On the existence of sound and complete axiomatizations of the monitor concept
Gerth, R.T.

Published: 01/01/1987

Document Version
Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

• A submitted manuscript is the author's version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.
Link to publication

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal.

Take down policy
If you believe that this document breaches copyright please contact us (openaccess@tue.nl) providing details. We will immediately remove access to the work pending the investigation of your claim.

Download date: 24. Jan. 2019
On the Existence of Sound and Complete Axiomatizations of the Monitor Concept

by

Rob Gerth
On the Existence of Sound and Complete Axiomatizations of the Monitor Concept

by

Rob Gerth

January, 1989
ON THE EXISTENCE OF SOUND AND COMPLETE AXIOMATIZATIONS OF THE MONITOR CONCEPT

Rob Gerth*†
Eindhoven University of Technology ‡

January 1989

Abstract

This paper presents an axiomatization for the partial correctness properties of Communicating Modules, a monitor-based programming language. This axiomatization is certified through soundness and (relative) completeness proofs, which constitute the major part of the paper. The system is based on the well-known notions of cooperation and interference freedom, however does not incorporate them as second order notions and is syntax-directed in a formal way.

1 Introduction

Monitors constitute the first attempt at formulating concurrent programming concepts beyond low-level mutual exclusion primitives such as semaphores ([Dij68]). The concept originates from Hoare and Brinch Hansen ([Hoa74, BHa73]) in their work on resource management in operating systems and is influenced by the SIMULA class concept ([DMN67]).

Monitors combine ideas from abstract data types with a notion of concurrency that derives from the independence of the various sets of data in the system achieved through the aforementioned data-abstraction. Programming languages based on it, include Concurrent Pascal [BHa75], Distributed Processes [BHa78], Mesa [MMS79] and most recently, Wirth's Modula (-2) [Wir84]. Also, the rendezvous concept of Ada [ARM83] clearly derives from it. In a different but related area, these ideas surface in the concept of object in object oriented systems [Am86].

Although the monitor concept is a relatively old one, it has never been adequately axiomatized (in the sense of [Hoa69]). It is well known that previous attempts, [Hoa74, How76], resulted in sets of rules that are incomplete in the technical sense of the word. Recent attempts to correct this, [AB81], remained unsuccessful.

This contrasts sharply with work on other concepts of concurrent programming: Concurrent languages based on the sharing of variables between concurrent proceses were successfully axiomatized by Owicki, [OG76]. Hoare's “Communicating Sequential Processes” has been dealt with in [AFdeR80, LG81, Sou84] and Ada in [GdeR84].

*The author was financially supported, through the Foundation for Computer Science Research in the Netherlands (SION), by the Netherlands Organisation for the Advancement of Pure Research (ZWO).
†The author is currently working in and partially supported by ESPRIT project 937: "Debugging and Specification of Ada Real-Time Embedded Systems (DESCARTES)".
‡Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O.Box 513, 5600 MB Eindhoven, The Netherlands. Electronic mail: mcvax!eutc3!wsinfrog!UUCP or WSDCROBG HEITUES.BITNET.
The current paper, implicitly, offers an explanation for this state of affairs. The reported axiomatisation in fact combines the notions of interference freedom — developed to axiomatize shared variable languages — and cooperation (in its generalized form of [GdeR84]) — introduced to axiomatise synchronously communicating languages. Both notions, although formulated in different ways, reflect the insight that the specification or verification of a concurrent agent in isolation from an interacting environment, has to incorporate assumptions about such interactions. Assumptions that have to be proved compatible or non-conflicting when combining the separate agents' specifications. It is this basic insight that is missing in earlier axiomatisation attempts.

The present axiomatisation evolved from work on Brinch Hansen's Distributed Processes, DP ([BH78]), reported in [RDKdeR81, GdeRR82a, GdeRR82b] with the following difference: usually, cooperation and interference freedom is formulated as the way to combine proofs of specifications rather than as the way to combine specifications themselves. Hence, the resulting proof systems might be better called verification algorithms, instead of formal axiomatisations. The paper shows that this traditional rendering is not forced by these notions, and gives an axiomatisation that complies with the usual meaning of the term. This axiomatisation is syntax-directed in the sense that every program constructor has an associated formal proof rule and every basic statement an associated axiom.

The current paper is a companion to [GdeR86]. That paper informally introduces and motivates the proposed axiomatisation. Here, the concentration is on the formal justification of the proof system. Formally speaking, this paper independent from [GdeR86]. However, the reader seeking (more) motivation is referred to that paper.

For a different approach towards axiomatizing monitors in the context of DP, the reader should consult [SS85, Gje88]. Those works are based on the Soundararajan-Dahl approach, [SoD82] and are most easily described as the rendering of an operational semantics into proof rules and assertions. The resulting set of rules is complete, too. In this approach one reasons directly with the computation history, whereas here one may choose auxiliary variables that retain just the needed information about the history. This has the advantage of ease of use; it has the technical disadvantage that the completeness of the proof system is more restricted. See also Section 7.3 and the conclusions in Section 8.

The next section introduces the language Communicating Modules, CM. Then its syntax is extended to provide "hooks" for the axiomatisation presented in Section 5. Section 3 gives a syntax directed operational semantics that will be used in the soundness and completeness proofs. Next, in Section 4, two essential theorems are proved: the local and global merging theorems. These theorems express when separate executions of program parts are compatible in the sense that they are part of an execution of the combination of the program parts. The theorems have non-trivial content, since the program parts may interact. Section 5 introduces the specification language and the proof system. The section concludes with a substitution lemma used in the next two sections. The soundness and completeness proofs are the subject of Section 6 and 7. A final discussion occupies Section 8.

This introduction concludes with

1.1 A summary of some notation

The (well-ordered) set of integers, \( \{0, 1, 2, \ldots \} \), is denoted by \( \omega \); its cardinality by \( \aleph_0 \). There is a denumerable, well-ordered set of variables \( \text{Var} \). For any \( n \in \omega \), \( \text{Var}_n \subseteq \text{Var} \) contains the
first n variables. Hence \( \text{Var} = \bigcup_{n \in \mathbb{N}} \text{Var}_n \). If \( \Sigma \) is some signature or similarity type, then \( Tm(\Sigma) \)
and \( L(\Sigma) \) denote the set of terms and first order formulae over \( \Sigma \). Elements of \( L(\Sigma) \) are usually denoted by letters \( p, q, r \); terms by \( e, t \) and variables by \( u, v, x, y, z \). As usual, \( p[e/x] \) (\( t[e/x] \)) stands for the formula (term) obtained by substituting the term or expression \( e \) for every free occurrence of \( x \) in \( p \) (\( t \)). The set of free variables of a formula or term \( \phi \) is denoted by \( FV(\phi) \).

~-structures or \( \Sigma \)-algebra's, \( \mathcal{A} \), are defined as usual and give interpretations of the symbols in \( \Sigma \). Given a \( \Sigma \)-structure \( \mathcal{A} \), states \( \sigma, \tau, \nu \) are partial functions from \( \text{Var} \) into \( |\mathcal{A}| \), the universe of \( \mathcal{A} \). The domain of a state (or any other function) \( \sigma \), is \( \text{Dom}(\sigma) \); its range is \( \text{Ran}(\sigma) \). \( \Omega \) denotes the totally undefined state; i.e., the partial function \( \text{Var} \mapsto |\mathcal{A}| \) with \( \text{Dom}(\Omega) = \emptyset \). Define \( St_n = \{ \sigma : \text{Var} \mapsto |\mathcal{A}| \mid \text{Dom}(\sigma) \subseteq \text{Var}_n \} \) and \( St = \bigcup_{n \in \mathbb{N}} St_n \). For a state \( \sigma, \sigma \upharpoonright V \) restricts the domain of \( \sigma \) to \( V \subseteq \text{Var} \); \( \sigma(a/x) \) (\( a \in |\mathcal{A}| \)) denotes the state \( \sigma' \) such that for \( y \neq x \sigma'(y) = \sigma(y) \) and \( \sigma'(x) = a \). For states \( \sigma, \tau \) such that \( \sigma \upharpoonright W = \tau \upharpoonright W \) where \( W = \text{Dom}(\sigma) \cap \text{Dom}(\tau) \), \( \sigma \cup \tau \) is defined in the obvious way. For any states, \( \sigma \) and \( \tau \), let \( \sigma(\tau) = \sigma(\tau(x)/x, x \in \text{Dom}(\tau)) \). The value of a term \( t \) in a state \( \sigma, \sigma(t) \), and the truth-value or satisfaction of a formula \( p \) in a state \( \sigma, \sigma \models p \) are defined as usual, provided \( FV(p) \subseteq \text{Dom}(\sigma) \), and are undefined otherwise.

In the sequel, states are always assumed to have large enough domains so that they valuate every variable in a term or formula used. Write \( \mathcal{A} \models p \) if \( p \in L(\Sigma) \) is valid in \( \mathcal{A} \), i.e., if \( \mathcal{A}, \sigma \models p \) holds for every state \( \sigma \) (for which \( FV(p) \subseteq \text{Dom}(\sigma) \)). Let \( \text{Th}(\mathcal{A}) \) denote the set \{ \( p \in L(\Sigma) \mid \mathcal{A} \models p \} \), where \( \Sigma \) is \( \mathcal{A} \)'s signature. The term computable will be used in its informal sense; recursive will be its formalisation.

## 2 The language communicating modules, CM

As stated in the introduction, monitors combine

1. the notion of abstract data type, where the concepts of data and the set of legal (=meaningful) operations on it, are seen as logically inseparable, with

2. a notion of concurrency that derives from the logical independence of the various data sets within a system, originating in the abstraction of (1).

Interactions within a system occur through the data type interface. The logical integrity of the data type abstraction and the functionality of the operations are maintained by

1. imposing strict synchronization between a monitor and the entity requesting its service, while performing this service and by

2. allowing a monitor to be serving at most one request at a time.

This does not imply that the data type operations of a monitor are strictly serialized, but merely that a monitor cannot be serving two or more requests at the same time. In fact, it implies the possibility of a finer grain of serialization in monitors than there is in sequential abstract data types.

When a monitor is servicing a requestor, hence is performing a data type operation, the requestor is said to be active within the monitor and to have acquired the monitor-lock, effectively locking out (the servicing of) any other requestor until the former relinquishes the lock. At such a time a monitor may start (again) servicing someone else.
Even at this level of description one can discern an interleaving of actions: actions associated with the data type operations and bracketed in time by the acquiring and relinquishing of the monitor lock by the requestors of the particular operations.

Traditionally, a monitor is a passive object, only reacting to external requests. Modules are a generalization of this concept and may also initiate requests to other modules.

2.1 Syntax
Let \( \Sigma \) be a signature. Partition \( \text{Var} \) as \( \text{Var}^R \cup \text{Var}^{IC} \), \( \text{Var}^{IC} = \{ \text{ico} \mid i \in \omega \} \). The programming language \( \text{CM}(\Sigma) \) is generated by the following Backus-Naur grammar \((z, \alpha, \beta, \gamma)\):

- \( \text{CM}(\Sigma) ::= [MD_1 || \cdots || MD_n] \quad n \geq 1 \)
- \( MD ::= M_i ::= \text{DC} : [S] \)
- \( DC ::= \alpha_j(\#\#\#) : [S] \quad \text{DC} \)
- \( S ::= z := e \mid \text{wait} | \text{call} M_i. \alpha_j(\#\#\#) | S_1 ; S_2 | \text{if} \ b \ \text{then} \ S_1 \ \text{else} \ S_2 \ \text{fi} | \text{while} \ b \ \text{do} \ S \ \text{od} \)

Note that no variable of the form \( \text{ico} \) can appear in any \( \text{CM}(\Sigma) \)-program. These so-called instance counters have a special meaning in the proof system of Section 5.2. The non-terminal \( \text{DC} \) may also produce the empty string.

2.2 Informal semantics
A module consists of a number of procedure-declarations and an initial statement. Execution of a module starts with its initial statement and continues until either the initial statement terminates or a wait-statement is encountered. Such statements are the primary way to establish synchronisation.

Synchronisation occurs in a module:

- when arriving at a wait-statement,
- upon completing the execution of the initial statement, and
- upon completing the execution of an (instance of an) entry procedure.

Such points are called waiting points.

By synchronisation is meant either

- the act of honouring and arbitrarily selected call to one of the module's entries (global synchronisation) or
- the act of passing some wait-statement having been a waiting point at an earlier time and hence possibly different from the one execution just arrived at (local synchronisation).

Observe that at waiting points the monitor-lock is relinquished.

Honouring a call constitutes the only form of communication and synchronisation between modules. It results in a new procedure-instance being activated and executed. Until its completion, the caller remains fully synchronized, whence its execution suspended, with the callee. The parameter-mechanism is call-by-value-result and within a procedure-body no assignment to any
value-parameter is allowed. Formal parameters are local with respect to the procedure-body. All other variables are global with respect to the module. Modules do not share variables.

In Section 3, the meaning of a program or module is formally defined in the form of an operational semantics.

The following notation and conventions will be used throughout the paper:

- the modules in a program comprising of \( n \) modules, are named \( M_1, M_2, \ldots, M_n \),
- module \( M_i \) contains procedures \( a_{i1}, a_{i2}, \ldots, a_{in} \); its initial statement is denoted by \( a_{i0} \),
- procedure \( a_{ij} \) in \( M_i \) (\( j \geq 0 \)) is declared as \( a_{ij}(u_{ij} \# v_{ij}); [S_j] \); the initial statement, \( a_{i0} \), as : \([S_0]\),
- \( L_{i,j} = \{ u_{i,j}, v_{i,j} \} \) (\( L_{i,0} = \emptyset \)); \( V_{i,j} \) is the set of variables, not including \( L_{i,j} \), that appear free within procedure \( a_j \) of module \( M_i \); \( V_i = \bigcup_{j=0}^{n} V_{i,j} \), \( L_i = \bigcup_{j=0}^{n} L_{i,j} \).

I shall usually ignore the superscripts in procedure-names. Note that by this convention, I assume procedure-names to be unique. \( L_{i,j} \) collects the local variables of procedure \( a_{ij} \).

The following context conditions apply to any program:

- \( V_i \cap V_j = \emptyset \) if \( i \neq j \),
- \( L_{i,k} \cap L_{j,l} = \emptyset \) if \( i \neq j \) or \( k \neq l \),
- \( V_i \cap \bigcup_{j=1}^{n} L_j = \emptyset \),
- in any statement \( \text{call} M_i.a_j(e \# f) \), the variables in \( f \) are pairwise disjoint and \( FV(e) \cap \{ f \} = \emptyset \).

### 2.3 The extended language, \( CM^*(\Sigma) \)

Some syntactic extensions to \( CM(\Sigma) \) are necessary in order to obtain the proof system of Section 5. Specifically, labels are introduced and so-called bracketed sections.

Introduce a denumerable set, \( \text{Lab} \), of labels with typical elements \( \ell, \ell', \ell'', \ldots \) such that \( \text{Lab} \cap \text{Var} = \emptyset \). In the grammar generating \( CM^*(\Sigma) \), the same convention as in Section 2.1 is used.

- \( CM(\Sigma) ::= [MD_1 || \cdots || MD_n] \) \( n \geq 1 \)
- \( MD ::= M_i :: DC :: [S.\ell] \)
- \( DC ::= a_j(u \# v); [S_1; T_1]; S_2'; T_2'] DC \mid \)
- \( T ::= S \mid \)
- \( S ::= e ::= e \mid \ell.\text{wait.} \ell' \mid \ell.(T_1; \ell'.\text{call} M_i.a_j(e \# f); T_2; \ell'). S_1; S_2 \mid \text{if } b \text{ then } S_1 \text{ else } S_2 \text{ fi } \mid \text{while } b \text{ do } S \text{ od} \)

In a procedure body, \( T_1 \) and \( T_2 \) are called the prelude respectively the postlude of the procedure. Statements \( \langle T_1; \ell \rangle \), \( \langle \ell'.(T_2) \rangle \) and \( \langle \ell.(\cdots.\ell'.\text{call} \cdots; \ell') \rangle \) are called bracketed sections. A label that either labels the front of a wait or the initial statement will be said to label a waiting point.

In addition to the ones introduced in Section 2.2, the following context conditions apply to \( CM^*(\Sigma) \) programs:
• any label may have at most one occurrence
• the statements \( T_1 \) and \( T_2 \) within bracketed sections, may contain no wait or call-statements.

These syntactic extensions induce no semantic differences, other than that executing a bracket, \( \ell.() \) or \( \ell.\ell() \), is equivalent with executing a skip-action (e.g. \( z := z \)).

For any \( CM^*(\Sigma) \)-statement, procedure, module or program \( T \), \( FLB(T) \) denotes the set of labels occurring in \( T \). If \( \ell \in FLB(\alpha_i) \) and \( \alpha_j \) is a procedure of \( M_i \) then \( L(\ell) \) denotes \( L_{i,j} \).

3 Operational semantics for \( CM^*(\Sigma) \)

In this section the behaviour or semantics of \( CM^*(\Sigma) \) programs is formally defined. I will use the structured operational semantics approach as advocated by G. Plotkin [Pl82].

3-1 DEFINITION. A labeled \( \Sigma \) transition system, \( \llbracket \Sigma \rrbracket \), is a tuple \((C, \rightarrow, SC, TC, TL, A)\), where

- \( C \) is a set of configurations
- \( SC \subseteq C \) is a set of start configurations
- \( TC \subseteq C \) is the set of terminal configurations
- \( TL \) is a set of transitions labels or records
- \( \rightarrow \subseteq C \times TL \times C \) is the transition relation
- \( A \) is a \( \Sigma \)-structure

A structured operational semantics is an \( \llbracket \ldots \rrbracket \) which transition relation is defined using induction on the structure of the configurations. In the current case this implies that also the semantics of \( CM^*(\Sigma) \) modules and statements has to be defined, independent of a surrounding program.

To define the set of configurations, \( CM^*(\Sigma) \) has to be extended, again, to \( CM^*(\Sigma) \):

3-2 DEFINITION. \( CM^*(\Sigma) \) is generated as in Section 2.3 except that the productions for the non-terminals \( DC \) and \( S \) are replaced by

- \( DC ::= \alpha_j(\bar{\bar{u}}\#\bar{v}) :: [S] \ DC \) |
- \( S ::= z := e | \ell.wait.\ell | \ell.\ell | \ell.() | \ell.() | \ell.(() | \ell.) | \text{end}_{\ell,i,j} | \ell.callM_i,\alpha_j(\bar{\bar{u}}\#\bar{v}) | \ell.rend_{\ell,i,j} | S_1; S_2 | \text{if} \; b \; \text{then} \; S_1 \; \text{else} \; S_2 \; \text{fi} | \text{while} \; b \; \text{do} \; S \; \text{od} | \Lambda \)

A block-\( \ell \)-action signifies that a wait has been encountered and that the monitor lock was released at this point. In the configuration of a caller, \( \ell.rend_{\ell,i,j} \) records that an instance of procedure \( \alpha_j \) in \( M_i \) has been activated but not yet completed. The set of value-result parameters of the call is \( \bar{v} \). Statements \( \text{end}_{\ell,i,j} \) are used to identify the caller (procedure \( \alpha_j \) in \( M_i \)) which caused the current instance to be created. Here, \( \bar{v} \) denotes the set of formal value-result parameters of the corresponding procedure. \( \Lambda \) denoted the empty statement.

Fix some signature \( \Sigma \) and a \( \Sigma \)-structure \( A \). From now on, I assume that \( \Sigma \) contains \( +, -, 0 \) and \( 1 \) and that \( A \) contains as sub-structure the standard model \((\omega, +, -, 0, 1)\). This assumption is needed to evaluate the instance counters and, later on, is needed to reason about them. The semantics of \( CM(\Sigma) \)-programs, however, is not influenced.
3-3 DEFINITION (The configuration set C).

- A local configuration, $LC$, has the form $Id : (S, B)$, where
  - $Id = (i, j, k) \in \omega^3$; $i$ indexes a module, $j$ a procedure and $k$ characterizes the instance,
  - $S$ is a $CM^*(\Sigma)$-statement or procedure,
  - $\theta = (\nu, \rho)$, where $\nu \in St$ with $Dom(\nu) \subseteq Var$ and $\rho \in Lab \cup \{\emptyset\}$.

