A compositional proof system for real-time systems based on explicit clock temporal logic: soundness and completeness

Citation for published version (APA):

Document status and date:
Published: 01/01/1991

Publisher 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 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

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.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license above, please follow below link for the End User Agreement:
www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:
openaccess@tue.nl
providing details and we will investigate your claim.

Download date: 13. Jul. 2023
A Compositional Proof System for Real-Time Systems Based on Explicit Clock Temporal Logic: Soundness and Completeness

by

P. Zhou       J. Hooman       R. Kuiper

Computing Science Note 91/25
Eindhoven, September 1991
COMPUTING SCIENCE NOTES

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

Copies can be ordered from:
Mrs. F. van Neerven
Eindhoven University of Technology
Department of Mathematics and Computing Science
P.O. Box 513
5600 MB EINDHOVEN
The Netherlands
ISSN 0926-4515

All rights reserved
editors: prof.dr.M.Rem
prof.dr.K.M.van Hee.
A Compositional Proof System for Real-Time Systems
Based on Explicit Clock Temporal Logic:
Soundness and Completeness *

P. Zhou J. Hooman R. Kuiper

Dept. of Mathematics and Computing Science
Eindhoven University of Technology
P.O.Box 513
5600 MB Eindhoven, The Netherlands

October 8, 1991

Abstract
To specify and verify real-time systems, we consider a real-time version of temporal logic
which is called Explicit Clock Temporal Logic. Timing properties are specified by simply
extending the classical framework of temporal logic with a special variable which explicitly
refers to a global notion of time. Programs are written in an Occam-like real-time language
in which concurrent processes communicate by synchronous message passing along chan­
nels. A proof system is provided to formally verify that a program satisfies a specification
expressed in this logic. The proof system is compositional, that is, the verification of a
complex statement can be done on the basis of the verifications of its components, without
knowing the implementation of them. This allows splitting the verification of large systems
into the verification of subsystems. The proof system is shown to be sound and relatively
complete.

1 Introduction
In this paper we investigate the formal specification and verification of real-time systems. One
of our objectives was that the approach should be able to deal with a reasonably realistic
language. Therefore, we consider an Occam-like real-time programming language [Occ88] with
synchronous message passing along unidirectional channels between concurrent processes. An­
other aim was to build on existing formalisms and enable easy future extension or adaptation.
In general, to specify and verify real-time systems, an existing non-real-time method can be
extended with some notion of time. Here we also follow this approach, and use an extension of
linear time temporal logic [Pnu77,MP82,OL82]. The standard logic enables expressing safety
properties (such as “non-termination”, “no communication along channel c”, and “program
variable $x$ is always greater than 5”) as well as liveness properties (such as “termination”,
“eventually communicate along channel $c$”, and “eventually $x$ has the value 8”). To specify
real-time properties (such as “termination within 7 time units”, “communicate on channel $c$
at time 4”, and “during the next 3 time units $x$ has a positive value”) we have to extend

*This research was supported by ESPRIT-BRA project 3096 "Formal Methods and Tools for the Development of Distributed and Real-Time Systems (SPEC)".

1
temporal logic with a quantitative notion of time. As already observed in [PH88, HLP90], one can distinguish two main approaches.

In one approach, new temporal operators are introduced, by extending the standard ones with time bounds. Already in [BH81] a quantitative "leads to" operator has been introduced to verify real-time applications. In [SPE84] a temporal logic with statements about time intervals has been used to prove correctness of local area network protocols. A general discussion of this extension in the context of linear time, often called Metric Temporal Logic (MTL), can be found in [Koy90]. This logic has been applied to the specification of real-time communication properties of a transmission medium [KVR83]. In a similar way, branching time temporal logic, also called Computation Tree Logic (CTL), is extended to real-time by adding time bounds to the modal operators. See, for instance, [EMSS9] where algorithms for model checking and satisfiability analysis are also presented, for a logic with discrete time. It is shown in [ACD90] that the model checking results can be extended to CTL over a dense time domain.

We investigate the alternative approach, called Explicit Clock Temporal Logic (ECTL), in which temporal logic is extended with a distinguished variable that explicitly refers to clock time. Such a logic has been used in [Ost89] to reason about real-time discrete event systems. A similar real-time version can be found in [Har88]. This approach has the advantage of building upon a well-established classical temporal logic framework to which only axioms and rules for proving timing properties have to be added. Also, further extensions can be envisaged, like extra structure on the time domain, that leave the underlying logic unchanged. It is even possible to leave choices about the time domain, like this being discrete or dense, open till later. This allows for investigating the effect of different choices on, e.g., the possibilities for automatic verification without drastic changes to the formalism.

We mention some works that we feel are relevant to the present approach, though not directly related. Logics for reasoning about real-time systems are classified in [AH90] according to their complexity and expressiveness. A tableau-based decision procedure is given for a version of metric temporal logic. To obtain decidability a discrete time domain is used. Also a decidable version of the explicit clock approach (called TPTL) is considered in which there is a "freezing" quantification that binds a variable to the value of the clock at a certain state. In [HLP90] a decision procedure and a model checking algorithm are given for a suitably restricted version of ECTL. The expressibility of this logic is shown to be incomparable with TPTL.

Given the choice of programming language and the real-time version of temporal logic, the task is to develop a proof method to verify that a program satisfies a property expressed in this logic. In classical verification methods, such as [MP82] for temporal logic, the complete program text must be available. Global proof systems, based on the method of [MP82], and decision procedures for explicit clock versions of temporal logic can be found in [Har88, Ost89].

In contrast with these methods, we formulate a compositional proof system in which the specification of a compound programming language construct (such as sequential composition and parallel composition) can be deduced from specifications for its constituent parts without
any further information about the internal structure of these parts. Compositionality can be considered as a prerequisite for hierarchical, structured, program derivation. A separation of concerns is desired, implying a separation of the use of (and the reasoning about) a module from its implementation. By means of a compositional proof system the design steps can be verified during the process of top-down program construction. To obtain a compositional proof system, our starting point is the compositional system for classical temporal logic as described in [BKP84]. The present paper also builds on the approach to compositionality and real time introduced in [HW89]. With respect to that paper, the main difference is that the emphasis there was on achieving compositionality in as simple a setting as possible. Therefore, a quite sparse model of computation was used. The programming language did not contain data variables and consequently also transmission of values was not incorporated in the model. Furthermore, that paper forms a complement to the present one in the sense that the logic was MTL-styled rather than ECTL-styled. Related compositional proof systems based on MTL for different versions of the programming language have been formulated in [Ho09].

This paper is structured as follows. In Section 2 we describe our programming language, its informal semantics, and the basic timing assumptions. A formal denotational semantics can be found in Section 3. To specify real-time properties of programs we formulate in Section 4 the syntax and the interpretation of our version of ECTL. To verify that a program satisfies a specification written in this logic, Section 5 contains a compositional proof system. The soundness and completeness of the proof system are discussed in Section 6. Conclusion can be found in Section 7. The proofs of lemmas are given in Appendix A. All details of the soundness proof can be found in Appendix B. Preciseness proof which is used in the completeness proof of Section 6 is given in Appendix C.

2 Real-Time Programming Language

2.1 Syntax and Informal Semantics

We consider a real-time programming language which is akin to Occam [Occ88]. The language is based on a real-time extension of CSP with nested parallelism and synchronous message passing via channels [KSR+88]. A real-time statement delay e is added which suspends an execution for the value of expression e time units. Such a delay-statement may also occur in the guard of a guarded command. Processes communicate and synchronize by message passing via unidirectional channels which connect exactly two processes. Communication is synchronous.

Let \( VAR \) be a nonempty set of program variables, \( CHAN \) be a nonempty set of channel names, and \( VAL \) be a denumerable domain of values of program variables. The syntax of our real-time programming language is given in Table 1, with \( c, c_i \in CHAN, x, x_i \in VAR, \vartheta \in VAL, \) and \( n \in IN, \) where \( IN \) denotes the set of all natural numbers.

Define \( \text{var}(S) \) as the set of variables occurring in \( S \). Let \( \text{wvar}(S) \) be the set of all write-variables of \( S \), i.e., the set of variables occurring in the left-hand side of an assignment or as a variable in an input statement. Obviously, \( \text{wvar}(S) \subseteq \text{var}(S) \). The set of (directional)
Table 1: Syntax of Programming Language

<table>
<thead>
<tr>
<th>Syntax</th>
<th>e ::=</th>
<th>$\varnothing$</th>
<th>x</th>
<th>$e_1 + e_2$</th>
<th>$e_1 \times e_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean Expression</td>
<td>b ::=</td>
<td>$e_1 = e_2$</td>
<td>$e_1 &lt; e_2$</td>
<td>$\neg b$</td>
<td>$b_1 \lor b_2$</td>
</tr>
<tr>
<td>Statement</td>
<td>S ::=</td>
<td>skip</td>
<td>$x := e$</td>
<td>delay $e$</td>
<td>$c!e$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$S_1; S_2$</td>
<td>$G$</td>
<td>$\ast G$</td>
<td>$S_1</td>
</tr>
<tr>
<td>Guarded Command</td>
<td>G ::=</td>
<td>$[[ \bigwedge_{i=1}^{n} b_i \rightarrow S_i ]]$</td>
<td>$[[ \bigwedge_{i=1}^{n} b_i; c_i?x_i \rightarrow S_i</td>
<td></td>
<td>b; \text{delay } e \rightarrow S ]]$</td>
</tr>
</tbody>
</table>

channels occurring in a statement $S$, denoted by $dch(S)$, is defined as the set containing all channels occurring in $S$ together with all directional channels $c!$ and $c?$ occurring in $S$. For instance, $dch(c!5; d?y||c?x) = \{ c, c!, c?, d, d? \}$.

Informally, the statements have the following meanings:

Atomic statements

- `skip` terminates immediately.
- `x := e` assigns the value of expression $e$ to the variable $x$.
- `delay e` suspends execution for (the value of) $e$ time units.
- `c!e` sends the value of expression $e$ on channel $c$ as soon as a corresponding input statement is available. Since we assume synchronous communication, such an output statement is suspended until a parallel process executes an input statement of the form $c?x$.
- `c?x` receives a value via channel $c$ and assigns this value to the variable $x$. Similar to the output statement, such an input statement has to wait for a corresponding output statement before a synchronous communication takes place.

Compound statements

- $S_1; S_2$ indicates sequential composition of $S_1$ and $S_2$.
- Guarded command $[[ \bigwedge_{i=1}^{n} b_i \rightarrow S_i ]]$ is executed as follows. If none of the $b_i$ evaluates to true then this command terminates after the evaluation of the booleans. Otherwise, non-deterministically select one of the $b_i$'s which evaluates to true and execute the corresponding statement $S_i$.
- Guarded command $[[ \bigwedge_{i=1}^{n} b_i; c_i?x_i \rightarrow S_i || b; \text{delay } e \rightarrow S ]]$ is executed as follows. A guard $b_i; c_i?x_i$ or $b; \text{delay } e$ is open if the boolean part evaluates to true. If none of the guards is open, the guarded command terminates after evaluation of the booleans. Otherwise, wait until an io-statement of the open io-guards can be executed and continue with the corresponding $S_i$. If the delay guard is open ($b$ evaluates to true) and no io-guard can be taken within $e$ time units (after the evaluation of the booleans), then $S$ is executed. If $b$ evaluates to true and $e$ yields 0 then $S$ is executed immediately after the evaluation of the booleans. Boolean expressions equivalent to true are often omitted in guards.

Example 2.1 Observe that delay-values can be arbitrary expressions, for instance, $d?x; [d?y \rightarrow S_1 || c?x \rightarrow S_2 || \text{delay } (x + 6) \rightarrow S_3]$.
Example 2.2 By means of a guarded command, we can easily express a time-out. For instance, \([x > 0; c?y \rightarrow z := y \Vert \text{delay} \ 10 \rightarrow \text{skip}]\) informally means that if \(x > 0\) and the input communication can take place within 10 time units then the assignment is executed, otherwise after 10 time units there is a time-out and the skip-statement is executed.

- \(\star G\) indicates repeated execution of guarded command \(G\) as long as one of the guards is open. When none of the guards is open, \(\star G\) terminates.
- \(S_1 | | S_2\) indicates parallel execution of \(S_1\) and \(S_2\). No program variable should occur in both \(S_1\) and \(S_2\), i.e. \(\text{var}(S_1) \cap \text{var}(S_2) = \emptyset\).

Henceforth we use \(\equiv\) to denote syntactic equality.

2.2 Basic Timing Assumptions

In order to describe the real-time behavior of programs, we must make assumptions about the execution time of atomic statements and the extra time needed to execute compound constructs. In our proof system, the correctness of a program with respect to a specification, which may express timing properties, is verified relative to these assumptions. For simplicity, we assume in this paper that there is no overhead for compound statements and that a delay \(e\) statement takes exactly \(e\) time units. Furthermore we assume given positive constants \(K_a\), \(K_c\) and \(K_g\) such that every assignment takes \(K_a\) time units, each communication takes \(K_c\) time units, and the evaluation of the guards in a guarded command takes \(K_g\) time units.

The most important assumption involves parallel composition. Observe that to determine the execution time of a simple program \(x := 0 \Vert y := 1\) we need information about the number of available processors and the allocation of processes on processors. Note that an execution of \(x := 0 \Vert y := 1\) terminates after \(K_a\) time units if both processes \(x := 0\) and \(y := 1\) have their own processor. If, however, the two processes are executed on a single processor then this program will take at least \(2 \times K_a\) time units, since then the processes have to be scheduled in some order. In general, we have to make an assumption about the assignment of processes to processors at parallel composition. In this paper we use the maximal parallelism model to represent the situation that each process has its own processor. Consequently any action is executed as soon as possible. Observe that maximal parallelism implies minimal waiting: a process only waits when it tries to execute an input or output statement and the communication partner is not available. Hence it is never the case that one process waits to perform \(c!e\) and, simultaneously, another process waits to execute \(c?x\). This maximal parallelism assumption has been generalized in [Hoog91a] to multiprogramming where several processes can be executed on a single processor and scheduling is based on priorities which are assigned to statements in the program.

3 Denotational Semantics

To formally define the meaning of a program, we give a denotational semantics for our programming language. In Section 3.1 we define a model to describe computations of programs.
This semantic model is used in Section 4 to interpret our assertion language. In Section 3.2 we present the denotational semantics which is used to define validity of correctness formulas, that is, to define formally when a program satisfies an assertion. Finally, in Section 3.3 we discuss some properties of the semantics.

3.1 Computational Model

In our semantics the timing behavior of a program is expressed from the viewpoint of an external observer with his own clock. Let this clock range over a time domain TIME. Thus, although parallel components of a system might have their own, physical, local clock, the observable behavior of a system is described in terms of a single, conceptual, global clock.

To define the timing behaviour of a statement delay e, we have to relate expressions in the programming language to our time domain. For simplicity we have assumed that delay e takes e time units and hence, implicitly, that VAL \subseteq TIME. Furthermore we assume that the standard operators +, -, \times and \leq are defined on TIME. Note that we allow our time domain to be dense (a domain is dense if between every two points there exists a third point).

Henceforth, we use i, j, \ldots to denote non-negative integers, and \tau, \hat{\tau}, \tau_0, \ldots to denote values from TIME. For notational convenience, we use a special value \infty with the usual properties, such as \infty \not\in TIME, and for all \tau \in TIME \cup \{\infty\}: \tau \leq \infty, \tau + \infty = \infty + \tau = \infty, etc.

A computation of a program is represented by a mapping which assigns to each point of time during this computation a pair consisting of a state and a set of communication records. The state represents the values of the program variables at that point of time. The communication records denote the state of affairs on the channels of the program. To denote the real-time communication behaviour, we use records of the form (c, \vartheta), indicating a communication along channel c with value \vartheta. In addition to the communications at any point of time, the model includes information about those processes waiting to send or waiting to receive messages on their channels at any given time. (The need for this additional information in a compositional framework follows from the fact that this information is present in the fully abstract semantics given in [HGR87] for a similar language.) Using this information, the formalism enforces minimal waiting in our maximal parallelism model by requiring that no pair of processes is ever simultaneously waiting to send and waiting to receive, respectively, on a shared channel. The informal description above is formalized in the following definitions.

Definition 3.1 (States) The set of states STATE is defined as the set of mappings from VAR to VAL, STATE = \{s | s : VAR \rightarrow VAL \}.

Thus a state s \in STATE assigns to each program variable x a value s(x).

Definition 3.2 (Variant) The variant of a state s with respect to a variable x and a value \vartheta, denoted by (s : x \mapsto \vartheta), is defined as (s : x \mapsto \vartheta)(y) = \begin{cases} \vartheta & \text{if } y = x \\ s(y) & \text{if } y \neq x \end{cases}
Definition 3.3 (Communication Records) The set of communication records $COMM$ is defined as:

$$COMM = \{ c! \mid c \in CHAN \} \cup \{ c? \mid c \in CHAN \} \cup \{ (c, \varnothing) \mid c \in CHAN \text{ and } \varnothing \in VAL \}.$$ 

Let $[\tau_0, \tau_1]$ denote a closed interval of time points: $[\tau_0, \tau_1] = \{ \tau \in TIME \mid \tau_0 \leq \tau \leq \tau_1 \}$. Then a model, representing a real-time computation of a program, is defined as follows:

Definition 3.4 (Model) Let $\tau_0 \in TIME$, $\tau_1 \in TIME \cup \{ \infty \}$, and $\tau_1 \geq \tau_0$. A model $\sigma$ is a mapping $\sigma : [\tau_0, \tau_1] \rightarrow STATE \times \varphi(COMM)$. 

Definition 3.5 (Begin/End) For a model $\sigma$ with domain $[\tau_0, \tau_1]$, define $\begin{align*}
\begin{array}{c}
\text{begin}(\sigma) = \tau_0 \\
\text{end}(\sigma) = \tau_1.
\end{array}
\end{align*}$

Consider a model $\sigma$ and a point $\tau$ with $\begin{align*}
\begin{array}{c}
\text{begin}(\sigma) \leq \tau \leq \text{end}(\sigma).
\end{array}
\end{align*}$ Then $\sigma(\tau) = (\text{state}, \text{comm})$ with $\text{state} \in STATE$, and $\text{comm} \subseteq COMM$. Henceforth we refer to the two fields of $\sigma(\tau)$ by $\sigma(\tau).\text{state}$ and $\sigma(\tau).\text{comm}$, respectively. Informally, if $\sigma$ models a computation of a program $S$, $\begin{align*}
\begin{array}{c}
\text{begin}(\sigma) \text{ and } \text{end}(\sigma)
\end{array}
\end{align*}$ denote, resp., the starting time and the termination time of this computation of $S$ ($\text{end}(\sigma) = \infty$ if $S$ does not terminate). Furthermore, $\sigma(\text{begin}(\sigma)).\text{state}$ specifies the initial state of the computation, and if $\text{end}(\sigma) < \infty$ then $\sigma(\text{end}(\sigma)).\text{state}$ gives the final state. In general, $\sigma(\tau).\text{state}$ represents the values of program variables. For a channel name $c$, the set $\sigma(\tau).\text{comm}$ might contain a communication record $(c, \varnothing)$, $c!$ or $c?$ with the following meaning:

- $(c, \varnothing) \in \sigma(\tau).\text{comm}$ if the value $\varnothing$ is transmitted along channel $c$ at time $\tau$;
- $c! \in \sigma(\tau).\text{comm}$ if $S$ is waiting to send along channel $c$ at time $\tau$;
- $c? \in \sigma(\tau).\text{comm}$ if $S$ is waiting to receive along channel $c$ at time $\tau$.

To make the model convenient for sequential composition, we do not look at the $\text{comm}$ field at the last point. Only $\sigma(\text{end}(\sigma)).\text{state}$ is interesting for the specification and reasoning. $\sigma(\text{end}(\sigma)).\text{comm}$ will have an arbitrary value. Henceforth, we use the following definitions.

Definition 3.6 (Channels Occurring in Model) The set of (directional) channels occurring in a model $\sigma$, denoted by $dch(\sigma)$, is defined as $dch(\sigma) = \bigcup_{\begin{align*}
\begin{array}{c}
\text{begin}(\sigma) \leq \tau < \text{end}(\sigma)
\end{array}
\end{align*}} \{ c! \mid c \in \sigma(\tau).\text{comm} \} \cup \{ c? \mid c \in \sigma(\tau).\text{comm} \} \cup \{ c \mid \text{there exists a } \varnothing \text{ such that } (c, \varnothing) \in \sigma(\tau).\text{comm} \}$.

Definition 3.7 (Projection onto Channels) Let $cset \subseteq DCHAN$. Define the projection of a model $\sigma$ onto $cset$, denoted by $[\sigma]_{cset}$, as follows: $\begin{align*}
\begin{array}{c}
\text{begin}([\sigma]_{cset}) = \text{begin}(\sigma), \text{end}([\sigma]_{cset}) = \text{end}(\sigma), \text{for all } \tau, \text{begin}(\sigma) \leq \tau \leq \text{end}(\sigma), [\sigma]_{cset}(\tau).\text{state} = \sigma(\tau).\text{state}, \text{and}
\end{array}
\end{align*}$

$$[\sigma]_{cset}(\tau).\text{comm} = \{ c! \mid c \in \sigma(\tau).\text{comm} \wedge c \in cset \} \cup \{ c? \mid c \in \sigma(\tau).\text{comm} \wedge c \in cset \} \cup \{ (c, \varnothing) \mid (c, \varnothing) \in \sigma(\tau).\text{comm} \wedge c \in cset \}.$$
Definition 3.8 (Projection onto Variables) Let \( vset \subseteq VAR \). Define the projection of a model \( \sigma \) onto \( vset \), denoted by \( \sigma \uparrow vset \), as follows:

\[
\begin{align*}
\text{begin}(\sigma \uparrow vset) &= \text{begin}(\sigma), \\
\text{end}(\sigma \uparrow vset) &= \text{end}(\sigma), \\
\text{for all } \tau, \begin{aligned}
\text{begin}(\sigma) \leq \tau \leq \text{end}(\sigma), \\
(\sigma \uparrow vset)(\tau) \text{.comm} &= \sigma(\tau) \text{.comm},
\end{aligned}
\end{align*}
\]

for all \( x \in VAR \), \( (\sigma \uparrow vset)(\tau) \text{.state}(x) = \begin{cases} 
\sigma(\tau) \text{.state}(x), & \text{if } x \in vset \\
(\sigma(\text{begin}(\sigma)) \text{.state}(x), & \text{if } x \notin vset.
\end{cases} \)

Definition 3.9 (Concatenation) The concatenation of any two models \( \sigma_1 \) and \( \sigma_2 \), denoted by \( \sigma_1 \sigma_2 \), is a model \( \sigma \) such that

- if \( \text{end}(\sigma_1) = \infty \), then \( \sigma = \sigma_1 \);
- if \( \text{end}(\sigma_1) < \infty \), \( \text{end}(\sigma_1) = \text{begin}(\sigma_2) \), and \( \sigma_1(\text{end}(\sigma_1)) \text{.state} = \sigma_2(\text{begin}(\sigma_2)) \text{.state}, \) then \( \sigma \) has domain \( [\text{begin}(\sigma_1), \text{end}(\sigma_2)] \) and is defined as follows:

\[
\sigma(\tau) = \begin{cases} 
\sigma_1(\tau), & \text{for all } \tau, \text{begin}(\sigma_1) \leq \tau < \text{end}(\sigma_1); \\
\sigma_2(\tau), & \text{for all } \tau, \text{begin}(\sigma_2) \leq \tau \leq \text{end}(\sigma_2).
\end{cases}
\]

- otherwise undefined.

Definition 3.10 (Concatenation of Sets of Models) The concatenation of any two sets of models \( \Sigma_1 \) and \( \Sigma_2 \) are defined as follows:

\[
\text{SEQ}(\Sigma_1, \Sigma_2) = \{ \sigma_1 \sigma_2 \mid \sigma_1 \in \Sigma_1 \text{ and } \sigma_2 \in \Sigma_2 \text{ such that } \sigma_1 \sigma_2 \text{ is defined} \}
\]

It is easy to prove that \( \text{SEQ} \) is associative.

### 3.2 Formal Semantics

A good starting point for the development of a compositional proof system is the formulation of a denotational, and hence compositional, semantics. In such a semantics the meaning of a statement must be defined without any information about the environment in which it will be placed. Hence, the semantics of a statement in isolation must characterize all potential computations of the statement. When composing this statement with (part of) its environment, the semantic operators must remove the computations that are no longer possible. To be able to select the correct computations from the semantics, any dependency of an execution on the environment must be made explicit in the semantic model.

To define such a compositional semantics, we first define the evaluation of expressions and boolean expressions in the programming language.

The evaluation of an expression \( e \), denoted by \( \mathcal{E}(e) \), is a function \( \mathcal{E}(e) : \text{STATE} \rightarrow \text{VAL} \), such that

- \( \mathcal{E}(\varnothing)(s) = \varnothing \),
- \( \mathcal{E}(x)(s) = s(x) \),
- \( \mathcal{E}(e_1 + e_2)(s) = \mathcal{E}(e_1)(s) + \mathcal{E}(e_2)(s) \),
- \( \mathcal{E}(e_1 \times e_2)(s) = \mathcal{E}(e_1)(s) \times \mathcal{E}(e_2)(s) \).

