta'_{(1)} = \omega_1 (\text{id}_{c_i}), \delta'_{(2)}(c) = \delta_{(2)}(c) \), for every \( c \). It then follows by lemma 5.28 that: \( \sigma', \delta', \omega_1 \models SP_{L^-}^\rho (\rho_i, \text{init})[r_i, \text{bl}_{c_i} / v_i, b_{c_i}] \land b_{c_i} = \text{bl}_{c_i} \circ (\text{self}) \land \text{Subs}(\text{ire}, \text{stl}, \text{cr}) \).

For \( \omega_2 = \omega_1 \{ \omega_1 (\text{bl}_{c_i}) / b_{c_i} \} \) and \( \delta''_{(1)} = \delta'_{(1)} \), for \( c = c_i \); \( \delta''_{(2)}(c) = \delta'_{(2)}(c) \), otherwise; \( \delta''(c) = \delta'(c) \setminus \delta'_{(1)} \), we have \( \sigma', \delta'', \omega_2 \models SP_{L^-}^\rho (\rho_i, \text{init})[r_i / v_i] \land \text{Subs}(\text{ire}, \text{stl}, \text{cr}) \).

Doc. No.
Next, let
\[ \sigma'' = \begin{cases} 
\sigma'(w_2(r_i), v_i) & \text{if } v_i \in IVar \\
\sigma'(w_2(r_i)) & \text{if } v_i \in TVar.
\end{cases} \]

It follows that \( \sigma'', \delta'' \models SP_{L-}(\rho_i, \text{init}) \land \text{Subs}(\overline{\text{ire}}, \overline{\text{sl}}, \overline{\delta}). \)

So by theorem 6.21 there exist \( f \) and \( \sigma_0 \) such that:

- \( f(\sigma'') = \mathcal{P}(\rho)(\gamma)(f(\delta''))(\sigma_0), \) with \( \gamma \) arbitrary,
- \( \sigma_0, f(\delta''), \omega' \models \text{init}, \)

where \( \omega' = f(\omega_2) \downarrow L^- \). Let \( \sigma_1 = f(\sigma'') \). Now by theorem 6.19 we have that \( \sigma_1, f(\delta''), f(\omega_2) \models \text{Subs}(\text{ire}, \overline{\text{sl}}, \overline{\delta}). \) So from \( \{ \text{cr}_{c} : c \in C \} \subseteq L^- \) and the compatibility of \( \omega' \) and \( \sigma_0 \) we then infer the compatibility of \( f(\omega_2) \downarrow L^+ \) and \( \sigma_0 \). Let \( \omega'' = f(\omega_2) \downarrow L^+ \). We have that \( \sigma_0, f(\delta''), \omega'' \models \text{init}, \) so we have \( \sigma'', \delta'', \omega_2 \models SP_{L+}(\rho_i, \text{init}). \)

From this it follows, by "reversing" the part of the above argument which led to the statement \( \sigma'', \delta'', \omega_2 \models SP_{L-}(\rho_i, \text{init}), \) that \( \sigma, \delta, \omega \models Q_i^+[\epsilon_i/r_i]. \)

Now we are ready for the following theorem.

**Theorem 6.51**

Let the program \( \rho = (U|c : v \leftarrow e_0!m(e_1, \ldots, e_n)) \) be closed and let \( BVar \subseteq L \subseteq LVar \) such that \( \overline{\text{sl}} \cup \overline{\text{sl}} \cup \overline{\text{ire}} \subseteq L. \) Then we have

\[ \models \{ \text{init} \} \rho \{ \text{SP}_{L-}(\rho, \text{init}) \}. \]

**Proof**

Let \( P_i = \text{R}(\text{init}) \land \bigwedge_j f_j^i \downarrow (e_j'[\overline{\text{ire}}/\overline{\text{ire}}, \overline{\delta}], \overline{Q}_i^- = \text{R}(SP_{L-}(\rho_i, \text{init})[r_i/v_i]) \) and \( Q_i^+ = \text{R}(SP_{L+}(\rho_i, \text{init})[r_i/v_i]) \). Now by lemma 6.22 we get

\[ \models \{ \text{init} \} \rho_i \{ SP_{L-}^{\rho_i}(\rho_i, \text{init}) \} \]

So we have, by lemma 6.48,

\[ \models \{ P_i \land \bigwedge_j v_j^i \downarrow \text{nil} \land \text{self} \notin b_{\rho_i} \} \{ U|c_i^i : S_i \} \{ Q_i^-[\epsilon_i/r_i] \}. \]

An application of theorem 6.40 then gives us (note that the restrictions on the logical variables are satisfied)

\[ F_1', \ldots, F_k' \models \{ P_i \land \bigwedge_j v_j^i \downarrow \text{nil} \land \text{self} \notin b_{\rho_i} \} \{ U|c_i^i : S_i \} \{ Q_i^-[\epsilon_i/r_i] \}, \]

Doc. No.
where
\[ F'_i = \{ \text{init} \} \rho_i \{ SP_{L+}^{\alpha}(\rho_i, \text{init}) \}. \]

Now by lemma 6.46 and lemma 6.47 an application of the consequence rule gives us
\[ F_i \vdash F'_i \]
where
\[ F_i = \left\{ P_i[\bar{e}^i/\text{self}, \bar{u}^i][\bar{f}/\bar{u}^i][b_{c_i} \circ \langle \text{self} \rangle / b_{c_i}] \right\} \rho_i \{ SP_{L+}^{\alpha}(\rho_i, \text{init}) \}. \]

So we have
\[ F_1, \ldots, F_k \vdash \left\{ P_i \land \bigwedge_j v_j^i = \text{nil} \land \text{self} \notin b_{c_i} \right\} \langle U | c'_i : S_i \rangle \{ Q^{-}_i[e_i/r_i] \}. \]

By theorem 6.33 we have
\[ \vdash \{ \text{Subs}(\bar{t}_r, \bar{s} \bar{I}, \bar{c} \bar{r}) \} \langle U | c'_i : S_i \rangle \{ \text{Subs}(\bar{t}_r, \bar{s} \bar{I}, \bar{c} \bar{r}) \}. \]

So by the conjunction rule we infer
\[ \{ P_i \land \bigwedge_j v_j^i = \text{nil} \land \text{self} \notin b_{c_i} \land \text{Subs}(\bar{t}_r, \bar{s} \bar{I}, \bar{c} \bar{r}) \} \]
\[ F_1, \ldots, F_m \vdash \langle U | c'_i : S_i \rangle \{ Q^{-}_i[e_i/r_i] \}. \]

By proposition 6.50 an application of the consequence rule gives us
\[ F_1, \ldots, F_m \vdash \left\{ P_i \land \bigwedge_j v_j^i = \text{nil} \land \text{self} \notin b_{c_i} \right\} \langle U | c'_i : S_i \rangle \{ Q^{-}_i[e_i/r_i] \}. \]

We now can apply rule (NMR), making use of lemma 6.46, yielding the derivability of the correctness formula:
\[ \{ P_i \land \bigwedge_j v_j^i = \text{nil} \land \text{self} \notin b_{c_i} \} \langle U | c'_i : S_i \rangle \{ Q^{-}_i[e_i/r_i] \}. \]

Applying next (MI) or (MT) gives us the derivability of
\[ \left\{ P_i[\bar{e}^i/\text{self}, \bar{u}^i][\bar{f}/\bar{u}^i][b_{c_i} \circ \langle \text{self} \rangle / b_{c_i}] \right\} \rho_1 \{ SP_{L+}(\rho_1, \text{init}) \}. \]

So an application of the consequence rule (the assertion \text{init} by lemma 6.46 implies the precondition, and \vdash SP_{L+}(\rho_1, \text{init}) \rightarrow SP_{L}(\rho_1, \text{init})) gives us the desired result
(note that \rho_1 = \rho by definition)
\[ \vdash \{ \text{init} \} \rho \{ SP_{L}(\rho, \text{init}) \}. \]

We conclude with the completeness theorem:

Doc. No.
Theorem 6.52
Let $\rho^c = (U| c : S)$ be a closed program. We have for an arbitrary correctness formula $\{p^c\} \rho^c \{Q^c\}$:

$$\models \{p^c\} \rho^c \{Q^c\} \text{ implies } \vdash \{p^c\} \rho^c \{Q^c\}.$$

Proof
Let $P'$ and $Q'$ result from substituting for every variable of $\text{stl}$ and $\text{ire}$ a corresponding new variable (new with respect to the sets $LVar(P^c, Q^c), \text{stl}, \text{ire}$). Let $L \subseteq LVar (L \text{ finite})$ be such that $BVar \subseteq L$, $LVar(P', Q') \subseteq L$ and $\text{stl} \cup \text{stl} \cup \text{ire} \subseteq L$. By the soundness of the substitution rule we have $\vdash \{P'\} \rho^c \{Q'\}$, so applying theorem 6.40 gives us

$$F_1, \ldots, F_n \vdash \{P'\} \rho^c \{Q'\},$$

where $F_i = \{\text{init}\} \rho_t \{SP^c_t(\rho_t, \text{init})\}, \rho_t = (U| \forall e_i : v_i \leftarrow e_i^0 !m_i(e_i^1, \ldots, e_i^n))$ and $e_i^0 !m_i(e_i^1, \ldots, e_i^n)$, $i = 1, \ldots, n$, are all the send-expressions occurring in $S$, and if such an expression $e_i^0 !m_i(e_i^1, \ldots, e_i^n)$ occurs in $S$ as a statement we have that $v_i = \text{re}_{d_i}$, assuming $d_i$ to be the type of the result expression of $m_i$. By theorem 6.51 we have the derivability of $F_i$, so we infer that $\vdash \{P'\} \rho^c \{Q'\}$. Finally an application of the substitution rule gives us the derivability of $\{P^c\} \rho^c \{Q^c\}$. \qed

Doc. No.
7 Conclusions

In the previous sections we have given a proof system for SPOOL that fulfills the requirements we have listed in the introduction:

- The only possible operations on object references (pointers) are testing for equality and dereferencing.
- In each state of the system only the existing objects play a role in assertions about that state.