- A module configuration $MC$ has the form $(X | 0 | \sigma)$ or $(X | a | LC_0, \ldots, LC_n, \sigma)$, where
  - $X$ is either $\Lambda$ or a $CM^*(\Sigma)$ module,
  - $\sigma$ is a state such that $Dom(\sigma) \cap Dom(\nu_i) = \emptyset$ for $i = 1 \ldots n$.

- A program configuration $PC$, has the form $(MC_0, \ldots, MC_m)$, where
  - $MC_0, \ldots, MC_m$ are module configurations.

- The configuration set, $C$, consists of all program and module configurations.

During execution of a module, several procedure instances coexist together with the module's initial statement. The local configurations record the progress in each of these instances. Since formal parameters are local variables, each $LC$ has a local state; the label records control information. The identification, $Id$, of a local configuration indicates where the configuration originates from: $Id = (i, j, k) \neq (0, 0, k)$ implies that it records a configuration of procedure or initial statement $a_j$ while $k$ identifies the instance; $Id = (0, 0, k)$ gives no such information and is the "identification" of a configuration of some statement. The variables that are global in the module, are valued by the $MC$'s state. Its activity pointer points to the $LC$ that is currently active or equals $-1$, signifying a change of activity at a waiting point.

The variables in $VarIC$ are proof-variables and are used to count the number of instances of a procedure. I assume that there is some canonical enumeration of the procedure names in a program, so that I can write $ic.\alpha$ for the $VarIC$-variable that refers to procedure $\alpha$ (in module $M_i$).

Conventions: As generic indicants for module configurations, $C, C', C'', C_i, \ldots$ are used. $C$ has the form $(M_j | a | LC_0, \ldots, LC_m, \sigma)$ where $LC_i \equiv Id_i : (S_i, \nu_i, \rho_i)$ and $\rho_i \equiv (\nu_i, \rho_i)$. In $C_{\beta}$ the components of $C$ inherit the sub and superscripts (except for a module text):

$$\langle M_j | \alpha^\beta | Id^\beta_{\rho,0} : (S^\alpha_{\rho,0}, \theta^\alpha_{\rho,0}), \ldots, Id^\alpha_{\rho,m} : (S^\alpha_{\rho,m}, \theta^\alpha_{\rho,m}), \sigma^\beta \rangle$$

Program configurations are generically denoted as $C, C', \ldots \ C$ has the form $(C^1, \ldots, C^n)$ and otherwise follows the above conventions. Finally, sometimes only part of a configuration is explicitly given; the other parts are then assumed to follow these conventions. Similar conventions hold for program configurations.

3-4 DEFINITION (The transition label set, $TL$).

- $TL = \{\epsilon\} \cup \{(i, j, h, \nu, \ell, \sigma) | i, j, h \in \omega, \nu \in St, \ell \in Lab\} \cup \{(i, j, a, k, l, ind) | i, j, a, k, l \in \omega, a \subseteq |A|, ind \in \{in, te\}\}$.

- Records of the form $(i, j, a, k, l, ind)$ are called global records; the other ones are called local records.
Transition labels will be interpreted as words or sequences consisting of 0 or 1 records. Global records originate from module communications; \( \ell \) is the sequence of transmitted values, the first index pair — a module and procedure index — specifies the sender, the second pair the receiver and \( \text{ind} \) indicates whether the record witnesses the initiation of a rendezvous (in) or the termination of one (\( \text{te} \)). Non-empty local records originate from waiting points and the index pair points to the originator. The pair of states, \( \nu \) and \( \sigma \), record the local state, \( \nu \), of the procedure instance and the global state, \( \sigma; \ell \) identifies the waiting point. Finally, \( h \) characterizes the executing procedure instance.

3-5 DEFINITION (The front label of a statement, \( S \), \( \text{lab}(S) \)).
- for \( S \equiv x := e \), if \( b \) then \( S' \) else \( S'' \) fi, while \( b \) do \( S \) od, \( a(\bar{u}\#\bar{v}) : [\ell.S] \), \( \text{ends}_{s,i,j} \) or \( \Lambda \): \( \text{lab}(S) = \emptyset \),
- for \( S \equiv \ell.\text{wait}.\ell', \text{block}.\ell, \ell, \ell.(, \ell), \ell.\text{call}M_1.a_1(\bar{e}\#\bar{z}) \) or \( \ell.\text{rend}_{s,i,j} : \text{lab}(S) = \{\ell\} \)
- for \( S \equiv S_1; S_2 \): \( \text{lab}(S) = \text{lab}(S_2) \) if \( S_1 \equiv \Lambda \) \( \text{lab}(S_1) \) otherwise.

All is set now for the definition of the transition relation. In its definition, whenever an \( MC \) of the form \( \langle X | a | \cdots \rangle \), occurs, the shown \( LC \) is the one pointed to by \( a \), unless \( a = -1 \). Write \( C \rightarrow \lambda \rightarrow C' \) instead of \( (C, \lambda, C') \in \rightarrow \).

3-6 DEFINITION (The transition relation, \( \rightarrow \)).
- \( \rightarrow \subseteq C \times TL \times C \) is the smallest relation satisfying
  1. \( \langle A | 0 | Id : (x := e, \nu, \emptyset) , \sigma \rangle \xrightarrow{\epsilon} \langle A | 0 | Id : (A, \nu', \emptyset), \sigma' \rangle \), where\(^1\)
     \( \nu', \sigma' = \nu(\nu \cup \sigma(e)/x), \sigma \) if \( x \in \text{Dom}(\nu) \)
     \( = \nu \sigma(\nu \cup \sigma(e)/x) \) if \( x \notin \text{Dom}(\nu) \)
  2. \( \langle A | 0 | Id : (\ell.\text{wait}.\ell', \nu, \ell), \sigma \rangle \xrightarrow{(Id, \nu, \ell, \sigma)} \langle A | -1 | Id : (\text{block}.\ell', \nu, \ell), \sigma \rangle \)
  3. \( \langle A | -1 | Id : (\text{block}.\ell, \nu, \ell), \sigma \rangle \xrightarrow{\epsilon} \langle A | 0 | Id : (\text{block}.\ell, \nu', \ell), \sigma' \rangle \)
  4. \( \langle A | 0 | Id : (\text{block}.\ell, \nu, \ell), \sigma \rangle \xrightarrow{\epsilon} \langle A | 0 | Id : (A, \nu, \emptyset), \sigma \rangle \)
  5. \( \langle A | 0 | r, s, k : (\ell.\text{call}M_1.a_2(\bar{t}\#\bar{e}), \nu, \ell), \sigma \rangle \xrightarrow{(r, s, \sigma \cup \nu(\bar{e}, \bar{z}), i, j, in)} \langle A | 0 | r, s, k : (\ell.\text{rend}_{s,i,j}, \nu, \ell), \sigma \rangle \)
  6. \( \langle A | 0 | r, s, k : (\ell.\text{rend}_{s,i,j}, \nu, \ell), \sigma \rangle \xrightarrow{(i, j, \bar{a}, r, s, \bar{t}e)} \langle A | 0 | r, s, k : (\ell.\text{rend}_{s,i,j}, \nu, \ell), \sigma' \rangle \)

  where for \( x_k \in \bar{z} \) \( \nu'(x_k), \sigma'(x_k) = a_k, \sigma(x_k) \) if \( x_k \in \text{Dom}(\nu) \) and \( \nu(x_k), a_k \) if \( x_k \notin \text{Dom}(\nu) \)

  \( \nu' \upharpoonright \bar{z}^C = \nu \upharpoonright \bar{z}^C, \sigma' \upharpoonright \bar{z}^C = \sigma \upharpoonright \bar{z}^C \)
  7. \( \langle A | 0 | Id : (\ell, \Omega, \ell), \sigma \rangle \xrightarrow{(Id, \Omega, \ell, \sigma)} \langle A | -1 | Id : (\ell, \Omega, \ell), \sigma \rangle \)
  8. \( \langle A | -1 | Id : (\ell, \Omega, \ell), \sigma \rangle \xrightarrow{\epsilon} \langle A | 0 | Id : (\ell, \Omega, \ell), \sigma' \rangle \)
  9. \( \langle A | 0 | Id : (\ell, \nu, \ell), \sigma \rangle \xrightarrow{\epsilon} \langle A | 0 | Id : (\ell, \nu, \emptyset), \sigma \rangle \)

\(^1\)Remember that any state is implicitly assumed to valuate all the appropriate variables.
10. \( \langle \Lambda \mid 0 \mid Id : (\ell, \nu, \ell), \sigma \rangle \xrightarrow{\epsilon} \langle \Lambda \mid 0 \mid Id : (\Lambda, \nu, \emptyset), \sigma \rangle \)

11. \( \langle \Lambda \mid 0 \mid Id : (\Lambda, \theta), \sigma \rangle \xrightarrow{\epsilon} \langle \Lambda \mid 0 \mid \sigma \rangle \)

12. \( \langle \Lambda \mid 0 \mid i, j, k : (a_j^i (u \# 0) : [S], \nu, \emptyset), \sigma \rangle \xrightarrow{(r, s, \bar{b}, \bar{c}, i, j, \text{in})} \langle \Lambda \mid 0 \mid i, j, k : (\text{end}_{s, r, s}, \Omega \{\bar{b}, \bar{c}/\bar{a}, \bar{b}\}, \emptyset), \sigma \rangle \),

where \( \bar{b} = \sigma \cup \nu (u) \) and \( \bar{c} = \sigma \cup \nu (\emptyset) \)

13. \( \langle \Lambda \mid 0 \mid Id : ([S] \ell, \Omega, \emptyset), \sigma \rangle \xrightarrow{\varepsilon} \langle \Lambda \mid 0 \mid Id : (S \ell, \Omega, \emptyset), \sigma \rangle \)

14. \( \langle \Lambda \mid 0 \mid i, j, k : (\text{end}_{\bar{c}, r, \sigma}, \nu, \emptyset), \sigma \rangle \xrightarrow{(i, j, \nu(\theta), r, s, \text{te})} \langle \Lambda \mid 0 \mid i, j, k : (\Lambda, \nu, \emptyset), \sigma \rangle \)

15. \( \langle \Lambda \mid 0 \mid Id : ([\text{if } b \text{ then } S_1 \text{ else } S_2 \text{ fi}, \nu, \emptyset), \sigma \rangle \xrightarrow{\varepsilon} \langle \Lambda \mid 0 \mid Id : (S_1, \nu, \text{lab}(S_1)), \sigma \rangle \)

if \( A, \sigma \cup \nu \models b \)

16. \( \langle \Lambda \mid 0 \mid Id : ([\text{if } b \text{ then } S_1 \text{ else } S_2 \text{ fi}, \nu, \emptyset), \sigma \rangle \xrightarrow{\varepsilon} \langle \Lambda \mid 0 \mid Id : (S_2, \nu, \text{lab}(S_2)), \sigma \rangle \)

if \( A, \sigma \cup \nu \nvdash b \)

17. \( \langle \Lambda \mid 0 \mid Id : ([\text{while } b \text{ do } S \text{ od}, \nu, \emptyset), \sigma \rangle \xrightarrow{\varepsilon} \langle \Lambda \mid 0 \mid Id : (S; \text{while } b \text{ do } S \text{ od}, \text{lab}(S)), \sigma \rangle \)

if \( A, \sigma \cup \nu \models b \)

18. \( \langle \Lambda \mid 0 \mid Id : ([\text{while } b \text{ do } S \text{ od}, \nu, \emptyset), \sigma \rangle \xrightarrow{\varepsilon} \langle \Lambda \mid 0 \mid Id : (\Lambda, \nu, \emptyset), \sigma \rangle \)

if \( A, \sigma \cup \nu \nvdash b \)

19. \( \langle \Lambda \mid a \mid Id : (S, \nu, \rho), \sigma \rangle \xrightarrow{\lambda} \langle \Lambda \mid a' \mid Id : (S', \nu', \rho'), \sigma' \rangle \), where

\( S \equiv S'; T \) if \( S' \equiv \Lambda \) and \( T \) otherwise

20. \( \langle \Lambda \mid a \mid Id : (S, \theta), \sigma \rangle \xrightarrow{\lambda} \langle \Lambda \mid a' \mid Id : (S', \theta'), \sigma' \rangle \), provided

\( M \mid -1 \mid \cdots Id : (T, \theta), \sigma \rangle \xrightarrow{\lambda} \langle M \mid b \mid \cdots Id : (S', \theta'), \sigma' \rangle \)

\( S \not\equiv \ell, \) if \( a = -1 \) then \( \sigma, \nu = \sigma', \nu', \) and if \( a' = -1 \) then \( b = -1 \) else \( b = i \)

21. \( \langle M \mid i \mid \cdots Id : (\ell, \theta), \sigma \rangle \xrightarrow{(Id, \nu, \ell, \sigma)} \langle M \mid -1 \mid \cdots Id : (\ell, \theta), \sigma \rangle \)

22. \( \langle \Lambda \mid 0 \mid l, j, k : (a_j^i (u \# 0) : [S], \Omega, \emptyset), \sigma \rangle \xrightarrow{\lambda} \langle \Lambda \mid 0 \mid l, j : (S', \theta'), \sigma' \rangle \), provided \( a_j \) is declared in \( M_i \) as in the premiss, \( Id_i \neq (l, j, k) \) for \( i < n \) and \( \sigma'' = \sigma' (i.c.a_j^i + 1/i.c.a_j^i) \).

In case \( j = 0 \), the declaration stands for the initial statement of \( M_i \) and I assume the parameter part to be empty.
23. \((M \mid i \mid LC_0 \cdots LC_{i-1}, Id : (\Lambda, \nu, \emptyset), LC_{i+1} \cdots LC_n, \sigma) \xrightarrow{(Id, \Omega, \emptyset, \sigma')} (M \mid -1 \mid LC_0 \cdots LC_{i-1}, LC_{i+1} \cdots LC_n, \sigma')\),

where \(\sigma' = \sigma\{ic.a_j^i - 1/ic.a_j^i\}\).

24. \((M, \mid -1 \mid Id : (\ell, \emptyset), \sigma) \xrightarrow{\ell} (M, \mid 0 \mid \sigma)\)

25. \((M_k \mid \cdots) \xrightarrow{\lambda} (M_k \mid \cdots)'\),
\[\left((M_1 \mid \cdots) \cdots (M_k \mid \cdots) \cdots (M_n \mid \cdots)\right) \xrightarrow{\lambda} \left((M_1 \mid \cdots) \cdots (M_k \mid \cdots)' \cdots (M_n \mid \cdots)\right)\]

provided \(\lambda\) is local and \((M_k \mid \cdots)' \neq (M_k \mid 0 \mid \tau)\) for any \(\tau\).

27. \((M \mid \cdots) \xrightarrow{\lambda} (M \mid \cdots)'\), \((M_j \mid \cdots) \xrightarrow{\lambda} (M_j \mid \cdots)'\)

\[\left((M_1 \mid \cdots) \cdots (M_i \mid \cdots) \cdots (M_j \mid \cdots) \cdots (M_n \mid \cdots)\right) \xrightarrow{\lambda} \left((M_1 \mid \cdots) \cdots (M_i \mid \cdots)' \cdots (M_j \mid \cdots)' \cdots (M_n \mid \cdots)\right)\]

provided \(\lambda\) is global.

\[(M_1 \mid -1 \mid Id_1 : (\ell_1, \emptyset_1), \sigma_1), \ldots, (M_n \mid -1 \mid Id_n : (\ell_n, \emptyset_n), \sigma_n) \xrightarrow{\ell} (M_1 \mid 0 \mid \sigma_1), \ldots, (M_n \mid 0 \mid \sigma_n)\]

\(\rightarrow^*\) is the reflexive and transitive closure of \(\rightarrow\).

Remarks: The above definition intends to capture not only the behaviour of \(CM^*(\Sigma)\)-programs, but also the behaviour of modules and statements, independent from their context. So, e.g., the states in axiom 3 can change arbitrarily, reflecting the fact that nothing is known about the module text, hence about the statements that can be interleaved at waiting points. In contrast, rule 20 does not allow such changes. Likewise for axiom 8 versus axiom 24. Axioms 3, 7, 8 and 11 are irrelevant as far as the transisitons of modules and programs are concerned. Additionally, rule 24 can be ignored for program transitions.

3–7 DEFINITION (Start and terminal configurations). Let \(\tau\) be any state.

1. for a statement or initial statement \(S\)
   \(- SC_{\tau}(S) = \{ (\Lambda \mid 0, 0, 0 : (S, \Omega, lab(S)), \tau) \}\)
   \(- TC_{\tau}(S) = (\Lambda \mid 0 \mid \tau)\)
2. for a declaration, \(D\), of a procedure \(a_j^i\) (\(j \neq 0\))
   \(- SC_{\tau}(D) = \{ (\Lambda \mid 0 \mid i, j, k : (D, \Omega, \emptyset), \tau) \mid k \in \omega \}\)
   \(- TC_{\tau}(D) = (\Lambda \mid 0 \mid \tau)\)
3. for a module \(M_i\) with initial statement \(S_0, \ell\)
   \(- SC_{\tau}(M_i) = (M_i \mid 0 \mid i, 0, 0 : (S_0, \ell, \Omega, \emptyset), \tau), \quad \text{where } \tau = \tau\{0/ic.a_j^i \mid j = 1..n_i\}\)
   \(- TC_{\tau}(M_i) = (M_i \mid 0 \mid \tau)\)
4. for a program \(P \equiv [M_i \mid \cdots \mid M_n]\)
   \(- SC_{\tau}(P) = (SC_{\tau, \ell_0}(M_i), \ldots, SC_{\tau, \ell_n}(M_n))\)
- \( TC_\tau(P) = (TC_\tau|_{M_1}, \ldots, SC_\tau|_{M_n}) \), where \( \forall i \leq i \leq n \)
- \( \mathcal{SC} = \{ SC_\tau(X) \mid \tau \text{ a state}, X \text{ a } CMe(\Sigma)\text{-statement, procedure, module or program} \} \)
- \( \mathcal{TC} = \{ TC_\tau(X) \mid \tau \text{ a state}, X \text{ a } CMe(\Sigma)\text{-statement, procedure, module or program} \} \).

3-8 Definition (Configuration states, \( s(C) \)).
- for a module configuration \( C \equiv (X | a | Id_0 : (S_0, \theta_0), \ldots, Id_n : (S_n, \theta_n), \sigma) \),
  \( s(C) = \{ (a, \bar{\theta}_0, \ldots, \bar{\theta}_n, \sigma) \mid \text{for } 0 \leq i \leq n, \text{ if } a = -1 \text{ or } a = i \text{ then } \bar{\theta}_i = \theta_i \text{ else } \bar{\theta}_i = (\nu_i, \emptyset) \} \),
- for a program configuration \( C = (MC_1, \ldots, MC_m) \)
  \( s(C) = \{ \{ \delta_1, \ldots, \delta_m \} \mid \delta_i \in s(MC_i), 1 \leq i \leq m \} \).

Configuration states extract from configurations the information on which satisfaction of specifications depend. Configuration states, usually denoted by \( \delta, \delta', \ldots \), inherit the notational conventions as introduced for configurations.