We define when a boolean expression \( b \) holds in a state \( s \), denoted by \( B(b)(s) \), as follows:

- \( B(e_1 = e_2)(s) \) iff \( \mathcal{E}(e_1)(s) = \mathcal{E}(e_2)(s) \),
\[ \mathcal{B}(e_1 < e_2)(s) \iff \mathcal{E}(e_1)(s) < \mathcal{E}(e_2)(s), \]
\[ \mathcal{B}(\neg b)(s) \iff \neg \mathcal{B}(b)(s), \text{ and} \]
\[ \mathcal{B}(b_1 \lor b_2)(s) \iff \mathcal{B}(b_1)(s) \text{ or } \mathcal{B}(b_2)(s). \]

The meaning of a program \( S \), denoted by \( \mathcal{M}(S) \), is a set of models representing the possible computations of \( S \) starting at any arbitrary time.

**Skip**

A skip-statement terminates immediately without any state change.

\[ \mathcal{M}(\text{skip}) = \{ \sigma \mid \text{begin}(\sigma) = \text{end}(\sigma) \} \]

**Assignment**

An assignment \( x := e \) terminates after \( K_a \) time units (recall that every assignment statement takes \( K_a \) time units to execute). All intermediate states before termination are the same as the initial state. The state at termination also equals to the initial state except that the value of \( x \) is replaced by the value of \( e \) in the initial state. The \( \text{comm} \) field is empty during the execution period since the assignment does not (try to) communicate.

\[ \mathcal{M}(x := e) = \{ \sigma \mid \text{end}(\sigma) = \text{begin}(\sigma) + K_a, \text{ for all } \tau, \text{begin}(\sigma) \leq \tau < \text{end}(\sigma), \]
\[ \sigma(\tau).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}, \sigma(\tau).\text{comm} = \emptyset, \text{ and} \]
\[ \sigma(\text{end}(\sigma)).\text{state} = (\sigma(\text{begin}(\sigma)).\text{state} : x \mapsto \mathcal{E}(e)(\sigma(\text{begin}(\sigma)).\text{state})) \} \]

**Delay \( e \)**

A delay \( e \) statement terminates after exactly (the value of) \( e \) time units.

\[ \mathcal{M}(\text{delay } e) = \{ \sigma \mid \text{end}(\sigma) = \text{begin}(\sigma) + \mathcal{E}(e)(\sigma(\text{begin}(\sigma)).\text{state}), \text{ for all } \tau, \]
\[ \text{begin}(\sigma) \leq \tau < \text{end}(\sigma), \sigma(\tau).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}, \sigma(\tau).\text{comm} = \emptyset, \]
\[ \text{and } \sigma(\text{end}(\sigma)).\text{state} = \sigma(\text{begin}(\sigma)).\text{state} \} \]

**Input and Output**

Observe that in the execution of an io-statement there are, in general, two time-periods: first there is a waiting period during which no communication partner is available (recall that communication is synchronous) and, secondly, when such a partner is ready to communicate, there is a period (of \( K_c \) time units) during which the actual communication takes place. For an output command \( cle \) these two periods are represented by two sets of models \( \text{Wait}(c!) \) and \( \text{Send}(c, e) \) defined below. Then the semantics of \( cle \) is defined as follows.

\[ \mathcal{M}(c!e) = \text{SEQ}(\text{Wait}(c!), \text{Send}(c, e)) \]

with

\[ \text{Wait}(c!) = \{ \sigma \mid \text{there exists } \tau \in \text{TIME} \cup \{ \infty \} \text{ such that } \text{end}(\sigma) = \tau, \text{ for all } \tau_1, \]
\[ \text{begin}(\sigma) \leq \tau_1 < \text{end}(\sigma), \sigma(\tau_1).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}, \sigma(\tau_1).\text{comm} = \{ c! \}, \]
and \( \sigma(\text{end}(\sigma)).\text{state} = \sigma(\text{begin}(\sigma)).\text{state} \)

\[
\begin{align*}
\text{Send}(c, e) &= \{ \sigma \mid \text{end}(\sigma) = \text{begin}(\sigma) + K_c, \text{for all } \tau_1, \text{begin}(\sigma) \leq \tau_1 < \text{end}(\sigma), \\
& \quad \sigma(\tau_1).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}, \sigma(\tau_1).\text{comm} = \{(c, E(c)(\sigma(\text{begin}(\sigma)).\text{state}))\} \\
& \quad \text{and } \sigma(\text{end}(\sigma)).\text{state} = \sigma(\text{begin}(\sigma)).\text{state} \}
\end{align*}
\]

To represent all potential computations of an input statement \( c?x \), the semantics contains a model for every possible value that can be received. The value of \( x \) in the final state equals the value in the communication record.

\[
\mathcal{M}(c?x) = \mathcal{SEQ}(\text{Wait}(c?), \text{Receive}(c, x))
\]

where \( \text{Wait}(c?) \) is defined similar to \( \text{Wait}(c!) \), and

\[
\text{Receive}(c, x) = \{ \sigma \mid \text{end}(\sigma) = \text{begin}(\sigma) + K_c, \text{there exists a value } \emptyset \in \text{VAL} \text{ such that,} \\
& \quad \text{for all } \tau_1, \text{begin}(\sigma) \leq \tau_1 < \text{end}(\sigma), \sigma(\tau_1).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}, \\
& \quad \sigma(\tau_1).\text{comm} = \{(c, \emptyset)\}, \text{and } \sigma(\text{end}(\sigma)).\text{state} = (\sigma(\text{begin}(\sigma)).\text{state} : x \mapsto \emptyset) \}
\]

### Sequential Composition

Using the \( \mathcal{SEQ} \) operator defined before, sequential composition is straightforward:

\[
\mathcal{M}(S_1; S_2) = \mathcal{SEQ}(\mathcal{M}(S_1), \mathcal{M}(S_2))
\]

Since \( \mathcal{SEQ} \) is associative, the sequential composition is also associative.

### Guarded Command

For a guarded command \( G \), first define

\[
b_G = \begin{cases} 
\bigvee_{i=1}^n b_i & \text{if } G = \left[ \prod_{i=1}^n b_i \rightarrow S_i \right] \\
\bigvee_{i=1}^n b_i \lor b & \text{if } G = \left[ \prod_{i=1}^n b_i ; c_i ? x_i \rightarrow S_i ; \text{delay } c \rightarrow S \right]
\end{cases}
\]

Consider \( G = \left[ \prod_{i=1}^n b_i \rightarrow S_i \right] \). Then there are two possibilities: either none of the booleans evaluates to true and the command terminates after \( K_g \) time units, or at least one of the booleans yields true and then the corresponding statement \( S_i \) is executed. Recall that the evaluation of the guards takes \( K_g \) time units. In the semantics below this is represented by statement \( \text{delay } K_g \).

\[
\mathcal{M}(\left[ \prod_{i=1}^n b_i \rightarrow S_i \right]) = \{ \sigma \mid B(\neg b_G)(\sigma(\text{begin}(\sigma)).\text{state}), \text{and } \sigma \in \mathcal{M}(\text{delay } K_g) \} \cup \\
\{ \sigma \mid \text{there exists a } k, 1 \leq k \leq n, \text{ such that } B(b_k)(\sigma(\text{begin}(\sigma)).\text{state}), \text{and } \sigma \in \mathcal{M}(\text{delay } K_g ; S_k) \}
\]

Next, consider \( G = \left[ \prod_{i=1}^n b_i ; c_i ? x_i \rightarrow S_i ; \text{delay } c \rightarrow S \right] \).

We should consider the following four possibilities:

- None of the booleans evaluates to true and then the guarded command terminates after \( K_g \) time units.
- \( b \) evaluates to true and at least one of the \( c_i?x_i \) for which \( b_i \) evaluates to true can perform the communication within \( e \) time units after the evaluation of the booleans, then the corresponding \( S_i \) is executed.
• $b$ evaluates to true and none of the open io-guards can perform a communication within $e$ time units after the evaluation of the booleans, then $S$ is executed.

• $b$ evaluates to false, then the command waits to communicate on those $c_i$ whose guards are open.

This leads to the following definition:

$$M([\prod_{i=1}^{n} b_i; c_i?x_i \rightarrow S_i; \prod b; \text{delay } e \rightarrow S]) =$$

$$\{\sigma | B(-b_G)(\sigma(\text{begin}(\sigma)).\text{state}), \text{and } \sigma \in M(\text{delay } K_g)\} \cup$$

$$\text{SEQ}(M(\text{delay } K_g), \text{BoundWait}(G), \text{Comm}(G)) \cup$$

$$\text{SEQ}(M(\text{delay } K_g), \text{TimeOut}(G), M(S)) \cup$$

$$\text{SEQ}(M(\text{delay } K_g), \text{AnyWait}(G), \text{Comm}(G))$$

where

$$W\text{ait}(G) = \{\sigma | B(b_G)(\sigma(\text{begin}(\sigma)).\text{state}), \text{there exists } a \in \text{TIME} \cup \{\infty\} \text{ such that}$$

for all $\tau_i, \text{begin}(\sigma) \leq \tau_i < \text{end}(\sigma), \sigma(\tau_i).\text{state} = \sigma(\text{begin}(\sigma)).\text{state},$

$$\sigma(\tau_i).\text{comm} = \{c_i? | B(b_i)(\sigma(\text{begin}(\sigma)).\text{state}), 1 \leq i \leq n \},$$

$$\sigma(\text{end}(\sigma)).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}, \text{and } \sigma(\text{end}(\sigma)) = \tau\}$$

$$\text{Comm}(G) = \{\sigma | \text{there exists a } k, 1 \leq k \leq n, \text{such that } B(b_k)(\sigma(\text{begin}(\sigma)).\text{state}), \text{and}$$

$$\sigma \in \text{SEQ}(\text{Receive}(c_k, x_k), M(S_k))\}$$

$$\text{BoundWait}(G) = \{\sigma | \sigma \in \text{Wait}(G), B(b)(\sigma(\text{begin}(\sigma)).\text{state}), \text{and}$$

$$\text{end}(\sigma) < \text{begin}(\sigma) + \varepsilon(e)(\sigma(\text{begin}(\sigma)).\text{state})\}$$

$$\text{TimeOut}(G) = \{\sigma | \sigma \in \text{Wait}(G), B(b)(\sigma(\text{begin}(\sigma)).\text{state}), \text{and}$$

$$\text{end}(\sigma) = \text{begin}(\sigma) + \varepsilon(e)(\sigma(\text{begin}(\sigma)).\text{state})\}$$

$$\text{AnyWait}(G) = \{\sigma | \sigma \in \text{Wait}(G) \text{ and } B(-b)(\sigma(\text{begin}(\sigma)).\text{state})\}$$

**Iteration**

For a model in the semantics of the iteration construct $\ast G$ we have the following possibilities:

• Either it is the concatenation of a finite sequence of models from $M(G)$ such that the last model corresponds to an execution where all boolean guards evaluate to false or it represents a non-terminating computation of $G$.

• Or it is the concatenation of an infinite sequence of models from $M(G)$ that all represent terminating computations in which not all booleans yield the value false.

This leads to the following definition:

$$M(\ast G) = \{\sigma | \text{there exist a } k \in \mathbb{N}, k \geq 1, \text{ and } \sigma_1, \ldots, \sigma_k \text{ such that } \sigma = \sigma_1 \cdots \sigma_k,$$

for all $i, 1 \leq i \leq k, \sigma_i \in M(G), \text{for all } j, 1 \leq j \leq k - 1, \text{end}(\sigma_j) < \infty,$

$$B(b_G)(\sigma_j(\text{begin}(\sigma_j)).\text{state}), \text{and either } \text{end}(\sigma_k) = \infty \text{ or }$$

$$B(-b_G)(\sigma_k(\text{begin}(\sigma_k)).\text{state})\} \cup \{\sigma | \text{there exists an infinite sequence of models } \sigma_1, \sigma_2, \ldots \text{ such that } \sigma = \sigma_1 \sigma_2 \cdots ,$$

for all $i \geq 1, \sigma_i \in M(G), \text{end}(\sigma_i) < \infty, \text{and } B(b_G)(\sigma_i(\text{begin}(\sigma_i)).\text{state})\}$$
Parallel Composition

The semantics of $S_1 \parallel S_2$ consists of all models $\sigma$ such that there exist models $\sigma_1 \in \mathcal{M}(S_1)$ and $\sigma_2 \in \mathcal{M}(S_2)$ such that the $comm$-field of $\sigma$ is the point-wise union of the $comm$-fields of $\sigma_1$ and $\sigma_2$, provided the following requirements are fulfilled:

1. $end(\sigma) = max(end(\sigma_1), end(\sigma_2))$, to express that $S_1 \parallel S_2$ terminates when both processes have terminated.

2. Since communication is synchronous, $S_1$ and $S_2$ should communicate simultaneously on shared channels which connect the two processes.

3. In our execution model we assume minimal waiting for communications, i.e. two processes should not be simultaneously waiting to send and waiting to receive on a shared channel. Formally, for all $\tau$, $begin(\sigma) \leq \tau < end(\sigma)$ and for all $c \in dch(S_1) \cap dch(S_2)$:
   
   $\neg((c! \in \sigma(\tau).comm \land c? \in \sigma(\tau).comm))$.

For the $state$-field of $\sigma$, recall that there are no shared variables, i.e. $var(S_1) \cap var(S_2) = \emptyset$. Hence the value of a variable $x$ during the execution of $S_1 \parallel S_2$ can be obtained from the state of $S_i$ if $x \in var(S_i)$, and from the initial state otherwise. This leads to the following definition for the semantics of parallel composition.

$\mathcal{M}(S_1 \parallel S_2) = \{ \sigma \mid dch(\sigma) \subseteq dch(S_1) \cup dch(S_2), \text{ for } i = 1, 2, \text{ there exist } \sigma_i \in \mathcal{M}(S_i) \}
\begin{array}{l}
\text{such that } begin(\sigma) = begin(\sigma_1) = begin(\sigma_2), \\
end(\sigma) = max(end(\sigma_1), end(\sigma_2)), \\
[s]_{dch(S_i)(\tau)}.comm = \begin{cases}
\sigma_i(\tau).comm & begin(\sigma_i) \leq \tau < end(\sigma_i) \\
\emptyset & end(\sigma_i) \leq \tau < end(\sigma) 
\end{cases} \\
\begin{array}{l}
(s \uparrow var(S_i))_{\tau}.state = \begin{cases}
\sigma_i(\tau).state & begin(\sigma_i) \leq \tau \leq end(\sigma_i) \\
\sigma_i(end(\sigma_i)).state & end(\sigma_i) < \tau \leq end(\sigma) 
\end{cases} \\
\end{array}
\end{array}$

and for all $c \in dch(S_1) \cap dch(S_2)$, for all $\tau$, $begin(\sigma) \leq \tau < end(\sigma)$,

$\neg((c! \in \sigma(\tau).comm \land c? \in \sigma(\tau).comm))$.

We can prove that Parallel composition is commutative and associative.

3.3 Properties of the Semantics

First we define three well-formedness properties.

Definition 3.11 (Well-Formedness) A model $\sigma$ is well-formed iff for all $c \in CHAN$, for all $\vartheta, \vartheta_1, \vartheta_2 \in VAL$, and for all $\tau$, $begin(\sigma) \leq \tau < end(\sigma)$:

1. $\neg((c! \in \sigma(\tau).comm \land c? \in \sigma(\tau).comm))$. 
   (Minimal waiting: It is not allowed to be simultaneously waiting to send and waiting to receive on a particular channel.)
2. $\neg((c, \vartheta) \in \sigma(\tau).comm \land c! \in \sigma(\tau).comm)$ and $\neg((c, \vartheta) \in \sigma(\tau).comm \land c? \in \sigma(\tau).comm)$. 
   (Exclusion: It is not allowed to be simultaneously communicating and waiting to communicate on a given channel.)
3. \((c, \vartheta_1) \in \sigma(\tau).\text{comm} \land (c, \vartheta_2) \in \sigma(\tau).\text{comm} \rightarrow \vartheta_1 = \vartheta_2.\)

(Uniqueness: At most one value is transmitted on a particular channel at any point of time.)

Then we have the following theorem.

**Theorem 3.12** For any program \(S\), if \(\sigma \in \mathcal{M}(S)\) then

1. \(dch(\sigma) \subseteq dch(S)\), and
2. \(\sigma\) is well-formed.

By induction on the structure of \(S\) and the definition of well-formedness, we can easily prove this theorem.

### 4 Assertion Language

We define an assertion language which is based on ordinary linear temporal logic augmented with a global clock variable denoted by \(T\). Intuitively, \(T\) refers to the current point of time during execution. We use \(\text{start}\) to express the starting time of a computation and \(\text{term}\) to denote the termination time of a computation \((\text{term} = \infty\) for a non-terminating computation). We also use \(\text{last}(x)\) to refer to the value of program variable \(x\) at the last state of a computation model. To specify the communication behaviour of programs, we use a primitive \(\text{comm}(c, \text{exp})\) to express a communication along channel \(c\) with value \(\text{exp}\). We also use \(\text{comm}(c)\) to abstract from the value communicated. Furthermore, the assertion language includes primitives \(\text{wait}(c!)\) and \(\text{wait}(c?)\) to denote that processes are waiting to communicate. Similar to the semantics, this is required to express maximal parallelism. By including the strong until operator, \(U\), from classical temporal logic we obtain the standard modal operators. In order to give compositional proof rules for sequential composition and iteration, we add the "combine" operator \(\mathcal{C}\) and the "iterated combine" operator \(\mathcal{C}^*\) from [BKP84]. To express properties of program variables we have expressions of type \(\text{VAL}\). We also have expressions of type \(\text{TIME}\) to allow references to points of time.

In addition to program variables and time variables, specifications may also use so-called logical variables which are not affected by program execution. These logical variables can be used to record the value of a program variable or time variable. Let \(\mathcal{VVAR}\) be a set of logical variables ranging over \(\text{VAL}\), and \(\mathcal{TVAR}\) be a set of logical variables ranging over \(\text{TIME} \cup \{\infty\}\). The syntax of this specification language is given in Table 2, with \(\vartheta \in \text{VAL}, v \in \mathcal{VVAR}, x \in \mathcal{VAR}, \tau \in \text{TIME} \cup \{\infty\}, t \in \mathcal{TVAR},\) and \(c \in \text{CHAN}\).

Let \(dch(\varphi)\) denote the set of all \(c, c!,\) or \(c?\) occurring in \(\varphi\), and \(\var{\varphi}\) denote the set of all program variables in \(\varphi\).

To interpret logical variables we use a logical variable environment \(\gamma\), which is a mapping which assigns a value from \(\text{VAL}\) to each logical variable \(v \in \mathcal{VVAR}\) and a value from \(\text{TIME} \cup \{\infty\}\) to each logical variable \(t \in \mathcal{TVAR}\). The values of \(v\) and \(t\) in an environment \(\gamma\) are denoted by \(\gamma(v)\) and \(\gamma(t)\), respectively.
The interpretation of assertions is defined over the computational model of section 3.1. First we define the value of expression \( vexp \) in a model \( a \) at time \( T \) as:

- \( \mathcal{V}(\emptyset)\gamma(a, T) = \emptyset \)
- \( \mathcal{V}(v)\gamma(a, T) = \gamma(v) \)
- \( \mathcal{V}(x)\gamma(a, T) = \begin{cases} a(T).state(x) & \text{if } T \leq \text{end}(a) \\ a(\text{end}(a)).state(x) & \text{if } T > \text{end}(a) \end{cases} \)
- \( \mathcal{V}(\text{last}(x))\gamma(a, T) = \sigma(\text{end}(a)).state(x) \)
- \( \mathcal{V}(vexp_1 + vexp_2)\gamma(a, T) = \mathcal{V}(vexp_1)\gamma(a, T) + \mathcal{V}(vexp_2)\gamma(a, T) \)
- \( \mathcal{V}(vexp_1 \times vexp_2)\gamma(a, T) = \mathcal{V}(vexp_1)\gamma(a, T) \times \mathcal{V}(vexp_2)\gamma(a, T) \)

Next we define the value of time-expression \( texp \) in a model \( a \) at time \( T \) as:

- \( \mathcal{T}(\hat{t})\gamma(a, T) = \hat{t} \)
- \( \mathcal{T}(t)\gamma(a, T) = \gamma(t) \)
- \( \mathcal{T}(T)\gamma(a, T) = T \)
- \( \mathcal{T}(\text{start})\gamma(a, T) = \text{begin}(a) \)
- \( \mathcal{T}(\text{term})\gamma(a, T) = \text{end}(a) \)
- \( \mathcal{T}(vexp)\gamma(a, T) = \mathcal{V}(vexp)\gamma(a, T) \)
- \( \mathcal{T}(texp_1 + texp_2)\gamma(a, T) = \mathcal{T}(texp_1)\gamma(a, T) + \mathcal{T}(texp_2)\gamma(a, T) \)
- \( \mathcal{T}(texp_1 - texp_2)\gamma(a, T) = \mathcal{T}(texp_1)\gamma(a, T) - \mathcal{T}(texp_2)\gamma(a, T) \)
- \( \mathcal{T}(texp_1 \times texp_2)\gamma(a, T) = \mathcal{T}(texp_1)\gamma(a, T) \times \mathcal{T}(texp_2)\gamma(a, T) \)

The interpretation of an assertion \( \varphi \) at time \( T \geq \text{begin}(a) \) in a model \( a \) and environment \( \gamma \) is denoted by \( \langle a, T \rangle \gamma |= \varphi \) and defined by induction on the structure of \( \varphi \):

- \( \langle a, T \rangle \gamma |\!|= texp_1 = texp_2 \text{ iff } T(texp_1)\gamma(a, T) = T(texp_2)\gamma(a, T) \).
- \( \langle a, T \rangle \gamma |\!|= texp_1 < texp_2 \text{ iff } T(texp_1)\gamma(a, T) < T(texp_2)\gamma(a, T) \).
- \( \langle a, T \rangle \gamma |\!|= \text{comm}(c, vexp) \text{ iff } T < \text{end}(a) \text{ and } (c, \mathcal{V}(vexp)\gamma(a, T)) \in \sigma(T).\text{comm} \).
- \( \langle a, T \rangle \gamma |\!|= \text{comm}(c) \text{ iff } T < \text{end}(a) \text{ and there exists a value } \vartheta \in \text{VAL such that } (c, \vartheta) \in \sigma(T).\text{comm} \).
- \( \langle a, T \rangle \gamma |\!|= \text{wait}(c!) \text{ iff } T < \text{end}(a) \text{ and } c! \in \sigma(T).\text{comm} \).
- \( \langle a, T \rangle \gamma |\!|= \text{wait}(c?) \text{ iff } T < \text{end}(a) \text{ and } c? \in \sigma(T).\text{comm} \).
• \( (a, T) \gamma \models \varphi_1 \lor \varphi_2 \iff (a, T) \gamma \models \varphi_1 \) or \( (a, T) \gamma \models \varphi_2 \).
• \( (a, T) \gamma \models \neg \varphi \iff \neg (a, T) \gamma \models \varphi \).
• \( (a, T) \gamma \models \varphi_1 \lor \varphi_2 \iff \) there exists a \( \tau_2 \geq \tau \), such that \( (a, \tau_2) \gamma \models \varphi_2 \), and for all \( \tau_1, \tau \leq \tau_1 < \tau_2 : (a, \tau_1) \gamma \models \varphi_1 \).
• \( (a, T) \gamma \models \varphi_1 \land \varphi_2 \iff \) there exist models \( \sigma_1 \) and \( \sigma_2 \) such that \( \sigma = \sigma_1 \sigma_2, \) \( end(\sigma_1) \geq \tau \), \( (a, T) \gamma \models \varphi_1 \), and \( (a, begin(\sigma_2)) \gamma \models \varphi_2 \).
• \( (a, T) \gamma \models \varphi_1 \Rightarrow \varphi_2 \iff \) either there exist a \( k \geq 1 \) and models \( \sigma_1, \ldots, \sigma_k \) such that \( \sigma = \sigma_1 \cdots \sigma_k \),
\[
(\sigma_1, \tau) \gamma \models \varphi_1, \quad \tau \leq end(\sigma_1) < \infty, \quad \text{for all } j, 2 \leq j \leq k - 1, \quad (a, begin(\sigma_j)) \gamma \models \varphi_1, \quad end(\sigma_j) < \infty, \quad \text{and if end(\sigma_k) < \infty then } (a, begin(\sigma_k)) \gamma \models \varphi_2, \quad \text{otherwise}
\]
\( (a, \tau) \gamma \models \varphi_1 \); 

- or there exist infinite models \( \sigma_1, \sigma_2, \sigma_3, \ldots \) such that \( \sigma = \sigma_1 \sigma_2 \sigma_3 \cdots, \) \( end(\sigma_i) \geq \tau \),
\[
\text{for all } i \geq 1, \quad end(\sigma_i) < \infty, \quad (a, \tau) \gamma \models \varphi_1, \quad \text{and for all } j \geq 2, \quad (a, begin(\sigma_j)) \gamma \models \varphi_1.
\]

We use the standard abbreviations such as \( true \equiv 0 = 0, \varphi_1 \land \varphi_2 \equiv \neg (\neg \varphi_1 \lor \neg \varphi_2) \), \( \varphi_1 \lor \varphi_2 \equiv \neg \varphi_1 \lor \varphi_2 \lor \exp_1 \leq \exp_2 \equiv \exp_1 = \exp_2 \lor \exp_1 < \exp_2 \lor \exp_1 = \exp_2 \lor \exp_1 < \exp_2 \), etc.