In fact, we have given even two proof systems fulfilling these requirements: one with recursively defined predicates and one with the ability to reason about finite sequences of objects.

The technique which we have given for computing the weakest precondition for an assignment with respect to a given postcondition, a generalized version of substitution, seems very powerful. Especially the fact that is possible to do this for a new assignment, in the situation that it is not possible to mention the newly created object in the state before the statement, is a little bit surprising.

The proof rule for message passing, incorporating the passing of parameters and result, context switching, and the constancy of the variables of the sending object, is a very complex rule. It seems to work fine for our proof system, but its properties have not yet been studied extensively enough. It would be interesting to see whether the several things that are handled in one rule could be dealt with by a number of different, simpler rules.

We have proved completeness for the proof system based on the assertion language containing quantification over finite sequences using the standard techniques (see [3], for example). But how to apply these techniques to the proof system based on recursive predicates remains an open problem.

Therefore we must conclude that there is still some work to be done on these issues. In addition, in the present proof systems the protection properties of object are not reflected very well. While in the programming language it is not possible for one object to access the internal details (variables) of another one, in the assertion language this is allowed. In order to improve this it might be necessary to develop a system in which an object presents some abstract view of its behaviour to the outside world. Perhaps techniques developed to deal with abstract data types are useful here.
References


A A generalisation of the rule (MR)

In this section we show that in the recursion rule (MR), as introduced in definition 5.33 and adapted in definition 6.4, we can replace $U^-$ by $U$ itself, thus allowing nested applications of (MR) to the same methods. Let (NMR) denote the recursion rule resulting from (MR) by replacing all occurrences of $U^-$ by $U$. Furthermore let $\vdash$ denote the derivability using (NMR) ($\vdash$ denotes derivability using (MR)). We have the following theorem:

**Theorem A.1**
For every correctness formula $F$ we have $\vdash F$ iff $\vdash F$.

**Proof**
$\Rightarrow$: We prove that if $F_1, \ldots, F_n \vdash F$ then $F_1, \ldots, F_n \vdash F$ by induction on the length of the derivation. We treat the case that the last rule applied is (NMR). So let the following be an instance of (NMR):

$$
\frac{\bar{F}_1, \ldots, \bar{F}_n}{F_1'}
$$

where $F_1' = F$. Let $U$ be the unit occurring in this application of (NMR). We may assume without loss of generality that all the methods declared by $U$ are specified by one of the $F_i$. (Otherwise, let $\{\rho_1, \ldots, \rho_k\}$, where $\rho_i = \langle U | c_i : v_i \leftarrow e_i^m_m(\epsilon_i^1, \ldots, \epsilon_i^n) \rangle$, be all the send statements occurring in $U$. Now simply add to $F_1, \ldots, F_n$ for $i = 1, \ldots, k$. $G_i = \{\text{true}\} \rho_i \{\text{true}\}$, and note that

$$
G_1, \ldots, G_k \vdash \{\text{true}\} \langle U | c_i : S_i \rangle \{\text{true}\}
$$

where $e_i^j$ is the type of $e_i^m$ and $S_i$ denotes the body of $m_i$.) We shall prove by induction on the number of applications of (NMR) in the derivation $F_1, \ldots, F_n \vdash F_1', \ldots, F_n'$ that for some $\bar{H}_1, \ldots, \bar{H}_k, H_1, \ldots, H_k, H_1', \ldots, H_k'$ such that for $1 \leq i \leq k$

$$
\frac{H_i'}{\bar{H}_i}
$$

is an instance of (MI) or (MT), we have:

$$
\bar{F}_1, \ldots, \bar{F}_n, \bar{H}_1, \ldots, \bar{H}_k \vdash \bar{F}_1', \ldots, \bar{F}_n', \bar{H}_1', \ldots, \bar{H}_k'
$$

where, for $G = \{P\} \langle U | c : S \rangle \{Q\}$, $\bar{G}$ denotes $\{P\} \langle E | c : S \rangle \{Q\}, E$ being the empty unit. Having proved this we apply (MR) thus yielding $\vdash F_1' (= F)$. Here we go:

**Induction basis**: Assume that no application of (NMR) occurs in the derivation $F_1, \ldots, F_n \vdash F_1', \ldots, F_n$. So we have that $F_1, \ldots, F_n \vdash F_i', \ldots, F_n'$, where $\vdash$ denotes
derivability from \( \vdash \) without (MR). It is not difficult to see that it suffices to prove by induction on the length of the derivation that for an arbitrary correctness formula \( G \) if \( F_1, \ldots, F_n \vdash G \) then for some \( \bar{H}_1, \ldots, \bar{H}_k, H_1, \ldots, H_k, H_1', \ldots, H_k' \) we have

\[
F_1, \ldots, F_n, \bar{H}_1, \ldots, \bar{H}_k \vdash \bar{G}, \bar{H}_1', \ldots, \bar{H}_k',
\]

where for \( i = 1, \ldots, k \)

\[
\frac{H_i'}{H_i}
\]

is an instance of (MI) or (MT). We treat the only interesting case that the last rule applied is an instance of (MI) or (MT). So suppose \( F_1, \ldots, F_n \vdash G', \bar{G} \), where

\[
\frac{G'}{\bar{G}}
\]

is an instance of (MI) or (MT). Now by the induction hypothesis we know that for some \( \bar{H}_1, \ldots, \bar{H}_k, H_1, \ldots, H_k, H_1', \ldots, H_k' \):

\[
F_1, \ldots, F_n, \bar{H}_1, \ldots, \bar{H}_k \vdash \bar{G}', \bar{H}_1', \ldots, \bar{H}_k',
\]

such that for \( i = 1, \ldots, k \)

\[
\frac{H_i'}{H_i}
\]

is an instance of (MI) or (MT). Now let \( \bar{H}_{k+1} = \bar{G}, H_{k+1} = G \), and \( H_{k+1}' = G' \). We then have that

\[
F_1, \ldots, F_n, \bar{H}_1, \ldots, \bar{H}_{k+1} \vdash \bar{G}, \bar{H}_1', \ldots, \bar{H}_{k+1}'.
\]

**Induction step:** Let for \( i = 1, \ldots, m \)

\[
\frac{\bar{G}^i_1, \ldots, \bar{G}^i_n}{G^i_1, \ldots, G^i_n | \vdash G^i_1', \ldots, G^i_n'}
\]

be all the applications of (NMR) in the derivation \( F_1, \ldots, F_n | \vdash F_1', \ldots, F_n' \) such that

\[
F_1, \ldots, F_n, G^i_1, \ldots, G^i_n' | \vdash F_1', \ldots, F_n'.
\]

By the same induction argument as used in the basis step above we have for some \( \bar{H}_1, \ldots, \bar{H}_k, H_1, \ldots, H_k, H_1', \ldots, H_k' \) (such that for \( i = 1, \ldots, k \)

\[
\frac{H_i'}{H_i}
\]

is an instance of (MI) or (MT)) that

\[
F_1, \ldots, F_n, H_1, \ldots, H_k, G^i_1, \ldots, G^i_n' | \vdash F_1', \ldots, F_n', H_1', \ldots, H_k'.
\]
where \( \vdash = \) denotes derivability from \( \vdash \) minus the rules (MR), (MI), and (MT). Now, applying the induction hypothesis gives us for \( i = 1, \ldots, m \): \( \bar{H}_i^1, \ldots, \bar{H}_{k_i}^i \), \( H_i', \ldots, H_{k_i}' \) such that

\[
\bar{G}_i^1, \ldots, \bar{G}_n^i, \bar{H}_1^i, \ldots, \bar{H}_{k_i}^i \vdash \bar{G}_1', \ldots, \bar{G}_n', \bar{H}_1', \ldots, \bar{H}_{k_i}'.
\]