3-9 Definition (\( CM^*(\Sigma) \)-computations and semantics).
For any \( CM^*(\Sigma)\text{-statement, procedure, module or program } T, \text{ set of states } X \text{ and set of configurations } Y \):
- Define
  \( C(T, X, Y) = \{ C_0 \overset{\lambda_1}{\rightarrow} C_1 \overset{\lambda_2}{\rightarrow} \cdots \overset{\lambda_n}{\rightarrow} C_n \mid C_0 \in SC_\tau(T), \tau \in X, \forall 0 \leq i \leq n C_i \in Y \} \),
- The set of \((X, Y\text{-legal}) computations, \( \text{Comp}(T, X, Y) \), is defined by
  - \( C(T, X, Y) \) if \( T \) is a module or program, and
  - \( C(T, X, Y) \cup \) \( \begin{cases} C_m \overset{\lambda_{m+1} \cdots \lambda_n}{\rightarrow} C_n & \exists C_0 \overset{\lambda_1 \cdots \lambda_m}{\rightarrow} C_m \text{ such that} \\ \text{where } \alpha_{m-1} = -1 \text{ and} \\ C_0 \overset{\lambda_1 \cdots \lambda_n}{\rightarrow} C_n \in C(T, St, Y) \end{cases} \)
    if \( T \) is a statement or procedure
- its semantics, \( \llbracket T \rrbracket(X, Y) \), is
  \( \{ (\delta_0 \cdots \delta_n, t) \mid \exists C_0 \overset{\lambda_1 \cdots \lambda_n}{\rightarrow} C_n \in \text{Comp}(T, X, Y) \text{ such that} \\ \text{if } C_n = TC_\sigma(T) \text{ then } t = \bot \text{ otherwise } t = T \text{ and} \\ \delta_i = s(C_i) \text{ for } 0 \leq i \leq n \} \).

This definition of computation sequence, and hence of semantics, reflects the knowledge of the state at waiting points: only in modules and programs is the state known when execution resumes at a waiting point; for statements and procedures the state at these points is arbitrary (see, e.g., the transition rule 3 in Definition 3-6). For that reason, suffixes of computation sequences are
included, too. This will become clearer when defining satisfaction of specifications in Definition 5-3.

Observe that the usual notion of computation and semantics is obtained as $\text{Comp}(\cdot, St, C)$ and $[\cdot](St, C)$.

As a matter of notation, if no restrictions are placed on states or configurations, the corresponding sets are not mentioned. E.g., instead of $\text{Comp}(\cdot, St, C)$ I shall write $\text{Comp}(\cdot)$. Moreover, whenever I associate configuration states with the configurations in a computation, the conditions of the second part of Definition 3-8 will be assumed.

For future use, there are four simple observations to be made:

The relation between instance-counters ($\text{Var}^{IC}$) and configurations is given by the following:

3-10 OBSERVATION. Let $M_1$ be some module, let $C_0 \xrightarrow{\lambda} C_n \in \text{Comp}(T)$ and let $a_k$ be some procedure in $M_1$. Then

- $\sigma_n(\text{ic}.a_k) = m \leftrightarrow$ there are $m$ LC's, $Id_j : (S_j, \theta_j)$, in $C_n$ such that $Id_j = (l, k, h)$ for some $h$
  and for $j = 1..m$.

This is obvious.

3-11 OBSERVATION. Given, for $i = 0, 1, C_0 \xrightarrow{\lambda^i} C_n \in \text{Comp}(M_1, \tau)$, assume that $\lambda^0 = \lambda^1$ and $\sigma^0_n = \sigma^1_n$. Then, if for some $i$ and $j$, $\theta^0_{n,i} = \theta^1_{n,j}$, $Id^0_{n,i} = Id^1_{n,j}$ and $\rho^0_{n,i} \neq \emptyset$, conclude that $LC^0_{n,v,i} = LC^1_{n,v,j}$.

If $M_1$ only contains straightline code (i.e., no while loops) this is clear. Next, observe that between any two successive arrivals “at” $\rho^0_{n,i}$ in the procedure instance determined by $Id^0_{n,i}$ at least one record is generated. Moreover, if this record is a global one, so that the generating procedure instance is not known, there is another local record that does identify the generating instance.

In the sequel this observation shall mostly be used implicitly.

3-12 OBSERVATION. Let $C_0 \xrightarrow{\lambda} C_n \in \text{Comp}(M_1)$ with $a_n = -1$ and let $\nu \in St, \ell \in \text{Lab}$. Then the following two statements are equivalent:

- $(\nu, \ell) = \theta_{n,i}, \ell \in \text{FLB}(a_j)$ and $Id_{n,i} = (l, j, k)$
- $\lambda = \lambda_0 \ast (l, j, k, \nu, \ell, \sigma) \ast \lambda_1$, where
  1. $\ell \in \text{FLB}(a_j)$,
  2. if $\ell$ labels the rear of a wait, then $\ell'$ labels its front and if $\ell$ labels the rear of $a_j$ then
     $\ell' \equiv \ell$
  3. $\lambda_1$ does not contain a local record of the form $(l, j, k, \nu, \ell, \sigma)$ for any $\nu, \sigma$ and $\ell$.

Notation: $(h, \ell, \nu)$ is determined by $\lambda$.

Because $a_n = -1$ every $\rho_{n,i}$ labels a waiting point. Hence, ‘arriving’ at any of the $\theta_{n,i}$'s has been witnessed by some local record. Consider the last time the computation arrived at $(\nu, \ell)$. Clearly, $\lambda$ has the form as suggested. Alternatively, if $\lambda$ has the above form then the configuration responsible for producing the local record cannot have moved during the $\lambda_1$-computation (remember, $a_n = -1$).
OBSERVATION. For any \( CM^*(\Sigma) \)-statement, procedure, module or program \( T \) and computable sets of states \( X \), and configurations, \( Y \), \( \text{Comp}(T,X,Y) \) and \([T][X,Y] \) are computable relations.

4 The merging lemmas

The aim is a syntax directed axiomatization of communicating modules. Specifically, it must be possible (1) to combine the specifications of procedures and the initial statement into a module specification and (2) to combine module specifications into a program specification.

Now, specifications describe sets of allowed or legal computations of the specified program parts. Also, for completeness of the axiom system, specifications must be able to fully characterize the legal computations. Consequently the following question arises:

Given computations of some statements. When are such computations compatible in the sense that they are sub-computations of the composite statement?

In this section the two less trivial cases are treated. Section 4.1 contains the local merging lemma which states the conditions under which computations of a set of procedures and an initial statement can be combined into a single computation of the resulting module. In Section 4.2 the global merging lemma is formulated, which states when module-computations can be combined.

4.1 The local merging lemma, \( LML \)

4–1 DEFINITION (local reachability, \( lr \)).

Let \( M_i \) be a \( CM^*(\Sigma) \)-module, \( \tau_0, \tau_1, \sigma \in St, K \) a set of configurations, \( \ell_0, \ldots, \ell_k \in Lab, h_0, \ldots, h_k \in w \) and \( \lambda \) a record sequence. Define for \( i = 0 \ldots k, j_i \in l \ell_i \in FLB(a_i) \).

Then \( (h_0, \ell_0, \ldots, h_k, \ell_k) \) is \((M_i, \tau, K, \sigma)\)-lr iff

\[
\exists C_0 \xrightarrow{\lambda} C_n \in \text{Comp}(M_i, \{\tau\}, K) \text{ such that }
\]

- \( \sigma \upharpoonright V_1 = \sigma_n \upharpoonright V_1 \) and \( \lambda = \lambda_n \),
- there is an injection, \( cf : \{0 \ldots k\} \hookrightarrow \{0 \ldots m\} \), where \( m \) is the number of local records in \( C_n \), and \( \forall i = 0 \ldots k \) \( (\nu_i, \ell_i) = \theta_{n,cf(i)} \) and \( \text{Id}_{n,cf(i)} = (1, j_i, h_i) \)

So, configurations as characterized by \((\nu_j, \ell_j), h_j \) and \( \sigma \), are locally reachable from some state \( \tau \), precisely if there is a computation of \( M_i \), starting in \( \tau \), reaching such a configuration via intermediate configurations in \( K \) and which associated record sequence is \( \lambda \).

4–2 DEFINITION (LC-independence). Let \( C_0^i \xrightarrow{\lambda} C_n^i \in \text{Comp}(M_i, \tau, K) \) for \( i = 0, 1 \) and let \( C_n^i \in C \) be obtained from \( C_0^i \) by replacing or adding LC's from \( C_n^1 \). Then, \( K \) is called LC-independent if

\[
C_0 \xrightarrow{\lambda} C_n \in \text{Comp}(M_i, \tau) \Rightarrow C_0 \xrightarrow{\lambda} C_n \in \text{Comp}(M_i, \tau, K)
\]
LEMMA (Local Merging Lemma, LML).
With notation as in Definition 4-1, suppose that
• \((\nu_0, \nu_{-1}, \ldots, \nu_{k-1}, \nu_k)\) is \((M_1, \tau_1, K, \nu_1, \ldots, \nu_{k-1}, \sigma, \lambda)\)-ir, and
• \(K\) is LC-independent.
Then \((\nu_0, \nu_{-1}, \ldots, \nu_{k-1}, \nu_k)\) is \((M_1, \tau_1, K, \nu_1, \ldots, \nu_{k-1}, \sigma, \lambda)\)-ir, provided
• \(\forall \nu_1 < k \quad \nu_i = \nu_k \Rightarrow \nu_i \not= \nu_k\),
• there is at most one \(\nu_i \in \text{FLB}(a_0^k)\) and
• at most one \(i, l\) does not label a waiting point.

PROOF. W.l.o.g., assume that \(\text{Dom}(\tau_0) \subseteq \nu_1\) for \(i \leq 2\) and that \(\text{Dom}(\sigma) \subseteq \nu_i\). Let \(\tau = \tau_0 = \tau_1 = \tau_2\). If \(\lambda\) does not contain local records, then \(\nu_0, \ldots, \nu_k \in \text{FLB}(a_0^k)\), so that the Lemma holds vacuously.

Otherwise, split \(\lambda = \lambda^1 \cdot \lambda^2\), where \(\lambda^2\) is the largest suffix of \(\lambda\) that does not contain any local record. By assumption, there are computations,\(\lambda^1 \cdot \lambda^2\), \(\lambda^1 \cdot \lambda^2\) both in \(\text{Comp}(M_1, \{\tau\}, K)\), such that \((\nu_i, \nu_{i+1}) = \theta_{n, cf(i)}\), \(I_{n, cf(i)} = (i, j_i, h_i)\) for \(i < k\) and \((\nu_k, \nu_{k+1}) = \theta_{n, cf(k)}\), \(I_{n, cf(k)} = (i, j_k, h_k)\); moreover, \(\sigma_n = \sigma\). Define \(m\) as the (largest) index such that \(a_m = -1\); likewise, define \(\tilde{m}\) such that \(\tilde{a}_{\tilde{m}} = -1\).

Choose any \(L_{\tilde{m}+1}\) from \(\tilde{C}_m\) and apply Observation 3-12 to the second computation in (1): \(\tilde{\lambda} = \lambda_0 \cdot (l, j, p, \tilde{v}_{m+1}, \tilde{v}_{m+1}, \tilde{\sigma}) \cdot \tilde{\lambda}_1\) and \(\tilde{\lambda}_1\) does not witness any other activity in the corresponding procedure instance. Now, apply the Observation (in the reverse direction) to the first computation in (1) and conclude that \(\tilde{\theta}_{m,i} = \theta_{m,j}\) for some \(j\). Repeating this argument gives that every local state in \(\tilde{C}_m\) is also reached in \(C_m\). If \(m = n\), this concludes the proof.

Next, let \(m < n\). the \(C_{m-1} \rightarrow C_m\) and \(\tilde{C}_{m-1} \rightarrow \tilde{C}_m\)-transitions are both witnessed by the same last (local) record in \(\tilde{\lambda}\), so that \(\tilde{\sigma}_m = \tilde{\sigma}_{\tilde{m}}\).

Finally, the \(C_0 \rightarrow \lambda^1 \cdot \lambda^2\)-computation must be extended. There are two separate cases.
1) \(a_{m+1} \not\in \text{Ran}(cf)\). This means that \((\nu_i, \nu_{i+1}) = \theta_{m, cf(i)}\) for \(i < k\). If \(\tilde{\theta}_{m, \tilde{a}_{m+1}}\) exists, define \(I\) as the index of the corresponding local state in \(C_m\); otherwise, let \(I\) be 1 larger than the number of LC's in \(C_m\). Define configurations \(C_{m+i}\) for \(1 \leq i \leq n - m\) by
• \(LC_{m+i,j} = LC_{m,j}\) for \(j \not= I\),
• \(LC_{m+i,I} = LC_{m+i,\tilde{a}_{m+1}}\),
• \(\sigma_{m+i} = \tilde{\sigma}_{m+1}\), and
• \(a_{m+i} = I\).
As \(K\) is LC-independent, I have \(C_0 \rightarrow \lambda^1 \cdot \lambda^2 \rightarrow C_{m+i} \in \text{Comp}(M_1, \{\tau\}, K)\). Hence, \(\theta_{m+n-i, \tilde{a}_{m+i}} = (\nu_i, \nu_{i+1})\) for \(i < k\).
Moreover, by construction, \(\theta_{m+n-i, \tilde{a}_{m+i}} = (\nu_k, \nu_{k+1})\) and \(\sigma_{m+n-i} = \sigma\). The Lemma follows.
2) \(\tilde{a}_{m+1} \not\in \text{cf}(k)\). Hence, \(\tilde{\theta}_{m, \tilde{a}_{m+i}} = (\nu_k, \nu_{k+1})\). The first computation in (1) proves the Lemma.
There seems to be a third case: \( a_{m+1} \in \text{Ran}(cf) \) and \( a_{n+1} = cf(k) \); say \( a_{m+1} = cf(0) \). This, however, cannot happen because either \( \ell_0 \) or \( \ell_k \) labels a waiting point, but \( \lambda \) does not contain a local record.

4.2 The global merging lemma, GML

4-4 Definition (projection). Let \( \lambda \) be some record sequence of a program \([M_1 || \cdots || M_n]\).
- \( \lambda \downarrow l \) is the subsequence of \( \lambda \) obtained by erasing all records that do not involve module \( M_i \).
- \( \lambda \downarrow g \) is the subsequence of \( \lambda \downarrow l \) obtained by erasing all local records.

4-5 Definition (global reachability, gr). Let \( P \) be a CM*Σ-program, \([M_1 || \cdots || M_n]\); \( \tau, \nu_0, \ldots, \nu_k \in \omega \) and \( \ell_0, \ldots, \ell_k \in \text{Lab} \) such that \( \ell_i \in \text{FLB}(M_i) \) for \( i \leq k \).
Then \( (h_0, \ell_0, \ldots, h_k, \ell_k) \) is \((P, \tau, \nu_0, \ldots, \nu_k, \sigma, \lambda)\)-gr if

\[
\exists C_0 \xrightarrow{\lambda} C_n \in \text{Comp}(P, \tau) \quad \text{such that}
\]

- \( \lambda \downarrow i = \lambda \downarrow i \) for every \( i \in \text{Ran}(l) \)
- there is a function \( cf: \{0 \ldots k\} \rightarrow \omega \) such that for all \( i = 1 \ldots k \sigma \upharpoonright V_{t(i)} = \sigma^t_{q(i)} \upharpoonright V_{t(i)}, \)
- \( \theta_n^t_{q(i)} = (\nu, \ell_t) \) and \( Id_{q(i)}^t = (i(i), \tau, \nu) \) with \( \ell_t \in \text{FLB}(\sigma_i^{q(i)}) \).

4-6 Lemma (Global Merging Lemma, GML). With notation as above, suppose

- \( (h_0, \ell_0, \ldots, \ell_{k-1}, \ell_k) \) is \((P, \tau, \nu_0, \ldots, \nu_{k-1}, \sigma, \lambda')\)-gr,
- \( \ell_k \) is \((P, \tau, \nu_k, \sigma, \lambda'')\)-gr,
- \( \ell_k \) is \((P, \tau, \nu_k, \sigma, \lambda'')\)-gr, and
- \( \tau \upharpoonright V = \tau_j \upharpoonright V \) for \( i, j = 0 \ldots 2 \) and \( V = \bigcup_{i=1}^n V_i \), \( \lambda \downarrow g \downarrow l(i) = \lambda' \downarrow g \downarrow l(i) \) for \( i < k \) and \( \lambda \downarrow g \downarrow l(k) = \lambda'' \downarrow g \downarrow l(k) \).

Then \( (h_0, \ell_0, \ldots, h_k, \ell_k) \) is \((P, \tau, \nu_0, \ldots, \nu_k, \sigma, \lambda)\)-gr, where \( \tau \upharpoonright V = \tau_0 \upharpoonright V \), \( \lambda \downarrow l(i) = \lambda' \downarrow l(i) \) for \( i < k \) and \( \lambda \downarrow l(k) = \lambda'' \downarrow l(k) \).

Proof. W.l.o.g., assume that \( \tau_0 = \tau_1 = \tau_2 = \tau \). The Lemma is proven with induction on the number of global records in \( \lambda \). A stronger version of the Lemma is, however, needed to carry this induction:

Suppose

1. \( \hat{C}_0 \xrightarrow{\lambda} \hat{C}_n \in \text{Comp}(P, \tau) \),
2. \( \hat{C}_0 \xrightarrow{\lambda} \hat{C}_n \in \text{Comp}(P, \tau) \),
3. \( \hat{C}_0 \xrightarrow{\lambda} \hat{C}_n \in \text{Comp}(P, \tau) \) and
4. \( A_0 \cup A_1 \subseteq \{1 \ldots n\} \) with \( A_0 \cap A_1 = \emptyset \) and \( \lambda \downarrow g \downarrow i = \lambda \downarrow g \downarrow i \) if \( i \in A_0 \), \( \lambda \downarrow g \downarrow i = \lambda \downarrow g \downarrow i \) if \( i \in A_1 \).

15
Then there is a computation \( C_0 \xrightarrow{\lambda} C_n \in \text{Comp}(P, \tau) \), with \( \lambda \downarrow i = \tilde{\lambda} \downarrow i \) for \( i \in A_0 \),
\[
\lambda \downarrow i = \tilde{\lambda} \downarrow i \quad \text{for } i \in A_1, \quad \lambda \downarrow i = \tilde{\lambda} \downarrow i \quad \text{for } i \notin A_0 \cup A_1 \quad \text{and} \quad C^n_i = \begin{cases} \tilde{C}^n_i & \text{if } i \in A_0 \\ C^n_i & \text{if } i \in A_1 \\ C^n_i & \text{otherwise} \end{cases}
\]

Note that the reformulation is symmetrical with respect to the partition of \( \{1 \ldots n\} \).

If \( \tilde{\lambda} \) does not contain any global records (hence, neither do \( \tilde{\lambda} \), \( \bar{\lambda} \) and \( \lambda \) ) the claim obviously holds, because the module computations all are independent.

Next, split \( \lambda \) as \( \lambda_0 \cdot \lambda_1 \), where \( \lambda_1 \) is the smallest suffix of \( \lambda \) containing one global record, \( (p, q, \bar{a}, r, s, \text{ind}) \). By symmetry, there are only two cases: (1) \( p \) and \( r \) are in different partitions and (2) \( p \) and \( r \) are in the same partition. The strengthened form of the Lemma is needed in case \( \{p, r\} \nsubseteq A_0 \cup A_1 \).

Case 1) W.l.o.g., let \( p \in A_0 \) and \( r \in A_1 \). The splitting of \( \lambda \) induces splittings of \( \tilde{\lambda} \) and \( \bar{\lambda} \) into \( \lambda_0 \cdot \lambda_1 \) and \( \lambda_0 \cdot \tilde{\lambda}_1 \) such that for \( i = 0, 1 \): \( \lambda_i \downarrow_g j = \tilde{\lambda}_i \downarrow_g j \) if \( j \in A_0 \) and \( \lambda_i \downarrow_g j = \bar{\lambda}_i \downarrow_g j \) if \( j \in A_1 \) and \( \tilde{\lambda}_1 \) and \( \bar{\lambda}_1 \) are as small as possible. Define \( \bar{\lambda} \) to be the largest index such that \( \tilde{C}_0 \xrightarrow{\lambda_0} \tilde{C}_m \xrightarrow{\lambda_1} \tilde{C}_n \); likewise, define \( \bar{\lambda} \) and \( \bar{\lambda}_1 \) w.r.t. the latter two computations. Induction gives a computation \( C_0 \xrightarrow{\lambda_0} C_m \xrightarrow{\lambda_1} C_n \in \text{Comp}(P, \tau) \) such that \( \lambda_0 \downarrow i = \tilde{\lambda} \downarrow i \) for \( i \in A_0 \), \( \lambda_0 \downarrow i = \bar{\lambda}_0 \downarrow i \) for \( i \in A_1 \), \( \lambda_1 \downarrow i = \tilde{\lambda}_1 \downarrow i \) if \( i \notin A_0 \cup A_1 \), \( C_m^1 = \tilde{C}_m \) if \( i \in A_0 \), \( C_m^1 = \tilde{C}_m^1 \) if \( i \in A_1 \) and \( C_m^1 = \tilde{C}_m^1 \) otherwise. By definition of \( C_m \) (i.e., of \( \bar{\lambda} \) and \( \bar{\lambda}_1 \)) a transition to \( C_{m+1} \) is possible producing the global record in \( \bar{\lambda}_1 \), where \( C_{m+1}^1 = C_{m+1}^1 \) for \( i \notin \{p, \tau\} \), \( C_{m+1}^p = \tilde{C}_{m+1}^p \) and \( C_{m+1}^r = \tilde{C}_{m+1}^r \). The remainder of the three computations (if any) are independent and hence can be grafted onto \( C_{m+1} \): first all the steps involving modules (whose indices are) in \( A_0 \) from computation 1; then the steps involving modules in \( A_1 \) from the second one; and finally the steps in the remaining modules from the third computation. This results in a computation \( C_0 \xrightarrow{\lambda_0} C_m \xrightarrow{\lambda_1} C_n \in \text{Comp}(P, \tau) \).