In the proof system we will frequently use the following abbreviations:

- For a finite set \( cset \) of channels and directional channels, define \( empty(cset) \equiv \Lambda_{c \in cset} \neg wait(c) \land \Lambda_{c \in cset} \neg wait(c?) \land \Lambda_{c \in cset} \neg comm(c) \).

- For a finite set \( vset \) of program variables, define \( inv(vset) \equiv \Lambda_{x \in vset} x = v_x \Rightarrow \Box (x = v_x) \) where \( v_x \) is a logical variable recording the initial value of \( x \).

Furthermore we have the usual abbreviations from temporal logic:

- \( \Diamond \varphi \equiv true \lor \varphi \) (eventually \( \varphi \) will be true)

- \( \square \varphi \equiv \neg \Diamond \neg \varphi \) (henceforth \( \varphi \) will be true)

- \( \varphi_1 \lor \varphi_2 \equiv (\varphi_1 \lor \varphi_2) \lor \Diamond \varphi_1 \) (weak until: either eventually \( \varphi_2 \) will hold and until that point \( \varphi_1 \) holds continuously, or \( \varphi_1 \) holds henceforth)

Next we define validity of assertions and correctness formulas of the form \( S \sat \varphi \).

Definition 4.1 (Valid Assertion) An assertion \( \varphi \) is valid, denoted by \( \models \varphi \), iff
\[ (a, \begin{begin} \sigma \end{begin}) \gamma \models \varphi \text{ for any model } \sigma \text{ and any environment } \gamma. \]

For instance, \( \models T = \begin{start} \end{start}, \models T = t \rightarrow \Box (T \geq t), \models \Box (T = \begin{term} \end{term} \land x = v \rightarrow \Box x = v), \) and
\[ \models \Box (T = \begin{term} \end{term} \rightarrow \Box empty(\{c\})). \]

Definition 4.2 (Satisfaction) A program \( S \) satisfies an assertion \( \varphi \), denoted by
\[ \models S \sat \varphi, \text{ if } (a, begin(\sigma)) \gamma \models \varphi \text{ for any } \sigma \in \mathcal{M}(S) \text{ and any environment } \gamma. \]

We also say that \( S \sat \varphi \) is valid if \( \models S \sat \varphi \).

Finally we give a few simple examples to illustrate our assertion language. General safety properties can be specified, e.g.,
• Program $S$ does not terminate: $S$ sat $term = \infty$.
  Note that we could also use $S$ sat $\square \neg (T = term)$.
• $S$ does not perform any communication along channel $c$: $S$ sat $\square \neg \text{comm}(c)$.

Some examples of real-time safety properties:
• If $S$ starts its execution with $x = 0$, then $S$ will terminate in less than 5 time units with $x = 8$: $S$ sat $x = 0 \rightarrow term \leq start + 5 \land \text{last}(x) = 8$.
• If $S$ communicates on channel $c$ then $S$ is waiting to send or communicating on channel $d$ within 25 time units:
  $S$ sat $\square (T = t \land \text{comm}(c) \rightarrow \diamond (T \leq t + 25 \land (\text{wait}(d) \lor \text{comm}(d))))$.
  Note that logical variable $t$ is implicitly universally quantified.
• During the execution of $S$, the program variable $x$ has value 5 at 3 time units after the start of the execution, after 5 time units $x$ has value 8 and $y$ has value 9, and finally after 7 time units program $S$ terminates with $x = 10$ and $y = 12$:
  $S$ sat $\square ((T = \text{start} + 3 \rightarrow x = 5) \land (T = \text{start} + 5 \rightarrow x = 8 \land y = 9) \land (T = \text{start} + 7 \rightarrow x = 10 \land y = 12)) \land \text{term} = \text{start} + 7$.

Liveness properties can also be expressed:
• $S$ terminates: $S$ sat $term < \infty$. (Or, equivalently, $S$ sat $\diamond T = term$.)
• $S$ either communicates along channel $c$ infinitely often or eventually it waits forever to send on $c$: $S$ sat $(\square \diamond \text{comm}(c)) \lor (\square \text{wait}(c!))$.

5 Proof System

In this section, we give a compositional proof system for our correctness formulae. First we formulate axioms and rules which are generally applicable to any statement. Next we axiomatize the programming language by formulating axioms and rules for all atomic statements and compound programming constructs.

Let $vexp_1$, $vexp_2$ be expressions of type VAL. The well-formedness properties of the semantics models are axiomatized by the following axiom, for any finite $cset \subseteq DCHAN$:

**Axiom 5.1 (Well-Formedness)** $S$ sat $WF_{cset}$

where

- $WF_{cset} \equiv \square (\text{MinWait}_{cset} \land \text{Exclusion}_{cset} \land \text{Unique}_{cset})$
- $\text{MinWait}_{cset} \equiv \land_{\{c!\in cset\}} \neg (\text{wait}(c!) \land \text{wait}(c?))$
- $\text{Exclusion}_{cset} \equiv \land_{\{c!\in cset\}} \neg (\text{comm}(c) \land \text{wait}(c!)) \land \land_{\{c?,c\in cset\}} \neg (\text{comm}(c) \land \text{wait}(c?))$
- $\text{Unique}_{cset} \equiv \land_{c\in cset} \text{comm}(c,vexp_1) \land \text{comm}(c,vexp_2) \rightarrow vexp_1 = vexp_2$

The next general axiom expresses that a program does not (try to) communicate on channels that do not syntactically occur in the program. For each finite set $cset \subseteq DCHAN$, we have the following axiom:

**Axiom 5.2 (Communication Invariance)** $S$ sat $\square \emptyset(cset)$

provided $cset \cap dch(S) = \emptyset$. 

16
Similarly, the proof system has an axiom to express that certain program variables are not changed by a program. Then the following axiom expresses that if \( x \notin wvar(S) \) then \( x \) will not be changed by \( S \).

**Axiom 5.3 (Variable Invariance)** \( S \) sat \( \text{inv}(\{x\}) \)
provided \( x \notin wvar(S) \).

Furthermore, we have the usual conjunction rule and consequence rule.

**Axiom 5.4 (Conjunction)** \[
\frac{S \text{ sat } \varphi_1, S \text{ sat } \varphi_2}{S \text{ sat } \varphi_1 \land \varphi_2}
\]

**Axiom 5.5 (Consequence)** \[
\frac{S \text{ sat } \varphi_1, \varphi_1 \rightarrow \varphi_2}{S \text{ sat } \varphi_2}
\]

Next we give axioms for five atomic statements. Statement **skip** terminates immediately.

**Axiom 5.6 (Skip)** \( \text{skip} \) sat \( \text{term} = \text{start} \)

The assignment axiom expresses that \( x := e \) terminates after \( K_a \) time units and that the final value of \( x \) equals the value of \( e \) in the initial state. If \( x \) occurs in the expression \( e \), the initial value of \( x \) is needed to evaluate the value of \( e \). Therefore we use a logical variable \( v \) to record the initial value of \( x \).

**Axiom 5.7 (Assignment)** \[
x := e \text{ sat } x = v \rightarrow (x = v \lor (T = \text{term} = \text{start} + K_a \land x = e[v/x]))
\]

**Example 5.1** With this axiom and the Consequence Rule we can derive, for instance,
\[
x := x + 1 \text{ sat } x = v \rightarrow \Diamond(x = v + 1 \land T = \text{term} = \text{start} + K_a).
\]

**Example 5.2** We show that we can derive
\[
x := y + 4 \text{ sat } y = 5 \rightarrow \Diamond(x = y + 4 \land T = \text{term} = \text{start} + K_a).
\]
By the Assignment Axiom and the Consequence Rule we obtain
\[
x := y + 4 \text{ sat } x = v \rightarrow \Diamond(x = y + 4 \land T = \text{term} = \text{start} + K_a).
\]
Since \( v \) does not occur in the consequence of this implication, we can substitute \( x \) for \( v \).

By the Consequence Rule, this leads to
\[
x := y + 4 \text{ sat } \Diamond(x = y + 4 \land T = \text{term} = \text{start} + K_a).
\]
Since \( y \notin wvar(x := y + 4) \), we can derive from the Variable Invariance Axiom
\[
x := y + 4 \text{ sat } y = v \rightarrow \Box y = v.
\]
Hence, by the Conjunction Rule and the Consequence Rule,
\[
x := y + 4 \text{ sat } y = v \rightarrow \Diamond(x = v + 4 \land T = \text{term} = \text{start} + K_a).
\]
Since \( y = v \rightarrow \Diamond(x = v + 4 \land T = \text{term} = \text{start} + K_a) \) implies \( y = 5 \rightarrow \Diamond(x = 9 \land T = \text{term} = \text{start} + K_a) \), the Consequence Rule leads to
\[
x := y + 4 \text{ sat } y = 5 \rightarrow \Diamond(x = 9 \land T = \text{term} = \text{start} + K_a).
\]

Statement **delay \( e \)** terminates after exactly (the value of) \( e \) time units.
Axiom 5.8 (Delay) \[ \text{delay } e \text{ sat } \text{term} = \text{start} + e \]

An output statement starts waiting to send a message, and as soon as a communication partner is available the communication takes place during \(K_c\) time units. Note that we use a weak until operator in the axiom below to allow an infinite waiting period (i.e., deadlock) when no partner becomes available.

Axiom 5.9 (Output) \[ c!e \text{ sat } \text{wait}(c!) \cup (T = \text{term} - K_c \land (\text{comm}(c, e) \cup T = \text{term})) \]

Similarly, an input statement \(c?x\) waits to receive a value on the channel \(c\). When the communication finishes the value received is assigned to variable \(x\). Thus at the last state of the execution model \(x\) possesses that value.

Axiom 5.10 (Input) \[ c?x \text{ sat } x = v \rightarrow [(x = v \land \text{wait}(c?)) \cup (T = \text{term} - K_c \land (\text{comm}(c, \text{last}(x))) \cup T = \text{term})] \]

Using the \(C\) operator we can easily formulate an inference rule for sequential composition.

Rule 5.11 (Sequential Composition Rule) \[
\frac{S_1 \text{ sat } \varphi_1, S_2 \text{ sat } \varphi_2}{S_1; S_2 \text{ sat } \varphi_1 \land \varphi_2}
\]

Example 5.3 Consider the program \(x := x + 1; x := x + 2\). By the Assignment Axiom and the Consequence Rule we can derive:

\[
x := x + 1 \text{ sat } x = v_1 \rightarrow [(x = v_1 \land \text{wait}(c?)) \cup (T = \text{term} - K_a \land (x = v_1 + 1))]
\]

\[
x := x + 2 \text{ sat } x = v_2 \rightarrow [(x = v_2 \land \text{comm}(c, \text{last}(x))) \cup (T = \text{term} - K_a \land (x = v_2 + 2))]
\]

Then the Sequential Composition Rule and the Consequence Rule lead to

\[
x := x + 1; x := x + 2 \text{ sat } x = v \rightarrow \Box (T = \text{start} + K_a \land x = v + 1) \land \Box (T = \text{start} + 2 \times K_a \rightarrow x = v + 3)
\]

Note that instead of \(\Box (T = \text{start} + K_a \land x = v + 1))\) we could have used \(\Box (T = \text{start} + K_a \land x = v + 1))\).

Now consider a guarded command \(G\). Recall that \(b_G\) is defined as (see section 3.2)

\[
b_G \equiv \begin{cases} 
\bigvee_{i=1}^{n} b_i & \text{if } G \equiv [\bigcup_{i=1}^{n} b_i \rightarrow S_i] \\
\bigvee_{i=1}^{n} b_i \lor b & \text{if } G \equiv [\bigcup_{i=1}^{n} b_i; c?x_i \rightarrow S_i; \parallel b; \text{delay } e \rightarrow S]
\end{cases}
\]

We use a logical variable \(v_y\) to refer to the initial value of program variable \(y\) where \(y \in \text{var}(G)\). Define \(\text{Quiet} \equiv \bigwedge_{y \in \text{var}(G)} y = v_y \land \text{empty}(\text{ach}(G))\).

First we give an axiom which expresses that if none of the booleans evaluates to true then the guarded command terminates after \(K_y\) time units (during which the booleans are evaluated).

Furthermore we express that there is no activity on the channels of \(G\) and no variable of \(G\) is changed during the evaluation of the guards.

Axiom 5.12 (Guarded Command Evaluation)

\[
G \text{ sat } \bigwedge_{y \in \text{var}(G)} y = v_y \rightarrow (\text{Quiet} \cup (T = \text{start} + K_g \land \bigwedge_{y \in \text{var}(G)} y = v_y)) \land \neg b_G \rightarrow \text{term} = \text{start} + K_g)
\]
Now consider a guarded command with purely boolean guards $G = \{\prod_{i=1}^{n} b_i \rightarrow S_i\}$. If at least one of the booleans yields true then after the evaluation of the booleans (the evaluation period has length $K_g$) one of the statements $S_i$ for which $b_i$ evaluates to true is executed. This leads to the following rule:

**Rule 5.13 (Guarded Command with Purely Boolean Guards)**

\[
S_i \text{ sat } \varphi_i, \text{ for } i = 1, \ldots, n \\
\prod_{i=1}^{n} b_i \rightarrow S_i \text{ sat } b_G \rightarrow \text{term = start + } K_g \text{ C } \prod_{i=1}^{n} (b_i \land \varphi_i)
\]

Next we formulate a rule for $G = \{\prod_{i=1}^{n} b_i; c_i?x_i \rightarrow S_i ; b; \text{delay } e \rightarrow S\}$, using

\[
\begin{align*}
\text{Wait} & \equiv \Lambda_{y \in \text{var}(G)} y = v_y \land \text{empty(dch}(G) - \{c_1?, \ldots, c_n?\}) \land \\
& \quad (b \rightarrow T < \text{start} + e) \land \Lambda_{i=1}^{n} (b_i \rightarrow \text{wait}(c_i)), \\
\text{InTime} & \equiv \Lambda_{y \in \text{var}(G)} y = v_y \land T = \text{term} \land (b \rightarrow T < \text{start} + e), \\
\text{EndTime} & \equiv \Lambda_{y \in \text{var}(G)} y = v_y \land b \land T = \text{term} = \text{start} + e, \\
\text{Eval} & \equiv \text{term} = \text{start} + K_g, \\
\text{Comm} & \equiv (\text{Wait} \cup \text{InTime}) \text{ C } \prod_{i=1}^{n} (b_i \land \varphi_i \land \text{comm}(c_i)), \text{ and } \\
\text{Timeout} & \equiv (\text{Wait} \cup \text{EndTime}) \text{ C } \varphi.
\end{align*}
\]

**Rule 5.14 (Guarded Command with IO-guards)**

\[
\begin{align*}
c_i?x_i; S_i \text{ sat } \varphi_i, \text{ for } i = 1, \ldots, n, \ S \text{ sat } \varphi \\
\prod_{i=1}^{n} b_i; c_i?x_i \rightarrow S_i \prod b; \text{delay } e \rightarrow S \text{ sat } \\
\Lambda_{y \in \text{var}(G)} y = v_y \land b_G \rightarrow \text{Eval} \text{ C } (\text{Comm C Timeout})
\end{align*}
\]

The inference rule for an iterated guarded command is:

**Rule 5.15 (Iteration)**

\[
G \text{ sat } \varphi \quad \star G \text{ sat } (b_G \land \varphi) \text{ C } (\neg b_G \land \varphi)
\]

Next consider parallel composition of $S_1$ and $S_2$. Suppose we have deduced specifications $\varphi_1$ and $\varphi_2$ for, respectively, $S_1$ and $S_2$. If $\varphi_1$ and $\varphi_2$ do not contain $\text{term}$ then we have the following simple rule:

**Rule 5.16 (Simple Parallel Composition)**

\[
S_1 \text{ sat } \varphi_1, S_2 \text{ sat } \varphi_2, \text{ neither } \varphi_1 \text{ nor } \varphi_2 \text{ contain } \text{term} \\
S_1||S_2 \text{ sat } \varphi_1 \land \varphi_2
\]

provided $\text{dch}(\varphi_i) \subseteq \text{dch}(S_i)$ and $\text{var}(\varphi_i) \subseteq \text{var}(S_i)$, for $i = 1, 2$.

If one of $\varphi_1$ and $\varphi_2$ contains $\text{term}$, we have to take into account that the termination times of $S_1$ and $S_2$ are, in general, different. Observe that if $S_1$ terminates after (or at the same time as) $S_2$ then the model representing this computation satisfies $\varphi_1 \land (\varphi_2 \text{ C } \text{true})$. Furthermore we have to express that the variables of $S_2$ are not changed and there is no activity on the channels of $S_2$ after the termination of $S_2$. Similarly, for $S_1$ and $S_2$ interchanged. Then it leads to the following general rule for parallel composition:
Rule 5.17 (Parallel Composition) Let $\psi_1 \equiv inv(var(S_2)) \land \square empty(dch(S_2))$ and $\psi_2 \equiv inv(var(S_1)) \land \square empty(dch(S_1))$.

\[
\frac{S_1 \text{ sat } \psi_1, S_2 \text{ sat } \psi_2}{S_1 \parallel S_2 \text{ sat } (\psi_1 \land (\psi_2 \lor \psi_1)) \lor (\psi_2 \land (\psi_1 \lor \psi_2))}
\]

provided $dch(\psi_1) \subseteq dch(S_1)$ and $var(\psi_1) \subseteq var(S_1)$, for $i = 1, 2$.

Example 5.4 Consider a program $c!5 \parallel c?x$. Since we have assumed maximal parallelism, the communication takes place immediately, and hence this program should satisfy $comm(c, 5) U (T = term = start + K_c \land x = 5)$. By the Input and Output Axioms and the Consequence Rule, we obtain $c!5 \text{ sat } \psi_1$ and $c?x \text{ sat } \psi_2$ with

$\psi_1 \equiv wait(c!) U (T = term - K_c \land (comm(c, 5) U T = term))$ and

$\psi_2 \equiv wait(c?) U (T = term - K_c \land (comm(c, x) U T = term) \land (x = v_1 \rightarrow (x = v_1)))$.

Suppose $\psi_1 \equiv inv(\{x\}) \land \square empty(\{c, e\})$ and $\psi_2 \equiv \square empty(\{c, e\})$. Then the General Parallel Composition Rule leads to

$c!5 \parallel c?x \text{ sat } (\psi_1 \land (\psi_2 \lor \psi_1)) \lor (\psi_2 \land (\psi_1 \lor \psi_2))$.

The Well-Formedness Axiom and the Conjunction Rule allow us to add $MinWait_{\{c, e\}}$, $Exclusion_{\{c, e\}}$, and $Unique_{\{c\}}$ to $(\psi_1 \land (\psi_2 \lor \psi_1)) \lor (\psi_2 \land (\psi_1 \lor \psi_2))$. Consider $\psi_1 \land (\psi_2 \lor \psi_1) \land MinWait_{\{c, e\}} \land Exclusion_{\{c, e\}} \land Unique_{\{c\}}$. It implies $\psi_1 \land (\psi_2 \lor \psi_1) \land (comm(c, 5) U T = term) \lor (comm(c, 5) U T = term)$ which implies $T = term - K_c \land (comm(c, 5) U T = term) \land (x = 5)$. Since $\models T = start$, we can then derive $comm(c, 5) U (T = term = start + K_c \land x = 5)$.

Similarly, we have $d?x; c?y \text{ sat } (wait(d?) \land comm(d)) U (comm(d) \land \square empty(d))$.

Using the Conjunction Rule and the Consequence Rule, we can combine these two formulae into $c!0; d!1 \parallel d?x; c?y \text{ sat } (wait(c!) \land \square empty(c) \land \square empty(d)) U (comm(c) \land \square empty(d))$.

Since $((wait(c!) \land \square empty(c) \land \square empty(d))) U (comm(c) \land \square empty(d)) \land (comm(c) \land \square empty(d)) \land (comm(c) \land \square empty(d)) \land (\square empty(c) \land \square empty(d)) \land (\square empty(c) \land \square empty(d))$.

Example 5.5 Consider program $c!0; d!1 \parallel d?x; c?y$. Since this program leads to deadlock, we should be able to prove $c!0; d!1 \parallel d?x; c?y \text{ sat } (wait(c!) \land \square empty(d))$.

By the Output Axiom, the Communication Invariance Axiom, and the Consequence Rule, we can derive $c!0 \text{ sat } wait(c!) U comm(c) \land c!0 \text{ sat } \square \neg comm(d)$.

Using the Conjunction Rule and the Consequence Rule, we can combine these two formulae into $c!0 \text{ sat } (wait(c!) \land \neg comm(d)) U (comm(c) \land \neg comm(d))$.

Since $((wait(c!) \land \neg comm(d)) U (comm(c) \land \neg comm(d))) \land (comm(c) \land \neg comm(d)) \land (\neg comm(c) \land \neg comm(d))$.

Similarly, we have $d?x; c?y \text{ sat } (wait(d?) \land \neg comm(d)) U (comm(d) \land \neg comm(d))$.

From the Simple Parallel Composition Rule, we obtain $c!0; d!1 \parallel d?x; c?y \text{ sat } (\neg comm(c) \land \neg comm(d)) U (comm(c) \land \neg comm(d)) \land \neg comm(d))$.

\[\text{\Box} \]
Clearly this assertion implies \((\text{wait}(c) \land \text{wait}(d))\) and hence, by the Consequence Rule, \(c!0; d!1 || d?x; c?y \text{ sat } \Box (\text{wait}(c) \land \text{wait}(d))\).

### 6 Soundness and Completeness

In order to prove the soundness of our proof system, we need the following lemmas.

**Lemma 6.1** For any expression \(e\) from the programming language, any model \(\sigma\), any environment \(\gamma\), and any \(\tau \in \text{TIME}\), \(\gamma \geq \text{begin}(\sigma), \mathcal{E}(e)(\sigma(\tau).\text{state}) = \mathcal{V}(e)(\gamma(\sigma, \tau)).\)

The proofs of all lemmas can be found in Appendix A.

**Lemma 6.2** For any boolean expression \(b\) from the programming language, any model \(\sigma\), any environment \(\gamma\), and any \(\tau \in \text{TIME}\), \(\gamma \geq \text{begin}(\sigma), \mathcal{B}(b)(\sigma(\tau).\text{state}) \iff (\sigma, \tau) \models b.\)

Regarding the soundness of our real-time proof system, we must show that every formula \(S \text{ sat } \varphi\) derivable in the proof system is indeed valid.

**Theorem 6.3** (Soundness) The proof system is sound.

**Proof:** We have to show that all axioms are valid and all inference rules preserve the validity, i.e. if the hypotheses of any rule are valid, so is the conclusion. For most axioms and inference rules, soundness follows directly from the definition of the semantics, by using Lemma 6.1 and Lemma 6.2. The details of the proof appear in Appendix B.

We would also like the proof system to be complete, i.e. if \(S \text{ sat } \varphi\) is valid then it is derivable from our proof system. Observe that the Consequence Rule relies on implications that are formulae in ECTL (Explicit Clock Temporal Logic), and hence the completeness of our proof system also requires that every valid ECTL formula is provable. Since proof systems for ECTL are beyond the scope of this paper, we prove relative completeness: Every valid specification is derivable in our proof system, assuming that any valid ECTL formula can be proved.

In order to prove the relative completeness of our proof system, we need the following lemmas. The first nine lemmas express some properties of the projection operations.

**Lemma 6.4** For any model \(\sigma\) and any \(\text{cset} \subseteq \text{DCHAN}, \text{dch}(\sigma) \subseteq \text{cset} \iff \sigma = [\sigma]_{\text{cset}}.\)

**Lemma 6.5** For any expression \(vexp\) of type \(\text{VAL}\), any model \(\sigma\), any environment \(\gamma\), and any \(\text{cset} \subseteq \text{DCHAN}, \mathcal{V}(vexp)(\gamma(\sigma, \text{begin}(\sigma))) = \mathcal{V}(vexp)([\sigma]_{\text{cset}}, \text{begin}([\sigma]_{\text{cset}})).\)

**Lemma 6.6** For any expression \(vexp\) of type \(\text{VAL}\), any model \(\sigma\), any environment \(\gamma\), and any \(\text{vset} \subseteq \text{VAR}, \mathcal{V}(vexp)(\gamma(\sigma, \text{begin}(\sigma))) = \mathcal{V}(vexp)(\gamma(\sigma \uparrow \text{vset}, \text{begin}(\sigma \uparrow \text{vset})), \text{if } \text{var}(vexp) \subseteq \text{vset}.)\)
Lemma 6.7 For any expression $texp$ of type $TIME$, any model $\sigma$, any environment $\gamma$, and any $cset \subseteq DCHAN$, $T(texp)(\sigma, begin(\sigma)) = T(texp)(\sigma)|_{cset, begin([\sigma]|_{cset})}$.