Now it follows by a straightforward induction on the length of the derivation

\[
F_1, \ldots, F_n, H_1, \ldots, H_k, G_1', \ldots, G_n' \vdash F_1', \ldots, F_n', H_1', \ldots, H_k'.
\]

that

\[
\mathcal{F} \cup \bigcup_i \mathcal{G}_i \cup \bigcup_i \mathcal{H}_i \vdash \mathcal{F}' \cup \bigcup_i \mathcal{G}_i' \cup \bigcup_i \mathcal{H}_i'.
\]

where

- \( \mathcal{F} = \{ \bar{F}_1, \ldots, \bar{F}_{n+k} \}, \ F_{n+i} = H_i, i = 1, \ldots, k, \)
- \( \mathcal{F}' = \{ \bar{F}_1', \ldots, \bar{F}_{n+k}' \}, \ F_{n+i}' = H_i', i = 1, \ldots, k, \)
- \( \mathcal{G}_i = \{ \bar{G}_1^i, \ldots, \bar{G}_n^i \}, 1 \leq i \leq m, \)
- \( \mathcal{G}_i' = \{ \bar{G}_1^i', \ldots, \bar{G}_n^i' \}, 1 \leq i \leq m, \)
- \( \mathcal{H}_i = \{ \bar{H}_1^i, \ldots, \bar{H}_{k_i}^i \}, 1 \leq i \leq m, \)
- \( \mathcal{H}_i' = \{ \bar{H}_1^i', \ldots, \bar{H}_{k_i}' \}, 1 \leq i \leq m. \)

\( \Leftarrow: \) This is proved in a similar way as the other direction.\[\square\]
B  Expressibility

In this section we show how to formulate the assertion $SP_{x}(\rho^{c}, P^{c})$ in our assertion language, for an arbitrary closed program $\rho^{c}$, $BVar \subseteq L \subseteq LVar$ ($L$ finite), such that $LVar(P^{c}) \subseteq LVar$.

As in section 6 we assume the sets $C$, $IVar$, and $TVar$ to be finite.

B.1  Coding mappings

Assumption B.1

We assume the existence of the following coding mappings:

- For every instance variable or temporary variable $v \in IVar$ we have $[v] \in N$, and for an arbitrary program $\rho$ we have $[\rho] \in N$.
- For every $d \in C^{+}, [.]_{d} : O_{1}^{d} \rightarrow N$ denotes an injection such that $[\bot]_{d} = 0$. In addition, we assume that the function $[.]$ is surjective.
- For every state $\sigma \in \Sigma$ such that $OK(\sigma)$, $[\sigma] \in N$.
- For every context $\delta^{c} \in \Delta^{c}$: $[\delta^{c}] \in N$.

Furthermore we assume that the mappings $[.]$ and $[.]$ are definable in our assertion language. That is, we regard the following function symbols as abbreviations for assertions that are expressible in our assertion language:

- $Ic(n) = m$ (mnemonic: integer coding) iff $[n] = m$.
- $Bc(b) = m$ (mnemonic: Boolean coding) iff $[b] = m$.
- $Id(n) = m$ (mnemonic: integer decoding) iff $[m] = n$.

To be precise, with the first assumption above we mean that there is an assertion $Ic(z_{1}) = z_{2}$, where $z_{1}$ and $z_{2}$ are integer logical variables, such that for every $\sigma \in \Sigma, \delta \in A, \omega \in \Omega$ with $OK(\sigma, \delta, \omega)$ we have

$$\sigma, \delta, \omega \vdash Ic(z_{1}) = z_{2} \text{ iff } [\omega(z_{1})] = \omega(z_{2}).$$

In fact from now on for every $c \in C$ and $\alpha \in O^{c}$ we identify $[\alpha]_{c}$ with $\alpha$. So we assume $O^{c} \subseteq N$.

In the same way we assume the following predicates and functions to be expressible in our assertion language:

Doc. No.
• $E^c(n, m)$ (mnemonic: exists) iff there exist $\sigma \in \Sigma$ and $\alpha \in \sigma^{(c)}$ such that $[\sigma]_c = n$ and $[\sigma] = m$.

• $A^c(n) = m$ (mnemonic: active) iff there exists $\delta \in \Delta^c$ such that $[\delta] = n$ and $[\delta(1)]_c = m$.

• $B^c(n, m)$ (mnemonic: blocked) iff there exist $\delta \in \Delta$ and $\alpha \in \delta^{(2)(c)}$ such that $[\alpha]_c = n$ and $[\alpha] = m$.

• $Val^c_k(l, m) = n$ (mnemonic: value) iff there exist $\sigma \in \Sigma$, $\alpha \in \sigma^{(c)}$, and $\sigma^c \in IVar^{(c)}$ such that $[\alpha] = k$, $[\sigma^c] = l$, $[\sigma] = m$, and $[\sigma(\alpha)(\sigma^c)]_d = n$.

• $Val_d(l, m) = n$ iff there exist $\sigma \in \Sigma$ and $u_d \in TVard$ such that $[u_d] = l$, $[\sigma] = m$, and $[\sigma(u_d)]_d = n$.

• $T^c(n, m, l, k)$ (mnemonic: transforms) iff there exist a closed $\rho \in Progc^{(c)}$, $\delta \in \Delta^c$, and $\sigma, \sigma' \in \Sigma$ such that $OK(\sigma, \delta)$, $[\rho] = n$, $[\delta] = m$, $[\sigma] = l$, $[\sigma'] = k$, and $\sigma' = P^c[\rho][(\gamma)(\delta)(\sigma)]$ (where $\gamma$ is arbitrary).

The above assumptions may appear quite implausible at first sight, but they can be justified by Church's Thesis, which states that every function or relation that can be effectively calculated is recursive, together with the (mathematical) fact that every recursive function is representable in the standard Peano theory of natural numbers and therefore it is certainly definable in our assertion language. (For a discussion of these issues, see [5] or [9].)

B.2 Arithmetizing Truth

To express the strongest postcondition we have to arithmetize the truth of an assertion in a state. More precisely, we will define a translation which transforms an arbitrary assertion into an assertion in which no instance variables or temporary variables occur. The idea of this translation is similar to the one given in the definitions 6.26 and 6.28. But instead of transforming an assertion into an assertion referring to a sequence of logical variables used to store the state, we now transform it into an assertion referring to the code of a state. This is necessary to be able to use the predicates of assumption B.1, in particular the predicate $T$.

To get started we introduce some new variables: Let $bij^c$ denote a sequence of some variables $bij^c \in LVar^c$, $c \in C$. We shall use these variables to store the essential parts of the bijections that constitute an osi (see definition 6.17). The way in which this is done will be made precise in definition B.3, but here we can already explain how the $bij^c$ can be used as a kind of decoding tables. To that end we assume that we
have a certain state $\sigma$ such that for every $c \in C$ and $\alpha \in O_1^\sigma$,

$$\text{elt}(\beta, [\alpha]_c) = \begin{cases} 
\alpha & \text{if } \alpha \in \sigma^{(c)} \\
\bot & \text{otherwise}.
\end{cases}$$

where $\beta \in O^{\sigma}$ is the value of $bij^c$ in a certain $\omega$. So every existing object of class $c$ occurs in the sequence denoted by $bij^c$ at a position which equals its code number. It is important to note that we cannot express this property of the sequence denoted by $bij^c$ in the assertion language: There exists no assertion $P(bij^c)$ such that for every $\sigma, \delta, \omega$ with $OK(\sigma, \delta, \omega)$ we have $\sigma, \delta, \omega \models P(bij^c)$ precisely if the above property holds. This is because at the level of the assertion language objects simply are not integers. Fortunately we shall not need the expressibility of exactly this property, but only of this property modulo an $osl$. This is the subject of section B.3.

**Definition B.2**

Let $z^\sigma, z^\sigma$ be some logical integer variables. We assume that the value of $z^\sigma$ equals the code $[\alpha]$ of some state $\sigma$, and that the value of $z^\sigma$ equals $[\alpha]_c$ for some $\alpha \in \sigma^{(c)}$. For every logical expression $l_2$ we define $l_2[x^\sigma, z^\sigma]$ as a triple $(\bar{i}, l_1, l_2)$, where $\bar{i}$ denotes a sequence of logical integer variables, and $l_1$ and $l_2$ are logical expressions. Note that we do not define this transformation for logical expressions of type $d^*$ with $d \in C^+$. The idea behind this transformation $l_2[ar{i}, z^\sigma, z^\sigma] = (\bar{i}, l_1, l_2)$ can be described as follows: The expression $l_1$ is constructed such that it is only true if the variables $\bar{i}$ contain the code numbers of certain objects that are relevant for the evaluation of $l_2$. To do this, $l_1$ can consult the variables $bij$ as a translation table from code numbers to actual objects. Using this information, $l_2$ is a translation of $l_2$ such that every operation on objects described by $l_2$ is translated into a corresponding arithmetical operation on code numbers.

Here is the formal definition:

- $x_d^\sigma[z^\sigma, z^\sigma] = (\epsilon, \text{true}, \text{Val}_d(z^\sigma, k, z^\sigma))$, where $k = [x_d^\sigma]$ and $\epsilon$ is the empty sequence.
- $u_d[z^\sigma, z^\sigma] = (\epsilon, \text{true}, \text{Val}_d(k, z^\sigma))$, where $k = [u_d]$.
- $\text{nil}[z^\sigma, z^\sigma] = (\epsilon, \text{true}, 0)$.
- $\text{self}[z^\sigma, z^\sigma] = (\epsilon, \text{true}, z^\sigma)$.
- $l[z^\sigma, z^\sigma] = (\epsilon, \text{true}, \text{Bc}(l))$, where $l = \text{true}, \text{false}$.
- $n[z^\sigma, z^\sigma] = (\epsilon, \text{true}, [n])$.
Next we define for every assertion $Pc$ its transformation $Pc[z^a, z^s]$.