By construction, \( C_n \) and \( \lambda_1 \) (hence \( \lambda_0 \cdot \lambda_1 \)) satisfy the conditions of the Lemma.

Case 2) W.l.o.g., let \( p, r \in A_0 \). As in case 1, the label sequences \( \lambda \) and \( \tilde{\lambda} \) can be split, which also determines \( \bar{\lambda} \) and \( \bar{\lambda}_1 \). Since the second computation is not involved in the last communication, I can take \( \lambda_0 = \bar{\lambda} \), \( \lambda_1 = \varepsilon \) and \( \bar{\lambda}_1 = \bar{\lambda} \). Note that \( \lambda_0 \downarrow_g i = \tilde{\lambda} \downarrow_g i \) for \( i \in A_1 \). The rest of the argument is as in the first case.

The strengthened form of the Lemma together with its proof show the essential triviality of the global merging Lemma: a transition label sequence really determines the complete computation. An inspection of the proof also suggests that if \( A_0 \) and \( A_1 \) are singleton sets (or empty) it suffices to assume local instead of global reachability for the \( A_0 \) and \( A_1 \) computations. In fact, the following special case is worth recording:

4–7 LEMMA. With notation as above, assume that
- \( (h, \ell) \) is \( (M_l, r, K, \nu, \sigma, \bar{\lambda}) \)-ir,
- \( (\ldots) \) is \( (P, \tau, \sigma, \lambda) \)-gr and
- \( \tau \uparrow V_l = \tau \uparrow V_l \) and \( \lambda \downarrow_g l = \bar{\lambda} \).

Then \( (h, \ell) \) is \( (P, \tau, \nu, \sigma, \lambda) \)-gr.

PROOF. The proof is in fact very easy and does not require an induction. Just take the global computation, \( C_0 \xrightarrow{\lambda} C_n \in \text{Comp}(P, \tau) \) and remove all transitions involving \( M_l \). In their place,
substitute the transitions from $C_0 \xrightarrow{\lambda} C_m \in \text{Comp}(M_1, \tau, K)$. Because in both computations $M_1$ starts in the same state and because $\lambda : q \mapsto \lambda$, the resulting computation is in $\text{Comp}(P, \tau)$ and shows the required global reachability.

4–8 Observation. Local and global reachability are semi computable relations.

5 Specifications and Proofrules

5.1 Specifications and their interpretation

5.1 DEFINITION (Specifications). Let $T$ be a $CM^*(\Sigma)$-statement or procedure, $M_i$ a module and $P$ a program; $p, q, MI \in L(\Sigma)$. Specifications are of one of the following three forms:

• (1) $(CA, WA, CO, MI | \{p\}T\{q\})$ or (2) $(CA, \emptyset, CO, MI | \{p\}M_i\{q\})$, where ($T$ stands for $T$ or $M_i$)
  
  - $CA \subseteq \{\ell : p \mid \ell \text{ labels a closing bracket in } T, \ p \in L(\Sigma)\}$
  - $WA \subseteq \{\ell : p \mid \ell \text{ labels the rear of a wait in } T \text{ or } T \equiv T'. \ell, \ p \in L(\Sigma)\}$
  - $CO \subseteq \{\ell : p \mid \ell \text{ labels an opening bracket, a call or the front of a }$
  wait in $T, \ p \in L(\Sigma)\}$

  - in case (2),
    - $FV(MI) \cap L_i = \emptyset$,
    - for all $\ell : p$-term: $FV(p) \cap L(\ell) \subseteq L(\ell)$ and
    - any $ic. \in Var^{IC}$ that appears in any assertion refers to a procedure in $M_i$; i.e., has the form $ic.a_i$.

  - if $T$ is a procedure with formal parameters, $u$, then $FV(p, q) \cap \{u\} = \emptyset$

• (3) $(\emptyset, \emptyset, \emptyset, \text{true} \mid \{p\}P\{q\})$

5.2 DEFINITION. Let $A \subseteq \{\ell : p \mid \ell \in Lab, \ p \in L(\Sigma)\}$

• $A(\ell) = \bigwedge \{p \mid \ell \in A\} \in L(\Sigma)$. (Note that $\bigwedge \emptyset \equiv \text{true}$).

• $A$ is disjoint if $\nexists \ell \in Lab, p, q \in L(\Sigma)$ such that $\{\ell : p, \ell : q\} \subseteq A$ and $p \neq q$.

Intuitively, a formula like $\ell : p$ is true in configuration-state either if control is not at the $\ell$-labeled point, or $p$ is satisfied in the (local + global) state at such a point. The meaning of a specification for $T$ is, that on any execution sequence of $T$ that starts in a state satisfying $p$ and for which $CA$ and $WA$ are true in every configuration-state, $CO$ will be true in the last configuration state of the sequence, $MI$ will hold if it is a waiting point and $q$ will hold if $T$ terminated. So, e.g. $(\emptyset, \emptyset, \text{true} \mid \{p\}S\{q\})$ is an ordinary partial correctness specification and (hence) clause 3 expresses the paper’s basic interest in partial correctness properties.

This notion of specification is essential for syntax-directedness. The communication-assumption, $CA$, waiting-assumption, $WA$, and commitment, $CO$, make explicit (1) the various assumptions about the environment’s behaviour upon which validity of the specification (i.e. $CO$ and $q$) depends and (2) the behaviour to which the statement commits, necessary to validate the environment’s assumptions. Finally, there is a module-invariant, $MI$, that characterizes the (global) module state at waiting points; hence the states in which procedures start executing.
5–3 **DEFINITION** (satisfaction and validity). Let $\Sigma$ be a signature and $A$ a $\Sigma$-structure; $T$ a $CM^*(\Sigma)$-statement, procedure, module or program, $p \in L(\Sigma)$, $A \subseteq \{ \ell : p \mid \ell \in Lab, p \in L(\Sigma) \}$ and $\delta$ a configuration-state $\{(a_i, \theta_i, 0, \theta_i, 1, \ldots, \theta_i, n_i, \sigma_i) \mid i = 1..m \}$.

Let $\bar{\sigma} = \bigcup_{i=1}^{n} \sigma_i$ and $\bar{\nu} = \bigcup_{i=1}^{m} \nu_{i,a_i}$, $a_i \neq -1$, $i = 1..m$.

- $A, \delta \models p$ iff $A, \bar{\sigma} \cup \bar{\nu} \models p$.
- $A, \delta \models A$ iff $a_i \neq -1 \Rightarrow A, \sigma_i \cup \nu_{i,j} \models \rho_{i,j}$ for $j = 0..n_i$, $i = 1..m$.
- $A, \delta \models^* A$ iff $A, \sigma_i \cup \nu_{i,j} \models \rho_{i,j}$ for $j = 0..n_i$, $i = 1..m$.

**Satisfaction** can be trivially extended to conjunctions of first order formulae and formulae of the form $A$. Validity is defined in the standard way.

- Let $\tilde{p} = \{ \sigma \mid A, \sigma \models p \}$ and $\tilde{A} = \{ C \mid A, s(C) \models A \}$,
  
  $\vdash A, (\delta_0 \cdots \delta_n, t) \models (CA, WA, CO, MI \mid \{p\}T\{q\})$ iff
  
  $(\delta_0 \cdots \delta_n, t) \in [T](\tilde{p}, \tilde{A} \cup \tilde{WA})$ and
  
  $A, \delta_0 \cdots \delta_n \models CO \& a_n = -1 \Rightarrow A, \delta_n \models MI \& t = T \Rightarrow A, \delta_n \models q$.

- $\models (CA, WA, CO, MI \mid \{p\}T\{q\})$ iff
  
  $\forall (\delta_0 \cdots \delta_n, t) \in [T] A, (\delta_0 \cdots \delta_n, t) \models (CA, WA, CO, MI \mid \{p\}T\{q\})$.

The definition itself is straightforward. Note that local states can only be specified by "labeled" formulae and that satisfaction of non-labeled formulae at waiting points does not involve the local state. The meaning of satisfaction of a labeled formula interacts with the definition of configuration state: remember that in a (module) configuration state, $\delta = (a, \theta_0, \ldots, \theta_m, \sigma)$, the label part of a local state, $\theta_i$, is included only if $a = i$ or $a = -1$. In other words

$A, \delta \models A$ iff $a \neq -1 \Rightarrow \sigma \cup \nu_a \models \rho_a$.

Hence, if $a \neq -1$ then the relations $\models$ and $\models^*$ coincide, but if $a = -1$ then $A, \delta \models A$ is vacuously true, whereas for $\models^* 1$ have that

$a = -1 \Rightarrow A, \delta \models^* A$ iff $\sigma \cup \nu_i \models \rho_i$ for $i = 1..m$.

Note that if $a = -1$ then $\rho_i \neq \emptyset$ for $i = 1..m$.

The definition of satisfaction can be turned around — as usual — and be used to characterize sets of states, respectively, configuration states by formulae, respectively, sets of labeled formulae. In the sequel, such correspondences will be implicitly understood and I shall write, e.g., $[S](p, CA)$.

---

2 Remember the assumption that states always have domains that contain all the appropriate variables.
5–4 **Observation.** Satisfaction is a computable relation. Non-validity is a semi-computable relation.

5.2 **The proof system, \(PS(T)\)**

Let \(T \subseteq L(\Sigma)\) for some signature \(\Sigma\). In the rules below, some of the premises are \(L(\Sigma)\)-formulae. The interpretation of such a rule — as usual — is that it can be applied provided every \(L(\Sigma)\)-formula among its premises is in \(T\).

The proof system consists of the following rules and axioms.

5.2(1.) **assignment axiom.**

\[
\{\emptyset, \emptyset, \emptyset, \text{true} | \{p[e/x]\}x := e(p)\}
\]

5.2(2.) **wait axiom.**

\[
\frac{p \land \neg MI}{\{0, \{\ell : r\}, \{\ell : q\}, MI | \{p\} \ell \text{wait}.\ell'\{r\}}
\]

5.2(3.) **call rule.**

\[
\frac{\{0, 0, 0, \text{true} | \{p\} S_1(\forall \neq q), \{0, 0, 0, \text{true} | \{q\} S_2\{s\}\}}{\{\ell'' : r\}, \emptyset, \{\ell : p, \ell' : q\}, \text{true} | \{p\} S_1; \ell'.\text{call} M_1, a_1(\ell' \# \emptyset); S_2; \ell''; (r \land s)}
\]

5.2(4.) **sequential composition rule.**

\[
\frac{\langle CA_1, WA_1, CO_1, MI_1 | \{p_i\} S_1\{q_i\} \rangle, i = 1, 2, q_1 \rightarrow p_2}{\langle CA_1 \cup CA_2, WA_1 \cup WA_2, CO_1 \cup CO_2, MI_1 \lor MI_2 | \{p_1\} S_1; S_2\{q_2\}\rangle'}
\]

provided that \(CA_1 \cup CA_2, WA_1 \cup WA_2\) and \(CO_1 \cup CO_2\) are disjoint.

5.2(5.) **if rule.**

\[
\frac{\langle CA_1, WA_1, CO_1, MI_1 | \{p \land \neg b\} S_1\{q\} \rangle, \langle CA_2, WA_2, CO_2, MI_2 | \{p \land \neg \emptyset\} S_2\{q\} \rangle}{\langle CA_1 \cup CA_2, WA_1 \cup WA_2, CO_1 \cup CO_2, MI_1 \lor MI_2 | \{p\} \text{if } b \text{ then } S_1 \text{ else } S_2 \text{ fi}(q)\rangle'}
\]

provided that \(CA_1 \cup CA_2, WA_1 \cup WA_2\) and \(CO_1 \cup CO_2\) are disjoint.

5.2(6.) **while rule.**

\[
\frac{\langle CA, WA, CO, MI \mid \{p \land b\} S\{p\}\rangle}{\langle CA, WA, CO, MI \mid \{p\} \text{while } b \text{ do } S \text{ od}\{p \land \neg b\}\rangle}
\]

5.2(7.) **initial statement rule.**

\[
\frac{\langle CA, WA, CO, MI \mid \{p\} S\{MI\}\rangle}{\langle CA, WA \cup \{\ell : q\}, CO, MI \mid \{p\} S.l\{q\}\rangle'}
\]

provided \(WA \cup \{\ell : q\}\) is disjoint.

5.2(8.) **procedure rule.**

\[
\frac{\langle \emptyset, \emptyset, \emptyset, \text{true} | \{p\} S_1\{q\}, \langle CA, WA, CO, MI \mid \{q \land \emptyset\} S\{s\} \rangle}{\langle \emptyset, \emptyset, \emptyset, \text{true} | \{s\} S_2\{t\}\rangle, t \rightarrow MI}
\]

\[
\langle CA \cup \{\ell : r\}, WA, CO \cup \{\ell' : s\}, MI \mid \{p\} a_1(\ell' \# \emptyset); S_1; \ell'; (s_2\{t\}\rangle'
\]

provided \(\text{FV}(p, t) \cap \{\emptyset, \emptyset\} = \emptyset\) and \(CA \cup \{\ell : r\}\) and \(CO \cup \{\ell' : s\}\) are disjoint.
5.2(9.) module rule.

Let the module $M_i$ be declared as

\[
M_i :: \alpha_i(u_i \# v_i) : [: S_i]
\]

\[
\ldots
\]

\[
\alpha_k(u_k \# v_k) : [: S_k]
\]

\[
[S_0, \ell_0]
\]

Then

\[
\begin{align*}
(C_{A_j}, WA_j, CO_y, MI & | \{MI\} a_j'(u_j \# v_j) : [S_j] \{MI\}), \quad j = 1, \ldots, k \\
(C_{A_0}, WA_0, CO_0, MI & | \{p \land IN\} S_0 \{MI \land WA_0(\ell_0)\}), \quad MI \land WA_0(\ell_0) \to q \\
\bigcup_{j=0}^{k} WA_j & \neq (C_{A_j}, WA_j, MI, \{u_j, v_j\}, a_j'(u_j \# v_j) : [S_j, S_j]), \quad j = 1, \ldots, k \\
\bigcup_{j=1}^{k} WA_j & \neq (C_{A_0}, WA_0, false, \emptyset, S_0)
\end{align*}
\]

for every $\ell$wait.$\ell'$ in $M_i$:

\[
\bigcup_{i=0}^{k} CA_i, \emptyset, \bigcup_{i=0}^{k} CO_i, MI | \{p\} M_i(q),
\]

provided $\bigcup_{j=0}^{k} CA_j$, $\bigcup_{j=0}^{k} WA_j$ and $\bigcup_{j=0}^{k} CO_j$ are disjoint and where

- $IN \equiv \bigwedge \{ic.a_j = 0 \mid j = 1 \ldots n_i\}$.

Let $A = \{\ell : p \mid \ell \in Lab, p \in L(\Sigma)\}$. Then the expression

\[
A \neq (CA, WA, p, z, S)
\]

stands for the set of interference freedom specifications

\[
\{(CA, WA(q'), CO, true | \{p'\}S(q')) \mid \ell : q \in A\}
\]

where

- $q' \equiv q[\bar{y}/z]$ ($\bar{y}$ does not appear free in $CA$, $WA$, $p$, $q$ or $S$),
- $p' = p \land q'$,
- $WA(r) \equiv \{l' : WA(\ell') \land \pi \land ic.a_j \geq N \mid l'$ labels the rear of a wait, in $S$; $FLB(a_j) = FLB(S)$ for $j > 0$ and if $\ell \in FLB(a_j)$ then $N = 2$ else $N = 1\}$
- $CO \equiv \{\ell : q' \mid \ell$ labels the front of a wait$\}$,

5.2(10.) program rule.

\[
(C_{A_i}, 0, CO_i, MI_i | \{p_i\} M_i(q_i)), \quad i = 1, \ldots, n
\]

\[
\operatorname{Coop}((C_{A_i}, 0, CO_i, MI_i | \{p_i\} M_i(q_i)) \mid i = 1, \ldots, n), GI
\]

\[
(0, 0, 0, true | \{p_1 \land \cdots \land p_n \land GI\} [M_1 \mid \cdots \mid M_n] \{q_1 \land \cdots \land q_n \land GI\})
\]

provided

- $\bigcup_{i=1}^{n} CA_i$, $\bigcup_{i=0}^{n} WA_i$ and $\bigcup_{i=1}^{n} CO_i$ are disjoint
• $FV(\text{CA}_i, \text{CO}_i, \text{MI}_i, p_i, q_i) \cap V_j = \emptyset$ for $i \neq j$

• no variable free in $GI$ appears on the left-hand side of any assignment outside a bracketed section in any $M_i$ nor as a formal parameter of any call or procedure.

The expression

$$\text{Coop} \left( \{ (\text{CA}_i, \text{WA}_i, \text{CO}_i, \text{MI}_i, \{ p_i \} M_i, \{ q_i \} ) \mid i = 1, \ldots, n \} , GI \right)$$

stands for the set of cooperation specification pairs

$$\langle \emptyset, \emptyset, \emptyset, \text{true} \mid \{ \text{CO}_i(t) \land \text{MI}_j \land GI \} S_1 ; c.a_k := ic.a_k' + 1 ; S'_1[.] \{ \text{CA}_j(t')[.] \land GI \} \rangle$$

and

$$\langle \emptyset, \emptyset, \emptyset, \text{true} \mid \forall \exists \text{CO}_i(t) \land \text{CO}_j(t)[.] \land GI \} S'_2[.] ; ic.a_k := ic.a_k' - 1 ; S_2 \rangle$$

{CA}_i(t) \land GI \rangle$$

where $[,] \equiv [\varepsilon, \varepsilon/\emptyset, \emptyset]$, for any matching call-procedure pair

$t.(.; S_1; \ell.\text{call} M_j.a_k(\#\#); S_2; \ell.)$ in $M_i$ and

$a_k'(\emptyset, \emptyset) : [S'_1[.]; S_2[.] ; \ell.]$ in $M_j$

5.2(11.) consequence rule.

$$(\text{CA}, \text{WA}, \text{CO}, \text{MI} | \{ p \} S(q)) \Rightarrow p' \rightarrow p, q \rightarrow q'$$

\forall t \in FLB(S) : \text{CA}(t) \rightarrow \text{CA}(t'), \text{WA}(t) \rightarrow \text{WA}(t'), \text{CO}(t) \rightarrow \text{CO'}(t)$$

if $S$ is not a statement or contains a wait: $MI \rightarrow MI'$

$$(\text{CA}', \text{WA}', \text{CO}', \text{MI'} | \{ p' \} S(q'))$$

5.2(12.) substitution rule.

$$(\text{CA}, \text{WA}, \text{CO}, \text{MI} | \{ p \} S(q)) \Rightarrow (\text{CA}[t/z], \text{WA}[t/z], \text{CO}, \text{MI} | \{ p[t/z] \} S(q))$$

provided $z \notin FV(\text{CO}, \text{MI}, q, S)$.

5.2(13.) auxiliary variable rule.