Lemma 6.8 For any expression $texp$ of type $TIME$, any model $\sigma$, any environment $\gamma$, and any $vset \subseteq VAR$, $T(texp)(\sigma, begin(\sigma)) = T(texp)(\sigma | vset, begin(\sigma | vset))$, if $\text{var}(texp) \subseteq vset$.

Lemma 6.9 For any $cset \subseteq DCHAN$ and any assertion $\varphi$, if $dch(\varphi) \subseteq cset$, then for any model $\sigma$ and any environment $\gamma$, $(\sigma, \text{begin}(\sigma)) \gamma \models \varphi$ iff $(\sigma|_{cset}, \text{begin}(\sigma|_{cset})) \gamma \models \varphi$.

Lemma 6.10 For any $vset \subseteq VAR$ and any assertion $\varphi$, if $\text{var}(\varphi) \subseteq vset$, then for any model $\sigma$ and any environment $\gamma$, $(\sigma, \text{begin}(\sigma)) \gamma \models \varphi$ iff $(\sigma | vset, \text{begin}(\sigma | vset)) \gamma \models \varphi$.

Lemma 6.11 For any model $\sigma$, any environment $\gamma$, and any $cset_1, cset_2 \subseteq DCHAN$, if $(\sigma, \text{begin}(\sigma)) \gamma \models \square \text{empty}(cset_2 - cset_1)$ then $[\sigma]|_{cset_1 \cup cset_2} = [\sigma]|_{cset_1}$.

Lemma 6.12 For any model $\sigma$, any environment $\gamma$, and any $vset_1, vset_2 \subseteq VAR$, if $(\sigma, \text{begin}(\sigma)) \gamma \models \text{inv}(vset_2 - vset_1)$, then $\sigma \uparrow (vset_1 \cup vset_2) = \sigma \uparrow vset_1$.

The next lemma expresses the relation between a well-formed model and the assertion $WF_{cset}$.

Lemma 6.13 For any model $\sigma$ and any environment $\gamma$, if $dch(\sigma) \subseteq cset$ and $(\sigma, \text{begin}(\sigma)) \gamma \models WF_{cset}$, then $\sigma$ is well-formed.

In order to prove the relative completeness of our system, we need to define a property of assertions called preciseness. Before giving the definition, we first define the following concept.

Definition 6.14 (Invariant) A program variable $x$ is invariant with respect to a model $\sigma$ iff for all $\tau$, $\text{begin}(\sigma) \leq \tau \leq \text{end}(\sigma)$, $\sigma(\tau).\text{state}(x) = \sigma(\text{begin}(\sigma)).\text{state}(x)$.

Next we give the definition of preciseness:

Definition 6.15 (Preciseness) An assertion $\varphi$ is precise for a statement $S$ iff

1. $S \text{ sat } \varphi$, i.e. $(\sigma, \text{begin}(\sigma)) \gamma \models \varphi$, for any $\sigma \in \mathcal{M}(S)$ and any environment $\gamma$;

2. If $\sigma$ is a well-formed model, $dch(\sigma) \subseteq dch(S)$, for any program variable $x \notin \text{wvar}(S)$, $x$ is invariant with respect to $\sigma$, and $(\sigma, \text{begin}(\sigma)) \gamma \models \varphi$ for any environment $\gamma$, then $\sigma \in \mathcal{M}(S)$; and

3. $dch(\varphi) = dch(S)$ and $\text{var}(\varphi) = \text{var}(S)$.

A precise assertion $\varphi$ for $S$ thus characterizes all possible computations of $S$: $\varphi$ is valid for $S$, and any “reasonable” computation satisfying $\varphi$ is a possible computation of $S$.

We first prove that for any program $S$ a precise specification can be derived from the axioms and inference rules (Theorem 6.16). We then show (in Theorem 6.17) that any assertion $\varphi_2$ which is valid for $S$ can be derived from a precise assertion $\varphi_1$ for $S$ and three predicates. Hence, relative completeness follows directly (Theorem 6.18).
Theorem 6.16 If $S$ is a statement then a precise specification for $S$ can be derived by using the proof system.

The proof of this theorem can be found in Appendix C.

Theorem 6.17 If $\varphi_1$ is precise for $S$ and $\varphi_2$ is valid for $S$, then

$\models [\varphi_1 \land WF_{dch(\varphi_1)} \land \Box empty(dch(\varphi_2) - dch(\varphi_1)) \land inv(var(\varphi_2) - var(\varphi_1))] \rightarrow \varphi_2$. 

Proof: Let $\varphi_1$ is precise for $S$ and $\varphi_2$ is valid for $S$. Consider a model $\sigma$ and an environment $\gamma$. Assume $(\sigma, begin(\sigma))\gamma \models \varphi_1 \land WF_{dch(\varphi_1)} \land \Box empty(dch(\varphi_2) - dch(\varphi_1)) \land inv(var(\varphi_2) - var(\varphi_1))$. We show $(\sigma, begin(\sigma))\gamma \models \varphi_2$. By $(\sigma, begin(\sigma))\gamma \models \varphi_1$, Lemma 6.9 leads to $([\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}})\varphi_2$. By Lemma 6.10, $([\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}})var(\varphi_1) \models \varphi_1$. Since $dch(WF_{dch(\varphi_1)}) = dch(\varphi_1)$, we obtain $([\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}})WF_{dch(\varphi_1)}$. Then by Lemma 6.13, $[\sigma]_{dch(\varphi_1)}$ is well-formed. By definition, $[\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}}var(\varphi_1)$ is also well-formed. Since $\varphi_1$ is precise for $S$, we have $dch(\varphi_1) = dch(S)$ and $var(\varphi_1) = var(S)$. By the definition of projection onto variables, every variable $x \notin wvar(S)$ is invariant with respect to $[\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}}var(\varphi_1)$. Hence by the definition of preciseness, $[\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}}var(\varphi_1) \in M(S)$. From $(\sigma, begin(\sigma))\gamma \models \Box empty(dch(\varphi_2) - dch(\varphi_1))$, Lemma 6.11 leads to $[\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}}WF_{dch(\varphi_2)}$. Then by Lemma 6.12, $[\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}}var(\varphi_2) = \sigma \begin{{tag}{\gamma}}var(\varphi_1)$. Thus $[\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}}var(\varphi_1) \cup var(\varphi_2) = [\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}}var(\varphi_1)$. Therefore $[\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}}var(\varphi_1) \cup var(\varphi_2) \in M(S)$. Since $\varphi_2$ is valid for $S$, for any environment $\gamma$, $([\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}}var(\varphi_1) \cup var(\varphi_2)) \begin{{tag}{\gamma}}begin(\sigma) \gamma \models \varphi_2$. From $var(\varphi_2) \subseteq var(\varphi_1) \cup var(\varphi_2)$, Lemma 6.10 leads to $([\sigma]_{dch(\varphi_1)} \begin{{tag}{\gamma}}var(\varphi_1) \cup var(\varphi_2)) \begin{{tag}{\gamma}}begin(\sigma) \gamma \models \varphi_2$. By $dch(\varphi_2) \subseteq (dch(\varphi_1) \cup dch(\varphi_2))$, Lemma 6.9 leads to $(\sigma, begin(\sigma))\gamma \models \varphi_2$. Then we have proved our theorem.

Theorem 6.18 (Relative Completeness) If assertion $\varphi$ is valid for program $S$, then $S \models \varphi$ is derivable in the proof system.

Proof: By Theorem 6.16, we can derive $S \models \varphi_1$ where $\varphi_1$ is a precise assertion for $S$. By the Well-Formedness Axiom we can derive $S \models WF_{dch(\varphi_1)}$. Since $dch(\varphi_1) = dch(S)$, we obtain that $[dch(\varphi) - dch(\varphi_1)] \cap dch(S) = \emptyset$. Then by the Communication Invariance Axiom, $S \models \Box empty(dch(\varphi) - dch(\varphi_1))$. From the Variable Invariance Axiom, we can derive $S \models inv(var(\varphi) - var(\varphi_1))$ since $[var(\varphi) - var(\varphi_1)] \cap dch(S) = \emptyset$. Then the Conjunction Rule leads to $S \models \varphi_1 \land WF_{dch(\varphi_1)} \land \Box empty(dch(\varphi) - dch(\varphi_1)) \land inv(var(\varphi) - var(\varphi_1))$. By Theorem 6.17, $[\varphi_1 \land WF_{dch(\varphi_1)} \land \Box empty(dch(\varphi) - dch(\varphi_1)) \land inv(var(\varphi) - var(\varphi_1))] \rightarrow \varphi$ is valid, and, by our relative completeness assumption, provable. Hence, by the Consequence Rule, $S \models \varphi$ is derivable in the proof system.

7 Conclusion

We have formulated a proof system to verify that a program satisfies a specification written in a version of explicit clock temporal logic. We have also shown that the proof system is
sound, that is, every formula $S \text{ sat } \varphi$ which can be proven in our proof system is indeed valid. Furthermore we have established relative completeness, that is, if valid formulas from our assertion language can be proven, then any valid formula $S \text{ sat } \varphi$ can also be derived in our axiomatic system.

Important is that our axiomatization is compositional, and hence allows us to reduce the complexity of the verification problem. In contrast with for instance [Ost89], we have not required a discrete time domain. Often a dense time domain is convenient, since it allows events to be arbitrary close to each other in time. This is important when reactive systems are modeled. Such systems have an intensive interaction with the environment and external events may occur at any moment of time. Moreover, by having dense time we can easily reason about the timing of atomic actions on one level of abstraction and their refinement into several actions on a lower, more concrete, level. A close look at the development of the theory reveals that this choice is orthogonal to the rest of the theory. Therefore, should for other reasons, e.g., efficient automatic verification, a discrete domain appear more attractive, then this can be substituted without causing changes to the theory elsewhere.

As mentioned in the introduction, the proof system from this paper is closely related to the compositional axiomatization given in [HW89] where MTL is used instead of ECTL. In MTL, explicit bounds are added to the modal operators to obtain quantitative timing. For instance, there is a real-time until operator $\varphi_1 U_{<d} \varphi_2$ which expresses that $\varphi_2$ will be true within $d$ time units and until that point $\varphi_1$ holds. In our framework this operator could be defined as follows: $(\sigma, \tau) \gamma \models \psi_1 U_{<d} \psi_2$ iff there exists a $\tau_1, \tau \leq \tau_1 < \tau + d$, such that $(\sigma, \tau_1) \gamma \models \psi_2$, and for all $\tau_2, \tau \leq \tau_2 < \tau_1, (\sigma, \tau_2) \gamma \models \psi_1$. Observe that $\varphi_1 U_{<d} \varphi_2$ in MTL is equivalent to $T = t - (\varphi_1 U (T < t + d \land \varphi_2))$ in ECTL, where $\varphi_1$ and $\varphi_2$ are formulae in ECTL which are equivalent to $\varphi_1$ and $\varphi_2$, respectively. From this transformation, it is clear that in MTL all timing properties are specified relative to a starting point, whereas ECTL allows direct references to the value of the clock. In future work we will address the precise relation between these two approaches and investigate, by means of examples, which version is most applicable for specific applications.

The present paper is part of a larger, more ambitious, endeavour to describe scheduling with respect to limited resources in an abstract, compositional, manner. The desired abstraction would be to describe how, for a given scheduler and resources, combination of two components influences their execution time without modeling the effect of the scheduler at the computation step level. In this paper we believe to have obtained some more insight in the description of time properties, be it in the limited context of maximal parallelism.

References


Appendix A

Proofs of Lemmas

Proof of Lemma 6.1

Consider any expression $e$ from the programming language, any model $\sigma$, any environment $\gamma$, and any $\tau \in \text{TIME}$, $\tau \geq \text{begin}(\sigma)$. Prove $E(e)(\sigma(\tau).\text{state}) \equiv \mathcal{V}(e)\gamma(\sigma, \tau)$.

**Proof:** We give the proof by induction on the structure of $e$.

- $e \equiv \emptyset$. Then $E(\emptyset)(\sigma(\tau).\text{state}) = \emptyset = \mathcal{V}(\emptyset)\gamma(\sigma, \tau)$.
- $e \equiv x$. Then $E(x)(\sigma(\tau).\text{state}) = \sigma(\tau).\text{state}(x) = \mathcal{V}(x)\gamma(\sigma, \tau)$.
- $e \equiv e_1 + e_2$. By the induction hypothesis,

  $E(e_1)(\sigma(\tau).\text{state}) = \mathcal{V}(e_1)\gamma(\sigma, \tau)$ and
  $E(e_2)(\sigma(\tau).\text{state}) = \mathcal{V}(e_2)\gamma(\sigma, \tau)$.

  Then,
  
  $E(e_1 + e_2)(\sigma(\tau).\text{state}) = E(e_1)(\sigma(\tau).\text{state}) + E(e_2)(\sigma(\tau).\text{state}) = \mathcal{V}(e_1)\gamma(\sigma, \tau) + \mathcal{V}(e_2)\gamma(\sigma, \tau) = \mathcal{V}(e_1 + e_2)\gamma(\sigma, \tau)$.

- $e \equiv e_1 \times e_2$. By the induction hypothesis,

  $E(e_1)(\sigma(\tau).\text{state}) = \mathcal{V}(e_1)\gamma(\sigma, \tau)$ and
  $E(e_2)(\sigma(\tau).\text{state}) = \mathcal{V}(e_2)\gamma(\sigma, \tau)$.

  Then,
  
  $E(e_1 \times e_2)(\sigma(\tau).\text{state}) = E(e_1)(\sigma(\tau).\text{state}) \times E(e_2)(\sigma(\tau).\text{state}) = \mathcal{V}(e_1)\gamma(\sigma, \tau) \times \mathcal{V}(e_2)\gamma(\sigma, \tau) = \mathcal{V}(e_1 \times e_2)\gamma(\sigma, \tau)$.

Proof of Lemma 6.2

Consider any boolean expression $b$ from the programming language, any model $\sigma$, any environment $\gamma$, and any $\tau \in \text{TIME}$, $\tau \geq \text{begin}(\sigma)$. Prove that $B(b)(\sigma(\tau).\text{state}) \iff (\sigma, \tau)\gamma \models b$.

**Proof:** The proof is given by induction on the structure of $b$.

- $b \equiv e_1 = e_2$. Thus, $B(e_1 = e_2)(\sigma(\tau).\text{state}) \iff E(e_1)(\sigma(\tau).\text{state}) = E(e_2)(\sigma(\tau).\text{state}) \iff$, by Lemma 6.1, $\mathcal{V}(e_1)\gamma(\sigma, \tau) = \mathcal{V}(e_2)\gamma(\sigma, \tau) \iff (\sigma, \tau)\gamma \models e_1 = e_2$.
- $b \equiv e_1 < e_2$. Thus, $B(e_1 < e_2)(\sigma(\tau).\text{state}) \iff E(e_1)(\sigma(\tau).\text{state}) < E(e_2)(\sigma(\tau).\text{state}) \iff$, by Lemma 6.1, $\mathcal{V}(e_1)\gamma(\sigma, \tau) < \mathcal{V}(e_2)\gamma(\sigma, \tau) \iff (\sigma, \tau)\gamma \models e_1 < e_2$.
- $b \equiv \neg b_1$. Thus, $B(\neg b_1)(\sigma(\tau).\text{state}) \iff \neg B(b_1)(\sigma(\tau).\text{state}) \iff$, by the induction hypothesis, $\neg (\sigma, \tau)\gamma \models b_1$.
- $b \equiv b_1 \lor b_2$. Thus, $B(b_1 \lor b_2)(\sigma(\tau).\text{state}) \iff B(b_1)(\sigma(\tau).\text{state}) \lor B(b_2)(\sigma(\tau).\text{state}) \iff$, by the induction hypothesis, $(\sigma, \tau)\gamma \models b_1$ or $(\sigma, \tau)\gamma \models b_2$.

Proof of Lemma 6.4

Consider a model $\sigma$ and $\text{cset} \subseteq \text{DCHAN}$. Prove that $\text{dch}(\sigma) \subseteq \text{cset}$ iff $\sigma = [\sigma]_{\text{cset}}$.

**Proof:** By definition of projection, $\text{begin}(\sigma) = \text{begin}([\sigma]_{\text{cset}})$, $\text{end}(\sigma) = \text{end}([\sigma]_{\text{cset}})$, and for all $\tau_1$, $\text{begin}(\sigma) \leq \tau_1 \leq \text{end}(\sigma)$, $\sigma(\tau_1).\text{state} = [\sigma]_{\text{cset}}(\tau_1).\text{state}$. Then we only have to prove that, for all $\tau$, $\text{begin}(\sigma) \leq \tau < \text{end}(\sigma)$, $\sigma(\tau).\text{comm} = [\sigma]_{\text{cset}}(\tau).\text{comm}$ iff $\text{dch}(\sigma) \subseteq \text{cset}$. Let $c \in \text{CHAN}$ and $\emptyset \in \text{VAL}$. By definition, for all $\tau$, $\text{begin}(\sigma) \leq \tau < \text{end}(\sigma)$,

$$[\sigma]_{\text{cset}}(\tau).\text{comm} = \{ c! | c! \in \sigma(\tau).\text{comm} \land c! \in \text{cset} \} \cup$$

$$\{ c? | c? \in \sigma(\tau).\text{comm} \land c? \in \text{cset} \} \cup$$

$$\{(c, \emptyset) | (c, \emptyset) \in \sigma(\tau).\text{comm} \land c \in \text{cset} \}$$
and

$$dch(\sigma) = \bigcup_{begin(\sigma) \leq \tau < end(\sigma)} \{c! | c! \in \sigma(\tau).comm\} \cup \{c? | c? \in \sigma(\tau).comm\} \cup \{c | \text{there exists a } \vartheta \text{ such that } (c, \vartheta) \in \sigma(\tau).comm\}$$

Assume $dch(\sigma) \subseteq cset$. We show $\sigma(\tau).comm = [\sigma]_{cset(\tau)}.comm$, for all $\tau$, $begin(\sigma) \leq \tau < end(\sigma)$. If $c! \in \sigma(\tau).comm$ then $c! \in dch(\sigma)$. By the assumption, $c! \in cset$ and thus $c! \in [\sigma]_{cset(\tau)}.comm$. Similarly, if $c? \in \sigma(\tau).comm$ then $c? \in [\sigma]_{cset(\tau)}.comm$. If $(c, \vartheta) \in \sigma(\tau).comm$, then $c \in dch(\sigma)$. By the assumption, $c \in cset$ and hence $(c, \vartheta) \in [\sigma]_{cset(\tau)}.comm$. Thus $\sigma(\tau).comm \subseteq [\sigma]_{cset(\tau)}.comm$. On the other hand, if $c! \in [\sigma]_{cset(\tau)}.comm$, then $c! \in \sigma(\tau).comm$. If $c? \in [\sigma]_{cset(\tau)}.comm$, then $c? \in \sigma(\tau).comm$. If $(c, \vartheta) \in [\sigma]_{cset(\tau)}.comm$, then $(c, \vartheta) \in \sigma(\tau).comm$. Therefore $[\sigma]_{cset(\tau)}.comm \subseteq \sigma(\tau).comm$. Hence $\sigma(\tau).comm = [\sigma]_{cset(\tau)}.comm$.

Now assume $\sigma(\tau).comm = [\sigma]_{cset(\tau)}.comm$, for all $\tau$, $begin(\sigma) \leq \tau < end(\sigma)$. We prove $dch(\sigma) \subseteq cset$. Consider any $c! \in dch(\sigma)$. By definition, there exists a $\tau$, $begin(\sigma) \leq \tau < end(\sigma)$, such that $c! \in \sigma(\tau).comm$. By the assumption, $c! \in [\sigma]_{cset(\tau)}.comm$ and then $c! \in cset$. Similarly, if $c? \in dch(\sigma)$, then $c? \in cset$. Suppose $c \in dch(\sigma)$. Then there exists a value $\vartheta$ such that $(c, \vartheta) \in \sigma(\tau).comm$ for some $\tau$, $begin(\sigma) \leq \tau < end(\sigma)$. By the assumption again, $(c, \vartheta) \in [\sigma]_{cset(\tau)}.comm$ and then $c \in cset$. Hence $dch(\sigma) \subseteq cset$. Therefore $\sigma(\tau).comm = [\sigma]_{cset(\tau)}.comm$ iff $dch(\sigma) \subseteq cset$.

**Proof of Lemma 6.5**

Consider any expression $vexp$ of type $VAL$, any model $\sigma$, any environment $\gamma$, and any $cset \subseteq DCHAN$. Prove that $V(vexp)\gamma(\sigma, begin(\sigma)) = V(vexp)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.

**Proof:** We give the proof by induction on the structure of $vexp$. Observe that, by the definition of projection onto channels, $begin(\sigma) = begin([\sigma]_{cset})$, for any $cset \subseteq DCHAN$.

- $vexp \equiv \emptyset$. Then $V(\emptyset)\gamma(\sigma, begin(\sigma)) = \emptyset = V(\emptyset)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $vexp \equiv v$. Then $V(v)\gamma(\sigma, begin(\sigma)) = \gamma(v) = V(v)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $vexp \equiv x$. Then $V(x)\gamma(\sigma, begin(\sigma)) = \sigma(begin(\sigma)).state(x) = [\sigma]_{cset}(begin([\sigma]_{cset})).state(x) = V(x)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $vexp \equiv last(x)$. Then $V(last(x))\gamma(\sigma, begin(\sigma)) = \sigma(end(\sigma)).state(x) = [\sigma]_{cset}(end([\sigma]_{cset})).state(x) = V(last(x))\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $vexp \equiv vexp_1 + vexp_2$. By the induction hypothesis,
  $V(vexp_1)\gamma(\sigma, begin(\sigma)) = V(vexp_1)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$ and
  $V(vexp_2)\gamma(\sigma, begin(\sigma)) = V(vexp_2)\gamma([\sigma]_{cset}, begin([\sigma]_{cset})).$
  Thus $V(vexp_1 + vexp_2)\gamma(\sigma, begin(\sigma)) = V(vexp_1 + vexp_2)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $vexp \equiv vexp_1 \times vexp_2$. The proof is similar as for $vexp \equiv vexp_1 + vexp_2$. 

"
Proof of Lemma 6.6

Consider any expression $vexp$ of type $VAL$, any model $\sigma$, any environment $\gamma$, and any $vset \subseteq VAR$. Prove that $V(vexp)\gamma(\sigma, begin(\sigma)) = V(vexp)\gamma(\sigma \uparrow vset, begin(\sigma \uparrow vset))$, if $var(vexp) \subseteq vset$.

Proof: By the definition of projection onto variables, we obtain $begin(\sigma) = begin(\sigma \uparrow vset)$, for any $vset \subseteq VAR$. Follow the definition and the induction proof for Lemma 6.5, we can easily prove this lemma.

Proof of Lemma 6.7

Consider any expression $texp$ of type $TIME$, any model $\sigma$, any environment $\gamma$, and any $cset \subseteq DCHAN$. Prove that $T(texp)\gamma(\sigma, begin(\sigma)) = T(texp)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.

Proof: By definition, $begin(\sigma) = begin([\sigma]_{cset})$, for any $cset \subseteq DCHAN$. The proof is given by induction on the structure of $texp$.

- $texp \equiv \tau$. Then $T(\tau)\gamma(\sigma, begin(\sigma)) = \tau = T(\tau)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $texp \equiv t$. Then $T(t)\gamma(\sigma, begin(\sigma)) = \gamma(t) = T(t)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $texp \equiv T$. Then $T(T)\gamma(\sigma, begin(\sigma)) = begin(\sigma) = begin([\sigma]_{cset}) = T(T)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $texp \equiv start$. Then $T(start)\gamma(\sigma, begin(\sigma)) = begin(\sigma) = begin([\sigma]_{cset}) = T(start)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $texp \equiv term$. Then $T(term)\gamma(\sigma, begin(\sigma)) = end(\sigma) = end([\sigma]_{cset}) = T(term)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $texp \equiv vexp$. By definition, $T(vexp)\gamma(\sigma, begin(\sigma)) = V(vexp)\gamma(\sigma, begin(\sigma))$ and $T(vexp)\gamma([\sigma]_{cset}, begin([\sigma]_{cset})) = V(vexp)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$. By Lemma 6.5, $V(vexp)\gamma(\sigma, begin(\sigma)) = V(vexp)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$. Then it leads to $T(vexp)\gamma(\sigma, begin(\sigma)) = T(vexp)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $texp \equiv texp_1 + texp_2$. By the induction hypothesis, $T(texp_1)\gamma(\sigma, begin(\sigma)) = T(texp_1)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$ and $T(texp_2)\gamma(\sigma, begin(\sigma)) = T(texp_2)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$. Thus, by definition, $T(texp_1 + texp_2)\gamma(\sigma, begin(\sigma)) = T(texp_1 + texp_2)\gamma([\sigma]_{cset}, begin([\sigma]_{cset}))$.
- $texp \equiv texp_1 - texp_2$ and $texp \equiv texp_1 \times texp_2$. The proofs are similar as for $texp \equiv texp_1 + texp_2$.

Proof for Lemma 6.8

Consider any expression $texp$ of type $TIME$, any model $\sigma$, any environment $\gamma$, and any $vset \subseteq VAR$. Prove that $T(texp)\gamma(\sigma, begin(\sigma)) = T(texp)\gamma(\sigma \uparrow vset, begin(\sigma \uparrow vset))$, if $var(texp) \subseteq vset$.