- $l^c[z^a, z^s] = \exists i(l_1 \land l_2 = Bc(true))$, where $l^c[z^a, z^s] = (i, l_1, l_2)$.
- $(P_1 \land P_2)[z^a, z^s] = P_1[z^a, z^s] \land P_2[z^a, z^s]$.
- $(\exists z_{a}P)[z^a, z^s] = \exists z_{a}P[z^a, z^s]$ for $a = \text{Int, Bool, Int*, Bool*}$.
- $(\exists z_{d}P)[z^a, z^s] = \exists z_{d}(z_{d} \in \text{bij}^d \land P[z^a, z^s])$ for every $d \in C$. Here $z_{d} \in \text{bij}^d$ abbreviates $\exists i z_{d} = \text{bij}^d \cdot i$ (cf. definition 6.28).
- $(\exists z_{d^*}P)[z^a, z^s] = \exists z_{d^*}(z_{d^*} \subseteq \text{bij}^d \land P[z^a, z^s])$ for every $d \in C$. Here $z_{d^*} \subseteq \text{bij}^d$ abbreviates $\forall i z_{d^*} \cdot i \in \text{bij}^d$ (cf. definition 6.28).
\( (\forall z_d P)[z^{\alpha}, z^{\sigma}] = \forall z_d P[z^{\alpha}, z^{\sigma}] \)
for \( a = \text{Int}, \text{Bool}, \text{Int}^*, \text{Bool}^* \).

\( (\forall z_d P)[z^{\alpha}, z^{\sigma}] = \forall z_d (z_d \in \text{bij}^d \rightarrow P[z^{\alpha}, z^{\sigma}]) \)
for every \( d \in C \).

\( (\forall z_d^* P)[z^{\alpha}, z^{\sigma}] = \forall z_d^* (z_d^* \subseteq \text{bij}^d \rightarrow P[z^{\alpha}, z^{\sigma}]) \)
for every \( d \in C \).

In this transformation we assume that the quantified variables are distinct from any of
the variables of \( \text{bij} \). Note that the result of this transformation applied to an arbitrary
assertion is a quantification-restricted assertion.

To describe the semantics of this transformation we need the following definition.

**Definition B.3**
Let \( \omega \in \Omega, \sigma \in \Sigma \), and let \( f \) be an \( \text{osi} \) (see definition 6.17). Then we write \( \text{Code}(\omega, \sigma, f) \) iff for every \( c \in C \) we have

- \( \sigma^{(c)}_\perp = \{\text{elt}(\beta^{c*}, n) : n \in \mathbb{N}\} \)
- for all \( \alpha \in \sigma^{(c)} \) and for all \( n \in \mathbb{N} \) we have
  \[ \text{elt}(\beta^{c*}, n) = \alpha \quad \text{iff} \quad f^c(\alpha) = n \]

where \( \beta^{c*} = \omega(\text{bij}^c) \).

We write \( \text{Code}_L(\omega, \sigma, f) \) if \( \text{Code}(\omega, \sigma, f) \) and additionally for every \( c \in C \) we have

- \( \omega(z) \in \omega(\text{bij}^c) \) for every \( z \in L \cap L\text{Var}_c \)
- \( \omega(z) \subseteq \omega(\text{bij}^c) \) for every \( z \in L \cap L\text{Var}_c^* \)

In a sense \( \text{Code}(\omega, \sigma, f) \) can be interpreted as saying that \( \omega(\text{bij}^c) \) codes the restriction
of the \( \text{osi} \) \( f \) to the existing objects of \( \sigma \).

Now we are ready for the following semantical interpretation of the transformation
described above.

**Theorem B.4**
Assume to be given the states \( \sigma, \sigma', \sigma'' \) such that \( \sigma \preceq \sigma'' \) and an \( \text{osi} \) \( f \) such that
\( f(\sigma^{(c)}) = \sigma'^{(c)} \) for every \( c \in C \). Furthermore let \( \omega \in \Omega \) and \( \delta \in \Delta^c \) be such that

Doc. No.
$\text{OK}(\omega, \delta, \sigma'')$ and $\text{Code}_L(\omega, \sigma, f)$, where $BVar \subseteq L \subseteq LVar$. Then for every assertion $P^c$ such that $LVar(P^c) \subseteq L$ and $LVar(P^c) \cap \overline{bij} = \emptyset$ we have

$$\sigma', \delta', \omega' \models P^c \iff \sigma'', \delta, \omega \{n, m/z^\alpha, z^\sigma\} \models P^c[z^\alpha, z^\sigma],$$

where $\delta' = f(\delta)$, $\omega' = f(\omega) \upharpoonright L$, $n = [f(\delta(1))]_c$, $m = [\sigma']$, and $z^\alpha, z^\sigma$ are new logical integer variables.

**Proof**

Induction on the complexity of $P^c$. The case $P^c = L^c$ is treated as follows. For every logical expression $L^c_\alpha$ such that $LVar(L^c_\alpha) \subseteq L$ and $LVar(L^c_\alpha) \cap \overline{bij} = \emptyset$ we prove, by induction on the complexity of $L^c_\alpha$, the following: Let $L^c_\alpha[z^\alpha, z^\sigma] = (i_1, l_1, l_2)$ where $i = i_1, \ldots, i_q$. Then there exists a unique sequence of natural numbers $k = k_1, \ldots, k_q$ such that

$$L[L_1](\omega(k, n, m/i, z^\sigma, z^\sigma))(\delta)(\sigma'') = t$$

and for this $k$ we have

$$[L[L_2](\omega')(\delta')(\sigma')]_d = L[L_2](\omega(k, n, m/i, z^\sigma, z^\sigma))(\delta)(\sigma'').$$

$\square$

**B.3 Expressing the coding relationship**

In this section we show how to express in the assertion language the relationship between a state and its code number. In definition B.6 we shall define the assertion $Bij(z^\sigma)$, which expresses, as accurately as possible, that the current state is coded by the value of $z^\sigma$ and that the logical variables $bij$ form a correct decoding table. However, it is only possible to express this up to isomorphism, as we shall see in lemma B.7.

**Definition B.5**

First we define the following auxiliary assertions:

- $CIC(x_c, z^\sigma, z^\sigma) = Ic((bij^c \cdot z^\sigma) \cdot x_c) = Val(x^c, k, z^\sigma)$,
  $CIC(x_c, z^\sigma, z^\sigma) = Ic((bij^c \cdot z^\sigma) \cdot x_c) = Val(x^c, k, z^\sigma)$,
  where $k = [x]$.

- $CIC_d(x^c_d, z^\sigma, z^\sigma) =
  ((bij^c \cdot z^\sigma) \cdot x^c_d \equiv nil \rightarrow Val_d(z^\alpha, k, z^\sigma) \equiv 0) \land
  ((bij^c \cdot z^\sigma) \cdot x^c_d \neq nil \rightarrow \forall p((bij^c \cdot z^\sigma) \cdot x^c_d = bij^d \cdot p \rightarrow Val_d(z^\sigma, k, z^\sigma) \equiv p)),$
  where $d \in C$ and $k = [x^c_d]$.

- $CT(u, z^\sigma) = Ic(u) = Val(k, z^\sigma)$,
  $CT(u, z^\sigma) = Ic(u) = Val(k, z^\sigma)$,
  where $k = [u]$. 

Doc. No.
\[ CT_d(u_d, z') = (u_d \doteq \text{nil} \rightarrow \text{Val}_d(k, z') \doteq 0) \wedge (u_d \nless \text{nil} \rightarrow \forall p(\text{bij}^d \cdot p \doteq u_d \rightarrow \text{Val}_d(k, z') = p)), \]

where \( d \in C \) and \( k = [u_d] \)

**Definition B.6**
Next we define the assertion \( \text{Bij}(z') \), where \( z' \) is some logical integer variable, as follows.

\[ \text{Bij}(z') = \bigwedge_c \forall z_c \exists ! i (\text{bij}^c \cdot i \doteq z_c) \wedge \bigwedge_c \forall i (E^c(i, z') \leftrightarrow \text{bij}^c \cdot i \nless \text{nil}) \wedge \bigwedge_i \forall i (\text{bij}^c \cdot i \nless \text{nil} \rightarrow \bigwedge_d \forall x \in \text{Var}_d \bigwedge_d \bigwedge_x \text{CT}_d(x, i, z')) \wedge \bigwedge_d \forall x \in \text{Var}_d \text{CT}_d(u, z') \]

The first conjunct states that for every \( c \) the sequence denoted by \( \text{bij}^c \) stores each existing object of class \( c \) exactly once. The second conjunct then can be interpreted as stating that every existing object of class \( c \) occurs in the sequence denoted by \( \text{bij}^c \) at a position which equals the code of some object that exists in the state coded by \( z' \). The third conjunct relates the local state of every existing object with the one of its corresponding code. Finally, the fourth conjunct relates the values of the temporary variables with their coded versions.