Let $AV$ be a set of variables such that $z \in AV \Rightarrow z$ appears in $S'$ only in assignments, $y := t$, where $y \in AV$ or as formal value parameter in a procedure declaration.

$S$ is obtained from $S'$ by deleting all assignments to variables in $AV$ and all occurrences as value parameter in a procedure declaration together with the corresponding actual parameters in the syntactically matching calls.

$$(\text{CA}, \text{WA}, \text{CO}, \text{MI} | \{ p \} S'(q))$$

$$(\text{CA}, \text{WA}, \text{CO}, \text{MI} | \{ p \} S(q))$$

provided $FV(q, \text{CO}, \text{MI}) \cap AV = \emptyset$.

5.2(14.) label (and bracketing) rule.

$$(\emptyset, \emptyset, \emptyset, \text{true} | \{ p \} S'(q))$$

$$(\emptyset, \emptyset, \emptyset, \text{true} | \{ p \} S(q))$$

provided $S$ is obtained from $S'$ by deleting every bracket or label.

Concluding this section are the two theorems proof of which justify the paper.

Note that if $S$ is a statement but does not contain a wait, so that no waitingpoint is reached while executing $S$, one may take an arbitrary $MI'$.
5–5 Theorem (Soundness). Let $A$ be a $\Sigma$-structure and $T \subseteq Th(A)$. $P$ is a $CM(\Sigma)$-program. Then

$$\vdash_{PS(T)} \langle \emptyset, \emptyset, \emptyset, true \mid \{p\} P\{q\} \rangle \Rightarrow A \models \langle \emptyset, \emptyset, \emptyset, true \mid \{p\} P\{q\} \rangle$$

5–6 Theorem (Completeness). Let $\Sigma$ be the signature of Peano-arithmetict and $N$ the standard model. Then

$$N \models \langle \emptyset, \emptyset, \emptyset, true \mid \{p\} P\{q\} \rangle \Rightarrow \vdash_{PS(Th(N))} \langle \emptyset, \emptyset, \emptyset, true \mid \{p\} P\{q\} \rangle$$

5.3 A substitution lemma

For the soundness of the program rule and for completeness for program specifications, some results on substitutions are needed to relate the value assignments at the start and end of procedure calls with the syntactic substitution in the cooperation specifications.

5–7 Lemma (The substitution lemma). Let $S, S'$ be $CM^s(\Sigma)$-statements not containing call or wait-statements. Let $u, v, \xi \subseteq Var$, $\varepsilon \subseteq Tm(\Sigma)$ and $p, q \in L(\Sigma)$ be such that $\{\xi\} = |\varepsilon|$, $|u| = |v|$, the variables in $u$ do not appear as left-hand-side of any assignments in $S$ and the variables in the lists $u, v$ and $\xi$ are pairwise disjoint. Additionally, assume that the following conditions hold:

1. $\forall \varepsilon \subseteq Tm(\Sigma) \forall i \in \{u, v\} : FV(p) \cap \{\varepsilon, i\} \cap FV(q) = \emptyset$ and $\langle FV(S') \cup \{u, v\} \rangle \cap (FV(\varepsilon) \cup \varepsilon) = \emptyset$. Then

$$[(\cdot) = (\varepsilon, \varepsilon/\xi, v)]: \begin{cases} 1. \quad A \models \{p\} S; S'[:q:] \iff A \models \{p\} S; u, v := E, \varepsilon; S'\{q\} \\ 2. \quad A \models \{p[:\cdot]\} S'[:\cdot]; S\{q\} \iff A \models \{p \land u = e\} S'[:\cdot] ; \varepsilon := \varepsilon; S\{q\}, \text{provided } \varepsilon \cap FV(p) = \emptyset. \end{cases}$$

The proof of this Lemma is delegated to the Appendix.

6 Soundness

Validity of rules is defined as usual: validity of the premisses implies validity of the consequence. Fix some $\Sigma$-structure $A$ and $T \subseteq Th(A)$.

6–1 Lemma. The axioms 1 and 2 and the rules 3,..., 14 are valid.

Although this paper's specifications are more detailed than partial correctness specifications, the validity proofs for some of the axioms and rules (e.g., sequential composition, if and while rules, consequence and substitution rules, the auxiliary variable rule) are completely analogous to the usual proofs; see e.g. [deBBO] and [Apt83]. For the assignment statement this is obvious, since its execution sequences do not include labels or waiting points. For, e.g., the sequential composition rule it is because assumptions and commitments cannot refer to labels in the component they are not associated with. In the proof below, only the non-trivial and new cases will be tackled.

Proof. [of Lemma 6–1]

Generically, for any $S_0^\delta$ considered below, let $(\delta_0^{\alpha, \beta}, \ldots, \delta_n^{\alpha, \beta}, t) \in [S_0^\delta]$ where $\delta_0^{\alpha, \beta} = s(SC_{\alpha}(S_0^\delta))$. The notational conventions of Section 3 will be heavily used. In the proofs, prefixes $(\delta_0^{\alpha, \beta} \cdot \ldots \cdot \delta_i^{\alpha, \beta}, 1)$ of the above sequence will be considered, too. Note that if the initial state is not constrained, any sequence in $[S_0^\delta]$ can be obtained as a suffix of a sequence as above. Usually, statements will be embedded within other statements; say, $S_0 \equiv S_1; S_2$. In such cases, the following
"aliasing" convention applies: the configuration-state sequence associated with $S_i$ is $\delta^i_0 \cdots \delta^i_n$, for $i = 0, 1, 2$. We have that $\delta^0_0 = \delta^1_0 = \delta^2_0, \ldots, \delta^0_n = \delta^1_n = \delta^2_n, \delta^0_{n+1} = \delta^1_{n+1}, \ldots, \delta^0_{n+k} = \delta^2_{n+k}$. I shall mostly ignore the terminal states in completed computation sequences, since it is usually the last but one state that is needed in the arguments below.

6-1(1) wait axiom: $S \equiv \ell . \text{wait} . \ell', WA \equiv \{ \ell : r \}$ and $CO \equiv \{ \ell : q \}$.

By Definition 3-9, $\delta_0 = (0, (\Omega, \ell), \sigma), \delta_1 = (-1, (\Omega, \ell'), \sigma)$, and $\delta_3 = (0, (\Omega, 0), \sigma')$. First assume that $\delta_0 \models p$. Then $\delta_0 \models CO$ and $\delta_1 \models MI$ because $p \rightarrow CO(\ell) \wedge MI$. Note that $\delta_2 \models WA$ is trivially true and that $\delta_3 \models WA$ holds by assumption. Next, $\delta_2 \models WA$ implies $\delta_3 \models r$. Here, I ignored the terminating configuration, $\delta_4 = (0, \sigma')$ as explained above. Obviously, I also have that $\delta_4 \models r$.

6-1(2) call rule: $S' \equiv \ell . \text{call} M_i \cdot a_j (\bar{e} = \bar{\bar{e}}), S \equiv \ell . (S_1 ; S_2 ; \ell'), CA \equiv \{ \ell' : r \}$ and $CO \equiv \{ \ell : p, \ell' : q \}$.

Again by Definition 3-9, $\delta^0_0 = (0, (\Omega, \ell), \sigma), \delta^0_1 = (0, (\Omega, \ell'), \sigma), \delta^0_2 = (0, (\Omega, 0), \sigma')$ and $\delta^2_n = (0, (\Omega, 0), \sigma^2)$ where $\sigma' = \sigma(\bar{a} / \bar{x})$ and $\bar{a} \subseteq |A|$. Now, if $\delta^0_0 \models p$ then $\delta^0_0 \models CO$. Since $S_1$ does not contain any labels, the next point of interest is the front of $S'$. By validity of the first premiss of the call rule, $\delta^0_1 \models \forall \bar{e} q$ (where I assume that $S_1$ terminates as there is nothing to prove otherwise), so that also $\delta^0_2 \models \forall \bar{e} q$ and, hence, $\delta^0_0 \models q$. This implies that $\delta^0_0 \models CO, \delta^0_1 \models CO, \delta^0_2 \models q$ and $\delta^0_0 \models q$ (as $\delta^0_0 = \delta^0_0$). Validity of the second premiss yields $\delta^0_2 \models s$, hence $\delta_n \models CA(\ell') \wedge s$.

6-1(3) procedure rule: Apply the reasoning of (2) thrice.

6-1(4) initial statement rule: This is a direct consequence of the fact that every computation sequence of $[\ell, S]$ can be obtained from one of $S$, except for the sequence "starting at $\ell"$. This case is covered by the change of WA.

6-1(5) module rule: As above, assume that the premisses of the rule hold. The following stronger statement will be proved:

For any $C_0 \frac{\lambda_1}{\lambda_1} \cdots \frac{\lambda_n}{\lambda_n} C_n \in \text{Comp}(M_i, p, \bigcup_{i=0}^{k} CA_i)$ with $\delta_n = s(C_n)$:

\[ \delta_n \models \bigcup_{i=0}^{k} (CO_i \cup WA_i), \quad a_n = -1 \Rightarrow \delta_n \models MI \] and $C_n \in TC \Rightarrow \delta_n \models q$.

Note that $s(C_0) \equiv \text{IN}$ by Definition 3-7 and that $\delta_n \models CO_i \iff \delta_n \models CO_i$. Hence, I can concentrate on $WA_i$. Next, observe that $MI \wedge WA_0(\ell_0) \rightarrow q$. This means that $C_n \in TC \Rightarrow \delta_n \models q$ automatically follows from the first two claims and the fact that the $k + 1$st premiss of the rule establishes $WA_0(\ell_0) \wedge MI$ as post condition.

The proof uses induction on the number, $L$, of $\delta_i$'s with $a_i = -1$ for $i < n$. The computations in $a^*_j$ will be superscripted with $j$; those in the initial statement with 0. Define $\delta_i = s(C_i)$ for $i = 1..n$ and let $t = T$ if $C_n \in TC$ and $t = \bot$ otherwise.

$L = 0$ So, the computation is in fact within the initial statement. Validity of the initial statement specification implies that $\delta_n \models CO_0$ and $\delta_n \models MI$ in case $a_n = -1$, since by assumption $\delta_0 \models p \wedge \text{IN}$ and $\delta_1 \models CA_0$ for $0 \leq i \leq n$. Observe that $\delta_n \models \bigcup_{i=1}^{n} (WA_i \cup CO_i)$ trivially holds in this case and that $\delta_n \models WA_0$ either holds trivially (in case $a_n \neq -1$) or follows from the last premiss of the module rule.

$L > 0$ Let $n$ be the largest index $< n$ such that $a_n = -1$. Let $\bar{k} = a_{n-1}$ and $(l, \bar{k}) = Id_{a_{n-1}, l}$, 23
and let \( k = \alpha +=1 \) and \((l, h) = Id_{n+k}\). The situation is depicted in Figure 1 (when \( \alpha_n \neq -1 \)). Extract the \( \alpha'_h \)-computation leading to the \( k \)-th LC in \( C_n \) from this sequence:

First, inductively define a sequence \( \alpha_0, \alpha_1, \ldots, \alpha_n \) that traces the sequence of LC's that evolve into \( LC_{n,k} \):

- \( \alpha_n = k \)
- \( 0 < i < n - 1: \alpha_i = -1 \) if \( \alpha_{i+1} = -1 \) or \( C_i \) has less than \( \alpha_{i+1} \) LC's,
- \( = \alpha_{i+1} + 1 \) if \( \alpha_i \neq -1, \alpha_{i+1} = -1, \alpha_i < \alpha_{i+1} \) and \( C_i \) has more LC's than \( C_{i+1} \),
- \( = \alpha_{i+1} \) otherwise

This definition sets \( \alpha_i = -1 \) if the correct instance of \( d_h^{k} \) still is to be created and sets \( \alpha_i = \alpha_{i+1} + 1 \) if some instance terminates.

Next, define a sequence \( i_0, i_1, \ldots, i_n \) inductively as follows:

- \( i_0 \) is the index \( t \) such that \( \alpha_0 = \alpha_1 = \ldots = \alpha_{t-1} = -1 \) and \( \alpha_t \neq -1 \),
- \( 0 < j < r: i_j = i_{j-1} + 1 \) if \( \alpha_{i_{j-1}} \neq -1 \) and \( \alpha_{i_{j-1}+1} = -1 \),
- \( = \) the smallest index \( t > i_{j-1} \) such that \( \alpha_t = \alpha_i \) otherwise

This sequence points to those MC's, \( C_i \), in which activity is (the second case) or just ceased to be (the first case) within the LC pointed to by \( \alpha_i \).

The \( \alpha_h \)-computation can be extracted in the same way, resulting in sequences \( j_0, j_1, \ldots, \alpha_n \). Note that here the sequence ends in \( C_n \).

First I prove that

\[ A: \delta_n \models^* WAh \cup CO_h, \ \alpha_n = -1 \Rightarrow \delta_n \models MI. \]

By Definition 5-3, \( \delta_n \) can be replaced by \( s(LC_{n,k}) \).

Now, define \( \delta \) by \( \delta = n - 1 \) if \( t = \top \) and by \( \delta = n \) otherwise. Let \( \delta \) be the index such that \( j_\delta = n + 1 \) (note that \( \delta \) exists) and define a sequence of configuration states, \( \delta_\delta \), for \( \delta \leq i \leq \delta \) by:

\[ \delta_\delta = (p_{j_\delta}, \sigma_{j_\delta}, \sigma_{j_\delta}) \text{ where } p_{j_\delta} = -1 \text{ if } a_{j_\delta} = -1 \text{ and } p_{j_\delta} = 0 \text{ otherwise.} \]

Then, if \( h = 0 \)

\[ (\delta_\delta, \ldots, \delta_\delta, t) \models (CA_0, WAh, CO_h, MI | \{p \land IN\} s_0(MI \land WAh(t_0))) \]  (2)

\( r \) is implicitly determined by the condition that \( i_r = n \)
and, if \( h \neq 0 \)

\[
(\delta_1^h, \ldots, \delta_r^h, t) \models (CA_h, WA_h, CO_h, MI | \{MI\}d_h(u^\neq v) : [S_h]\{MI\})
\]

(3)

Suppose that \( \delta_1^h \models WA_h \) and \( \delta_1^h \models MI \) in case \( j_0 = \bar{n} + 1 \); i.e., in case the instance of \( \alpha_1^h \) was created in the \( C_n \rightarrow C_{n+1} \)-transition. Then, \( A \) would follow from satisfaction of (2) and (3) and the fact that the only resumption at a waiting point in the computation is "at" \( \delta_1^h = \varepsilon(LC_{n+1,k}) \).

Hence, there remains to show that

1. \( \delta_1^h \models WA_h \) if \( j_0 \neq \bar{n} + 1 \),
2. \( \delta_1^h \models MI \) if \( j_0 = \bar{n} + 1 \).

Two cases have to be distinguished.

(I) \( j_0 > i_\tau \) or \( k = k \). Here the easy cases are collected where no interleaving takes place: If \( j_0 > i_\tau \), this means that the instance pointed to by the \( j \)-sequence is created (the moment) after the other instance terminates. If \( k = k \) and \( j_0 < i_\tau \), this means that control remains in the same instance when passing the waiting point, so that \( j_h = i_k \) for \( k \leq r \). Let \( \tau \) be the largest index such that \( i_{\tau - 1} < \bar{n} \) and \( a_{i_{\tau - 1}} = -1 \) or 1 if such an \( \tau \) does not exist. Define configuration states, \( \delta_1^h \) by \( \delta_1^h = (p_1, \theta_1, a_{ij}, \sigma_i) \) where \( p_1 = -1 \) if \( a_{ij} = -1 \) and \( p_1 = 0 \) otherwise, for \( \tau \leq i \leq r \). It is straightforward to verify that if \( h = 0 \)

\[
(\delta_1^h \cdot \ldots \cdot \delta_{\tau}^h, t) \models^* (CA_0, WA_0, CO_0, MI | \{p \land IN\}S_0[MI \land WA_0(t_0)])
\]

(4)

and otherwise

\[
(\delta_1^h \cdot \ldots \cdot \delta_{\tau}^h, t) \models^* (CA_h, WA_h, CO_h, MI | \{MI\}S_h\{MI\})
\]

(5)

for some \( t \).

By assumption \( \delta_1^h \models p \land IN \) if \( h = 0 \) and \( \tau = 1 \); moreover, \( \delta_1^h \models CA_h \) for \( \tau \leq j \leq r \). Applying the induction hypothesis to \( (\delta_0 \cdot \ldots \cdot \delta_{\tau}^h, t) \in [(M_i \bigcap \bigcup_{i=0}^{k} CA_i)] \) yields \( \delta_1^h \models WA_h \) for \( \tau \leq j \leq r \) and \( \delta_1^h \models MI \) if \( h \neq 0 \) and \( \tau = 1 \). Note that \( \delta_1^h \models WA_h \), again, follows from the last premiss of the rule.

The claim now follows from validity of (4) and (5): first, \( \sigma_\tau^h = \sigma_1^h \) (i.e., \( \sigma_h = \sigma_{h+1} \)); whence \( \delta_1^h \models MI \) which completes the proof in case \( j_0 = \bar{n} + 1 \). Second, if \( j_0 \neq \bar{n} + 1 \) then \( h = k \) and, hence, \( \bar{n} = h \). This implies that \( \sigma_{\bar{n} - 1}^h = \sigma_{\bar{n}}^h \). Since \( \nu_0^h = \nu_1^h \), I have that \( \delta_1^h \models CO_h \) implies that \( \delta_1^h \models WA_h \) using the last premiss of the module rule.

(II) \( j_0 \leq i_\tau \) and \( k \neq k \). I.e., control passed a waiting point and switched to another already existing (!) \( LC \). Hence, a wait was encountered or the end of the initial statement or the end of a procedure instance.

To show: \( \delta_{n+1}^h \models WA_h \). For this, validity of the interference freedom specifications is needed.

So, let \( \rho_{n+1,k} = \ell \) (note that the \( LC \) is \( k \) and not \( \bar{k} \)). Let \( f \) be the cardinality of \( \text{Dom}(\nu_{n+1,k}) = \{x_1, \ldots, x_f\} \) and let \{\( y_1, \ldots, y_x \)\} be a collection of variables not part of the domain of any state appearing in any \( C_i \) for \( 0 \leq i \leq n \) and not appearing free in \( \bigcup_{i=0}^{k} CA_i, \bigcup_{i=0}^{k} WA_i, \bigcup_{i=0}^{k} CO_i, MI, p, q \) or \( M_i \). Observe that it suffices to show that

\[
(0, \theta_{n-1,k}, \sigma_{n-1} \{\nu_{n+1,k}(x_i)/y_i \; i = 1..f\}) \models \bar{q}.
\]

(6)
where $q = WA_h(l)[y_i/z_i, i = 1..f]$.

Again, let $\bar{r}$ be the largest index such that $i_\bar{r} < n$ and $a_{i_{\bar{r} - 1}} = -1$ or $1$ if this is impossible. Define $\nu = \Omega_1[y_{n+1,i}(z_i)/y_i, i = 1..f]$ and define a sequence of configuration states by $\delta_\nu = (p_{ij}, \theta_{i_j}, a_{ij}, c_{ij} \cup \nu)$ where $p_{ij} = -1$ if $a_{ij} = -1$ and $p_{ij} = 0$ otherwise, for $\bar{r} \leq j \leq r$. Then

$$\delta_\nu = (\delta_1 \cdots \delta_\nu, \bar{r}) \models (CA'_h, WA_h(q'), CO, true | \{p' \land q'\} S_h(q'))$$

for some $i$, where $q' = WA_h(l)[y_i/z_i, i = 1..f];$ $p' \equiv false$ if $h = 0$ and $p' \equiv MI$ otherwise. Observe that if $h = 0$ then $\bar{r} \neq 1$. Induction gives that $\delta_{i_{\bar{r} - 1}} \models* MI \land \bigcup_{i=0}^n WA_i;$ hence $\delta_\nu \models MI \land WA_h \land q'$. By definition $\delta_\nu \models CA_h (\bar{r} \leq j \leq r),$ so that I obtain

$$\delta_\nu = (\delta_1 \cdots \delta_\nu, \bar{r}) \in [S_h][p' \land q', CA_h \cup WA_h(q')]$$

Now, (7) gives $\delta_\nu \models CO$ and $\delta_\nu \models q'$ if $\bar{r} = T$. Hence, $\delta_{n+1} \models WA_h$.