Proof: Similar to the proof for Lemma 6.7.
Proof for Lemma 6.9

Consider any \( cset \subseteq DCHAN \) and any assertion \( \varphi \). Prove that if \( dch(\varphi) \subseteq cset \) then, for any model \( \sigma \) and any environment \( \gamma \), \( (\sigma, begin(\sigma)) \vdash \varphi \) iff \( (\sigma)_{cset} \in \{ \gamma \} \).

**Proof:** We give the proof by induction on the structure of \( \varphi \).

- \( \varphi \equiv texp_1 = texp_2 \). Then \( (\sigma, begin(\sigma)) \vdash texp_1 = texp_2 \) iff \( T(texp_1) = T(texp_2) \), by Lemma 6.7.

- \( \varphi \equiv comm(c, vexp) \). Then \( \{ c \} = dch(\varphi) \subseteq cset \), and thus \( c \in cset \). Hence \( (\sigma, begin(\sigma)) \vdash comm(c, vexp) \) iff \( end(\sigma) > begin(\sigma) \) and \( (c, vexp) \in \sigma(\sigma).comm \) iff \( end(\sigma) > \sigma.begin(\sigma) \).

- \( \varphi \equiv wait(c!) \). Thus \( \{ c! \} = dch(\varphi) \subseteq cset \) and thus \( c! \in cset \). Therefore \( (\sigma, begin(\sigma)) \vdash wait(c!) \) iff \( end(\sigma) > begin(\sigma) \) and \( c! \in \sigma(begin(\sigma)).comm \cap cset \) iff \( end(\sigma) > \sigma.begin(\sigma) \) and \( c! \in \sigma(begin(\sigma)).comm \) iff \( (\sigma)_{cset} \in \{ \gamma \} \).
Proof for Lemma 6.10

Consider any $vset \subseteq VAR$ and any assertion $\varphi$. Prove that if $\var{\varphi} \subseteq vset$ then, for any model $\sigma$ and any environment $\gamma$, $(\sigma, \beg\sigma) \vdash \varphi$ iff $(\sigma \uparrow vset, \beg(\sigma \uparrow vset)) \vdash \varphi$.

Proof: Similar to the proof for Lemma 6.9.

Proof of Lemma 6.11

Consider a model $\sigma$, an environment $\gamma$, and two sets $cset_1, cset_2 \subseteq DCHAN$. Prove that if $(\sigma, \beg\sigma) \vdash \Box \text{empty}(cset_2 - cset_1)$ then $[\sigma]_{cset_1 \cup cset_2} = [\sigma]_{cset_1}$.

Proof: By the definition of projection, $\beg([\sigma]_{cset_1 \cup cset_2}) = \beg(\sigma) = \beg([\sigma]_{cset_1})$, $\end([\sigma]_{cset_1 \cup cset_2}) = \end(\sigma) = \end([\sigma]_{cset_1})$, and for any $\tau$, $\beg(\sigma) \leq \tau \leq \end(\sigma)$, $[\sigma]_{cset_1 \cup cset_2}(\tau).state = [\sigma]_{cset_1}(\tau).state$. Then we only have to prove, for any $\tau$, $\beg(\sigma) \leq \tau < \end(\sigma)$, $[\sigma]_{cset_1 \cup cset_2}(\tau).comm = [\sigma]_{cset_1}(\tau).comm$. Since $cset_1 \cup cset_2 = cset_1 \cup (cset_2 - cset_1)$, we obtain $[\sigma]_{cset_1 \cup cset_2} = [\sigma]_{cset_1 \cup (cset_2 - cset_1)}$ and then $[\sigma]_{cset_1 \cup cset_2}(\tau).comm = [\sigma]_{cset_1 \cup (cset_2 - cset_1)}(\tau).comm = [\sigma]_{cset_1}(\tau).comm$.

Proof of Lemma 6.12

Consider a model $\sigma$, an environment $\gamma$, and two sets $vset_1, vset_2 \subseteq VAR$. Prove that if $(\sigma, \beg\sigma) \vdash \text{inv}(vset_2 - vset_1)$ then $\sigma \uparrow (vset_1 \cup vset_2) = \sigma \uparrow vset_1$.

Proof: Follow the proof for Lemma 6.11.

Proof of Lemma 6.13

Consider a model $\sigma$ and an environment $\gamma$. Prove that if $dch(\sigma) \subseteq cset$ and $(\sigma, \beg\sigma) \vdash WF_{cset}$, then $\sigma$ is well-formed.

Proof: Assume $(\sigma, \beg\sigma) \vdash WF_{cset}$. Then $(\sigma, \beg\sigma) \vdash \Box (\text{MinWait}_{cset} \wedge \text{Exclusion}_{cset} \wedge \text{Unique}_{cset})$. Hence, for all $\tau \geq \beg\sigma$, 1. $(\sigma, \tau) \vdash \neg(\text{wait}(c!) \wedge \text{wait}(c?))$, for all $\{c!, c?\} \subseteq cset$; 2. $(\sigma, \tau) \vdash \neg(\text{comm}(c) \wedge \text{wait}(c!))$, for all $\{c, c!\} \subseteq cset$, and $(\sigma, \tau) \vdash \neg(\text{comm}(c) \wedge \text{wait}(c?))$, for all $\{c, c?\} \subseteq cset$; 3. $(\sigma, \tau) \vdash \text{comm}(c, vexp_1) \wedge \text{comm}(c, vexp_2) \rightarrow vexp_1 = vexp_2$, for all $c \in cset$.

Given the interpretation of assertions (Section 4), this implies, for all $\tau \geq \beg\sigma$, 1. $\neg(c! \in \sigma(\tau).comm \wedge c? \in \sigma(\tau).comm)$, for all $\{c!, c?\} \subseteq cset$;
2. There does not exist a value $\theta \in VAL$ such that

$$(c, \theta) \in \sigma(\tau).\text{comm} \land c! \in \sigma(\tau).\text{comm} \lor (c, \theta) \in \sigma(\tau).\text{comm} \land c? \in \sigma(\tau).\text{comm}. $$

Thus, for any value $\theta \in VAL$,

$\neg((c, \theta) \in \sigma(\tau).\text{comm} \land c! \in \sigma(\tau).\text{comm})$, for all $\{c, c!\} \subseteq \text{cset}$, and

$\neg((c, \theta) \in \sigma(\tau).\text{comm} \land c? \in \sigma(\tau).\text{comm})$, for all $\{c, c?\} \subseteq \text{cset}$;

3. $(c, V(vexp_1)\gamma(\sigma, \tau)) \in \sigma(\tau).\text{comm} \land (c, V(vexp_2)\gamma(\sigma, \tau)) \in \sigma(\tau).\text{comm}$

$\rightarrow V(vexp_1)\gamma(\sigma, \tau) = V(vexp_2)\gamma(\sigma, \tau)$, for all $c \in \text{cset}$. Since $vexp_1$ and $vexp_2$ are arbitrary expressions of type $VAL$, let $\theta_1, \theta_2 \in VAL$ be such that $\theta_1 \equiv vexp_1$ and $\theta_2 \equiv vexp_2$. Hence $\theta_1 = V(vexp_1)\gamma(\sigma, \tau)$ and $\theta_2 = V(vexp_2)\gamma(\sigma, \tau)$. Thus, for all $\tau \geq \text{begin}(\sigma)$, $(c, \theta_1) \in \sigma(\tau).\text{comm} \land (c, \theta_2) \in \sigma(\tau).\text{comm} \rightarrow \theta_1 = \theta_2$, for all $c \in \text{cset}$.

Notice that if $c! \notin \text{cset}$ then, by $\text{dch}(\sigma) \subseteq \text{cset}, c! \notin \text{dch}(\sigma)$, and thus $c! \notin \sigma(\tau).\text{comm}$, for all $\tau, \text{begin}(\sigma) \leq \tau < \text{end}(\sigma)$. Similarly, if $c? \notin \text{cset}$ then $c? \notin \sigma(\tau).\text{comm}$ and if $c \notin \text{cset}$ then for any value $\theta \in VAL \ (c, \theta) \notin \sigma(\tau).\text{comm}$. Thus, for all $c \in \text{CHAN}$, for all values $\theta, \theta_1, \theta_2 \in VAL$, and for all $\tau, \text{begin}(\sigma) \leq \tau < \text{end}(\sigma)$:

1. $\neg(c! \in \sigma(\tau).\text{comm} \land c? \in \sigma(\tau).\text{comm})$;

2. $\neg((c, \theta) \in \sigma(\tau).\text{comm} \land c! \in \sigma(\tau).\text{comm}) \land \neg((c, \theta) \in \sigma(\tau).\text{comm} \land c? \in \sigma(\tau).\text{comm})$;

3. $(c, \theta_1) \in \sigma(\tau).\text{comm} \land (c, \theta_2) \in \sigma(\tau).\text{comm} \rightarrow \theta_1 = \theta_2$.

Hence $\sigma$ is well-formed.
Appendix B

Soundness Proof

In the soundness proof, we must show that every axiom in our proof system is indeed valid and every inference rule preserves validity, i.e. if the hypotheses of an inference rule are valid, so is the conclusion.

Well-Formedness

Consider a program $S$ and a finite set $\text{cset} \subseteq \text{DCHAN}$. We prove that $S$ sat $WF_{\text{cset}}$ is valid. Consider any $\sigma \in M(S)$ and any environment $\gamma$. Then, by Lemma 3.12, $\sigma$ is well-formed, that is, for all $\tau$, $\text{begin}(\sigma) \leq \tau < \text{end}(\sigma)$, for all $c \in \text{CHAN}$, and for all $\vartheta_1, \vartheta_2, \vartheta \in \text{VAL}$:

1. $\neg(c! \in \sigma(\tau).\text{comm} \land c \in \sigma(\tau).\text{comm})$;
2. $\neg((c, \vartheta) \in \sigma(\tau).\text{comm} \land c! \in \sigma(\tau).\text{comm})$ and $\neg((c, \vartheta) \in \sigma(\tau).\text{comm} \land c \in \sigma(\tau).\text{comm})$;
3. $(c, \vartheta_1) \in \sigma(\tau).\text{comm} \land (c, \vartheta_2) \in \sigma(\tau).\text{comm} \rightarrow \vartheta_1 = \vartheta_2$.

For any expressions $\text{vekp}_1$ and $\text{vekp}_2$ of type $\text{VAL}$, we have $\nu(\text{vekp}_1)\gamma(\sigma, \tau) \in \text{VAL}$ and $\nu(\text{vekp}_2)\gamma(\sigma, \tau) \in \text{VAL}$, for any $\tau$, $\text{begin}(\sigma) \leq \tau < \text{end}(\sigma)$. Since $\vartheta_1$ and $\vartheta_2$ are arbitrary values in $\text{VAL}$, we can replace $\vartheta_1$ and $\vartheta_2$ by $\nu(\text{vekp}_1)\gamma(\sigma, \tau)$ and $\nu(\text{vekp}_2)\gamma(\sigma, \tau)$, respectively. Thus, for all $\tau$, $\text{begin}(\sigma) \leq \tau < \text{end}(\sigma)$, for all $\vartheta \in \text{VAL}$, and for all expressions $\text{vekp}_1, \text{vekp}_2$:

1. $\neg(c! \in \sigma(\tau).\text{comm} \land c \in \sigma(\tau).\text{comm})$, for all $c$ with $\{c!, c?\} \subseteq \text{cset}$;
2. $\neg((c, \vartheta) \in \sigma(\tau).\text{comm} \land c! \in \sigma(\tau).\text{comm})$, for all $c$ with $\{c, c!\} \subseteq \text{cset}$, and $\neg((c, \vartheta) \in \sigma(\tau).\text{comm} \land c \in \sigma(\tau).\text{comm})$, for all $c$ with $\{c, c?\} \subseteq \text{cset}$;
3. $(c, \nu(\text{vekp}_1)\gamma(\sigma, \tau)) \in \sigma(\tau).\text{comm} \land (c, \nu(\text{vekp}_2)\gamma(\sigma, \tau)) \in \sigma(\tau).\text{comm} \rightarrow \nu(\text{vekp}_1)\gamma(\sigma, \tau) = \nu(\text{vekp}_2)\gamma(\sigma, \tau)$, for all $c \in \text{cset}$.

By the interpretation of assertions, we obtain that, for all $\tau$, $\text{begin}(\sigma) \leq \tau < \text{end}(\sigma)$, for all $\vartheta \in \text{VAL}$, and for all expressions $\text{vekp}_1, \text{vekp}_2$:

1. $\langle \sigma, \tau \rangle \gamma \models \bigwedge_{\{c, c!\} \subseteq \text{cset}} \neg(\text{wait}(c!))$;
2. $\langle \sigma, \tau \rangle \gamma \models \bigwedge_{\{c, c!\} \subseteq \text{cset}} \neg(\text{comm}(c) \land \text{wait}(c!)) \land \bigwedge_{\{c, c?\} \subseteq \text{cset}} \neg(\text{comm}(c) \land \text{wait}(c?))$;
3. $\langle \sigma, \tau \rangle \gamma \models \bigwedge_{c \in \text{cset}} \text{comm}(c, \text{vekp}_1) \land \text{comm}(c, \text{vekp}_2) \rightarrow \text{vekp}_1 = \text{vekp}_2$.

Furthermore, for all $\tau' \geq \text{end}(\sigma)$, for all $c \in \text{cset}$, and for all $\text{vekp}$, we have $\langle \sigma, \tau' \rangle \gamma \models \neg\text{wait}(c!) \land \neg\text{wait}(c?) \land \neg\text{comm}(c) \land \neg\text{comm}(c, \text{vekp})$. Thus, for all $\tau \geq \text{begin}(\sigma)$, and for all $\text{vekp}_1$ and $\text{vekp}_2$:

1. $\langle \sigma, \tau \rangle \gamma \models \bigwedge_{\{c, c!\} \subseteq \text{cset}} \neg(\text{wait}(c!))$;
2. $\langle \sigma, \tau \rangle \gamma \models \bigwedge_{\{c, c!\} \subseteq \text{cset}} \neg(\text{comm}(c) \land \text{wait}(c!)) \land \bigwedge_{\{c, c?\} \subseteq \text{cset}} \neg(\text{comm}(c) \land \text{wait}(c?))$;
3. $\langle \sigma, \tau \rangle \gamma \models \bigwedge_{c \in \text{cset}} \text{comm}(c, \text{vekp}_1) \land \text{comm}(c, \text{vekp}_2) \rightarrow \text{vekp}_1 = \text{vekp}_2$.

Thus, by definition, $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \Box (\text{MinWait}_{\text{cset}} \land \text{Exclusion}_{\text{cset}} \land \text{Unique}_{\text{cset}})$ and then $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models WF_{\text{cset}}$. Hence, $S$ sat $WF_{\text{cset}}$ is indeed valid.
Communication Invariance

Consider a program $S$ and a set $cset \subseteq DCHAN$ such that $cset \cap dch(S) = \emptyset$. We prove that $S \models \square \text{empty(cset)}$ is valid. Consider any $\sigma \in M(S)$ and any environment $\gamma$. From Theorem 3.12, we obtain that $dch(\sigma) \subseteq dch(S)$ and then $cset \cap dch(\sigma) = \emptyset$. Thus, by definition of $dch(\sigma)$, for all $\tau$, $\text{begin}(\sigma) \leq \tau < \text{end}(\sigma)$:

1. If $c \in cset$ then there does not exist any value $\theta$ such that $(c, \theta) \in \sigma(\tau).\text{comm}$;
2. If $c \in cset$ then $c \notin \sigma(\tau).\text{comm}$;
3. If $c \notin cset$ then $c \notin \sigma(\tau).\text{comm}$.

Thus, for all $\tau$, $\text{begin}(\sigma) \leq \tau < \text{end}(\sigma)$:

1. $\langle \sigma, \tau \rangle \gamma \models \neg \text{comm}(c)$, for all $c \in cset$;
2. $\langle \sigma, \tau \rangle \gamma \models \neg \text{wait}(c!)$, for all $c \in cset$;
3. $\langle \sigma, \tau \rangle \gamma \models \neg \text{wait}(c?)$, for all $c \notin cset$.

Furthermore, for any $c \in CHAN$, for all $\tau' \geq \text{end}(\sigma)$, we have $\langle \sigma, \tau' \rangle \gamma \models \neg \text{comm}(c) \land \neg \text{wait}(c!) \land \neg \text{wait}(c?)$. Thus, for all $\tau \geq \text{begin}(\sigma)$, $\langle \sigma, \tau \rangle \gamma \models \text{empty(cset)}$ and then $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \square \text{empty(cset)}$. Hence, $S \models \square \text{empty(cset)}$ is valid.

Variable Invariance

Consider a program $S$ and any program variable $x$ such that $x \notin \text{wvar}(S)$. We prove that $S \models x = v \rightarrow \square (x = v)$ is valid. Consider any $\sigma \in M(S)$ and any environment $\gamma$. Assume $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models x = v$. Then $\forall x \gamma(\sigma, \text{begin}(\sigma)) = \gamma(v)$. Using Lemma 6.1, $\sigma(\text{begin}(\sigma)).\text{state}(x) = \mathcal{E}(x)(\sigma(\text{begin}(\sigma)).\text{state}) = \forall x \gamma(\sigma, \text{begin}(\sigma)) = \gamma(v)$. By the induction on the structure of $S$, we can prove that, for all $\tau$, $\text{begin}(\sigma) \leq \tau \leq \text{end}(\sigma)$, for all $x \notin \text{wvar}(S)$, $\sigma(\tau).\text{state}(x) = \sigma(\text{begin}(\sigma)).\text{state}(x)$. Thus, for all $\tau$, $\text{begin}(\sigma) \leq \tau \leq \text{end}(\sigma)$, $\forall x \gamma(\sigma, \tau) = \sigma(\tau).\text{state}(x) = \sigma(\text{begin}(\sigma)).\text{state}(x) = \gamma(v)$ and then $\langle \sigma, \tau \rangle \gamma \models x = v$. For all $\tau' > \text{end}(\sigma)$, $\forall x \gamma(\sigma, \tau') = \sigma(\text{end}(\sigma)).\text{state}(x) = \gamma(v)$ and then $\langle \sigma, \tau' \rangle \gamma \models x = v$. Hence $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \square (x = v)$ and $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models x = v \rightarrow \square (x = v)$.

Conjunction

Consider a program $S$ such that $S \models \varphi_1$ and $S \models \varphi_2$ are valid. We prove that $S \models \varphi_1 \land \varphi_2$ is also valid. Consider any $\sigma \in M(S)$ and any environment $\gamma$. Since $S \models \varphi_1$ is valid, we obtain $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_1$. Similarly, $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_2$. Hence $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_1 \land \varphi_2$.

Consequence

Consider a program $S$ such that $S \models \varphi_1$ and $\varphi_1 \rightarrow \varphi_2$ are valid. We prove that $S \models \varphi_2$ is also valid. Since $S \models \varphi_1$ is valid, we obtain $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_1$. By the implication, $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_2$. Thus $S \models \varphi_2$ is valid.
We prove that the Skip Axiom (Axiom 5.6) is valid. Consider any \( \sigma \in M(\text{skip}) \) and any environment \( \gamma \). Then \( \text{begin}(\sigma) = \text{end}(\sigma) \) and hence \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \text{term} = \text{start} \).

**Assignment**

We prove that the Assignment Axiom (Axiom 5.7) is valid. Consider any \( a \in M(x := e) \) and any environment \( \gamma \). Assume \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models x = v \). We show that \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models x = v \) \( U \) (\( T = \text{term} = \text{start} + K_a \land x = e[v/x] \)). Since \( \sigma \in M(x := e) \), we obtain that, for all \( \tau \), \( \text{begin}(\sigma) \leq \tau < \text{end}(\sigma) \). Assume \( \text{state}(\sigma) = \text{state}(\text{begin}(\sigma)) \land \text{state}(x) = \text{state}(\text{begin}(\sigma)) \). By the assumption, \( \forall(\sigma, \tau) \gamma \models x = v \). Thus for all \( \tau \), \( \text{begin}(\sigma) \leq \tau < \text{end}(\sigma) \), \( \forall(x)(\sigma, \tau) \gamma \models x = e[v/x] \) and then \( \langle \sigma, \tau \rangle \gamma \models x = v \). From the semantics, \( \forall(\sigma, \tau) \gamma \models \text{term} = \text{start} \). Hence, \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models x = v \) \( U \) (\( T = \text{term} = \text{start} + K_a \land x = e[v/x] \)).

**Delay**

We prove that the Delay Axiom (Axiom 5.8) is valid. Consider any \( \sigma \in M(\text{delay } e) \) and any environment \( \gamma \). By Lemma 6.1, \( \forall(\sigma, \text{begin}(\sigma)) \gamma \models e \). Since \( \sigma \in M(\text{delay } e) \), \( \text{end}(\sigma) = \text{begin}(\sigma) + \text{E}(e) \text{state}(\sigma) = \text{E}(e) \text{state}(\sigma) \) and then \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models x = e[v/x] \). Since \( \text{end}(\sigma) = \text{begin}(\sigma) + K_a \), we obtain that \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \text{term} = \text{start} + K_a \rangle \gamma \models \text{term} = \text{start} + K_a \). Hence, \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models x = v \) \( U \) (\( T = \text{term} = \text{start} + K_a \land x = e[v/x] \)).

**Output**

We prove that the Output Axiom (Axiom 5.9) is valid. Consider any \( \sigma \in M(\text{ele}) \) and any environment \( \gamma \). Then,

1. Either \( \text{end}(\sigma) = \infty \) and \( \sigma \in \text{Wait}(e) \), i.e., for all \( \tau \geq \text{begin}(\sigma) \), \( \sigma(\tau).\text{comm} = \{e!\} \);
2. Or there exist models \( \sigma_1 \) and \( \sigma_2 \) such that \( \sigma = \sigma_1 \sigma_2 \), \( \sigma_1 \in \text{Wait}(e) \), \( \sigma_2 \in \text{Send}(e,e) \), and \( \text{end}(\sigma) < \infty \). Then, there exists a \( \tau \in \text{TIME} \) such that, \( \text{end}(\sigma_1) = \tau \), for all \( \tau_1 \), \( \text{begin}(\sigma_1) \leq \tau_1 < \text{end}(\sigma_1) \), \( \sigma_1(\tau_1).\text{state} = \sigma_1(\text{begin}(\sigma_1)).\text{state} \), \( \sigma_1(\tau_1).\text{comm} = \{e!\} \), \( \sigma_1(\text{end}(\sigma_1)).\text{state} = \sigma_1(\text{begin}(\sigma_1)).\text{state} \), \( \text{end}(\sigma_2) = \text{begin}(\sigma_2) + K_e \), for all \( \tau_2 \), \( \text{begin}(\sigma_2) \leq \tau_2 < \text{end}(\sigma_2) \), \( \sigma_2(\tau_2).\text{comm} = \{(e, e)!\} \), \( \sigma_2(\text{end}(\sigma_2)).\text{state} = \sigma_2(\text{begin}(\sigma_2)).\text{state} \), and \( \sigma_2(\text{end}(\sigma_2)).\text{state} = \sigma_2(\text{begin}(\sigma_2)).\text{state} \).