In the following lemma we show how this assertion \( \text{Bij}(z) \) can be used to describe the isomorphism between two states.

**Lemma B.7**
Let \( \sigma, \omega, f \) such that \( \text{OK}(\omega, \sigma), \text{Code}(\omega, \sigma, f) \) and \( \omega(z) = [\sigma'] \). Then:

\[ \sigma, \delta, \omega \models \text{Bij}(z) \text{ iff } f(\sigma) = \sigma', \]

for an arbitrary \( \delta \) such that \( \text{OK}(\sigma, \delta, \omega) \).

**Proof**
Straightforward.

**B.4 Expressing the strongest postcodition**

Finally we are ready for the theorem stating the expressibility of the strongest postcondition.

Doc. No.
Theorem B.8
Let $\rho^c$ be closed, $BVar \subseteq L \subseteq LVar$, $P^c$ such that $LVar(P^c) \subseteq L$ and $\overline{B} \cap L = \emptyset$. Then: $SP^c_L(\rho^c, P^c) \models \exists bi^{c_1}, \ldots, bi^{c_n}, z_1, z_2, z_3(Q)$ (assuming $C = \{c_1, \ldots, c_n\}$), where $Q = \bigwedge_{1 \leq p \leq 5} Q_p$, and

- $Q_1 = T([\rho^c], z_1, z_2, z_3),$
- $Q_2 = Bij(z_3),$
- $Q_3 = bi^{c} \cdot A^c(z_1) \models self,$
- $Q_4 = \bigwedge_c \forall i(B^c(i, z_1) \leftrightarrow bi^c \cdot i \in b_c),$
- $Q_5 = \exists z_{c_1}, \ldots, z_{c_n} \bigwedge_{1 \leq p \leq 4} R_p,$

where $R_1 = \bigwedge_c (z_{c^*} \subseteq bi^c)$, $R_2 = \bigwedge_c \forall i(E^c(i, z_2) \leftrightarrow z_{c^*} \cdot i \neq \text{nil})$, $R_3 = \bigwedge_c (\lambda z_c \in L(z_c \in z_{c^*}) \land \lambda z'_c \in L(z'_c \subseteq z_{c^*}))$, $R_4 = P^c[z, z'][z/\overline{bij}, A^c(z_1)/z, z_2/z']$

where $l_{1a} \subseteq l_{2a}$, for $a = d^*$, abbreviates the assertion $\forall i(l_{1a} \cdot i = \text{nil} \lor l_{1a} \cdot i = l_{2a} \cdot i)$, and $\overline{z}$ denotes a sequence $z_{c_1}, \ldots, z_{c_n}$ of fresh logical variables.

The quantification $\exists bi^{c_1}, \ldots, bi^{c_n}$ will correspond to the phrase (in theorem 6.21) "there exists an osi $f". The variables $z_1, z_2, z_3$ will correspond to $\delta', \sigma_0$, and $f(\sigma)$, respectively. The conjunction $\bigwedge_{1 \leq p \leq 4} Q_p$ then expresses $f(\sigma) = P[\rho^c](\gamma)(\delta')(\sigma_0)$. Finally, the assertion $Q_5$ expresses $\sigma_0, \delta', \omega' \models P$, where $\omega' = f(\omega) \downarrow L$. Let us look into this more closely. The conjunction $R_1 \land R_2$ states that the variable $z_{c^*}$, $1 \leq i \leq n$, stores all the existing objects of $\sigma_0$ (of class $c_i$) at a position which equals its code. The assertion $R_3$ then states that $\omega'$ is compatible with $\sigma_0$. Finally, the assertion $R_4$ expresses that $\sigma_0, \delta', \omega' \models P$.

Proof.
Let $\sigma, \delta, \omega \models SP^c_L(\rho^c, P^c)$. So there exists for $i = 1, \ldots, n$, $\alpha_i \in O^c_i$, and $\beta_1, \beta_2, \beta_3 \in N$ such that $\sigma, \delta, \omega \models Q$, where $\omega' = \omega(\alpha_i/bi^{c_i})$, $\{\beta_1, \beta_2, \beta_3/z_1, z_2, z_3\}$.

As $\sigma, \delta, \omega' \models Q_1$ there exists $\sigma_0, \sigma_1, \delta'$ such that $\sigma_1 = P[\rho^c](\gamma)(\delta')(\sigma_0), \gamma$ arbitrary, and $[\delta'] = \beta_1$, $[\sigma_0] = \beta_2$, $[\sigma_1] = \beta_3$.

Now let $f$ be an osi such that for $\alpha \in \sigma^{(c_i)}$ we have: $f(\alpha) = \beta$ iff elt($\omega'(bi^{c_i})$, $\beta$) = $\alpha$. (Note that as $\sigma, \delta, \omega' \models Q_2$ we have that for $\alpha \in \sigma^{(c_i)}$ there exists some $\beta \in N$ such that elt($\alpha_3, \beta$) = $\alpha$, furthermore we have $E^{c_i}(\beta, \beta_3)$ so $\beta \in \sigma_1^{(c_i)}$.) So we have $Code(\omega', \sigma, f)$ and by lemma B.7 we infer $f(\sigma) = \sigma_1$.

Doc. No.
From \(\sigma, \delta, \omega' \models Q_3\) it follows that \(\delta'_1 = f(\delta(1))\). Furthermore from \(\sigma, \delta, \omega' \models Q_4\) it follows that \(\delta'_{(2)} = \{f(\alpha) : \alpha \in \omega(\delta(2))\}\). Note that \(OK(\omega, \delta, \sigma)\) so we infer that \(\delta' = f(\delta)\).

Finally, we have \(\sigma, \delta, \omega' \models Q_5\). So there exists for \(i = 1, \ldots, n\), \(\alpha'_i \in \mathcal{O}^\omega\), \(\omega'' = \omega(\alpha'_i / z_{c_i})\); such that \(\sigma, \delta, \omega'' \models \bigwedge_{1 \leq j \leq 4} R_j\). Let \(\sigma'\) such that, for an arbitrary \(c\), \(\sigma(\omega') = f^{-1}(\sigma_0(\omega'))\). It then follows that \(\sigma' \preceq \sigma\) and by \(\sigma, \delta, \omega'' \models \bigwedge_{1 \leq j \leq 4} R_j\) we have \(Code_L(\omega'', \sigma', f), \omega'' = \omega(\alpha'_i / b_1 \cdots b_4)\) \(\{\delta'_1, \beta_2 / z, z'\}\). Furthermore we have \(\sigma, \delta, \omega'' \models P \{z, z'\}\), so we have by theorem B.4: \(\sigma_0, \delta', \omega \models P\), where \(\omega = f(\omega'') \downarrow L = f(\omega) \downarrow L\). This finishes one part of the proof.

On the other hand, let \(\sigma, \sigma_0, \delta, \omega, f\) such that:

- \(f(\sigma) = \mathcal{P}[\rho'(\gamma)(\delta')(\sigma_0), \gamma\) arbitrary.
- \(\sigma_0, \delta, \omega' \models P\).

where \(\delta' = f(\delta)\) and \(\omega' = f(\omega) \downarrow L\).

Let \(\beta_1 = [\delta'], \beta_2 = [\sigma_0], \beta_3 = [f(\sigma)]\) and \(\alpha_i \in \mathcal{O}^\omega\), for \(i = 1, \ldots, n\) (assuming \(C = \{c_1, \ldots, c_n\}\)), such that \(e(\alpha_i, m) = \alpha(\neq \bot)\) iff \(\alpha \in \sigma(\alpha)\) and \(f(\alpha) = m\). Furthermore let \(\omega'' = \omega(\alpha'_i / b_1 \cdots b_4)\) \(\{\beta_1, \beta_2, \beta_3 / z, z'\}\). Now from \(\alpha'_i\) being a subsequence of \(\alpha_i\) it immediately follows that \(\sigma, \delta, \omega'' \models R_1\).

Now \(f(\sigma) = \mathcal{P}[\rho'(\gamma)(\delta')(\sigma_0)\) so we have \(\sigma, \delta, \omega'' \models Q_1\).

We have \(Code(\omega'', \sigma, f)\), and \(\omega''(z_3) = [f(\sigma)]\), so by lemma B.7 we have \(\sigma, \delta, \omega'' \models Q_2\).

From \(\delta' = f(\delta)\), \(OK(\sigma, \delta, \omega)\) and \(OK(\sigma_0, \delta')\) it easily follows that \(\sigma, \delta, \omega'' \models Q_3 \land Q_4\).

Let, for \(i = 1, \ldots, n\), \(\alpha'_i\) be a subsequence of \(\alpha_i\), such that \(\sigma_0(\alpha_i) = \{\alpha : e(\alpha'_i, \alpha) \neq \bot\}\). Furthermore let \(\omega''' = \omega''(\alpha_i' / z_{c_i})\). From \(\alpha_i'\) being a subsequence of \(\alpha_i\) it immediately follows that \(\sigma, \delta, \omega''' \models R_2\).