B: $\delta_n \models* \bigcup_{i=1}^n WA_h$

If $a_n \neq -1$ and $a_{n-1} \neq -1$ this holds trivially. If this is not the case, induction gives $\delta_n \models* \bigcup_{i=1}^n WA_i$ and every $WA_i (i \neq h)$ must be shown interference free over the $\delta_i$-computation in $C_n \rightarrow* C_n$. This is fully analogous to the argument in case A-II and, hence, is omitted.

6-1(6) Program rule:

6-2 Definition. Acceptable configuration.

- A local configuration, $Id : (S, \theta),$ is acceptable if either
  - $S \equiv \ell.\text{rend}_{e,i,j}; S'$ or the following situations do not occur:
    - $S \equiv S'; \ell.\text{call}M_i, a_j(\ell \neq 0); S''$ and $S'$ does not contain an opening bracket,
    - $S \equiv S'; \ell.\ell; S''$ and $S'$ does not contain a call-statement, or
    - $S \equiv S'; \text{end}_{p,r,\ell}$ and $S'$ does not contain an opening bracket.

- A module configuration is acceptable if all its active LC's are

- A program configuration is acceptable if all its MC's are.

An inactive local configuration is always acceptable, since wait-statements never appear within bracketed sections. Hence, a configuration is acceptable if no local configuration is within a bracket section.

The following statement — implying soundness of the program rule — will be proved.

Suppose there is a program $P \equiv [M_1| \cdots | M_n]$ and there are $CA_i, CO_i, MI_i, p_i$ and $q_i$ ($i = 1..n$) such that the premisses of the program rule are valid. Then for any

$$C_0 \xrightarrow{\lambda_1} C_1 \xrightarrow{\lambda_m} C_m \in \text{Comp}(P, p_1 \land \cdots \land p_n \land G|),$$

where $\delta_i = s(C_i)$ for $0 \leq i \leq m$, $\delta_m \models* \bigcup_{i=1}^n CA_i, \delta_m \models G| if C_m is acceptable, and $C_m = TC_{\phi}(P) \Rightarrow \delta_n \models q_1 \land \cdots \land q_n \land G|$
For every \( \delta_i \), I can assume that \( \text{Dom}(\sigma_i^j) \cap V_k = \emptyset \) and (by definition) that \( \sigma_i^j \upharpoonright V = \sigma_i^k \upharpoonright V \) if \( V = \text{Dom}(\sigma_i^j) \cap \text{Dom}(\sigma_i^k) \) for \( k \neq j \) and for \( j, k = 1 \ldots n \). The proof is by induction on the computation length, \( m \).

\( m = 0 \) Then \( \delta_0 = \delta_m \), \( C_0 \) is acceptable and by assumption \( \delta_0 \models GI \). Note that \( CA_j (\alpha_{m,i} \delta_m) \equiv true \) for \( 1 \leq j \leq n \). Hence \( \delta_m \models \bigwedge_{i=1}^{n} CA_i \land GI \). Finally, \( C_0 \) cannot be a terminal configuration.

\( m > 0 \) If \( C_m \) is a terminal configuration, then \( \delta_m \models \bigcup_{i=1}^{n} CA_i \) is vacuously true. Since in this case \( C_{m-1} \) is acceptable too, induction implies \( \delta_{m-1} \models GI \), hence \( \delta_m \models GI \) as there is no (variable) state change involved in the \( m \)th \( CA \)-transition. The conditions on the assertions imply that \( \delta_k \models p_k \) and, using induction, that \( \delta_k \models CA_k \) for \( 0 \leq j < m \), \( 1 \leq k \leq n \). By projecting the computation sequence on the transitions of each of the individual modules, I may use validity of the module specifications to conclude that \( \delta_m \models q_k \) for \( 1 \leq k \leq n \). Because of the conditions on the module states and the assertions, I can conclude that \( \delta_m \models q_1 \land \cdots \land q_n \land GI \).

Now suppose that \( C_m \) is not a terminal configuration. Since \( \delta_m \models CA_k \) iff \( \delta_m \models CA_k \), I may assume that \( C_m \) is acceptable. Next, observe that because the free variables in \( GI \) may only be assigned to in bracketed sections, it is sufficient to show that \( GI \) is reestablished at the end of any bracketed section.

If \( C_{m-1} \) is acceptable then the result follows by induction. So assume otherwise. I.e., assume that \( C_{m-1} \) with \( \delta_m \models \neg 1 \), has \( \phi_{m,a_{m}} = t \) and \( t \) labels some closing bracket (in \( M_j \)). This implies that if \( \lambda_1 \cdots \lambda_m = \lambda \), then \( \lambda = \lambda' \cdot c \) with \( c \equiv (i, h, \bar{b}, j, k, \text{ind}) \) for some \( i, j, k, \text{h, ind} \) and \( \bar{b} \). The computation can be split as follows:

\[
C_0 \xrightarrow{\lambda' +} C_q \xrightarrow{c} C_{q+1} \xrightarrow{e} C_m
\]

There are two possibilities: Either \( c \) witnesses the start of a synchronization period between \( M_i \) and \( M_j \) or \( c \) witnesses the end of such a period. These cases are analyzed separately:

1. There are statements, \( \ell .(S_1 ; \ell .\text{call } M_j .a_k (\bar{t} \# \bar{v}); S_2 ; \ell ) \) in \( M_i \) and \( \alpha_k (\bar{u} \# \bar{v}) \equiv [S_1'; \ell '); S_2 ; \ell .(S_2; \text{end}; i, h, \text{a}) \), and \( \phi_{m,a_m} = \ell ' \).

This implies that there are configurations \( C_{p \cdot a_\ell} \) and \( C_{r \cdot a_\ell} \) such that \( C_{p \cdot a_\ell} \xrightarrow{\lambda''} C_{r \cdot a_\ell} \), \( \lambda'' \) is a postfix of \( \lambda' \), \( C_{r \cdot a_\ell} \equiv i, h, a : (\ell .(S_1 ; \ell .\text{call } M_j .a_k (\bar{t} \# \bar{v}); T_p , \phi_{p,a_\ell}); C_{q+1} \xrightarrow{e} C_r \) and \( C_{r \cdot a_\ell} \equiv j, k, b : (\ell '); S ; \ell .(S_2 ; \text{end}; i, h, \text{a}). \)

Claim: There is a computation \( \tilde{C}_0 \xrightarrow{\lambda' \cdot \ell} \tilde{C}_p \xrightarrow{c} \tilde{C}_{q+1} \xrightarrow{e} \tilde{C}_r \xrightarrow{e} \tilde{C}_m \) such that \( \tilde{C}_0 = C_0, \tilde{C}_m = C_m, \tilde{C}_p \) and \( \tilde{C}_r \) are acceptable, \( \tilde{C}_{p,a_j} \equiv C_{p,a_j} \), \( a_j = 1 \), \( \ell = \tilde{C}_{r,a_j} \equiv C_{r+1,a_j} \), \( \tilde{C}_{r,a_j} \equiv C_{r+1,a_j} \), \( \tilde{C}_{p,a_j} \equiv C_{p,a_j} \), \( \phi_{r,a_j} = \phi_{p,a_j} \) involves only \( M_i \)-transitions, \( \tilde{C}_{q+1} \xrightarrow{e} \tilde{C}_r \) only \( M_j \)-transitions and \( \tilde{C}_r \xrightarrow{e} \tilde{C}_m \) neither \( M_i \) nor \( M_j \)-transitions. Hence, \( \tilde{C}_{r,a_j} \equiv C_{r,a_j} \) and \( a_j = 1 \).

This claim follows trivially from the fact that \( C_m \) is acceptable and that in any computation, \( \tilde{C}_0 \xrightarrow{\lambda_1 \cdot \ell} \tilde{C}_k \xrightarrow{\lambda_1 \cdot \ell} \tilde{C}_l \), if on \( C_k \) \( \lambda_1 \cdot \ell \) no communications take place between two modules.
say $M_r$ and $M_s$, any ordering of transitions from $M_r$ and $M_s$ is accidental and can be changed. It suffices to show the Lemma w.r.t. this sequence.

Define $s(CA_k) = \delta_k$ for $0 \leq k \leq m$. By induction $\delta_p \models \bigcup_{i=1}^{n} CA_i \land GI$, which implies that $\delta_m \models \bigcup_{k \neq j} CA_k$, hence $\delta_m \models \bigcup_{k \neq j} CA_k$ because $FV(CA_k) \cap V = \emptyset$ for $j \neq k$ and $CA_i(\ell) = true$. It remains to show that $\delta_m \models CA_j \land GI$ and for this it suffices to show that $\delta_r \models CA_j \land GI$.

Now define configuration states $\delta_p$ and $\delta_r$ by

$$\delta_p = (0, (\Omega, \emptyset), \bigcup_{k=1}^{n} \sigma_k^{\ell} \cup \rho_i^{p,a_j} \cup \Omega^T)$$

and

$$\delta_r = (0, (\Omega, \emptyset), \bigcup_{k=1}^{n} \sigma_k^{\ell} \cup \rho_i^{p,a_j} \cup \rho_i^{p,a_j})$$

By definition, the right-hand sides are defined. Observe that $\delta_p \models CO_i(\ell) \land MI_j \land GI \Rightarrow \delta_p \models CO_i(\ell) \land MI_j \land GI$ and $\delta_r \models CA_j(\ell) \land GI \Rightarrow \delta_r \models CA_j(\ell) \land GI$.

As in the soundness proof of the module rule, extract from $\delta_0 \cdots \delta_m$ for $l = i, j$ the configuration state sequence $\delta_{k_0} \cdots \delta_{k_m}$ corresponding with the $M_l$-transitions in $\hat{C}_0 \cdots \hat{C}_p$. The $l$th premise of the program rule implies that $\langle \delta_{k_0}, \cdots \delta_{k_m} \rangle \models (\langle \emptyset, CA_i(\ell), MI_j \rangle \mid \{\ell \} \mid \{\emptyset \})$. Since by assumption $\delta_{k_0} \models p_i$ and by induction $\delta_{k_n} \models CA_i$ for $0 \leq v \leq m_i$, conclude that $\delta_{k_m} \models CO_i$ and $\delta_{k_m} \models MI_j$; hence that $\delta_p \models CO_i(\ell) \land MI_j \land GI$.

Next observe that there is a sequence $\langle \delta_0, \cdots \delta_d, \emptyset \rangle \in [S_1; IC_{A_i} := ic_{A_i} + 1; u, \emptyset := \epsilon; s; S_i']$ such that $\delta_0 = \delta_p$ and $\delta_d = \delta_r$. Validity of the cooperation specifications says

$$\models (\emptyset, \emptyset, \emptyset, true \mid \{CO_i(\ell) \land MI_j \land GI\}S_1; IC_{A_i} := ic_{A_i} + 1; S' \mid \{CA_j(\ell) \land GI\})$$

Substitution lemma 5-7(1) allows the statement-sequence in this specification to be replaced by $S_1; IC_{A_i} := ic_{A_i} + 1; u; \emptyset := \epsilon; s; S_i'$. Since $\delta_0 \models CO_i(\ell) \land MI_j \land GI$, this implies that $\delta_d \models CA_j(\ell) \land GI$ which concludes the proof.

(2) There are statements $\ell.(S_1; \hat{l}.call M_i.a_h(\ell \# \emptyset); S_2; \hat{l}.)$ in $M_j$ and $a_h(u \# \emptyset) : (\ell_h.S_1'; \ell'); S; \ell.'(S_1'; \ell_1')$ in $M_i$; $a_i' \neq -1$, $a_i' \neq -1$, $C_{\ell_i'} \equiv i, h, a : (end_{j,k,s}, \emptyset|\ell_1')$, $C_{\ell_i'} \equiv j, k, b : (\ell.rend_{i,k,s}, \emptyset|\ell_1')$, $T_{\ell_i'}(\emptyset|\ell_1')$ and $\rho_{m,a_i} l = \ell.$

The proof continues as a complete analog of the proof of case 1, except for the following: the cooperation specification that has to be used here, is

$$\models (\emptyset, \emptyset, \emptyset, true \mid \forall \emptyset \{CO_j(\ell) \land CA_i(\ell) \land GI\} S_2'; \emptyset; IC_{A_i} := ic_{A_i} - 1; S_2 \{CA_j(\ell) \land GI\})$$

Substitution lemma 5-7(2) implies

$$\models (\emptyset, \emptyset, \emptyset, true \mid \forall \emptyset \{CO_j(\ell) \land CA_i(\ell) \land GI\} S_2'; \emptyset; IC_{A_i} := ic_{A_i} - 1; S_2 \{CA_j(\ell) \land GI\})$$

Let $C_{\ell_{p,a_i}} \equiv (i, h, a : (\ell_p; S_2; end_{j,k,s}, \emptyset|\ell_1')$. Then, additionally, I must argue that $\nu_{\ell_{p,a_i}}(\emptyset) = \sigma_i^{\ell} \cup \rho_{p,a_i}^{\ell}(\ell)$. This, however, is easy because no $M_l$-transition occurred since the procedure instance was created and no $M_l$-transition will change the valuation of the variables in $\emptyset$.

\footnote{Remember that $\delta_{p,j} = -1$.}
6–3 THEOREM (Soundness theorem). Let \((CA, WA, CO, MI | \{p\}U\{q\})\) be any specification and \(T \subseteq Th(A)\). Then

\[ \vdash_{PS(T)} (CA, WA, CO, MI | \{p\}U\{q\}) \Rightarrow \mathcal{A} \models (CA, WA, CO, MI | \{p\}U\{q\}) \]

PROOF. The standard argument, using induction on the length of the proof and using Lemma 6-1.

7 Relative completeness

From now on, \(\Sigma\) denotes the signature of Peano-arithmetic (or some countable extension) and \(N\) is a standard model. Validity is relative to \(N\) and the proof system used is \(PS(Th(N))\).

7.1 Some definability results

7-1 THEOREM ([Wei87, Corollary 2.9.12]. Definability of recursive sets).
Let \(R \subseteq \omega\) be a recursive set. Then, there is a \(\phi_R \in L(\Sigma)\) such that \(\forall n \in \omega, n \in R \equiv \phi_R(n)\), where \(n\) is the term representing the integer \(n\) (i.e., \(n \equiv \text{succ}^n(0)\)) and \(\phi_R(n)\) is a sentence.

7-2 LEMMA. If \(R \subseteq St_n\) is computable, then there is a \(\phi_R \in L(\Sigma)\) such that \(\forall \sigma \in St_n, \sigma \in R \Rightarrow N, \sigma \models \phi_R\).

PROOF. For any \(\sigma \in St_n\), define \(\sigma \in (\omega^2)^n \equiv \omega^{2n}\) as the \(n\)-tuple of pairs \((a_0, \ldots, a_{n-1})\) satisfying for \(0 \leq i \leq n:

\[ a_i = \begin{cases} (i, v) & \text{if } z_i \in \text{Dom}(\sigma) \text{ and } v = \sigma(z_i) \\ (n, 0) & \text{otherwise} \end{cases} \]

Observe that \(\gamma : St_n \rightarrow \omega^{2n}\) is an injection. Let \(\prec \cdots \prec\) be the \((k-1)\text{-iterated pairing function}\) \(\omega^k \rightarrow \omega\) and let \(\pi^k_i (0 \leq i < k)\) be the associated projections.

Define \(\bar{R} \subseteq \omega\) by \((a_0, \ldots, a_{n-1}) \in R \iff < a_0 \succ \ldots \succ a_{n-1} \succ n \in \bar{R}\). Since \(\bar{R}\) is recursive (Church's thesis), there is a \(\phi_{\bar{R}} \in L(\Sigma)\) that defines it. Let \(\pi^k_i\) stand for the \(L(\Sigma)\)-formula that defines it. It is easy to show that the wanted formula, \(\phi_R\), is given by \(\exists y [\phi_{\bar{R}}(y) \rightarrow \bigwedge_{i=0}^{n-1} (\pi^k_i(y)) \neq n \rightarrow z_i = \pi^k_i(y))],\) where \(y \not\in Var_n\).

7-3 COROLLARY. Let \(Ms_n\) be the set of module specification states such that the set of variables that is valuated, is contained in \(Var_n\). If \(R \subseteq Ms_n\) is a computable set, then there is a \(\phi_R \in L(\Sigma)\) such that

\[ \forall \delta \in Ms_n : \delta \in R \iff \exists \bar{\delta} \in Ms_n \sigma[\nu] = \sigma[\nu] \& N, \bar{\delta} \models \phi_R \]

PROOF. Evident.

Note that in these lemma's, "recursive" can be replaced by "arithmetical" ([Wei87]). Definability as in Lemma 7-2 and Corollary 7-3 will be called representability. The representing formula for a module configuration state, \((a, \theta_1, \ldots, \theta_n, \sigma)\), does neither fix \(a\), nor \(\rho_1, \ldots, \rho_n\), nor the partition of \(Var_n\) into \(Dom(\sigma)\) and \(Dom(\nu_i)\) for \(i = 1 \ldots n\).
Facts:

1. For every specification, \( \langle CA, WA, CO, MI, \{p\}T(q) \rangle \), there is an \( n \in \omega \) such that the variables and formal parameters appearing (free) in the specification, is contained in \( \text{Var}_n \).

2. If \( \models \langle CA, WA, CO, MI, \{p\}T(q) \rangle \), then there is an a-priori upperbound, \( \bar{n} \), such that there is a proof of this specification for which any specification appearing in this proof has its free variables in \( \text{Var}_{\bar{n}} \).

Of course, this last fact is a consequence of the completeness proof. Inspection of this proof yields that a safe bound is \( 2m + n + \sum_{i=1}^{n} k_i \), where \( m \) bounds the cardinality of the set of variables in the specification to be proved, \( n \) is the number of modules and \( k_i \) is the number of procedures in the \( i \)-th module.

7-4 Lemma. Let \( \models \langle CA, WA, CO, MI, \{p\}T(q) \rangle \) and let all free variables be contained in \( \text{Var}_m \). If \( 6 \) is a configuration state, let \( \check{6} \) be the configuration state obtained by restricting every valuation of \( 6 \) to \( \text{Var}_m \). Then \( \models \langle CA, WA, CO, MI, \{p\}T(q) \rangle \) is equivalent with

\[
\forall (\delta_0 \cdots \delta_n, t) \in [T] \quad (\delta_0 \cdots \delta_n, t) \models \langle CA, WA, CO, MI, \{p\}T(q) \rangle
\]

Proof. Evident. \( \Box \)

The consequence of all this is, that given a valid specification, in its proof one can restrict oneself a priori to a finite set of variables. This allows the “completeness-assertions” to be defined and allows Lemma 7-3 to be used. In the representability definitions in the proof below it will be up to the reader to check that the sets to be represented are in fact arithmetical. These results are always straightforward consequences of the observations 3–13, 4.2 and 5–4.

From now on, every \( \text{CM}^e(\Sigma) \)-statement, procedure, module or program and every specification is assumed only to contain variables from the a priori fixed set \( \text{Var}_N \). Also, since \( < \cdots >_k \) is definable as a term ([Wei87]), it will be freely used in \( \text{CM}^e(\Sigma) \)-statements. Concatenation (i.e., pairing) of two sequences is denoted by \( h \cdot h' \) instead of by \( < h, h' > \). Finally, I shall write \( < \cdots > \) instead of \( < \cdots >_k \) and leave the determination of \( k \) to the context.

7.2 Completeness for statement and procedure specifications

7-5 Definition (weakest precondition).

If \( S \) is a statement or procedure, \( WP(CA, WA, CO, MI, q, S) \) represents the set

\[
\{ \delta_0 | \delta_0 = s(SC_0(T)) & \forall \delta_1, \ldots, \delta_n : (\delta_0 \cdots \delta_n, t) \in [T](CA \cup WA) \} \\
\delta_n \models CO & a_n = -1 \Rightarrow \delta_n \models MI & t = T \Rightarrow \delta_n \models q
\]

7-6 Lemma.