That is,

1. Either \( \text{end}(\sigma) = \infty \) and, for all \( \tau \geq \text{begin}(\sigma) \), \( \langle \sigma, \tau \rangle \gamma \models \text{wait}(e!) \). Hence \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \square \text{wait}(e!) \);
2. Or, from $\sigma = \sigma_1 \sigma_2$, we can derive that there exists a $\tau \in \text{TIME}$ such that, for all $\tau_1$, $\text{begin}(\sigma) \leq \tau_1 < \tau$, $\langle \sigma, \tau_1 \rangle \vdash \text{wait}(c!)$. Since $\text{end}(\sigma_1) < \infty$, we obtain $\text{begin}(\sigma_2) = \text{end}(\sigma_1) + 1 = \tau$. By Lemma 6.1, for all $\tau_2$, $\tau \leq \tau_2 < \text{end}(\sigma)$, $\mathcal{E}(e)(\sigma_2(\text{begin}(\sigma_2)).\text{state}) = \mathcal{V}(e) \gamma(\sigma_2, \text{begin}(\sigma_2)) = \mathcal{V}(e) \gamma(\sigma_2, \tau_2)$. Thus we have $\langle \sigma, \tau_2 \rangle \gamma \vdash \text{comm}(c, e)$. Since $\text{end}(\sigma_2) = \text{begin}(\sigma_2) + K_c$, we obtain $\text{end}(\sigma) = \tau + K_c$ and then $\langle \sigma, \tau \rangle \gamma \vdash T = \text{term} - K_c$ as well as $\langle \sigma, \text{end}(\sigma) \rangle \gamma \vdash T = \text{term}$. Hence $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \vdash \text{wait}(c!) \cup (T = \text{term} - K_c \land (\text{comm}(c, e) \cup T = \text{term})).$

Hence $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \vdash \text{wait}(c!) \cup (T = \text{term} - K_c \land (\text{comm}(c, e) \cup T = \text{term})).$

Input

We prove that the Input Axiom (Axiom 5.10) is valid. Consider any $\sigma \in \mathcal{M}(c?x)$ and any environment $\gamma$. Assume $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \vdash x = v$. Then $\sigma(\text{begin}(\sigma)).\text{state}(x) = \gamma(v)$. We show that $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \vdash (x = v \land \text{wait}(c!)) \cup (T = \text{term} - K_c \land (x = v \land \text{comm}(c, \text{last}(x))) \cup T = \text{term}))$. There are two possibilities:

1. Either $\text{end}(\sigma) = \infty$ and $\sigma \in \text{Wait}(c?)$, i.e., for all $\tau \geq \text{begin}(\sigma)$, $\sigma(\tau).\text{comm} = \{c?\}$, and $\sigma(\tau).\text{state} = \sigma(\text{begin}(\sigma)).\text{state};$

2. Or there exist models $\sigma_1$ and $\sigma_2$ such that $\sigma = \sigma_1 \sigma_2$, $\sigma_1 \in \text{Wait}(c?)$, $\sigma_2 \in \text{Receive}(c, x)$, and $\text{end}(\sigma_1) < \infty$. Thus, there exists a $\tau \in \text{TIME}$ such that, $\text{end}(\sigma_1) = \tau$, for all $\tau_1$, $\text{begin}(\sigma_1) \leq \tau_1 < \text{end}(\sigma_1)$, $\sigma_1(\tau_1).\text{state} = \sigma_1(\text{begin}(\sigma_1)).\text{state}$, $\sigma_1(\tau_1).\text{comm} = \{c?\}$, $\sigma_1(\text{end}(\sigma_1)).\text{state} = \sigma_2(\text{begin}(\sigma_2)).\text{state}$, $\text{end}(\sigma_2) = \text{begin}(\sigma_2) + K_c$, there exists a value $\theta \in \text{VAL}$ such that, for all $\tau_2$, $\text{begin}(\sigma_2) \leq \tau_2 < \text{end}(\sigma_2)$, $\sigma_2(\tau_2).\text{comm} = \{(c, \theta)\}$, $\sigma_2(\text{end}(\sigma_2)).\text{state} = \sigma_2(\text{begin}(\sigma_2)).\text{state}$, and $\sigma_2(\text{end}(\sigma_2)).\text{state} = \sigma_2(\text{begin}(\sigma_2)).\text{state} : x \mapsto \theta$.

That is,

1. Either $\text{end}(\sigma) = \infty$, for all $\tau \geq \text{begin}(\sigma)$, $\langle \sigma, \tau \rangle \gamma \vdash \text{wait}(c?)$ and $\langle \sigma, \tau \rangle \gamma \vdash x = v$. Hence, $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \vdash \square (x = v \land \text{wait}(c?));$

2. Or, from $\sigma = \sigma_1 \sigma_2$, we obtain $\text{begin}(\sigma_2) = \text{end}(\sigma_1) = \tau$. Thus for all $\tau_1$, $\text{begin}(\sigma) \leq \tau_1 < \tau$, $\langle \sigma, \tau_1 \rangle \gamma \vdash x = v \land \text{wait}(c?)$, for all $\tau_2$, $\tau \leq \tau_2 < \text{end}(\sigma)$, $\langle \sigma, \tau_2 \rangle \gamma \vdash x = v \land \text{comm}(c, \theta)$. Since $\text{end}(\sigma_2) = \text{begin}(\sigma_2) + K_c$, we obtain $\text{end}(\sigma) = \tau + K_c$ and then $\langle \sigma, \tau \rangle \gamma \vdash T = \text{term} - K_c$ as well as $\langle \sigma, \text{end}(\sigma) \rangle \gamma \vdash T = \text{term}$. Hence we have $\langle \sigma, \tau \rangle \gamma \vdash T = \text{term} - K_c \land ((x = v \land \text{comm}(c, \theta)) \cup T = \text{term})$. From $\sigma(\text{end}(\sigma)).\text{state}(x) = \theta$, by definition, we obtain $\mathcal{V}(\text{last}(x)) \gamma(\sigma, \text{end}(\sigma)) = \theta$. We can also derive that, for all $\tau_2$, $\tau_2 \leq \tau_2 < \text{end}(\sigma)$, $\mathcal{V}(\text{last}(x)) \gamma(\sigma, \tau_2) = \theta$. Thus we have $\langle \sigma, \tau \rangle \gamma \vdash (x = v \land \text{comm}(c, \text{last}(x))) \cup T = \text{term}$. Therefore $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \vdash (x = v \land \text{wait}(c!)) \cup (T = \text{term} - K_c \land ((x = v \land \text{comm}(c, \text{last}(x))) \cup T = \text{term})).$

Hence, $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \vdash x = v \rightarrow [(x = v \land \text{wait}(c!)) \cup (T = \text{term} - K_c \land ((x = v \land \text{comm}(c, \text{last}(x))) \cup T = \text{term}))].$
Sequential Composition

We prove that the Sequential Composition Rule (Rule 5.11) preserves validity. Assume \( S_1 \) sat \( \varphi_1 \) and \( S_2 \) sat \( \varphi_2 \) are valid. We show that \( S_1; S_2 \) sat \( \varphi_1 \land \varphi_2 \) is also valid. Consider any \( \sigma \in \mathcal{M}(S_1; S_2) \) and any environment \( \gamma \). Then there exist \( \sigma_1 \in \mathcal{M}(S_1) \) and \( \sigma_2 \in \mathcal{M}(S_2) \) such that \( \sigma = \sigma_1 \sigma_2 \). By definition, \( \text{end}(\sigma_1) \geq \text{begin}(\sigma_1) \). From \( S_1 \) sat \( \varphi_1 \) and \( S_2 \) sat \( \varphi_2 \), we obtain \( \langle \sigma_1, \text{begin}(\sigma_1) \rangle \models \varphi_1 \) and \( \langle \sigma_2, \text{begin}(\sigma_2) \rangle \models \varphi_2 \). By the definition of the \( \land \) operator, we can derive \( \langle \sigma, \text{begin}(\sigma) \rangle \models \varphi_1 \land \varphi_2 \), i.e., \( \langle \sigma, \text{begin}(\sigma) \rangle \models \varphi_1 \land \varphi_2 \). Hence, \( S_1; S_2 \) sat \( \varphi_1 \land \varphi_2 \) is indeed valid.

Guarded Command with Purely Boolean Guards

Consider \( G = \left[ \sum_{i=1}^{n} b_i \rightarrow S_i \right] \). We prove that the Guarded Command Evaluation Axiom (Axiom 5.12) is valid for \( G \). Let \( \sigma \in \mathcal{M}(G) \) and \( \gamma \) be any environment. There are two possibilities:

1. Either \( B(\neg b_G)(\sigma(\text{begin}(\sigma)).\text{state}) \) and \( \sigma \in \mathcal{M}(\text{delay } K_g) \);
2. Or there exists a \( k, 1 \leq k \leq n \), such that \( B(b_k)(\sigma(\text{begin}(\sigma)).\text{state}) \) and \( \sigma \in \mathcal{M}(\text{delay } K_g; S_k) \).

That is,

1. Either, from \( B(\neg b_G)(\sigma(\text{begin}(\sigma)).\text{state}) \), by Lemma 6.2, \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \neg b_G \). Since \( \sigma \in \mathcal{M}(\text{delay } K_g) \), \( \text{end}(\sigma) = \text{begin}(\sigma) + K_g \) and then \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \text{term} = \text{start} + K_g \). Hence, \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \neg b_G \rightarrow \text{term} = \text{start} + K_g \). Assume \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \wedge_{y \in \text{var}(G)} y = \eta_y \). From the semantics, for all \( \tau_1, \text{begin}(\sigma) \leq \tau_1 \leq \text{end}(\sigma), \sigma(\tau_1).\text{state} = \sigma(\text{begin}(\sigma)).\text{state} \) and then \( \langle \sigma, \tau_1 \rangle \gamma \models \wedge_{y \in \text{var}(G)} y = \eta_y \). Also, for all \( \tau_2, \text{begin}(\sigma) \leq \tau_2 < \text{end}(\sigma), \sigma(\tau_2).\text{comm} = \emptyset \). Thus,
   - for all \( c! \in dch(G) \), \( c! \notin \sigma(\tau_2).\text{comm} \);
   - for all \( c? \in dch(G) \), \( c? \notin \sigma(\tau_2).\text{comm} \);
   - for all \( c \in dch(G) \), there does not exist any value \( \theta \) such that \( (c, \theta) \in \sigma(\tau_2).\text{comm} \).

Then \( \langle \sigma, \tau_2 \rangle \gamma \models \wedge_{c \in dch(G)} \neg \text{wait}(c!) \land \wedge_{c? \in dch(G)} \neg \text{wait}(c?) \land \wedge_{c \in dch(G)} \neg \text{comm}(c) \), i.e. \( \langle \sigma, \tau_2 \rangle \gamma \models \text{empty}(dch(G)) \). We can also derive that \( \langle \sigma, \text{end}(\sigma) \rangle \gamma \models T = \text{start} + K_g \). Hence, \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \wedge_{y \in \text{var}(G)} y = \eta_y \land \text{empty}(dch(G)) \) U \( (T = \text{start} + K_g \land \wedge_{y \in \text{var}(G)} y = \eta_y) \). Thus, \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \text{Quiet} U (T = \text{start} + K_g \land \wedge_{y \in \text{var}(G)} y = \eta_y) \). Hence, \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \wedge_{y \in \text{var}(G)} y = \eta_y \rightarrow (\text{Quiet} U (T = \text{start} + K_g \land \wedge_{y \in \text{var}(G)} y = \eta_y) \land \neg b_G \rightarrow \text{term} = \text{start} + K_g) \);

2. Or, by \( B(b_k)(\sigma(\text{begin}(\sigma)).\text{state}) \), we obtain \( B(b_k)(\sigma(\text{begin}(\sigma)).\text{state}) \) and then \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models b_k \). Then \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \neg b_k \rightarrow \text{term} = \text{start} + K_g \). Since \( \sigma \in \mathcal{M}(\text{delay } K_g; S_k) \), there exist models \( \sigma_1 \in \mathcal{M}(\text{delay } K_g) \) and \( \sigma_2 \in \mathcal{M}(S_k) \) such that \( \sigma = \sigma_1 \sigma_2 \). From \( \sigma_1 \in \mathcal{M}(\text{delay } K_g) \), we can obtain the same result as previous case, i.e. \( \langle \sigma_1, \text{begin}(\sigma_1) \rangle \gamma \models \wedge_{y \in \text{var}(G)} y = \eta_y \rightarrow (\text{Quiet} U (T = \text{start} + K_g \land \wedge_{y \in \text{var}(G)} y = \eta_y)) \). Thus, \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \wedge_{y \in \text{var}(G)} y = \eta_y \rightarrow (\text{Quiet} U (T = \text{start} + K_g \land \wedge_{y \in \text{var}(G)} y = \eta_y)) \land (\neg b_G \rightarrow \text{term} = \text{start} + K_g) \).
Hence, we can conclude that the Guarded Command Evaluation Axiom is indeed valid for \( G \equiv \sqcup_{i=1}^{n} b_{i} \rightarrow S_{i} \).

Now we prove that the Guarded Command with Purely Boolean Guards Rule (Rule 5.13) preserves validity. Assume \( S_{i} \) sat \( \varphi_{i} \) are valid, \( i = 1, 2, \ldots, n \). Consider any \( \sigma \in \mathcal{M}(G) \) and any environment \( \gamma \). Then,

1. If \( B(\neg b_{G})(\sigma(begin(\sigma)).state) \), \( \langle \sigma, begin(\sigma) \rangle \gamma \models \neg b_{G} \) and then \( \langle \sigma, begin(\sigma) \rangle \gamma \models b_{G} \rightarrow (term = start + K_{g}) \subset \bigvee_{i=1}^{n} b_{i} \land \varphi_{i} \);
2. If \( B(b_{G})(\sigma(begin(\sigma)).state) \) and then \( \langle \sigma, begin(\sigma) \rangle \gamma \models b_{G} \).

   Since \( \sigma \in \mathcal{M}(delay K_{g}; S_{k}) \), there exist models \( \sigma_{1} \in \mathcal{M}(delay K_{g}) \) and \( \sigma_{2} \in \mathcal{M}(S_{k}) \) such that \( \sigma = \sigma_{1}\sigma_{2} \). Thus \( end(\sigma_{1}) = begin(\sigma_{1}) + K_{g} \) and hence \( \langle \sigma_{1}, begin(\sigma_{1}) \rangle \gamma \models (term = start + K_{g}) \subset \bigvee_{i=1}^{n} (b_{i} \land \varphi_{i}) \).

   i.e., \( \langle \sigma, begin(\sigma) \rangle \gamma \models (term = start + K_{g}) \subset \bigvee_{i=1}^{n} (b_{i} \land \varphi_{i}) \).

Then we can conclude that the Rule 5.13 preserves validity.

**Guarded Command with IO-guards**

Now we consider \( G \equiv \sqcup_{i=1}^{n} b_{i} ; c_{i} ? x_{i} \rightarrow S_{i} \sqcup b; delay e \rightarrow S \). We first prove that the Guarded Command Evaluation Axiom (Axiom 5.12) is also valid for \( G \). Let \( \sigma \in \mathcal{M}(G) \) and \( \gamma \) be any environment. There are four possibilities:

1. If \( B(\neg b_{G})(\sigma(begin(\sigma)).state) \) and \( \sigma \in \mathcal{M}(delay K_{g}) \);
2. Or \( \sigma \in SEQ(\mathcal{M}(delay K_{g}), BoundWait(G), Comm(G)) \);
3. Or \( \sigma \in SEQ(\mathcal{M}(delay K_{g}), TimeOut(G), M(S)) \);
4. Or \( \sigma \in SEQ(\mathcal{M}(delay K_{g}), AnyWait(G), Comm(G)) \).

Following the proof of Axiom 5.12 for the case \( G \equiv \sqcup_{i=1}^{n} b_{i} ; c_{i} ? x_{i} \rightarrow S_{i} \sqcup b; delay e \rightarrow S \), we can conclude that the Axiom 5.12 is also valid for \( G \equiv \sqcup_{i=1}^{n} b_{i} ; c_{i} ? x_{i} \rightarrow S_{i} \sqcup b; delay e \rightarrow S \).

Next we prove that the Guarded Command with IO-guards Rule (Rule 5.14) preserves validity. Assume \( c_{i} ? x_{i} ; S_{i} \) sat \( \varphi_{i} \), \( i = 1, 2, \ldots, n \) and \( S \) sat \( \varphi \) are valid. Then,

1. If \( B(\neg b_{G})(\sigma(begin(\sigma)).state) \), then \( \langle \sigma, begin(\sigma) \rangle \gamma \models \neg b_{G} \). Thus \( \langle \sigma, begin(\sigma) \rangle \gamma \models \bigwedge_{y \in var(\sigma)} y = v_{y} \land b_{G} \rightarrow Eval \subset (Comm \lor TimeOut) \);
2. If \( \sigma \in SEQ(\mathcal{M}(delay K_{g}), BoundWait(G), Comm(G)) \), there exist models \( \sigma_{1} \in \mathcal{M}(delay K_{g}) \), \( \sigma_{2} \in BoundWait(G) \), and \( \sigma_{3} \in Comm(G) \) such that \( \sigma = \sigma_{1}\sigma_{2}\sigma_{3} \).

   From \( \sigma_{1} \in \mathcal{M}(delay K_{g}) \), \( end(\sigma_{1}) = begin(\sigma_{1}) + K_{g} \) and then \( \langle \sigma_{1}, begin(\sigma_{1}) \rangle \gamma \models (term = start + K_{g} \subset \bigvee_{i=1}^{n} (b_{i} \land \varphi_{i}) \).

   From \( \sigma_{2} \in BoundWait(G) \), we obtain \( end(\sigma_{2}) < begin(\sigma_{2}) + \mathcal{E}(\epsilon)(\sigma_{2}(begin(\sigma_{2})).state) \),
3. If \( B(b)(\sigma_2(begin(\sigma_2)).state), for all \( \tau_2, begin(\sigma_2) \leq \tau_2 < end(\sigma_2), \sigma_2(\tau_2).state = \sigma_2(begin(\sigma_2)).state, \sigma_2(\tau_2).comm = \{e_i \mid B(b)(\sigma_2(begin(\sigma_2)).state)\}, 1 \leq i \leq n \}, \) and \( \sigma_2(end(\sigma_2)).state = \sigma_2(begin(\sigma_2)).state. \) Assume \( \langle \sigma, begin(\sigma) \rangle \models \land_{y \in var(G)} y = v_y. \) Then \( \langle \sigma_2, begin(\sigma_2) \rangle \models \land_{y \in var(G)} y = v_y. \) For all \( \tau_2, begin(\sigma_2) \leq \tau_2 \leq end(\sigma_2), \) \( \langle \sigma_2, \tau_2 \rangle \models \land_{y \in var(G)} y = v_y. \) For all \( \tau_2, begin(\sigma_2) \leq \tau_2 < end(\sigma_2), \) we can derive that \( \varphi \in \sigma_2(\tau_2).comm \) if \( B(b)(\sigma_2(begin(\sigma_2)).state), \) for all \( i, 1 \leq i \leq n. \) Then \( \langle \sigma_2, \tau_2 \rangle \models \land_{i=1}^n b_i \leftrightarrow wait(c_i). \) Since \( \sigma \in M(G), \) by Theorem 3.12, \( \sigma \) is well-formed. By the definition of well-formedness, we can obtain \( \langle \sigma_2, \tau_2 \rangle \models empty(dch(G) - \{c_1, \ldots, c_n\}). \) From \( end(\sigma_2) < begin(\sigma_2) + \varepsilon, \) we have \( \langle \sigma_2, \tau_2 \rangle \models b \) and then \( \langle \sigma, begin(\sigma) \rangle \models b_G. \) Thus \( \langle \sigma_2, \tau_2 \rangle \models b \rightarrow T < start + \varepsilon. \) It is obvious that \( \langle \sigma_2, end(\sigma_2) \rangle \models T = term. \) Hence \( \langle \sigma_2, begin(\sigma_2) \rangle \models \land_{y \in var(G)} y = v_y \land empty(dch(G) - \{c_1, \ldots, c_n\}) \land \land_{i=1}^n (b_i \leftrightarrow wait(c_i)) \land (b \rightarrow T < start + \varepsilon) \cup (\land_{y \in var(G)} y = v_y \land T = term \land (b \rightarrow T < start + \varepsilon)). \) Then we obtain \( \langle \sigma_2, begin(\sigma_2) \rangle \models Wait U InTime. \)

From \( \sigma_3 \in Comm(G), \) there exists a \( k, 1 \leq k \leq \nu, \) such that \( B(b_k)(\sigma_3(begin(\sigma_3)).state) \) and \( \sigma_3 \in SEQ(\{c_k, x_k\}, M(S_k)). \) Then \( \langle \sigma_3, begin(\sigma_3) \rangle \models b_k, \) \( \sigma_3 \in M(c_k ? x_k; S_k), \) and \( \langle \sigma_3, begin(\sigma_3) \rangle \models comm(c_k). \) By the assumption, \( \varphi \in sat \text{ valid.} \) Thus \( \langle \sigma_3, begin(\sigma_3) \rangle \models \varphi_k \) and then \( \langle \sigma_3, begin(\sigma_3) \rangle \models b_k \land \varphi_k \land comm(c_k). \) Hence \( \langle \sigma_3, begin(\sigma_3) \rangle \models \land_{i=1}^n (b_i \land \varphi_i \land comm(c_i)). \) Then \( \langle \sigma_2 \sigma_3, begin(\sigma_2) \rangle \models (Wait U InTime) \land \land_{i=1}^n (b_i \land \varphi_i \land comm(c_i)), \) i.e.,

\[ \langle \sigma_2 \sigma_3, begin(\sigma_2) \rangle \models Comm. \]

Hence \( \langle \sigma, begin(\sigma) \rangle \models \land_{y \in var(G)} y = v_y \land b_G \rightarrow Eval C Comm; \)

3. If \( \sigma \in SEQ(M(delays K_2), TimeOut(G), M(S)), \) there exists models \( \sigma_1 \in M(delays K_2), \sigma_2 \in TimeOut(G), \) and \( \sigma_3 \in M(S) \) such that \( \sigma = \sigma_1 \sigma_2 \sigma_3, \sigma_1 \in M(delays K_2) \) implies \( \langle \sigma_1, begin(\sigma_1) \rangle \models Eval. \)

\( \sigma_2 \in TimeOut(G) \) implies \( B(b)(\sigma_2(begin(\sigma_2)).state) \) and then \( \langle \sigma_2, begin(\sigma_2) \rangle \models b. \) Hence \( \langle \sigma, begin(\sigma) \rangle \models b_G. \) Since \( \varepsilon(\sigma_2(begin(\sigma_2)).state) = \varepsilon(\sigma_2(end(\sigma_2)).state) \land \land_{i=1}^n (b_i \rightarrow wait(c_i)). \) then \( \langle \sigma_2, begin(\sigma_2) \rangle \models T = start + \varepsilon. \) Assume \( \langle \sigma, begin(\sigma) \rangle \models \land_{y \in var(G)} y = v_y. \) We can also derive that, for all \( \tau_2, begin(\sigma_2) \leq \tau_2 < end(\sigma_2), \) \( \langle \sigma_2, \tau_2 \rangle \models empty(dch(G) - \{c_1, \ldots, c_n\}) \land \land_{i=1}^n (b_i \rightarrow wait(c_i)) \land (b \rightarrow T < start + \varepsilon), \) for all \( \tau_2, begin(\sigma_2) \leq \tau_2 \leq end(\sigma_2), \) \( \langle \sigma_2, \tau_2 \rangle \models \land_{y \in var(G)} y = v_y, \) \( \langle \sigma_2, \tau_2 \rangle \models b, \) and \( \langle \sigma_2, end(\sigma_2) \rangle \models T = term \land start + \varepsilon. \) Hence, \( \langle \sigma_2, begin(\sigma_2) \rangle \models Wait U EndTime. \)

Since \( S \) sat \( \varphi \) is valid, \( \langle \sigma_3, begin(\sigma_3) \rangle \models \varphi. \)

Thus \( \langle \sigma_2 \sigma_3, begin(\sigma_2) \rangle \models (Wait U EndTime) C \varphi, \) i.e.,

\[ \langle \sigma_2 \sigma_3, begin(\sigma_2) \rangle \models TimeOut. \]

Hence \( \langle \sigma, begin(\sigma) \rangle \models \land_{y \in var(G)} y = v_y \land b_G \rightarrow (Eval C TimeOut); \)
4. If \( \sigma \in SEQ(M(|delay| K_2), AnyWait(G), Comm(G)) \), there exist models 
\( \sigma_1 \in M(|delay| K_2), \sigma_2 \in AnyWait(G), \) and \( \sigma_3 \in Comm(G) \) such that \( \sigma = \sigma_1 \sigma_2 \sigma_3 \). 
\( \sigma_1 \in M(|delay| K_2) \) implies \( (\sigma_1, \text{begin}(\sigma_1)) \models Eval \).
\( \sigma_2 \in AnyWait(G) \) implies \( B(\neg \sigma_2(\text{begin}(\sigma_2)).\text{state}) \) and then \( (\sigma_2, \text{begin}(\sigma_2)) \models \neg b \).
Thus \( (\sigma_2, \text{begin}(\sigma_2)) \models b \rightarrow T < \text{start} + e \). From the semantics, we can also obtain 
\( B(b_2(\sigma_2(\text{begin}(\sigma_2)).\text{state})) \) and then \( (\sigma_2, \text{begin}(\sigma_2)) \models b G, \) i.e., \( (\sigma, \text{begin}(\sigma)) \models b G. \)
Assume \( (\sigma, \text{begin}(\sigma)) \models \land_{y \in \text{eval}(G)} y = v_y \). Similarly as previous case, we can derive that, for all \( \tau_2, \text{begin}(\sigma_2) \leq \tau_2 < \text{end}(\sigma_2), (\sigma_2, \tau_2) \models \text{empty}(\text{dch}(G) - \{c_1, \ldots, c_n\}) \land \land_{i=1}^n (b_i \leftarrow \text{wait}(c_i)), \) for all \( \tau_2, \text{begin}(\sigma_2) \leq \tau_2 \leq \text{end}(\sigma_2), (\sigma_2, \tau_2) \models \land_{y \in \text{eval}(G)} y = v_y \land (b \rightarrow T < \text{start} + e), \) and \( (\sigma_2, \text{end}(\sigma_2)) \models T \models \text{term} \). If \( \text{end}(\sigma_2) = \infty, (\sigma_2, \text{begin}(\sigma_2)) \models \Box \text{Wait} \). If \( \text{end}(\sigma_2) < \infty, (\sigma_2, \text{begin}(\sigma_2)) \models \text{Wait} U \text{InTime} \).
Hence, \( (\sigma_2, \text{begin}(\sigma_2)) \models \text{Wait} U \text{InTime} \).
\( \sigma_3 \in Comm(G) \) implies \( (\sigma_3, \text{begin}(\sigma_3)) \models \land_{i=1}^n (b_i \land \varphi_i \land \text{comm}(c_i)) \).
Thus \( (\sigma_2 \sigma_3, \text{begin}(\sigma_2)) \models (\text{Wait} U \text{InTime}) C \land_{i=1}^n (b_i \land \varphi_i \land \text{comm}(c_i)), \) i.e., \( (\sigma_2 \sigma_3, \text{begin}(\sigma_2)) \models \text{Comm} \). By \( \sigma = \sigma_1 \sigma_2 \sigma_3, (\sigma, \text{begin}(\sigma)) \models \text{Eval C Comm} \).
Hence \( (\sigma, \text{begin}(\sigma)) \models \land_{y \in \text{eval}(G)} y = v_y \land b G, \) by Lemma 6.2.