Now \(\alpha(\neq \bot)\) it in turn follows that \(\sigma, \delta, \omega'' \models R_2\). Furthermore we have that \(\sigma_0\) and \(\omega'\) are compatible, and \(\omega = f(\omega) \downarrow L = f(\omega'') \downarrow L\), from which it follows that: \(\sigma, \delta, \omega''' \models R_3\).

Finally, let \(\sigma'\) be such that for an arbitrary \(c\) we have \(\sigma'(\alpha') = f^{-1}(\sigma_0(\alpha')\) and \(\omega = \omega''(\alpha'_i / b_1 \cdots b_4)\) \(\{\delta'_1, \beta_2 / z, z'\}\). We then have that \(Code_L(\omega, \sigma', f)\) and \(\sigma' \preceq \sigma\). So from \(\sigma_0, \delta', \omega \models P\) and \(\omega = f(\omega) \downarrow L\) applying theorem B.4 it follows that \(\sigma, \delta, \omega \models P\) \(\{z, z'\}\). So we infer that \(\sigma, \delta, \omega''' \models R_4\).

Summerizing we conclude that: \(\sigma, \delta, \omega \models SP_1(L, \rho', P)\).
C A closure property of the semantics

In this appendix we prove a closure property of the semantics with respect to object-space isomorphisms. To get started it turns out to be convenient to have the following definition.

Definition C.1
Let $\beta^d_1, \ldots, \beta^d_n$ be some sequence of objects. We define $OK(\beta^d_1, \ldots, \beta^d_n, \delta, \sigma)$ iff $OK(\delta, \sigma)$ and additionally $\beta_i \in \sigma^{(d_i)}$, $i = 1, \ldots, n$.

Definition C.2
For

- $F \in \left( \prod_{i=1}^{n} O^d_i \right) \rightarrow \Delta^c \rightarrow \Sigma_\perp \rightarrow \left( \Sigma_\perp \times O^d_\perp \right)$, for some $c, n, d_0, \ldots, d_n$,
- $G \in \Delta^c \rightarrow \Sigma_\perp \rightarrow \left( \Sigma_\perp \times O^d_\perp \right)$, for some $c, d$,
- $H \in \Delta^c \rightarrow \Sigma_\perp \rightarrow \Sigma_\perp$, for some $c$,

we define

- $Cl(F)$ iff for an arbitrary $\beta^d_0, \ldots, \beta^d_n, \delta, \sigma, \sigma'$, $f$ such that $OK(\beta_1, \ldots, \beta_n, \delta, \sigma)$: if $F(\beta_1, \ldots, \beta_n)(\delta)(\sigma) = (\sigma', \beta_0)$ then there exists an $osi \ g$ such that $f^c \downarrow \sigma^c = g^c \downarrow \sigma^c$, for an arbitrary $c$, and $F(f^d_1(\beta_1), \ldots, f^d_n(\beta_n))(f(\delta))(f(\sigma)) = (g(\sigma'), g^{d_0}(\beta_0))$,
- $Cl(G)$ iff for an arbitrary $\beta, \delta, \sigma, \sigma'$, $f$ such that $OK(\delta, \sigma)$: if $G(\delta)(\sigma) = (\sigma', \beta)$ then there exists an $osi \ g$ such that $f^c \downarrow \sigma^c = g^c \downarrow \sigma^c$, for an arbitrary $c$, and $G(f(\delta))(f(\sigma)) = (g(\sigma'), g^{d_0}(\beta))$,
- $Cl(H)$ iff for an arbitrary $\delta, \sigma, \sigma'$, $f$ such that $OK(\delta, \sigma)$: if $H((\delta))(\sigma) = \sigma'$ then there exists an $osi \ g$ such that $f^c \downarrow \sigma^c = g^c \downarrow \sigma^c$, for an arbitrary $c$, and $H(f(\delta))(f(\sigma)) = g(\sigma')$.

(Here $\downarrow$ denotes the restriction operator.)

Now we are ready to analyse this closure property denoted by $Cl$. We start with the following lemma which states that the meaning of an arbitrary expression $s \in SExp$ satisfies this property assuming it holds for the meaning assigned to an arbitrary method:

Doc. No.
Lemma C.3
Let \( \gamma \) be an environment such that for an arbitrary method name \( m \) we have \( \text{Cl}(\gamma(m)) \). Then for every expression \( s \in S\text{Exp} \) we have \( \text{Cl}(\mathcal{Z}[s](\gamma)) \).

Proof
The proof proceeds by induction on the complexity of \( s \):

\( s = e : \) Note that we have by theorem 6.21 \( \mathcal{E}[e](\delta)(\sigma) = \mathcal{E}[e](f(\delta))(f(\sigma)) \) for an arbitrary \( \delta, \sigma \) such that \( \text{OK}(\delta, \sigma) \).

\( s = \text{new}_{d} : \) Let \( \mathcal{Z}[\text{new}_{d}](\gamma)(\delta)(\sigma) = (\sigma', \beta) \). So we have \( \text{pick}^{d}(\sigma(\sigma)) = \beta \). Let \( \beta' = \text{pick}^{d}(f(\sigma)) \) and \( g \) be an osi such that \( f^{c} \downarrow \sigma(c) = g^{c} \downarrow \sigma'(c) \), for an arbitrary \( c \), and \( g^{d}(\beta) = \beta' \). It follows that \( \mathcal{Z}[\text{new}_{d}](\gamma)(f(\delta))(f(\sigma)) = (g(\sigma'), \beta') \).

\( s = e_{0}m(e_{1}, \ldots, e_{n}) : \) Let for \( i = 0, \ldots, n \) \( \mathcal{E}[e_{i}](\delta)(\sigma) = \beta_{i} \) (\( \text{OK}(\delta, \sigma) \)) and \( \gamma(m)(\beta_{1}, \ldots, \beta_{n})(\delta')(\sigma) = (\sigma', \beta) \), where

\[
\begin{align*}
\delta'_{(1)} &= \beta_{0} \\
\delta'_{(2)}(c) &= \delta_{(2)}(c') \cup \delta'_{(1)} / c' \quad c' = c \\
\delta'_{(2)}(c) &= \delta_{(2)}(c') \quad c' \neq c,
\end{align*}
\]
assuming \( s \in S\text{Exp}_{d}^{2} \), for some \( d \).

As we have \( \text{Cl}(\gamma(m)) \) it follows that \( \gamma(m)(f(\beta_{1}), \ldots, f(\beta_{n}))(f(\delta'))(f(\sigma)) = (g(\sigma'), g(\beta)) \), for some osi \( g \) such that \( g^{c} \downarrow \sigma(c) = f^{c} \downarrow \sigma'(c) \), \( c \) arbitrary. (Note that by lemma 3.21 and \( \text{OK}(\delta, \sigma) \) we have \( \text{OK}(\beta_{1}, \ldots, \beta_{n}, \delta', \sigma) \).) By theorem 6.21 we have \( \mathcal{E}[e_{i}](f(\delta))(f(\sigma)) = f(\beta_{i}) \). Furthermore we have

\[
\begin{align*}
f(\delta'_{(1)}) &= f(\beta_{0}) \\
f(\delta'_{(2)}(c)) &= f^{c}(\delta_{(2)}(c)) \cup f^{c'}(\delta'_{(1)}) / c' \\
f(\delta'_{(2)}(c)) &= f^{c'}(\delta_{(2)}(c')) \quad c' \neq c'.
\end{align*}
\]

So we conclude \( \mathcal{E}[s](\gamma)(f(\delta))(f(\sigma)) = (g(\sigma'), g(\beta)) \). \( \square \)

Next we prove the closure property \( \text{Cl} \) for the meaning assigned to statements assuming it holds for the one assigned to expressions.

Lemma C.4
Let \( \gamma \) be an agreement-preserving environment such that for an arbitrary \( s \in S\text{Exp} \) we have \( \text{Cl}(\mathcal{Z}[s](\gamma)) \). Then we have \( \text{Cl}(\mathcal{S}[S](\gamma)) \) for an arbitrary \( S \in \text{Stat} \).

Proof
The proof proceeds by induction on the complexity of \( S \). We treat the following cases:

Doc. No.
$S = x_2 \leftarrow x_2$: Let $S[S](\gamma)(\delta)(\sigma) = \sigma'' (OK(\delta, \sigma))$ and $f$ be some osi. So we have $Z[s](\gamma)(\delta)(\sigma) = (\sigma', \beta)$ such that $\sigma'' = \sigma' \{\beta/\delta_1(x)\}$. By Cl($Z[s](\gamma)$) it then follows that there exists an osi $g$ such that $g^c \downarrow \sigma'' = f^c \downarrow \sigma'$, for an arbitrary $c$, and $Z[s](\gamma)(f(\delta))(f(\sigma)) = (g(\sigma'), g(\beta))$. Now $g(\sigma'') = g(\sigma') \{g^c(\delta_1(x))\}$, so we conclude $S[S](\gamma)(f(\delta))(f(\sigma)) = g(\sigma'')$.