1. \( \mathcal{N} \models \langle CA, WA, CO, MI, \{WP(CA, WA, CO, MI, q, S)\}, S(q) \rangle \)

2. \( \mathcal{N} \models \langle CA, WA, CO, MI, \{p\}S(q) \rangle \iff \mathcal{N} \models p \rightarrow WP(CA, WA, CO, MI, q, S) \)

Proof. Directly from the definitions. \( \Box \)
For any $CM^*(\Sigma)$-statement, procedure, module or program, $T$, and for any specification, $(CA, WA, CO, MI \mid \{p\}T(q))$:

$$\vdash_{PS(TM(\Sigma))} (CA, WA, CO, MI \mid \{p\}T(q)) \Rightarrow \vdash_{PS(TM(\Sigma))} (CA, WA, CO, MI \mid \{p\}T(q)),$$

where

- $\overline{CA}$, $\overline{WA}$ and $\overline{CO}$ are obtained from $CA$, $WA$ and $CO$ by removing all labeled formulae, $t : p$, for which the label $t$ does not appear in $T$, and
- $\overline{MI} = \{ \text{true} \}$ if no waiting point occurs in $T$ otherwise

**Proof.** This is a trivial application of the consequence rule. $\square$

Specifications as on the left-hand-side of Lemma 7-7 are called minimal.

**7-8 Theorem (completeness).**

If $S$ is a $CM^*(\Sigma)$-statement or procedure, then

$$S \models (CA, WA, CO, MI \mid \{p\}S(q)) \Rightarrow \vdash_{PS(TM(\Sigma))} (CA, WA, CO, MI \mid \{p\}S(q))$$

**Proof.** Structural induction on $S$. Here too, only the representative cases will be treated. Because of Lemma 7-7, I can assume the specification to be minimal.

7-8(1) $S \equiv s := e$:

Observe that $WP(0,0,0,\text{true},q, S)$ represents the set $\{(0, (\Omega, \ell), \sigma) \mid \sigma(e/x) \models q\}$ and hence is equivalent with $q[e/x]$ ([deB80]). The assignment axiom gives $\vdash (0,0,0,\text{true} \mid \{q[e/x]\} : e \models q)$. By Lemma 7-6(2) the consequence rule can be used to obtain the required specification.

7-8(2) $S \equiv \ell.\text{wait.}\ell'$:

$WP(0, WA, CO, MI, q, S)$ represents the set $\{(0, (0,\ell), 0') \mid 0' = CO(\ell) \wedge MI\}$. Hence, Lemma 7-6(2) implies $\vdash p \rightarrow CO(\ell) \wedge MI$. Since by assumption $\vdash WA(\ell) \rightarrow q$, the wait and consequence rule can be used to obtain $\vdash (0, WA, CO, MI \mid \{p\}\ell.\text{wait.}\ell' \models q)$.

7-8(3) $S \equiv s.\text{callM,a;}(e \# f,i;S_2)$:

Define $q' \equiv CA(\ell') \rightarrow q$ and $q'$ is the weakest such formula. Define $r \equiv WP(0,0,0,\text{true},q',S_2)$ and $CO' \equiv \{\ell : p, \ell : r\}$. To show (1) $\vdash \{0,0,0,\text{true} \mid \{CO'(\ell')\}S_2\{q'\}}$ and (2) $\vdash \{0,0,0,\text{true} \mid \{r\}S_2\{\text{true CO'}\}(\ell')\}$. Validity of (1) follows from the definitions of $r$ and $CO'(\ell')$. For validity of (2), first note that a call acts (locally) as a random assignment, $\models \sigma$, so that $\models \forall \exists CO'(\ell') \rightarrow WP(0,0,0,\text{true},CO'(\ell'), \text{callM,a;}(e \# f))$. Then validity of the specification and the definition of $q'$ (hence of $CO'(\ell')$) gives validity of (2). Induction yields proofs of (1) and (2) (in $PS(Th(\Sigma))$). The call rule yields $\vdash (CA,0,CO,\text{true} \mid \{q\}S(q' \wedge CA(\ell']))$. By definition $\models CO'(\ell') \rightarrow CO(\ell'), CO'(\ell') \rightarrow CO(\ell')$ and $q' \wedge CA(\ell') \rightarrow q$. So a final application of the consequence rule suffices.

7-8(4) $S \equiv s.a[\# b] : \{S_1;\ell;S_2\}$:

Define $\overline{CA}$, $\overline{WA}$ and $\overline{CO}$ in the obvious way as those parts of the assumption and commitment pertaining to $S$. Since the formal parameters $\overline{u}$ and $\overline{v}$ do not appear outside $S$, $FV(p,q) \cap \{\overline{u}, \overline{v}\} = \emptyset$ may be assumed. Let $r \equiv WP(0,0,0,\text{true}, \overline{q} \wedge MI, S_2) \wedge CO(\ell')$ and $s \equiv WP(\overline{CA}, \overline{WA}, \overline{CO}, MI, r, S)$. Clearly $\models CO'(\ell') \rightarrow r \mid q \wedge MI \rightarrow MI \models \{r\}S_2\{q \wedge MI\}$ and $\models (CA, WA, CO, MI \mid \{s\}S(r)}$. Next, define $s' \equiv CA(\ell') \rightarrow s$. Then $\models s' \wedge CA(\ell') \rightarrow s$ and $\models (0,0,0,\text{true} \mid \{s\}S(\ell') \models q).$
by the same reasoning as in (3). Hence, induction allows the procedure rule to be used:

\[ \vdash (CA, WA, CO, MT | \{p\}S(q)) \]

\[ \square \]

7.3 Restricted completeness for module specification

To obtain completeness results in this case, auxiliary variables are needed that record the computation history. The reason for this is the necessity of using the local merging lemma in order to show validity of the interference freedom specifications. For the same reason, I cannot show general completeness: for that I would need to be able to distinguish between coexisting instances, which is not always possible. Hence, each procedure, \( a_j \), obtains two extra read-only parameters, \( m_j \) and \( i_j \), which are intended to be initiated in each instance so as to uniquely identify this instance. Specifically, they are instantiated to the indices of the calling module and procedure. This makes the local states of coexisting instances unique, provided the communication assumption, CA, expresses the above intention.

Below, I assume that to every label, \( \ell \), a unique non-zero integer is associated that is also denoted by \( l \); associate 0 with "no label". Also, assume that "in" and "te" stand for some arbitrary but different values.

7–9 DEFINITION. Let \( M_i \) be some \( CM^e(\Sigma) \)-module. Introduce variables, generically denoted by \( m_j, i_j, h_i, h_i \), such that \( m_j, i_j, h_i, h_i \in V \), for \( j = 1 \ldots m_i \). Let \( \{g\} = V \) and let \( \{w_j\} = L_{i,j} \cup \{m_j, i_j\} \). The module \( M'_i \) is defined as \( M_i \) except that

- any wait-statement, \( \ell \).wait.\ell' in any procedure \( a_j \) \((j \geq 0)\) is replaced by
  \[ h_i := h_i < l, j, m_j, i_j, w_j >, \ell, \ell >; \ell \].wait.\ell'

- any call-statement, \( \ell \cdot \langle S; \ell \cdot \text{call}M \cdot a_r(\ell \# \#); S'; \ell'' \cdot \rangle \), in any \( a_j \) \((j \geq 0)\) is replaced by
  \[ \ell \cdot \langle S; h_i := h_i < l, j, l, j, \ell, \ell >, r, s, in >; h_i := < >; \ell \cdot \text{call}M \cdot a_r(\ell, j, \ell \# \#); h_i := h_i < r, s, l, j, te >; S; \ell'' \cdot \rangle \]

- any procedure \( a_j(\ell \# \#) \): \[ [S; \ell \cdot S'; \ell \cdot \langle S; S \cdot h_i := h_i < l, j, \ell, \ell >, m_j, i_j, u, \theta >, l, j, in >; h_i := < >; S; \ell \cdot \rangle] \]

- the initial statement: \[ [S_0; \ell_0] \]

7–10 DEFINITION (local coding, \( lc \)). Let \( l, m \in \omega \) and let \( \lambda_1 \cdots \lambda_\ell \) be a transition label sequence. Then

- \( m \) locally codes \( lc \) \( \lambda_1 \cdots \lambda_\ell \) \( l \) iff \( m = < < \lambda_i >, \ldots, < \lambda_i >, \rangle \), where \( \lambda_1 \cdots \lambda_\ell \) is the code of \( \lambda_1 \) as shown above.

Note that there is a 1–1 correspondence between a label sequence and its code.
7-11 Definition. Let $M_t$ be a $CM^+(\Sigma)$-module, $p \in L(\Sigma)$ and $A \subseteq \{ \ell : p \mid \ell \in FLB(M_t), p \in L(\Sigma) \}$.

- $SMI(A, p, M_t')$ represents

$$\left\{ (-1, \Omega, \sigma_n) \mid \exists C_0 \xrightarrow{\lambda_1} C_1 \cdots \xrightarrow{\lambda_n} C_n \in Comp(M_t', p, A) \text{ with } C_0 \in SC \right\}$$

such that $a_n = -1$ and $\sigma_n(h_i \cdot h_i) \leq \lambda_1 \cdots \lambda_n$.

- $COMP(A, p, M_t, \ell)$ represents

$$\left\{ (a_n, \theta_n, a_n, \sigma_n) \mid \exists C_0 \xrightarrow{\lambda_1} C_1 \cdots \xrightarrow{\lambda_n} C_n \in Comp(M_t', p, A) \text{ with } C_0 \in SC \right\}$$

such that $a_n \neq 1$, $\rho_n, a_n = \ell$ and $\sigma_n(h_i \cdot h_i) \leq \lambda_1 \cdots \lambda_n$.

- Let $\ell \in FLB(a_t')$. Then

  - if $j = 0$ then $U(\ell) = true$.
  - if $j > 0$ then

$$U(\ell) = \exists g, g' (active_\ell(h_i, g, g', m_j, i_j) \land \exists g'', active_\ell(g, g', g'', m_j, i_j) \land$$

$$l.c. a_j > 1 \land \exists g', g'', m, p \text{ active}_\ell(g, g', g'', m, p) \land$$

$$\text{active}_\ell(h, f, g, m, p) = \exists c, h = f' < m, p, c, l, j, i > \in g' \land$$

$$\exists g', g'', c', g = g' < l, j, c', m, p, te > g''$$

The predicate $active_\ell(h, f, g, m, p)$ expresses that the (code of the) history $h$ witnesses an active instance of procedure $a_t'$ which is being called by procedure $a_t''$ (in $M_m$); moreover $f$, respectively, $g$ codes the history before, respectively, after this instance becomes active. Then, the assertion $U(\ell)$ first claims that as long as an instance of $a_t'$ with particular values for $m_j$ and $a_t'$ is active, there can be no second instance with the same values for $m_j$ and $a_t'$. This implies that these values uniquely identify procedure instances. $U(\ell)$ also claims that if $l.c. a_j > 1$ holds, there must be another active instance of $a_t'$.

7-12 Lemma. Given a specification $\langle CA, WA, CO, MI \mid \{ p \} M_t' \{ q \} \rangle$, define

- $p \equiv \bar{p} \land h_i =<> \land \bar{h_i} =<> \land \bar{z} = \bar{z}$, with $\{ \bar{z} \} = V_1$ and $\{ \bar{z} \} \cap V_1 = \emptyset$

- $SWA \equiv \{ \ell : COMP(CA, p, M_t', \ell) \land U(\ell) \mid \ell \text{ labels the rear of a wait in } M_t' \text{ or the rear of its initial statement} \}$

- $SCO \equiv \{ \ell : COMP(CA, p, M_t', \ell) \land U(\ell) \mid \ell \text{ labels the front of a wait, a call or an opening bracket in } M_t' \}$

- $SMI \equiv SMI(CA, p, M_t')$

- $SP \equiv COMP(CA, p, M_t', \ell)$, where $\ell$ labels the rear of the initial statement.

- Assume that $CA$ is such that

  - if $\ell$ labels the first (closing) bracket in some $a_t'$ ($j > 0$) then $\models CA(\ell) \rightarrow U(\ell)$

  - $CA$ is LC-independent

(These two constraints are compatible.)

Then $\vdash_{PS(\Theta(N))} \langle CA, 0, SCO, SMI \mid \{ p \} M_t' \{ SP \} \rangle$
PROOF. Observe that \( \models SWA(\ell) \rightarrow SMI \) for any rear wait or rear initial statement label, \( \ell \).

For any \( A \subseteq \{ \ell : p \mid \ell \in Lab, p \in L(\Sigma) \} \), let \( A_i = \{ \ell : p \mid p \in A, \ell \in FLB(a_{i}^{'}) \} \).

Again, Lemma 7-7 allows the specification to be taken minimal. By Theorem 7-8, validity of the corresponding premises of the module rule has to be shown. Only validity of the interference freedom specifications will be treated in detail.

7-12(1) \( \models (CA_k, SWA_k, SCO_k, SMI \mid \{ SMI \} a_{i}^{k}(\hat{u}_{i}^{k} # \hat{v}_{i}^{k}) : [S_k]\{ SMI \}) \), \( k > 0 \):

The following fact follows directly from the definition of \( SWA, SCO \) and \( SMI \), and its proof is left to the reader:

Suppose that \( \langle \delta_{i}^{1}, \ldots, \delta_{i}^{m} \rangle \models (CA_k, SWA_k, SCO_k, SMI \mid \{ SMI \} a_{i}^{k}(\hat{u}_{i}^{k} # \hat{v}_{i}^{k}) : [S_k]\{ SMI \}) \),

\( \delta_{0} \models SMI \) and \( \delta_{i} \models CA_k \) for \( i = 0..n \). Then there is a computation \( C_{0} \xrightarrow{\lambda_{1}} C_{1} \xrightarrow{\lambda_{2}} \cdots \xrightarrow{\lambda_{m}} C_{n} \in Comp(M_{i}^{k}, p, CA) \), with \( \delta_{i} = s(C_{i}) \) for \( i = 0..n \) and \( 3i_{0}, i_{1}, \ldots, i_{m} \) such that \( \forall 0 \leq j \leq m. \delta_{j} \models (V_{i} \cup \{ ic_{a_{i}}^{j} \}) = \sigma_{i_{j}} \models (V_{i} \cup \{ ic_{a_{i}}^{j} \}) \), \( \delta_{j} = a_{i_{j}} \), if \( a_{i_{j}} = \bot \) then \( \delta_{j} = a_{i_{j}} \), and \( \delta_{m}(h_{i}^{-1} \bar{h}_{i}) \models \lambda_{1} \cdots \lambda_{m} \).

From this, validity is easily established.

7-12(2) \( \models (CA_k, SWA_k, SCO_k, SMI \mid \{ p \} S_{0} \{ SMI \wedge SWA_{0}(l_{0}) \}) \):

Analogous to 1, since a similar fact holds.

7-12(3) \( \models SMI \wedge SWA_{0}(l_{0}) \rightarrow SP \): Evident.

7-12(4) for every \( l. \) wait \( . l' \) in \( M_{i}^{k} \):

\( \models SWA(l') \rightarrow SWA(l) \): Immediately from the definitions.

7-12(5) \( SWA \# (CA_k, SWA_k, SMI, \{ u_{k}, \hat{v}_{k} \}, a_{k}^{k}(u_{k} # \hat{u}_{k}) : [S_k]) \) for \( k > 0 \):

So, for every \( l : q \in SWA \), I must prove that

\( \models \langle CA_k, SWA_k(q'), CO, true \rangle \models \{ SMI \wedge q' \} a_{i}^{k}(u_{k} # \hat{u}_{k}) : [S_k]\{ q\prime \} \geq \)

Let \( l \in FLB(a_{i}^{k}) \).

Then, I must show that

\( \forall C_{0} \xrightarrow{\lambda} C_{n} \in Comp(a_{i}^{k}(u_{k} # \hat{u}_{k}) : [S_k], SMI \wedge q', CA \cup SWA_k(q')) \)

\( s(C_{0}) \models CO \& \ C_{n} \in TC \Rightarrow s(C_{n}) \models q' \).

Fix a computation and let \( C_{i} = (h : a_{i} \mid LC_{i}, \sigma_{i}) \), \( LC_{i} = Id_{i} : (S_{i}, \theta_{i}) \) and \( \delta_{i} = s(C_{i}) \) for \( i \leq n \).

If \( C_{n} \notin TC \) or \( \rho_{0} \) does not label the front of a wait, there is nothing to prove. So, assume otherwise. In either case, I must show that \( \delta_{n} \models q' \). Obviously, it suffices to prove this on sequences for which \( a_{i} \neq \bot \) for \( i \leq n \). There are two cases; namely, \( \rho_{0} \neq \theta \) and \( \rho_{0} = \theta \). In the first case, the computation restarts at a block-statement. The latter case corresponds with a computation starting in the procedure's initial configuration.

Case 1: \( \rho_{0} \neq \theta \) Then \( \delta_{0} \models SWA(\rho_{0}) \wedge q' \), with \( q' \equiv SWA(\ell)[\hat{y}/\hat{u}_{k}, \hat{v}_{k}] \).

Let \( \nu_{0}(< m_{i}, i_{k}^{k} > h) = h \) and \( \sigma_{0}(< m_{i}, i_{k}^{k} > h) = h' \), where \( m_{i}, i_{k}^{k} \), and \( h' \), are the fresh variables substituted for \( m_{i}, i_{k}^{k} \), and \( h' \). Note that \( h \neq h' \).

By interpreting the assertions, I obtain (as explained below) that

1. \( \delta_{0} \models SWA(\rho_{0}) \Rightarrow (h, \rho_{0}) \models (M_{i}^{k}, p, CA, \nu_{0}, \sigma, \lambda), \text{Ir}, \sigma(h_{i}^{-1} \bar{h}_{i}) \models \lambda \) and \( \sigma \cup \nu \models U(\rho_{0}) \).

2. \( \delta_{0} \models q' \Rightarrow (h', \ell) \models (M_{i}^{k}, p, CA, \nu, \sigma, \lambda'), \text{Ir}, \sigma(h_{i}^{-1} \bar{h}_{i}) \models \lambda' \) and \( \sigma \cup \nu \models U(\ell) \),

where \( \sigma = \sigma_{0} \models V_{i} \) and \( \nu = \Omega(\sigma_{0}[\hat{y}/\hat{u}_{k}, \hat{v}_{k}] \).

These implications depend on the fact that \( (L_{k} \cup L_{k}) \cap V_{i} = \emptyset \). This determines the splitting of the variable valuations (in \( \delta_{0} \)) into \( \nu_{0}, \sigma \) and \( \nu, \sigma \), as this must be the case in any configuration of
The only moot point is why I can choose \( h \) in (1) and \( h' \) in (2): Since \( \sigma \cup \nu_0 = U(\rho_0) \) there can be no other active instance of \( a_l \) with the same values for \( m_l \) and \( i_l \). This means that there is a computation in which the LC leading to \((\nu_0, \rho_0)\) is identified by \((l, k, h)\). If \( k = k' \) then \( \delta_0[(c,a_l')] > 1 \) so that \( U(\rho_0) \) implies the existence of another active instance. As \( h \neq h' \), the same argument gives, both in the case that \( k = k' \) and in the case that \( k \neq k' \), the reachability of \((\nu, \ell)\) by an LC with identification \((l, k', h')\).

As \( CA \) is LC-independent, the LML applies, so that \((h, \rho_0, h', \ell)\) is \((M'_i, p, CA, \nu_0, \nu, \sigma, \lambda)-br\). Note that \( \lambda = \lambda' \) because they are both locally coded by the same integer.

Hence, there is a computation,

\[
C_0 \xrightarrow{\lambda} C_m \in \text{Comp}(M'_i, p, CA),
\]

with \( \delta_i = s(C_i) \) for \( i \leq m \) and such that \( \exists \tau, r \delta_{m,r} = (\nu, \ell), \delta_{m,r} \equiv (l, k, h'), \delta_{m,s} = \theta_0, \delta_{m,s} \equiv (l, k, h), \sigma_m = \sigma \) and \( \sigma(h_i \cdot h_i) = \lambda \). Also, I can assume that \( \sigma_m = -1 \) by definition of \( \text{SWA}(\rho_0) \) and of \( q' \) the last record in \( \lambda \) is a local one and the global state must be attainable at a waiting point.