Therefore, the Guarded Command with IO-guards Rule (Rule 5.14) preserves validity.

**Iteration**

We prove that the Iteration Rule (Rule 5.15) preserves validity. Assume \( G \models \varphi \) is valid. We prove that \( \star G \models (b G \land \varphi) C^* (\neg b G \land \varphi) \) is also valid. Consider any \( \sigma \in M(\star G) \) and any environment \( \gamma \). There are two possibilities:

1. Either there exist a \( k \in \mathbb{N}, k \geq 1 \), and models \( \sigma_1, \sigma_2, \ldots, \sigma_k \) such that \( \sigma = \sigma_1 \sigma_2 \ldots \sigma_k, \) for all \( i, 1 \leq i \leq k, \sigma_i \in M(G), \) for all \( j, 1 \leq j \leq k - 1, \text{end}(\sigma_j) < \infty, \) \( B(b_2(\sigma_j(\text{begin}(\sigma_j)).\text{state})), \) and either \( \text{end}(\sigma_k) = \infty \) and \( B(b_2(\sigma_k(\text{begin}(\sigma_k)).\text{state})), \) or \( B(\neg b_2(\sigma_k(\text{begin}(\sigma_k)).\text{state})), \) 
2. Or there exist an infinite sequence of models \( \sigma_1, \sigma_2, \ldots \) such that \( \sigma = \sigma_1 \sigma_2 \ldots, \) for all \( i \geq 1, \sigma_i \in M(G), \text{end}(\sigma_i) < \infty, \) and \( B(b_2(\sigma_i(\text{begin}(\sigma_i)).\text{state})), \) 

Since \( G \models \varphi \) is valid, we obtain \( (\sigma_i, \text{begin}(\sigma_i)) \models \varphi, \) for all \( \sigma_i \in M(G). \) Then,
1. Either there exist a \( k \in \mathbb{N}, k \geq 1, \) and models \( \sigma_1, \sigma_2, \ldots, \sigma_k \) such that \( \sigma = \sigma_1 \sigma_2 \ldots \sigma_k, \) for all \( j, 1 \leq j \leq k - 1, (\sigma_j, \text{begin}(\sigma_j)) \models \varphi, \text{end}(\sigma_j) < \infty, \) from \( B(b_2(\sigma_j(\text{begin}(\sigma_j)).\text{state})), \) by Lemma 6.2, \( (\sigma_j, \text{begin}(\sigma_j)) \models b G. \) Then \( (\sigma_j, \text{begin}(\sigma_j)) \models b G \land \varphi \). If \( \text{end}(\sigma_k) = \infty, \) from \( B(b_2(\sigma_k(\text{begin}(\sigma_k)).\text{state})), \) we obtain \( (\sigma_k, \text{begin}(\sigma_k)) \models b G \). By \( (\sigma_k, \text{begin}(\sigma_k)) \models b G, (\sigma_k, \text{begin}(\sigma_k)) \models b G \land \varphi. \) If \( \text{end}(\sigma_k) < \infty, \) from \( B(\neg b_2(\sigma_k(\text{begin}(\sigma_k)).\text{state})), \) we can derive \( (\sigma_k, \text{begin}(\sigma_k)) \models \neg b G \) and hence \( (\sigma_k, \text{begin}(\sigma_k)) \models \neg b G \land \varphi; \)
2. Or there exist an infinite sequence of models \( \sigma_1, \sigma_2, \ldots \) such that \( \sigma = \sigma_1 \sigma_2 \ldots, \) for all \( i \geq 1, (\sigma_i, \text{begin}(\sigma_i)) \models \varphi, \text{end}(\sigma_i) < \infty, \) and \( (\sigma_i, \text{begin}(\sigma_i)) \models b G. \) Thus, for all \( i \geq 1, (\sigma_i, \text{begin}(\sigma_i)) \models b G \land \varphi. \)

By the definition of the \( C^* \) operator, \( (\sigma_i, \text{begin}(\sigma_i)) \models (b G \land \varphi) C^* (\neg b G \land \varphi). \)
Parallel Composition

We prove the soundness of the General Parallel Composition Rule. Then the soundness of the Simple Parallel Composition Rule follows directly. Assume $S_1$ sat $\varphi_1$, $S_2$ sat $\varphi_2$, $\psi_1 \equiv \text{inv}( \text{var}(S_2)) \land \Box \text{empty}(dch(S_2))$, $\psi_2 \equiv \text{inv}( \text{var}(S_1)) \land \Box \text{empty}(dch(S_1))$, $dch(\varphi_1) \subseteq dch(S_1)$, $dch(\varphi_2) \subseteq dch(S_2)$, $\text{var}(\varphi_1) \subseteq \text{var}(S_1)$, and $\text{var}(\varphi_2) \subseteq \text{var}(S_2)$. We show the validity of $S_1 || S_2$ sat $(\varphi_1 \land (\varphi_2 \triangleleft_1 \psi_1)) \lor (\varphi_2 \land (\varphi_1 \triangleleft_1 \psi_2))$.

Consider any $\sigma \in \mathcal{M}(S_1 || S_2)$ and any environment $\gamma$. Then $dch(\sigma) \subseteq dch(S_1) \cup dch(S_2)$, and for $i \in \{1, 2\}$, there exist $\sigma_i \in \mathcal{M}(S_i)$ such that $\text{begin}(\sigma) = \text{begin}(\sigma_1) = \text{begin}(\sigma_2)$, $\text{end}(\sigma) = \max(\text{end}(\sigma_1), \text{end}(\sigma_2))$. Suppose $\text{end}(\sigma_1) \geq \text{end}(\sigma_2)$. Then $\text{end}(\sigma) = \text{end}(\sigma_1)$. We prove $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_1 \land (\varphi_2 \triangleleft_1 \psi_1)$.

- First we prove $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_1$. From the semantics, we have that, for all $\tau_1$, $\text{begin}(\sigma_1) \leq \tau_1 < \text{end}(\sigma_1)$, $[\sigma \uparrow \text{var}(S_1)]_{dch(S_1)}(\tau_1)\text{.comm} = \sigma_1(\tau_1)\text{.comm}$. Since $\text{begin}(\sigma_1) \leq \tau_1 \leq \text{end}(\sigma_1)$, $\sigma_1(\tau_1)\text{.state} = \sigma_1(\tau_1)\text{.state}$. From $\text{begin}(\sigma) = \text{begin}(\sigma_1)$, $\text{end}(\sigma) = \text{end}(\sigma_1)$, $\text{end}(\sigma) = \text{end}(\sigma_1)$, we can obtain $[\sigma \uparrow \text{var}(S_1)]_{dch(S_1)}(\tau_1)\text{.state} = \sigma_1(\tau_1)\text{.state}$. From $\psi_1 \equiv \text{inv}( \text{var}(S_2)) \land \Box \text{empty}(dch(S_2))$, we can easily find a model which satisfies $\psi_1$. Let $\sigma'$ be such a model that $\langle \sigma', \text{begin}(\sigma') \rangle \gamma \models \varphi_1$. By the definition of $C$ operator, $\langle \sigma', \text{begin}(\sigma) \rangle \gamma \models \varphi_2\triangleleft_1 \psi_1$, i.e., $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_2\triangleleft_1 \psi_1$.

- If $\text{end}(\sigma_2) = \infty$, then $\text{end}(\sigma_1) = \infty$ and $\text{end}(\sigma_2) = \text{end}(\sigma) = \infty$. Similarly as the proof above, we can also derive that $[\sigma \uparrow \text{var}(S_2)]_{dch(S_2)}(\tau_1)\text{.state} = \sigma(\tau_1)\text{.state}$. From $\sigma \in \mathcal{M}(S_2)$ and $S_2$ sat $\varphi_2$, we obtain $[\sigma \uparrow \text{var}(S_2)]_{dch(S_2)}(\sigma)\gamma \models \varphi_2$. Since $dch(\varphi_2) \subseteq dch(S_2)$ and $\varphi_2 \subseteq \varphi_2$, Lemma 6.9 and Lemma 6.10 lead to $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_2$. From $\psi_1 \equiv \text{inv}( \text{var}(S_2)) \land \Box \text{empty}(dch(S_2))$, we can easily find a model which satisfies $\psi_1$. Let $\sigma'$ be such a model that $\langle \sigma', \text{begin}(\sigma') \rangle \gamma \models \varphi_1$. By the definition of $C$ operator, $\langle \sigma', \text{begin}(\sigma) \rangle \gamma \models \varphi_2\triangleleft_1 \psi_1$, i.e., $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_2\triangleleft_1 \psi_1$.

- If $\text{end}(\sigma_2) < \infty$, from $S_2$ sat $\varphi_2$ and $\sigma_2 \in \mathcal{M}(S_2)$, we obtain $\langle \sigma_2, \text{begin}(\sigma_2) \rangle \gamma \models \varphi_2$. We define a model $\sigma_3$ such that $\text{begin}(\sigma_3) = \text{end}(\sigma_2)$, $\text{end}(\sigma_3) = \text{end}(\sigma)$, for all $\tau_1$, $\text{begin}(\sigma_3) \leq \tau_1 < \text{end}(\sigma_3)$, $\sigma_3(\tau_1)\text{.comm} = \sigma(\tau_1)\text{.comm}$, for all $\tau'_1$, $\text{begin}(\sigma_3) \leq \tau'_1 < \text{end}(\sigma_3)$, for all $x \in \text{VAR}$, if $x \in \text{var}(S_2)$, $\sigma_3(\tau'_1)\text{.state}(x) = \sigma(\tau'_1)\text{.state}(x)$, if $x \notin \text{var}(S_2)$, $\sigma_3(\tau'_1)\text{.state}(x) = \sigma(\text{end}(\sigma_2))\text{.state}(x)$. From the semantics, for all $\tau'_1$, $\text{end}(\sigma_3) \leq \tau'_1 < \text{end}(\sigma_3)$, for all $x \in \text{var}(S_2)$, $\sigma_3(\tau'_1)\text{.state}(x) = \sigma(\text{end}(\sigma_2))\text{.state}(x)$. Thus for all $\tau'_1$, $\text{begin}(\sigma_3) \leq \tau'_1 < \text{end}(\sigma_3)$, $\sigma_3(\tau'_1)\text{.state}(x) = \sigma(\text{end}(\sigma_2))\text{.state}(x)$. Furthermore, for all $\tau_2 > \text{end}(\sigma_3)$, $\forall x \gamma(\sigma_3, \tau_2) = \sigma_3(\text{end}(\sigma_2))\text{.state}(x)$. Hence $\langle \sigma_3, \text{begin}(\sigma_3) \rangle \gamma \models \text{inv}( \text{var}(S_2))$. Again from the semantics, for all $\tau_1$, $\text{end}(\sigma_2) \leq \tau_1 < \text{end}(\sigma)$, $[\sigma]_{dch(S_2)}(\tau_1)\text{.comm} = \emptyset$. Thus for all $\tau_1$, $\text{begin}(\sigma_3) \leq \tau_1 < \text{end}(\sigma_3)$, $[\sigma]_{dch(S_2)}(\tau_1)\text{.comm} = \emptyset$. Then $\langle \sigma_3, \tau_1 \rangle \gamma \models \text{empty}(dch(S_2))$. By definition, for all $\tau_2 \geq \text{end}(\sigma_3)$, $\langle \sigma_3, \tau_2 \rangle \gamma \models \text{empty}(dch(S_2))$. Thus we have $\langle \sigma_3, \text{begin}(\sigma_3) \rangle \gamma \models \Box \text{empty}(dch(S_2))$. Then $\langle \sigma_3, \text{begin}(\sigma_3) \rangle \gamma \models \text{inv}( \text{var}(S_2)) \land \Box \text{empty}(dch(S_2))$, i.e., $\langle \sigma_3, \text{begin}(\sigma_3) \rangle \gamma \models \psi_1$. By the definition of $C$ operator, we obtain
\((\sigma_2\sigma_3, \text{begin}(\sigma_2)) \gamma \models \varphi_2 \land \psi_1\). By definitions, we can also derive \([\sigma \uparrow \text{var}(S_2)]_{\text{dch}(S_2)} = \sigma_2\sigma_3\). Thus \([\sigma \uparrow \text{var}(S_2)]_{\text{dch}(S_2)}, \text{begin}(\sigma_2)) \gamma \models \varphi_2 \land \psi_1\). Since \(\text{dch}(\varphi_2) \subseteq \text{dch}(S_2)\) and \(\text{var}(\varphi_2) \subseteq \text{var}(S_2)\), we have \(\text{dch}(\varphi_2 \psi_1) \subseteq \text{dch}(S_2)\) and \(\text{var}(\varphi_2 \psi_1) \subseteq \text{var}(S_2)\).

Then Lemma 6.9 and Lemma 6.10 lead to \((\sigma, \text{begin}(\sigma)) \gamma \models \varphi_2 \land \psi_1\).

Therefore we have proved \((\sigma, \text{begin}(\sigma)) \gamma \models \varphi_1 \land (\varphi_2 \land \psi_1)\).

Similarly, for \(\text{end}(\sigma_1) \leq \text{end}(\sigma_2)\), we can show \((\sigma, \text{begin}(\sigma)) \gamma \models \varphi_2 \land (\varphi_1 \land \psi_2)\). Hence the General Parallel Composition Rule is sound.
Appendix C

Preciseness Proof

To prove Theorem 6.16 we show that for every program $S$ we can prove $S \text{ sat } \varphi$ where $\varphi$ is precise for $S$. To show that an assertion $\varphi$ is precise for a program $S$, we have to prove

1. $S \text{ sat } \varphi$, i.e. $(\sigma, \text{begin}(\sigma)) \gamma \models \varphi$ for all $\sigma \in M(S)$ and any environment $\gamma$;
2. $dch(\varphi) \subseteq dch(S)$, for any program variable $x \notin \text{wvar}(S)$, $x$ is invariant with respect to $\sigma$, and $(\sigma, \text{begin}(\sigma)) \gamma \models \varphi$ for any environment $\gamma$, then $\sigma \in M(S)$; and
3. $dch(\varphi) = dch(S)$ and $\text{var}(\varphi) = \text{var}(S)$.

By induction on the structure of $S$, we show that, for every program $S$, $S \text{ sat } \varphi$ with $\varphi$ precise for $S$.

Skip

By the Skip Axiom, skip $\text{ sat } \text{term} = \text{start}$. We show that the assertion $\text{term} = \text{start}$ is precise for statement skip. From the Soundness Theorem 6.3, skip $\text{ sat } \text{term} = \text{start}$ is valid. Let $\gamma$ be any environment. Consider a well-formed model $\sigma$ such that $(\sigma, \text{begin}(\sigma)) \gamma \models \text{term} = \text{start}$. Then $\text{end}(\sigma) = \text{begin}(\sigma)$, and hence $\sigma \in M(\text{skip})$. We also have $dch(\text{term} = \text{start}) = \varnothing = dch(\text{skip})$ and $\text{var}(\text{term} = \text{start}) = \varnothing = \text{var}(\text{skip})$. Hence $\text{term} = \text{start}$ is precise for skip.

Assignment

Let $\varphi \equiv x = v \rightarrow (x = v \cup (T = \text{term} = \text{start} + K_\varnothing x = e[v/x]))$. By the Assignment Axiom, $x := e \text{ sat } \varphi$. We show that $\varphi$ is a precise specification for $x := e$. By the Soundness Theorem 6.3, $x := e \text{ sat } \varphi$ is valid. Consider a well-formed model $\sigma$ such that $dch(\sigma) \subseteq dch(x := e)$ and every program variable $y \notin \text{wvar}(x := e)$ is invariant with respect to $\sigma$. Thus $dch(\sigma) = \varnothing$, for all $\tau_1, \text{begin}(\sigma) \leq \tau_1 < \text{end}(\sigma)$, $\sigma(\tau_1).\text{comm} = \varnothing$, and for every program variable $y \neq x$, for all $\tau_2, \text{begin}(\sigma) \leq \tau_2 \leq \text{end}(\sigma)$, $\sigma(\tau_2).\text{state}(y) = \sigma(\text{begin}(\sigma)).\text{state}(y)$. Let $\gamma$ be such an environment that $\gamma(v) = \sigma(\text{begin}(\sigma)).\text{state}(x)$. Thus we have $(\sigma, \text{begin}(\sigma)) \gamma \models x = v$. Assume $(\sigma, \text{begin}(\sigma)) \gamma \models \varphi$. Then we obtain $(\sigma, \text{begin}(\sigma)) \gamma \models x = v \cup (T = \text{term} = \text{start} + K_\varnothing x = e[v/x])$. Then $\text{end}(\sigma) = \text{begin}(\sigma) + K_\varnothing$ and for all $\tau_1, \text{begin}(\sigma) \leq \tau_1 < \text{end}(\sigma)$, $\sigma(\tau_1).\text{state}(x) = \sigma(\text{begin}(\sigma)).\text{state}(x)$. Furthermore, $\sigma(\text{end}(\sigma)).\text{state}(x) = \mathcal{V}(e[v/x])\gamma(\sigma, \text{end}(\sigma)) = \mathcal{V}(e[v/x])\gamma(\sigma, \text{begin}(\sigma)) = \mathcal{V}(e)\gamma(\sigma, \text{begin}(\sigma)) = \mathcal{E}(e)\sigma(\text{begin}(\sigma)).\text{state}$. Thus, for all $\tau_1, \text{begin}(\sigma) \leq \tau_1 < \text{end}(\sigma)$, $\sigma(\tau_1).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}$, $\sigma(\text{end}(\sigma)).\text{state} = (\sigma(\text{begin}(\sigma))).\text{state} : x \mapsto \mathcal{E}(e)\sigma(\text{begin}(\sigma)).\text{state}$. Hence $\sigma \in M(x := e)$. It is obvious that $dch(\varphi) = \varnothing = dch(x := e)$ and $\text{var}(\varphi) = \{x\} \cup \text{var}(e) = \text{var}(x := e)$. Hence $\varphi$ is a precise specification for $x := e$.  

43
Delay

Let $\phi \equiv term = start + e$. By the Delay Axiom, delay $e$ sat $\phi$. We show that $\phi$ is a precise specification for delay $e$. By the Soundness Theorem 6.3, delay $e$ sat $\phi$ is valid. Consider a well-formed model $\sigma$ such that $dch(\sigma) \subseteq dch(delay e)$ and every program variable $y \notin \text{wvar}(delay e)$ is invariant with respect to $\sigma$. Thus $dch(\sigma) = \emptyset$, for all $\tau_1$, begin($\sigma$) $\leq \tau_1 < \text{end}(\sigma)$, $\sigma(\tau_1).\text{comm} = \sigma$, and for every program variable $y$, for all $\tau_2$, begin($\sigma$) $\leq \tau_2 \leq \text{end}(\sigma)$, $\sigma(\tau_2).\text{state}(y) = \sigma(\text{begin}(\sigma)).\text{state}(y)$. Then $\sigma(\tau_2).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}$. Let $\gamma$ be an arbitrary environment. Assume $(\sigma, \text{begin}(\sigma))\gamma \models \phi$. Thus $\text{end}(\sigma) = \text{begin}(\sigma) + \forall(e)\gamma(\sigma, \text{begin}(\sigma)) = \text{begin}(\sigma) + E(e)\gamma(\text{begin}(\sigma)).\text{state}$. Hence $\sigma \in M(delay e)$. Finally, it is obvious that $dch(\phi) = \emptyset = dch(delay e)$ and $\text{var}(\phi) = \text{var}(e) = \text{var}(delay e)$. Therefore $\phi$ is a precise specification for delay $e$.

Output

Let $\phi \equiv \text{wait}(c!) \cup (T = \text{term} - K_c \land (\text{comm}(c,e) \cup T = \text{term}))$. By the Output Axiom, cle sat $\phi$. We show that $\phi$ is precise for cle. By the Soundness Theorem 6.3, cle sat $\phi$ is valid. Consider a well-formed model $\sigma$ such that $dch(\sigma) \subseteq dch(cle)$ and every program variable $y \notin \text{wvar}(cle)$ is invariant with respect to $\sigma$. Then $dch(\sigma) \subseteq \{c, cle\}$ and for every program variable $y$, for all $\tau$, begin($\sigma$) $\leq \tau \leq \text{end}(\sigma)$, $\sigma(\tau).\text{state}(y) = \sigma(\text{begin}(\sigma)).\text{state}(y)$. Hence $\sigma(\tau).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}$. Let $\gamma$ be any environment. Assume $(\sigma, \text{begin}(\sigma))\gamma \models \phi$. Then there are two possibilities:

- Either $(\sigma, \text{begin}(\sigma))\gamma \models \square \text{wait}(c!)$;
- Or $(\sigma, \text{begin}(\sigma))\gamma \models \text{wait}(c!) \cup (T = \text{term} - K_c \land (\text{comm}(c,e) \cup T = \text{term})).$

That is,

- Either for all $\tau \geq \text{begin}(\sigma)$, $(\sigma, \tau)\gamma \models \text{wait}(c!)$. Then $\text{begin}(\sigma) \leq \tau < \text{end}(\sigma)$ and hence $\text{end}(\sigma) = \infty$. By definition, for all $\tau \geq \text{begin}(\sigma)$, $c! \in \sigma(\tau).\text{comm}$. Since $\sigma$ is a well-formed model, for any value $\theta \in \text{VAL}$ and any $\tau$, begin($\sigma$) $\leq \tau < \text{end}(\sigma)$, $\neg(c! \in \sigma(\tau).\text{comm} \land (c, \theta) \in \sigma(\tau).\text{comm})$ is valid. Then $\sigma(\tau).\text{comm} = \{c!\}$. Together with $\sigma(\tau).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}$, we obtain $\sigma \in M(cle)$;
- Or there exists a $\tau \geq \text{begin}(\sigma)$, $\tau \in \text{TIME}$, such that, for all $\tau_1$, begin($\sigma$) $\leq \tau_1 < \tau$, $(\sigma, \tau_1)\gamma \models \text{wait}(c!)$ and $(\sigma, \tau)\gamma \models T = \text{term} - K_c \land (\text{comm}(c,e) \cup T = \text{term})$. We split $\sigma$ as two models $\sigma_1$ and $\sigma_2$ such that $\sigma = \sigma_1\sigma_2$ with $\text{end}(\sigma_1) = \tau$. Thus $\text{begin}(\sigma_2) = \text{end}(\sigma_1) = \tau$. Then we obtain that, for all $\tau_1$, begin($\sigma_1$) $\leq \tau_1 < \text{end}(\sigma_1)$, $\sigma_1(\tau_1).\text{comm} = \{c!\}$. Together with $\sigma(\tau).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}$, for all $\tau$, begin($\sigma$) $\leq \tau \leq \text{end}(\sigma)$, we obtain $\sigma_1 \in \text{Wait}(\sigma)$. From $(\sigma, \tau)\gamma \models T = \text{term} - K_c$, we obtain $\tau = \text{end}(\sigma) - K_c$ and then $\text{end}(\sigma_2) = \tau + K_c = \text{begin}(\sigma_2) + K_c$. From $(\sigma, \tau)\gamma \models \text{comm}(c,e) \cup T = \text{term}$, we can derive that, for all $\tau_2$, begin($\sigma_2$) $\leq \tau_2 < \text{end}(\sigma_2)$, $(c, \forall(e)\gamma(\sigma_2, \tau_2)) \in \sigma_2(\tau_2).\text{comm}$.

By the well-formedness of $\sigma$ and the invariance of program variables, $\sigma_2(\tau_2).\text{comm} = \{(c, \forall(e)\gamma(\sigma_2, \text{begin}(\sigma_2))\} = \{(c, \forall(e)\sigma_2(\text{begin}(\sigma_2)).\text{state}\}$. Together with $\sigma(\tau).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}$, for all $\tau$, begin($\sigma$) $\leq \tau \leq \text{end}(\sigma)$, we obtain $\sigma_2 \in \text{Send}(c,e)$ and hence $\sigma \in M(cle)$. 

44
It is easy to see that $dch(\varphi) = \{c, e!\} = dch(c!e)$ and $\text{var}(\varphi) = \text{var}(e) = \text{var}(c!e)$. Therefore $\varphi$ is precise for $c?x$.