$S = S_1; S_2$: Let $S[S](\gamma)(\delta)(\sigma) = \sigma' (OK(\delta, \sigma))$ and $f$ be some osi. So there exists a $\sigma''$ such that $S[S_1](\gamma)(\delta)(\sigma) = \sigma''$ and $S[S_2](\gamma)(\delta)(\sigma'') = \sigma'$. By the induction hypothesis we have for some osi $g$ such that $g^c \downarrow \sigma'' = f^c \downarrow \sigma'$ for an arbitrary $c$ and $S[S_1](\gamma)(f(\delta))(f(\sigma)) = g(\sigma'')$. Another application of the induction hypothesis gives us an $h$ such that $h^c \downarrow \sigma''(c) = g^c \downarrow \sigma'(c)$, for an arbitrary $c$, and $S[S_1](\gamma)(g(\delta))(g(\sigma'')) = h(\sigma')$. Putting these applications of the induction hypothesis together gives us $h^c \downarrow \sigma''(c) = g^c \downarrow \sigma'(c)$, for an arbitrary $c$, and $S[S](\gamma)(f(\delta))(f(\sigma)) = h(\sigma')$. (Note that by lemma 3.21 $\sigma \preceq \sigma''$ and, as $OK(\delta, \sigma)$, $f(\delta) = g(\delta)$.)

We proceed with the following lemma which states the closure property of the meaning of class definitions assuming it holds for the meaning of statements:

Lemma C.5

Let $\gamma$ be an agreement-preserving environment such that $Cl(S[S](\gamma))$ for an arbitrary statement $S$. Then we have for every method name $m$ defined by $D Cl(C[D](\gamma)(m))$ for an arbitrary class definition $D$.

Proof

Let $\gamma' = C[D](\gamma)$ and $f$ be some osi. Now let the method name $m$ be defined by $D$, say $m$ is declared as $\mu_{\delta_0, \ldots, \delta_k}$. We have $\gamma'(m) = M[\mu_{\delta_0, \ldots, \delta_k}](\gamma)$. Let $\mu_{\delta_0, \ldots, \delta_k} = (u_1, \ldots, u_k): S \uparrow$ e. Moreover let

Doc. No.
\[ \mathcal{M}[(u_1, \ldots, u_k): S \uparrow e](\gamma)(\beta_1, \ldots, \beta_k)(\delta)(\sigma) = (\sigma'', \beta) \]
where \[ \sigma^' = (\sigma(1), \sigma(2), \sigma(3)) \]
\[ \sigma(3)(u) = \beta_i \quad \text{if } u = u_i \]
\[ = \bot \quad \text{otherwise} \]
\[ \sigma'' = \mathcal{S}[S](\gamma)(\delta)(\sigma^') \]
\[ \beta = \mathcal{E}[e](\delta)(\sigma'') \]
\[ \sigma''' = (\sigma'''(1), \sigma'''(2), \sigma(3)) \]

Note that we assume \( \sigma \neq \bot \) and \( \delta(1) \) not to be blocked. If one of these do hold we have \( \sigma^' = \bot \) from which follows that \( \sigma''', \beta = \bot \). By the assumption about \( \gamma \) we have for some osi \( g \) \( g^c = f^c \) \( \sigma''(c) \), for every arbitrary \( c \), and \( \mathcal{S}[S](\gamma)(f(\delta))(f(\sigma^')) = g(\sigma''). \) (Note that \( \mathcal{O}(\beta_1, \ldots, \beta_k, \delta, \sigma) \) implies \( \mathcal{O}(\delta, \sigma') \).) As \( \sigma(c) = \sigma(c) \) for an arbitrary \( c \) we have \( g^c(\sigma(c)) = f^c(\sigma(c)) \) for an arbitrary \( c \). By theorem 6.21 we have \( g(\beta) = \mathcal{E}[e](g'(\delta))(g(\sigma'')). \) (Note that as \( \gamma \) is agreement-preserving we have by lemma 3.21 \( \sigma \preceq \sigma''' \), and so \( \mathcal{O}(\delta, \sigma''') \).) Putting this together gives us

\[ \mathcal{M}[(u_1, \ldots, u_k): S \uparrow e](\gamma)(f(\beta_1), \ldots, f(\beta_k))(f(\delta))(f(\sigma)) = \langle g(\sigma'''), g(\beta) \rangle. \]

\[ \square \]

In the next lemma we prove that the meaning of units satisfies the closure property \( \mathcal{C}I \).

**Lemma C.6**
Let \( U = D_1, \ldots, D_n \) be an unit such that every method occurring in it is defined by it. Then for every method name \( m \) we have \( \mathcal{C}I(\gamma'(m)), \) where \( U[U](\gamma_0) = \gamma' \) and \( \gamma_0 \) is the “empty” environment defined by

\[ \gamma_0(\beta)(\delta)(\sigma) = (\bot, \bot). \]

**Proof**
We have \( \gamma' = \bigcup_{i=1}^{n} \gamma_i, \gamma_0 \) being the “empty” environment and \( C[D_1] \circ \cdots \circ C[D_n](\gamma_i) = \gamma_i+1. \) We prove by induction that \( \mathcal{C}I(\gamma_i(m)), m \) arbitrary. From this it is not difficult to prove that \( \mathcal{C}I(\gamma'(m)). \)

\( i = 0: \) Evident.

\( i = j + 1: \) By the induction hypothesis we have \( \mathcal{C}I(\gamma_i(m)). \) Furthermore by lemma 3.21 we know that \( \gamma_i \) is agreement-preserving. From this follows by applying the lemmas C.3, C.4 and C.5 that \( \mathcal{C}I(\gamma_{i+1}(m)). \) (Note that lemma C.5 can be applied only for method names defined by \( U \), but as we have \( \gamma_i(m) = \gamma_0(m), \) for \( i \in \mathbb{N} \) and \( m \) not defined by \( U \) this suffices.) \( \square \)

Doc. No.
We conclude this appendix with the following theorem which states the closure property of the meaning assigned to closed programs:

**Theorem C.7**
For an arbitrary closed program \( \rho = \langle U | c : S \rangle \), environment \( \gamma \) we have \( Cl(P[\rho](\gamma)) \).

**Proof**
First note that as \( \rho \) is a closed program we have \( P[\rho](\gamma) = P[\rho](\gamma_0) \). We have by definition 3.18 that \( P[\rho](\gamma_0) = S[S](\gamma') \), where \( \gamma' = U[U](\gamma_0) \). By lemma C.6 we have \( Cl(\gamma'(m)) \) for every method name \( m \). So applying the lemmas C.3 and C.4 gives us \( Cl(S[S](\gamma')) \). (Note that by lemma 3.21 \( \gamma' \) is agreement-preserving.)

**Corollary C.8**
For an arbitrary closed program \( \rho, \sigma, \sigma', \delta, f \) such that \( \sigma' = \rho(\gamma)(\delta)(\sigma) \) there exists an osi \( g \) such that \( g^c \downarrow \sigma'(c) = f^c \downarrow \sigma(c) \) and \( g(\sigma') = \rho(\gamma)(f(\delta))(f(\sigma)) \).
In this series appeared:

<table>
<thead>
<tr>
<th>No.</th>
<th>Author(s)</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>85/01</td>
<td>R.H. Mak</td>
<td>The formal specification and derivation of CMOS-circuits.</td>
</tr>
<tr>
<td>85/02</td>
<td>W.M.C.J. van Overveld</td>
<td>On arithmetic operations with M-out-of-N-codes.</td>
</tr>
<tr>
<td>85/03</td>
<td>W.J.M. Lemmens</td>
<td>Use of a computer for evaluation of flow films.</td>
</tr>
<tr>
<td>85/04</td>
<td>T. Verhoeff, H.M.L.J. Schols</td>
<td>Delay insensitive directed trace structures satisfy the foam rubber wrapper postulate</td>
</tr>
<tr>
<td>86/01</td>
<td>R. Koymans</td>
<td>Specifying message passing and real-time systems.</td>
</tr>
<tr>
<td>86/02</td>
<td>G.A. Bussing, K.M. van Hee, M. Voorhoeve</td>
<td>ELISA, A language for formal specification of information systems.</td>
</tr>
<tr>
<td>86/03</td>
<td>Rob Hoogerwoord</td>
<td>Some reflections on the implementation of trace structures.</td>
</tr>
<tr>
<td>86/04</td>
<td>G.J. Houben, J. Paredaens, K.M. van Hee</td>
<td>The partition of an information system in several systems.</td>
</tr>
<tr>
<td>86/05</td>
<td>J.L.G. Dietz, K.M. van Hee</td>
<td>A framework for the conceptual modeling of discrete dynamic systems.</td>
</tr>
<tr>
<td>86/06</td>
<td>Tom Verhoeff</td>
<td>Nondeterminism and divergence created by concealment in CSP.</td>
</tr>
<tr>
<td>86/07</td>
<td>R. Gerth, L. Shira</td>
<td>On proving communication closedness of distributed layers.</td>
</tr>
<tr>
<td>86/09</td>
<td>C. Huizing, R. Gerth, W.P. de Roever</td>
<td>Full abstraction of a real-time denotational semantics for an OCCAM-like language.</td>
</tr>
<tr>
<td>86/10</td>
<td>J. Hooman</td>
<td>A compositional proof theory for real-time distributed message passing.</td>
</tr>
<tr>
<td>86/11</td>
<td>W.P. de Roever</td>
<td>Questions to Robin Milner - A responder’s commentary (IFIP86).</td>
</tr>
<tr>
<td>86/12</td>
<td>A. Boucher, R. Gerth</td>
<td>A timed failures model for extended communicating processes.</td>
</tr>
<tr>
<td>86/13</td>
<td>R. Gerth, W.P. de Roever</td>
<td>Proving monitors revisited: a first step towards verifying object oriented systems (Fund. Informatica</td>
</tr>
<tr>
<td>Year</td>
<td>Author(s)</td>
<td>Title</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>86/14</td>
<td>R. Koymans</td>
<td>Specifying passing systems requires extending temporal logic.</td>
</tr>
<tr>
<td>87/01</td>
<td>R. Gerth</td>
<td>On the existence of sound and complete axiomatizations of the monitor concept.</td>
</tr>
<tr>
<td>87/02</td>
<td>Simon J. Klaver, Chris F.M. Verberne</td>
<td>Federatieve Databases.</td>
</tr>
<tr>
<td>87/03</td>
<td>G.J. Houben, J.Paredaens</td>
<td>A formal approach to distributed information systems.</td>
</tr>
<tr>
<td>87/04</td>
<td>T. Verhoeff</td>
<td>Delay-insensitive codes - An overview.</td>
</tr>
<tr>
<td>87/05</td>
<td>R. Kuiper</td>
<td>Enforcing non-determinism via linear time temporal logic specification.</td>
</tr>
<tr>
<td>87/06</td>
<td>R. Koymans</td>
<td>Temporele logica specificatie van message passing en real-time systemen (in Dutch).</td>
</tr>
<tr>
<td>87/07</td>
<td>R. Koymans</td>
<td>Specifying message passing and real-time systems with real-time temporal logic.</td>
</tr>
<tr>
<td>87/08</td>
<td>H.M.J.L. Schols</td>
<td>The maximum number of states after projection.</td>
</tr>
<tr>
<td>87/10</td>
<td>T. Verhoeff</td>
<td>Three families of maximally nondeterministic automata.</td>
</tr>
<tr>
<td>87/11</td>
<td>P. Lemmens</td>
<td>Eldorado ins and outs. Specifications of a data base management toolkit according to the functional model.</td>
</tr>
<tr>
<td>87/12</td>
<td>K.M. van Hee and A. Lapinski</td>
<td>OR and AI approaches to decision support systems.</td>
</tr>
<tr>
<td>87/13</td>
<td>J.C.S.P. van der Woude</td>
<td>Playing with patterns - searching for strings.</td>
</tr>
<tr>
<td>87/14</td>
<td>J. Hooman</td>
<td>A compositional proof system for an occam-like real-time language.</td>
</tr>
<tr>
<td>87/16</td>
<td>H.M.M. ten Eikelder, J.C.F. Wilmont</td>
<td>Normal forms for a class of formulas.</td>
</tr>
<tr>
<td>87/17</td>
<td>K.M. van Hee, G.-J. Houben, J.L.G. Dietz</td>
<td>Modelling of discrete dynamic systems framework and examples.</td>
</tr>
</tbody>
</table>
87/18  C.W.A.M. van Overveld  An integer algorithm for rendering curved surfaces.

87/19  A.J. Seebregts  Optimalisering van file allocatie in gedistribueerde database systemen.

87/20  G.J. Houben J. Paredaens  The $R^2$-Algebra: An extension of an algebra for nested relations.

87/21  R. Gerth M. Codish Y. Lichtenstein E. Shapiro  Fully abstract denotational semantics for concurrent PROLOG.

88/01  T. Verhoeff  A Parallel Program That Generates the Möbius Sequence.


88/03  T. Verhoeff  Settling a Question about Pythagorean Triples.

88/04  G.J. Houben J. Paredaens D. Tahon  The Nested Relational Algebra: A Tool to Handle Structured Information.


88/06  H.M.J.L. Schols  Notes on Delay-Insensitive Communication.


88/09  A.T.M. Aerts K.M. van Hee  A Tutorial for Data Modelling.

88/10  J.C. Ebergen  A Formal Approach to Designing Delay Insensitive Circuits.


88/12  A.E. Eiben  Abstract theory of planning.

88/13  A. Bijlsma  A unified approach to sequences, bags, and trees.

88/15 R. Bos  
C. Hemerik  
An introduction to the category theoretic solution of recursive domain equations.

88/16 C.Hemerik  
J.P.Katoen  
Bottom-up tree acceptors.

88/17 K.M. van Hee  
G.J. Houben  
L.J. Somers  
M. Voorhoeve  
Executable specifications for discrete event systems.

88/18 K.M. van Hee  
P.M.P. Rambags  
Discrete event systems: concepts and basic results.

88/19 D.K. Hammer  
K.M. van Hee  
Fasering en documentatie in software engineering.

88/20 K.M. van Hee  
L. Somers  
M. Voorhoeve  
EXSPECT, the functional part.

89/1 E.Zs.Lepoeter-Molnar  
Reconstruction of a 3-D surface from its normal vectors.

89/2 R.H. Mak  
P.Struik  
A systolic design for dynamic programming.

89/3 H.M.M. Ten Eikelder  
C. Hemerik  
Some category theoretical properties related to a model for a polymorphic lambda-calculus.

89/4 J.Zwiers  
W.P. de Roever  
Compositionality and modularity in process specification and design: A trace-state based approach.

89/5 Wei Chen  
T.Verhoeff  
J.T.Udding  
Networks of Communicating Processes and their (De-)Composition.

89/6 T.Verhoeff  
Characterizations of Delay-Insensitive Communication Protocols.

89/7 P.Struik  
A systematic design of a parallel program for Dirichlet convolution.

89/8 E.H.L.Aarts  
A.E.Eiben  
K.M. van Hee  
A general theory of genetic algorithms.

89/9 K.M. van Hee  
P.M.P. Rambags  
Discrete event systems: Dynamic versus static topology.

89/10 S.Ramesh  
A new efficient implementation of CSP with output guards.

89/11 S.Ramesh  
Algebraic specification and implementation of infinite processes.

89/12 A.T.M.Aerts  
K.M. van Hee  
A concise formal framework for data modeling.
<table>
<thead>
<tr>
<th></th>
<th>Authors</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>89/14</td>
<td>H.C. Haesen</td>
<td>ELDA, data manipulatie taal.</td>
</tr>
<tr>
<td>89/15</td>
<td>J.S.C.P. van der Woude</td>
<td>Optimal segmentations.</td>
</tr>
<tr>
<td>89/16</td>
<td>A.T.M. Aerts, K.M. van Hee</td>
<td>Towards a framework for comparing data models.</td>
</tr>
<tr>
<td>89/17</td>
<td>M.J. van Diepen, K.M. van Hee</td>
<td>A formal semantics for Z and the link between Z and the relational algebra.</td>
</tr>
<tr>
<td>90/2</td>
<td>K.M. van Hee, P.M.P. Rambags</td>
<td>Dynamic process creation in high-level Petri nets, pp. 19.</td>
</tr>
<tr>
<td>90/4</td>
<td>A. Peeters</td>
<td>Decomposition of delay-insensitive circuits, p. 25.</td>
</tr>
<tr>
<td>90/7</td>
<td>M.B. Josephs</td>
<td>A logic for one-pass, one-attributed grammars, p. 14.</td>
</tr>
<tr>
<td>90/8</td>
<td>M.B. Josephs</td>
<td>Receptive Process Theory, p. 16.</td>
</tr>
<tr>
<td>90/9</td>
<td>A.T.M. Aerts, P.M.E. De Bra, K.M. van Hee</td>
<td>Combining the functional and the relational model, p. 15.</td>
</tr>
<tr>
<td>90/10</td>
<td>M.J. van Diepen, K.M. van Hee</td>
<td>A formal semantics for Z and the link between Z and the relational algebra, p. 30. (Revised version of CSNotes 89/17).</td>
</tr>
<tr>
<td>90/11</td>
<td>P. America, F.S. de Boer</td>
<td>A proof system for process creation, p. 84.</td>
</tr>
<tr>
<td>90/12</td>
<td>P. America, F.S. de Boer</td>
<td>A proof theory for a sequential version of POOL, p. 110.</td>
</tr>
<tr>
<td>90/14</td>
<td>F.S. de Boer</td>
<td>A proof system for the language POOL, p. 70.</td>
</tr>
<tr>
<td>90/15</td>
<td>F.S. de Boer</td>
<td>Compositionality in the temporal logic of concurrent systems,</td>
</tr>
<tr>
<td>Reference</td>
<td>Authors</td>
<td>Title</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>90/16 F.S. de Boer C. Palamidessi</td>
<td></td>
<td>A fully abstract model for concurrent logic languages, p. 23.</td>
</tr>
<tr>
<td>90/17 F.S. de Boer C. Palamidessi</td>
<td></td>
<td>On the asynchronous nature of communication in concurrent logic languages: a fully abstract model based on sequences, p. 29.</td>
</tr>
</tbody>
</table>