Next, extend (9) with \( C_m \xrightarrow{\lambda} C_{m+n} \) as follows:

- \( LC_{m+i,j} \equiv LC_{m,j} \) for \( j \neq s \),
- \( LC_{m+i,s} \equiv LC_{i,s} \),
- \( \sigma_{m+i} = \sigma_i \mid V_i \) and
- \( \bar{a}_{m+i} = s \)

This extension is well-defined because I can assume that \( Id_m = (l, k, h) \). Clearly, \( \sigma_{m+n} \cup \nu_{m+n,r} \models \text{SWA}(\ell) \) holds. This means that \( \sigma \mid V_i \mid \nu \models \text{SWA}(\ell) \), hence \( \sigma \models q' \) and, finally, \( \delta_0 \models q' \).

Case 2: \( \rho_0 = \emptyset \)  
The argument is analogous to Case 1, except that the LML is not needed.

This is completely analogous to case 1 above. The second case, \( \rho_0 = \emptyset \), does not apply because the precondition is false, reflecting the fact that on no computation sequence of \( M \) a procedure instance can be active before the initial statement has reached a waiting point.

7-4 Completeness for program specifications

Here, too, auxiliary variables are needed; this time in order to apply the global merging lemma.

7-13 Definition. Let \( P \) be a \( CM(\Sigma) \)-program \([M_1 \parallel \cdots \parallel M_n]\). Then

- \( \tilde{P} \) is a \( CM^*(\Sigma) \)-program \([\tilde{M}_1 \parallel \cdots \parallel \tilde{M}_n]\) such that \( P \) can be re-obtained by removing every bracket or label from \( \tilde{P} \)
- \( P' \) is the \( CM^*(\Sigma) \)-program, \([M'_1 \parallel \cdots \parallel M'_n]\), obtained from \( \tilde{P} \) by modifying every module \( M_i \) as in Definition 7-9.

7-14 Definition (global coding, gc). Let \( i, m \in \omega \) and let \( \lambda_1 \cdots \lambda_m \) be a transition label sequence. \( m \) globally codes (gc) \( \lambda_1 \cdots \lambda_m \) iff \( m = \langle \lambda_1, \ldots, \lambda_m \rangle \) where \( \lambda_1 \cdots \lambda_m = \lambda_1 \cdots \lambda_m \).

35
7-15 DEFINITION. Let \( P \) be a \( \text{CM}(\Sigma) \)-program \([M_1 \mid \cdots \mid M_n]\), \( p \in L(\Sigma), \ell \in \text{FLB}(M_k) \) and \( A \subseteq \{ \ell : p \mid \ell \in \text{Lab}, p \in L(\Sigma) \} \).

- \( \text{COMP}_p(\nu, \ell) \) represents

\[
\exists C_0 \xrightarrow{\lambda} C_m \in \text{Comp}(P, p) \text{ such that } a^k_m \neq -1, \theta^k_m a^k_m = (\nu, \ell), \sigma^k_m | V = \sigma | V \text{ and } \sigma(h_k \wedge h_k) \in V \cap k
\]

7-16 LEMMA. Given a \( \text{CM}(\Sigma) \)-program, \( P \equiv [M_1 \mid \cdots \mid M_n] \), and \( p \in L(\Sigma) \), let \( \{ \xi_i \} = \emptyset \) for \( i = 1 \ldots n \) and let \( \bar{z}_1, \ldots, \bar{z}_n \) be pairwise disjoint sequences of variables such that \( \bigcup_{i=1}^n \bar{z}_i \cap (\bigcup_{i=1}^n (V_i \cup L_i)) \cup FV(\beta) = \emptyset \) and \( |\bar{z}_i| = |\bar{z}_i| \) for \( i = 1 \ldots n \).

Define for \( i = 1 \ldots n \)

- \( p_i \equiv \bar{p}[\bar{z}_j/\bar{z}_j, j = 1 \ldots n, j \neq i] \wedge \bar{z}_i = \bar{z}_i \wedge h_i = <> \wedge h_i = <> \) and \( p \equiv \bigwedge_{i=1}^n p_i \)
- \( \text{SCA}_i \equiv \{ \ell : \text{COMP}_i(V_i \cup \{ \bar{z}_i \}, \ell) \cap U(\ell) \mid \ell \) labels a closing bracket in \( M_i \} \)
- \( \text{SGI} \) represents

\[
\left\{ (a, \theta, \sigma) \mid \exists C_0 \xrightarrow{\lambda} C_m \in \text{Comp}(P, p) \text{ with } \delta_n = s(C_n) \text{ such that } C_n \right. \\
\text{is acceptable, } \sigma(h_i) \geq \lambda \text{ and } \sigma'(h_i) = \sigma(h_i) \text{ for } i = 1 \ldots n \right\}
\]

Then, every specification in the set of cooperation specifications,

\[
\text{Coop}((\{ \text{SCA}_i, \emptyset, \text{SCO}_i, \text{SMI}_i \mid \{ p_i \} M_i^{i}(\{ \text{SP}_i \}) \mid i = 1 \ldots n \}, \text{SGI}),
\]

is valid.

Here, \( \text{SCO}_i, \text{SMI}_i \) and \( \text{SP}_i \) for \( i = 1 \ldots n \) are defined as in Lemma 7-15 (w.r.t. \( \text{SCA}_i \) and \( p_i \)). The indices \( i \) denote the modules to which they belong. Note that \( \text{SCA} \) is LC-independent because \( \text{COMP}_k \) is.

This proof is somewhat less detailed than that for module specifications, because the constructions of the computations are similar. It can be short because much of the work has been done in the proof of the GML.

PROOF. Take any matching call procedure pair

\[
\ell.(S_1; \bar{\ell}. \text{call} M_j.a_k(\bar{\#x}); S_2; \bar{\ell}) \quad \text{(in } M_1 \text{)} \quad \text{and} \\
a_k(\bar{\#}\bar{\#}) : [S'_1; \ell']; S'_2; \bar{\ell} \quad \text{(in } M_j \text{)}
\]

Since the assumptions, commitment and monitor invariant are trivial in the cooperation specifications, they will not be mentioned explicitly below.

7-16(1) \( \models \{ \text{SCO}_i(\ell) \wedge \text{SMI}_j \wedge \text{SGI} \} S_1; ic.a^j_k := ic.a^j_k + 1; S'_1[\cdot]\{ \text{SCA}_j(\ell'; i) \wedge \text{SGI} \} : \)

Substitution lemma 5-7(1) yields equivalence with

\[
\models \{ \text{SCO}_i(\ell) \wedge \text{SMI}_j \wedge \text{SGI} \} S_1; ic.a^j_k := ic.a^j_k + 1; \bar{u}, \bar{v} := \bar{e}, \bar{z}; S'_1[\cdot]\{ \text{SCA}_j(\ell'; i) \wedge \text{SGI} \}
\]

Denote the statement sequence in (10) by \( T \). Choose any configuration state, \( \delta \) such that \( \delta \models \text{SCO}_i(\ell) \wedge \text{SMI}_j \wedge \text{SGI} \) and let the configuration state, \( \bar{\delta} \), be determined by the condition that \( (\delta \cdot \cdots \cdot \bar{\delta}, T) \in [T] \). If there is no such \( \bar{\delta} \), (10) holds trivially. So assume otherwise. To show:
with their interaction. Moreover, a conscious attempt was made to obtain a notion which rather consider global verification algorithms (in the sense of the introduction).

and a proof system that comes close to being compositional. This contrasts with [Apt81, Apt83] with CSP-type concurrency. Published proofs in this area have dealt with simple shared variable concurrency. The foregoing proof is a long one indeed. The programming language is, however, quite powerful, embodying both Ada-type task interactions as well as shared variable concurrency. Previously published proofs in this area have dealt with simple shared variable concurrency (cf. [Apt81]) and with CSP-type concurrency (cf. [Apt83]) separately. This paper has to deal with both and also with their interaction. Moreover, a conscious attempt was made to obtain a notion of specification and a proof system that comes close to being compositional. This contrasts with [Apt81, Apt83] which rather consider global verification algorithms (in the sense of the introduction).

8 Conclusions

The foregoing proof is a long one indeed. The programming language is, however, quite powerful, embodying both Ada-type task interactions as well as shared variable concurrency. Previously published proofs in this area have dealt with simple shared variable concurrency (cf. [Apt81]) and with CSP-type concurrency (cf. [Apt83]) separately. This paper has to deal with both and also with their interaction. Moreover, a conscious attempt was made to obtain a notion of specification and a proof system that comes close to being compositional. This contrasts with [Apt81, Apt83] which rather consider global verification algorithms (in the sense of the introduction).
A second difference is in the formulation of the two merging lemmas of Section 4. Here, they are statements about the computations of modules and programs whose truth is independent from whether or not computations of procedures and modules are representable within the assertion language. Such a separation of concern is absent in earlier proofs and gives some conceptual clarity.

The proof system ultimately deals with partial correctness properties of $CM(\Sigma)$-programs. In fact, the axiomatisation is powerful enough to support the proof of arbitrary safety properties, as may be gleaned from the completeness proofs. However, to extend the notion of validity to program specification with non-trivial commitments is not so easy. The problem originates in the use of the global invariant, $GI$, and its bracketed sections. The $GI$ only holds in acceptable program configurations (in which no module is within a bracketed section), so that acceptability would have to be included in the validity definition. This added complication did not seem worth the trouble.

The proof system is not complete for module specifications. This points to a difference between the current proof system and a truly compositional one. The local merging lemma shows the need to distinguish procedure instances other than through the local and global states—which, indeed, may not show a difference. Here, this has been done by extending the local states of procedures. It might have been done differently. For instance, by introducing logical variables, $i_d^j$, that are initiated in each instance to the third component of the identifier of the corresponding LC. In either way, the existence of multiple instances can be postulated in the interference freedom specifications. However, whatever one does, such assumptions must be discharged by associating such instances with outstanding calls in other modules, for which one needs the communication histories. In the traditional compositional proof systems (see [Zwi89] for the state-of-the-art) these histories are directly accessible in the specification language, so that the connection between the coexistence of procedure instances and the communication histories can be expressed as axioms. This paper’s proof system must introduce auxiliary variables first, before anything can be expressed about communication histories (or rather, about their encodings). The restricted form of module completeness is a direct consequence of this.

Acknowledgements

I thank Frank de Boer for discovering the invalidity of a previous version of the local merging lemma which pointed to the incompleteness of an earlier form of the proof system.

The first version of the paper has been troffed by Mrs. E van Thiel.

A Appendix: the substitution lemma

Here the substitution lemma 5–7 is proved.

**A–1 DEFINITION.** Let $R$ be a binary relation on states, $R \subseteq St \times St$; $u, z, v \in Var$ and $e \in Tm(\Sigma) \setminus Var$. Then

- $R^e_u$ is defined by $\sigma[z/v] R \tau[z/v] \Leftrightarrow \sigma[z/v] R^e \tau[z/v]$
- $R^{e}_u$ is defined by $\sigma[e/u] R \tau \Leftrightarrow \sigma R^e \tau$.

If $z \in Var$ and $t \in Tm(\Sigma)$, let $z := t$ stand for the relation $\{(\sigma, \sigma(t)/y) \mid \sigma \in St\}$. 

38
A-2 LEMMA. Use the same notation as in Definition A-1

If (a) \( \sigma \circ R \Rightarrow \sigma(z) = \tau(z) \) and (b) \( \sigma \circ R \Rightarrow \sigma(\beta/z) \) \( \Rightarrow \) \( R \tau \) then

1. \( \sigma R^*_z \Rightarrow \sigma(u := e \circ R) \Rightarrow \tau(\zeta)/v \)

2. \( \sigma R^*_z \Rightarrow \sigma(v := z \circ R \circ z := v) \Rightarrow \tau(\zeta)/v \)

PROOF. (1) is trivial, so concentrate on (2).

For a state \( \nu \), if \( \nu = \nu(\beta/z), z \neq y \) then \( \nu(\beta/y) = \nu(\nu(z)/y) \nu(\nu(z)/y) \). Hence, if \( \sigma = \sigma(z) \) and \( \tau = \tau(z) \), then \( \sigma R^*_z \Rightarrow \tau(\zeta/z) \). By (a), \( \sigma(\beta) = \tau(z) \) and so by (b), \( \sigma R^*_z \Rightarrow \sigma(\sigma(z)/v) \Rightarrow \tau(\sigma(z)/v) \Rightarrow \tau(\tau(z)/v) \). The result follows since \( \sigma(\sigma(z)/v) := v(\sigma) \) implies \( \tau(\tau(z)/v) \).

For the rest of the section, let \( S \) denote \( CMc(\Sigma) \)-statements not containing any call or wait-staments. In other words, consider statements for which state-changes involving a variable \( z \), say - can only be effected through assignments \( z := e \). For statements, \( S \), the usual partial correctness semantics \( \llbracket S \rrbracket \), is given by

\[
\{ (\sigma, \tau) \mid \exists (\delta_0, \ldots, \delta_n, T) \in \llbracket S \rrbracket, \sigma = \sigma_0 \cup \nu_0(\#0), \tau = \sigma_0 \cup \nu_n(\#n) \}.
\]

Facts:

- \( \llbracket (z := e) \rrbracket = z := e \) (i.e., as a relation)
- \( \llbracket S[z/v] \rrbracket = \llbracket S \rrbracket \) provided \( z \notin FV(S) \)
- \( \llbracket S[e/u] \rrbracket = \llbracket S \rrbracket \) provided \( FV(e) \cap FV(S) = \emptyset \) and \( u \) does not appear as the left-hand-side of any assignment in \( S \).

These facts are sufficiently obvious so as not to warrant a proof. Note that the condition in the second fact implies assumptions (a) and (b) of Lemma A-2. Partial correctness "triples" in this paper's formalism are notated as \( \llbracket p, q, \tau \rrbracket \). In the rest of this section the (trivial) assumptions and commitments will be ignored and I shall write \( \llbracket p \rrbracket S[q] \).

A-3 LEMMA. Let \( u, v, z \in \operatorname{Var}, e \in Tm(\Sigma) \) and \( p, q \in L(\Sigma) \) be such that \( z \notin FV(S), FV(e) \cap FV(S) = \emptyset \) and \( u \) does not appear as the left-hand-side of an assignment in \( S \).

- \( A \models \llbracket p \rrbracket S[z/v][q] \Rightarrow A \models \llbracket p \rrbracket z := v; S[z := v] \llbracket q \rrbracket \), provided \( v \notin FV(q) \)
- \( A \models \llbracket p \rrbracket S[e/u][q] \Rightarrow A \models \llbracket p \rrbracket u := e; S[q] \).

PROOF. Directly from the definitions and Lemma A-2.

The next step is the extension to multiple substitutions.

A-4 LEMMA ([deB80]). Let \( e, t \in Tm(\Sigma), \tau \in Tm(\Sigma) \cup L(\Sigma) \), \( z, y \in \operatorname{Var} \) and suppose \( z \neq y \) and \( z \notin FV(t) \). Then \( r[e/z][t/y] = r[t/y][e[z/y]/z] \).

A-5 CORROLARY. With the same notations and conditions as in Lemma 5.3.4, if additionally \( y \notin FV(e) \), then \( r[e/z][t/y] = r[t/y][e[z/y]/z] \).

So under these conditions, simultaneous substitution acquires meaning. Obviously, these substitution-results hold for statements, too (provided the usual assumptions about non-variable substitutions hold). In the following (and in fact in the rest of the paper) simultaneous assignments, \( u_1, \ldots, u_n := e_1, \ldots, e_n \) or \( \bar{u} := \bar{e} \) (with \( u_i \neq u_j \) if \( i \neq j \)), will be used, with obvious meaning.

Now, Lemma 5-7 can be proven.
A - 6 Lemma (The substitution lemma). Let $S$, $S'$ be $CM^e(\Sigma)$-statements not containing call or wait-statements. Let $\bar{u}, \bar{v}, \bar{z} \subseteq \text{Var}$, $\bar{e} \subseteq Tm(\Sigma)$ and $p, q \in L(\Sigma)$ be such that $|\bar{u}| = |\bar{e}|$, $|\bar{v}| = |\bar{z}|$, the variables in $\bar{u}$ do not appear as left-hand-side of any assignments in $S$ and the variables in the lists $\bar{u}, \bar{v}$ are pairwise disjoint. Additionally, assume that the following conditions hold:

$u \cap \bar{v} = \emptyset$, $\text{FV}(\bar{e}) \cap \bar{z} = \emptyset$, $\{\bar{u}, \bar{v}\} \cap \text{FV}(q) = \emptyset$ and $(\text{FV}(S') \cup \{\bar{u}, \bar{v}\}) \cap (\text{FV}(\bar{e}) \cup \bar{z}) = \emptyset$. Then ([] $= [\bar{e}, \bar{v}/\bar{u}, \bar{e}]$):

1. $A \models [p; S; S']$ $\iff$ $A \models \{p\} S; \bar{u}, \bar{v} := \bar{e}, \bar{z}; S'$

2. $A \models [p; S; S']$ $\iff$ $A \models \{p \wedge \bar{u} = \bar{e}\} S'; \bar{z} := \bar{v}; S\{q\}$, provided $\text{in \ FV}(p) = 0$.

Proof. Define $WP(S, p) = \{\sigma (\sigma, \tau) \in \langle S \rangle \Rightarrow \tau = p\}$ and $SP(S, p) = \{\sigma (\sigma, \tau) \in \langle S \rangle \Rightarrow \sigma = p\}$. Extend the signature $\Sigma$ to $\tilde{\Sigma} = \Sigma \cup \{sp(S, p), wp(S, p) \mid S \text{ a } CM^e-\text{statement}, p \in L(\Sigma)\}$ and let $A$ be the extension of $A$ in which the new predicate symbols get their intended meaning:

$sp(S, p) \models \{0\} u, v := \bar{z}, \bar{e}; S'$

(1) By Lemma 5.3.3 (and corollary 5.3.5): $A \models \{p; S; S'\}$ $\iff$ $A \models \{p\} S; \bar{u}, \bar{v} := \bar{e}, \bar{z}; S'.$

Since the variables in $\bar{u}$ are never assigned to and $\text{FV}(S') \cap \{\bar{u}, \bar{v}\} \cap \text{FV}(\bar{e}) = \emptyset$, I have $A \models \{0\} u, v := \bar{e}, \bar{z}; S'\{\bar{u} = \bar{e}\}$. This implies equivalence of the left-hand side of (A) with $A \models \{p\} S; \bar{u}, \bar{v} := \bar{e}, \bar{z}; S\{q\}$ and hence with $A \models \{p\} S; \bar{u}, \bar{v} := \bar{e}, \bar{z}; S'\{q\}$.

(2) Since I can assume that $\bar{u} \cap \text{ wp}(S, q) = \emptyset$, Lemma 5.3.3 yields equivalence with $A \models \{p; q\} u, v := \bar{e}, \bar{z}; S'; \bar{z} := \bar{v}\{\text{wp}(S, q)\}$. Denote $\text{wp}(S, q) \models \bar{v} := \bar{e}, \bar{z}; S'; \bar{z} := \bar{v}\{\text{wp}(S, q)\}$. Again, [deB80] learns that $A \models sp(z := e, p) \iff \exists y(p[y/z] \land z = e[y/z])$, $y \notin \text{ FV}(z := e, p)$.

As $\text{ wp}(p; q) \cap \{u, v\} = \emptyset$, the left-hand side of (B) is equivalent with $A \models \{p \wedge \bar{u} = \bar{e}\} S'\{\bar{v}/\bar{z}\}$. Next observe that $(\text{FV}(p, \bar{e}, S', \bar{q}/\bar{z}) \cup \bar{u}) \cap \bar{z} = \emptyset$. This implies equivalence with $A \models \{p \wedge \bar{u} = \bar{e}\} S'; \bar{z} := \bar{v}\{\bar{q}\}$ and hence with $A \models \{p \wedge \bar{u} = \bar{e}\} S'; \bar{z} := \bar{v}; S\{q\}$. $

\square$

References


40