**Input**

Let $\varphi \equiv x = v \rightarrow [(x = v \wedge \text{wait}(c?))] \cup (T = \text{term} - K_c \wedge ((x = v \wedge \text{comm}(c, \text{last}(x))) \cup T = \text{term})]$. By the Input Axiom, $c?x \models \varphi$. We show that $\varphi$ is precise for $c?x$. From the Soundness Theorem 6.3, $c?x \models \varphi$. Consider a well-formed model $\sigma$ such that $dch(\sigma) \subseteq dch(c?x)$ and every program variable $y \notin \text{var}(c?x)$ is invariant with respect to $\sigma$. Then $dch(\sigma) \subseteq \{c, e!\}$ and, for all $\tau$, $\begin{cases} \begin{array}{l}
\text{begin}(\sigma) \leq \tau \leq \text{end}(\sigma), \\
\sigma(\tau).\text{state}(y) = \sigma(\text{begin}(\sigma)).\text{state}(y).
\end{array} \end{cases}$ Let $\gamma$ be such that $\gamma(v) = \sigma(\text{begin}(\sigma)).\text{state}(x)$. Then we have $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models x = v$. Assume $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi$. Thus we obtain $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models (x = v \wedge \text{wait}(c?)) \cup (T = \text{term} - K_c \wedge ((x = v \wedge \text{comm}(c, \text{last}(x))) \cup T = \text{term})]$. There are two possibilities:

- Either $(\sigma, \text{begin}(\sigma)) \gamma \models \Box (x = v \wedge \text{wait}(c?));$
- Or $(\sigma, \text{begin}(\sigma)) \gamma \models (x = v \wedge \text{wait}(c?)) \cup [T = \text{term} - K_c \wedge ((x = v \wedge \text{comm}(c, \text{last}(x))) \cup T = \text{term})].$

That is,

- Either $\text{end}(\sigma) = \infty$, for all $\tau \geq \text{begin}(\sigma)$, $\sigma(\tau).\text{state}(x) = \sigma(\text{begin}(\sigma)).\text{state}(x)$, and $c! \in \sigma(\tau).\text{comm}$. From the invariance of program variables different from $x$ and the well-formedness of $\sigma$, we obtain that, for all $\tau \geq \text{begin}(\sigma)$, $\sigma(\tau).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}$ and $\sigma(\tau).\text{comm} = \{c?\}$. Hence $\sigma \in M(c?x);$ 
- Or there exists a $\tau \geq \text{begin}(\sigma)$, $\tau \in \text{TIME}$, such that, for all $\tau_1$, $\text{begin}(\sigma) \leq \tau_1 < \tau$, $(\sigma, \tau_1) \gamma \models x = v \wedge \text{wait}(c!)$ and $(\sigma, \tau) \gamma \models T = \text{term} - K_c \wedge ((x = v \wedge \text{comm}(c, \text{last}(x))) \cup T = \text{term})$. We split $\sigma$ as two models $\sigma_1$ and $\sigma_2$ such that $\sigma = \sigma_1 \sigma_2$ with $\text{end}(\sigma_1) = \tau$. Then $\text{begin}(\sigma_2) = \text{end}(\sigma_1) = \tau$. We can obtain that, for all $\tau_1$, $\text{begin}(\sigma_1) \leq \tau_1 < \text{end}(\sigma_1)$, $\sigma_1(\tau_1).\text{state} = \sigma_1(\text{begin}(\sigma_1)).\text{state}$, $\sigma_1(\tau_1).\text{comm} = \{c?\}$. From $(\sigma, \tau) \gamma \models T = \text{term} - K_c$, we have $\tau = \text{end}(\sigma) - K_c$ and thus $\text{end}(\sigma_2) = \text{begin}(\sigma_2) + K_c$. We can also derive that, for all $\tau_2$, $\text{begin}(\sigma_2) \leq \tau_2 < \text{end}(\sigma_2)$, $(\sigma_2, \tau_2) \gamma \models x = v \wedge \text{comm}(c, \text{last}(x))$. Together with the invariance of program variables different from $x$, we then have $\sigma_2(\tau_2).\text{state} = \sigma_2(\text{begin}(\sigma_2)).\text{state}$. Since $\sigma = \sigma_1 \sigma_2$ and $\sigma_1(\text{end}(\sigma_1)).\text{state}(x) = \sigma_2(\text{begin}(\sigma_2)).\text{state}(x) = \gamma(v)$, we obtain that $\sigma_1(\text{end}(\sigma_1)).\text{state} = \sigma_1(\text{begin}(\sigma_1)).\text{state}$. Thus $\sigma_1 \in \text{Wait}(c?)$. By definition, $\forall(v(\text{last}(x))).\gamma(\sigma_2, \tau_2) = \sigma_2(\text{end}(\sigma_2)).\text{state}(x)$. Let $\psi = \sigma_2(\text{end}(\sigma_2)).\text{state}(x)$. Hence by the well-formedness of $\sigma$, we obtain that, for all $\tau_2$, $\text{begin}(\sigma_2) \leq \tau_2 < \text{end}(\sigma_2)$, $\sigma_2(\tau_2).\text{comm} = \{(c, \psi)\}$. Furthermore, we also have $\sigma_2(\text{end}(\sigma_2)).\text{state} = (\sigma_2(\text{begin}(\sigma_2)).\text{state} : x \mapsto \psi)$. Hence $\sigma_2 \in \text{Receive}(c, x)$ and then $\sigma \in M(c?x)$. 

It is obvious that $dch(\varphi) = \{c, e!\} = dch(c?x)$ and $\text{var}(\varphi) = \{x\} = \text{var}(c?x)$. Hence $\varphi$ is precise for $c?x$. 

45
We prove that $\varphi$ is precise for $G$. By the Soundness Theorem 6.3, $G$ sat $\varphi$ is valid. Consider a well-formed model $\sigma$ such that $dch(\sigma) \subseteq dch(G)$ and any program variable $y \notin wvar(G)$ is invariant with respect to $\sigma$. Let $\gamma$ be such an environment that, for all logical variables $v$ where $y \in var(G)$, $\gamma(v) = \sigma(begin(\sigma)).state(y)$. Then we have $\langle \sigma, begin(\sigma) \rangle \models \bigwedge_{\varphi \in \gamma} \varphi \land \Diamond \neg empty(dch(G) - dch(S)) \land inv(wvar(G) - wvar(S))$. By the definition of the $\land$ operator, there exist models $\sigma_1$ and $\sigma_2$ such that $\sigma = \sigma_1 \sigma_2$, $\langle \sigma_1, begin(\sigma_1) \rangle \models \varphi \land \Diamond \neg empty(dch(G) - dch(S)) \land inv(wvar(G) - wvar(S))$. From $\langle \sigma_2, begin(\sigma_2) \rangle \models \varphi$, by Lemma 6.2, $B(b)_{\langle \sigma_2, begin(\sigma_2) \rangle}$. From $\langle \sigma_2, begin(\sigma_2) \rangle \models inv(wvar(G) - wvar(S))$, every program variable $z \in wvar(G) - wvar(S)$ is invariant with respect to $\sigma_2$. By the assumption, any program variable $y \notin wvar(G)$ is invariant with respect to $\sigma$. Thus, any program variable $z \notin wvar(S)$ is invariant with respect to $\sigma_2$. From $\langle \sigma_2, begin(\sigma_2) \rangle \models inv(wvar(G) - wvar(S))$, we obtain $\sigma_2 \models inv(wvar(G) - wvar(S))$. Since $\sigma_2 \models inv(wvar(G) - wvar(S))$, and $\sigma_2 \models dch(\sigma) \subseteq dch(S)$, we obtain $\sigma_2 \models dch(\sigma) \\ 

[\bigwedge_{\varphi \in \gamma} \varphi \land \Diamond \neg empty(dch(G) - dch(S)) \land inv(wvar(G) - wvar(S))].$
Both cases lead to $\sigma \in M([\bigcup_{i=1}^{n} b_i \rightarrow S_i])$. It is obvious that $dch(\varphi) = dch(G)$ and $var(\varphi) = var(G)$. Hence $\varphi$ is precise for $\bigcup_{i=1}^{n} b_i \rightarrow S_i$.

Guarded Command with IO-guards

Consider $G \equiv [\bigcup_{i=1}^{n} b_i; c_i?x_i \rightarrow S_i \mid b; delay e \rightarrow S]$. By the induction hypothesis, we can derive $c_i?x_i; S_i$ sat $\varphi_i$ where $\varphi_i$ is precise for $c_i?x_i; S_i$. By the Communication Invariance Axiom, the Variable Invariance Axiom, and the Conjunction Rule, we obtain $c_i?x_i; S_i$ sat $\varphi_i \land$ empty($dch(G) - dch(c_i?x_i; S_i)) \land inv(wvar(G) - wvar(c_i?x_i; S_i))$. Similarly, we can derive $S$ sat $\varphi \land$ empty($dch(G) - dch(S)$) \land inv(wvar(G) - wvar(S))$ where $\varphi$ is precise for $S$. By the Guarded Command Evaluation Axiom, the Guarded Command with IO-guards Rule, the Conjunction Rule, and the Consequence Rule, we obtain $G$ sat $\psi$ with

$$
\psi \equiv \bigwedge_{y \in \text{var}(G)} y = v_y \rightarrow [(\text{Quiet} U (T = \text{start} + K_g \land \bigwedge_{y \in \text{var}(G)} y = v_y)) \land \\
(-b_G \rightarrow \text{term} = \text{start} + K_g)] \land [b_G \rightarrow (\text{Eval } C (\text{NComm} \lor \text{NTimeOut}))]
$$

where

$NComm \equiv (\text{Wait} \lor \text{InTime})C \psi_1, \quad \text{NTimeOut} \equiv (\text{Wait} \lor \text{EndTime})C \psi_2$

with

$$
\psi_1 = \bigvee_{i=1}^{n} [b_i \land \varphi_i \land \text{comm}(c_i) \land \Box \text{empty}(dch(G) - dch(c_i?x_i; S_i)) \land
inv(wvar(G) - wvar(c_i?x_i; S_i))]
$$

$$
\psi_2 \equiv \varphi \land \Box \text{empty}(dch(G) - dch(S)) \land inv(wvar(G) - wvar(S)).
$$

We prove that $\psi$ is precise for $G$. From the Soundness Theorem 6.3, $G$ sat $\psi$ is valid. Consider a well-formed model $\sigma$ such that $dch(\sigma) \subseteq dch(G)$ and any program variable $y \notin wvar(G)$ is invariant with respect to $\sigma$. Let $\gamma$ be such an environment that, for all logical variables $v_y$ where $y \in \text{var}(G)$, $\gamma(v_y) = \sigma(\text{begin}(\sigma)).\text{state}(y)$. Then we have $\langle \sigma, \text{begin}(\sigma) \rangle \gamma = \bigwedge_{y \in \text{var}(G)} y = v_y$. Assume $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \psi$. We prove that $\sigma \in M(G)$. Similarly as the preciseness proof for $G \equiv [\bigcup_{i=1}^{n} b_i \rightarrow S_i]$, we can derive that, for all $\tau_1$, $\text{begin}(\sigma) \leq \tau_1 \leq \text{begin}(\sigma) + K_g$, $\sigma(\tau_1).\text{state} = \sigma(\text{begin}(\sigma)).\text{state}$ and, for all $\tau_1', \text{begin}(\sigma) \leq \tau_1' < \text{begin}(\sigma) + K_g$, $\sigma(\tau_1').\text{comm} = \emptyset$. Next consider the validity of $b_G$. There are two possibilities:

- If $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models -b_G$, Lemma 6.2 leads to $B(\neg b_G)(\sigma(\text{begin}(\sigma)).\text{state})$. By assumption,
  $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \text{term} = \text{start} + K_g$ and hence $\text{end}(\sigma) = \text{begin}(\sigma) + K_g$. Then $\sigma \in M(\text{delay } K_g)$. Thus $\sigma \in M(G)$;

- If $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models b_G$, then $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models (\text{term} = \text{start} + K_g) \ C
((\text{Wait} \lor \text{InTime})C \psi_1) \lor ((\text{Wait} \lor \text{EndTime})C \psi_2))$.

For this case, consider the further three possibilities:

1. If $\langle \sigma, \text{begin}(\sigma) \rangle \gamma \models (\text{term} = \text{start} + K_g)C((\text{Wait} \lor \text{InTime})C \psi_1)$, there exist models $\sigma_1$ and $\sigma_2$ such that $\sigma = \sigma_1\sigma_2$, $\langle \sigma_1, \text{begin}(\sigma_1) \rangle \gamma \models \text{term} = \text{start} + K_g$, and $\langle \sigma_2, \text{begin}(\sigma_2) \rangle \gamma \models (\text{Wait} \lor \text{InTime})C \psi_1$. Then $\text{end}(\sigma_1) = \text{begin}(\sigma_1) + K_g$. By $\text{begin}(\sigma) = \text{begin}(\sigma_1)$, we obtain $\sigma_1 \in M(\text{delay } K_g)$. Furthermore, there exist models $\sigma_{21}$ and $\sigma_{22}$ such that $\sigma_2 = \sigma_{21}\sigma_{22}$, $\langle \sigma_{21}, \text{begin}(\sigma_{21}) \rangle \gamma \models \text{Wait} \lor \text{InTime}$, and $\langle \sigma_{22}, \text{begin}(\sigma_{22}) \rangle \gamma \models \psi_1$. We prove that $\sigma_{21} \in \text{BoundWait}(\sigma) \cup \text{AnyWait}(\sigma)$ and $\sigma_{22} \in \text{Comm}(\sigma)$. There

48
exists a $\tau_2 \geq \text{begin}(\sigma_{21})$ such that, for all $\tau_2' \leq \tau_2$, $\langle \sigma_{21}, \tau_2' \rangle \models \lambda y \in \text{var}(\sigma) \ y = v_y \wedge \text{empty}(\text{dch}(G) - \{c_1, \ldots, c_n\}) \wedge (b \rightarrow T < \text{start} + e) \wedge \Lambda^n_{i=1} (b_i \leftarrow \text{wait}(c_i))$ and $\langle \sigma_{21}, \tau_2 \rangle \models \lambda y \in \text{var}(G) \ y = v_y \wedge (T = \text{term}) \wedge (b \rightarrow T < \text{start} + e)$. Then, $\text{end}(\sigma_{21}) = \tau_2$ and, for any $y \in \text{var}(G)$, for all $\tau_2'' \leq \tau_2$, $\langle \sigma_{21}, \tau_2'' \rangle \models \text{state}(y) = \sigma_{21}(\text{begin}(\sigma_{21})).\text{state}(y)$. Together with the invariance of the variables $y \notin \text{var}(G)$, we obtain $\langle \sigma_{21}, \tau_2'' \rangle \models \text{state} = \sigma_{21}(\text{begin}(\sigma_{21})).\text{state}$. Since $\sigma$ is a well-formed model, so are $\sigma_{21}$ and $\sigma_{22}$. Since $\langle \sigma_{21}, \tau_2'' \rangle \models \text{empty}(\text{dch}(G) - \{c_1, \ldots, c_n\}) \wedge \Lambda^n_{i=1} (b_i \leftarrow \text{wait}(c_i))$, we obtain that $\sigma_{21}(\tau_2'').\text{comm} = \{c_i \mid E(b_i)(\text{begin}(\sigma_{21})).\text{state}, 1 \leq i \leq n\}$. By assumption, $\langle \sigma, \text{begin}(\sigma) \rangle \models b_G$. By Lemma 6.2, $B(b_G)(\sigma(\text{begin}(\sigma)).\text{state})$ and hence $B(b_G)(\sigma_{21}(\text{begin}(\sigma_{21})).\text{state})$. If $\langle \sigma_{21}, \text{begin}(\sigma_{21}) \rangle \models \sim b$, Lemma 6.2 leads to $B(b_G)(\text{begin}(\sigma_{21})).\text{state})$. From $\langle \sigma_{21}, \tau_2 \rangle \models b \rightarrow T < \text{start} + e$, we obtain $\tau_2 < \text{begin}(\sigma_{21}) + E(e)(\sigma_{21}(\tau_2)).\text{state}$. Then we can derive that $\text{end}(\sigma_{21}) < \text{begin}(\sigma_{21}) + E(e)(\sigma_{21}(\text{begin}(\sigma_{21})).\text{state})$ and then $\sigma_{21} \in \text{BoundWait}(G)$. If $\langle \sigma_{21}, \text{begin}(\sigma_{21}) \rangle \models \sim b$, $\sigma_{21} \in \text{AnyWait}(G)$.

Next consider $\sigma_{22}$. Since $\langle \sigma_{22}, \text{begin}(\sigma_{22}) \rangle \models \psi_1$, there exists a $k$, $1 \leq k \leq n$, such that $\langle \sigma_{22}, \text{begin}(\sigma_{22}) \rangle \models b_k \wedge \varphi_k \wedge \text{comm}(c_k) \wedge \Box \text{empty}(\text{dch}(G) - \text{dch}(c_k?x_k;S_k)) \wedge \text{inv}(\text{var}(G) - \text{var}(c_k?x_k;S_k))$. From Lemma 6.2, we get $B(b_k)(\sigma_{22}(\text{begin}(\sigma_{22})).\text{state})$. By definition, any program variable $z \notin \text{var}(G)$ is invariant with respect to $\sigma$. Thus, any program variable $z \notin \text{var}(c_k?x_k;S_k)$ is invariant with respect to $\sigma$. By Lemma 6.11, $[\sigma_{22}]_{\text{dch}(G) \cup \text{dch}(c_k?x_k;S_k)} = [\sigma_{22}]_{\text{dch}(c_k?x_k;S_k)}$. Using $\text{dch}(\sigma) \subseteq \text{dch}(G)$, we obtain $\text{dch}(\sigma_{22}) \subseteq \text{dch}(\sigma) \subseteq \text{dch}(G)$. By Lemma 6.4, $\sigma_{22} = [\sigma_{22}]_{\text{dch}(G)}$. Thus, $\sigma_{22} = [\sigma_{22}]_{\text{dch}(c_k?x_k;S_k)}$. By Lemma 6.4 again, $\text{dch}(\sigma_{22}) \subseteq \text{dch}(c_k?x_k;S_k)$. Together with the well-formedness of $\sigma_{22}$, $\langle \sigma_{22}, \text{begin}(\sigma_{22}) \rangle \models \varphi_k$, and the preciseness of $\varphi_k$ for $c_k?x_k;S_k$, we obtain $\sigma_{22} \in \mathcal{M}(c_k?x_k;S_k)$. Since $\mathcal{M}(c_k?x_k;S_k) = \mathcal{SEQ}(\mathcal{M}(c_k?x_k), \mathcal{M}(S_k))$ and $\langle \sigma_{22}, \text{begin}(\sigma_{22}) \rangle \models \text{comm}(c_k)$, $\sigma_{22} \in \mathcal{SEQ}(\text{Receive}(c_k, x_k), \mathcal{M}(S_k))$. Thus $\sigma_{22} \in \text{Comm}(G)$.

By $\sigma_{2} = \sigma_{21} \sigma_{22}$.

$\sigma_{2} \in \mathcal{SEQ}(\text{BoundWait}(G), \text{Comm}(G)) \cup \mathcal{SEQ}(\text{AnyWait}(G), \text{Comm}(G))$.

By $\sigma = \sigma_{1} \sigma_{2}$ and $\sigma_{1} \in \mathcal{M}(\text{delay } K_g)$,

$\sigma \in \mathcal{SEQ}(\mathcal{M}(\text{delay } K_g), \text{BoundWait}(G), \text{Comm}(G)) \cup \mathcal{SEQ}(\mathcal{M}(\text{delay } K_g), \text{AnyWait}(G), \text{Comm}(G))$ and hence $\sigma \in \mathcal{M}(G)$.

2. If $\langle \sigma, \text{begin}(\sigma) \rangle \models \langle \text{term} = \text{start} + K_g \rangle \square \text{Wait}$, there exist $\sigma_1$ and $\sigma_2$ such that $\sigma = \sigma_{1}\sigma_{2}$, $\langle \sigma_{1}, \text{begin}(\sigma_{1}) \rangle \models \text{term} = \text{start} + K_g$, and $\langle \sigma_{2}, \text{begin}(\sigma_{2}) \rangle \models \square \text{Wait}$. Then $\sigma_{1} \in \mathcal{M}(\text{delay } K_g)$. From $\langle \sigma_{2}, \text{begin}(\sigma_{2}) \rangle \models \square \text{Wait}$, we obtain that, for all $\tau_2 \geq \text{begin}(\sigma_{2})$, $\langle \sigma_{2}, \tau_2 \rangle \models \text{Wait}$. Hence, for all $\tau_2 \geq \text{begin}(\sigma_{2})$, $\langle \sigma_{2}, \tau_2 \rangle \models b \rightarrow T < \text{start} + e$. If $\langle \sigma_{2}, \tau_2 \rangle \models b$, $\tau_2 < \text{begin}(\sigma_{2}) + E(e)(\sigma_{2}).\text{state}$. But it cannot be true. Hence $\langle \sigma_{2}, \tau_2 \rangle \models \sim b$. By Lemma 6.2, $B(\sim b)(\sigma_{2}(\tau_2)).\text{state})$ and then $B(\sim b)(\text{begin}(\sigma_{2})).\text{state})$. Next we prove $\text{end}(\sigma_{2}) = \infty$. Suppose $\text{end}(\sigma_{2}) < \infty$. By definition, for all $\tau_3 \geq \text{end}(\sigma_{2})$, we can derive $\langle \sigma_{2}, \tau_3 \rangle \models \text{empty}(\text{dch}(G))$. By assumption,
Therefore all the cases lead to $\sigma \in \mathcal{M}(G).$ It is clear that $dch(\psi) = dch(G)$ and $\var(G) = \var(G).$ Hence, $\psi$ is precise for $G \equiv [\prod_{i=1}^{n} b_i; c_i x_i; S_i \rightarrow S_i] \parallel b; \text{delay } e \rightarrow S].$

### Iteration

Consider $\ast G.$ By the induction hypothesis, we can derive $G \text{ sat } \varphi$ where $\varphi$ is precise for $G.$ By the Iteration Rule, $\ast G \text{ sat } \psi$ with $\psi \equiv (b_G \land \varphi) \land (\neg b_G \land \varphi).$ We prove that $\psi$ is precise for $\ast G.$ By the Soundness Theorem 6.3, $\ast G \text{ sat } \psi$ is valid. Consider a well-formed model $\sigma$ such
that \( dch(\sigma) \subseteq dch(\ast G) \) and every program variable \( y \notin \text{wvar}(\ast G) \) is invariant with respect to \( \sigma \). Thus, \( dch(\sigma) \subseteq dch(G) \) and every program variable \( y \notin \text{wvar}(G) \) is invariant with respect to \( \sigma \). Let \( \gamma \) be an arbitrary environment. Assume \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \psi \). By definition of the \( C^* \) operator, there are two possibilities:

1. Either there exists a \( k \geq 1 \) and models \( \sigma_1, \sigma_2, \ldots, \sigma_k \) such that \( \sigma = \sigma_1 \sigma_2 \ldots \sigma_k \), for all \( j, 1 \leq j \leq k - 1 \), \( \text{end}(\sigma_j) < \infty \), \( \langle \sigma_j, \text{begin}(\sigma_j) \rangle \gamma \models b_\sigma \land \varphi \), and if \( \text{end}(\sigma_k) < \infty \), then \( \langle \sigma_k, \text{begin}(\sigma_k) \rangle \gamma \models \lnot b_G \land \varphi \), otherwise \( \langle \sigma_k, \text{begin}(\sigma_k) \rangle \gamma \models b_G \land \varphi \);

2. Or there exist infinite models \( \sigma_1, \sigma_2, \ldots \) such that \( \sigma = \sigma_1 \sigma_2 \ldots \), for all \( j \geq 1 \), \( \text{end}(\sigma_j) < \infty \), \( \langle \sigma_j, \text{begin}(\sigma_j) \rangle \gamma \models b_G \land \varphi \).

That is,

1. Either there exists a \( k \geq 1 \) and models \( \sigma_1, \sigma_2, \ldots, \sigma_k \) such that \( \sigma = \sigma_1 \sigma_2 \ldots \sigma_k \), for all \( j, 1 \leq j \leq k - 1 \), \( \text{end}(\sigma_j) < \infty \), \( \mathcal{B}(b_G)(\langle \sigma_j, \text{begin}(\sigma_j) \rangle \text{state}) \) (by Lemma 6.2). Since \( \sigma \) is well-formed, so are \( \sigma_1, \sigma_2, \ldots, \sigma_k \). Using \( dch(\sigma) \subseteq dch(G) \), we obtain \( dch(\sigma_j) \subseteq dch(G) \). Together with the invariance of program variables \( y \notin \text{wvar}(G) \) and the preciseness of \( \varphi \) for \( G \), \( \sigma_j \in \mathcal{M}(G) \). Similarly, \( \sigma_k \in \mathcal{M}(G) \). If \( \text{end}(\sigma_k) < \infty \), by Lemma 6.2, \( \mathcal{B}(b_G)(\langle \sigma_k, \text{begin}(\sigma_k) \rangle \text{state}) \). Otherwise \( \text{end}(\sigma_k) = \infty \);

2. Or there exist infinite models \( \sigma_1, \sigma_2, \ldots \) such that \( \sigma = \sigma_1 \sigma_2 \ldots \), for all \( j \geq 1 \), \( \text{end}(\sigma_j) < \infty \), \( \mathcal{B}(b_G)(\langle \sigma_j, \text{begin}(\sigma_j) \rangle \text{state}) \), and \( \sigma_j \in \mathcal{M}(G) \).

Therefore those two cases lead to \( \sigma \in \mathcal{M}(\ast G) \). It is obvious that \( dch(\psi) = dch(\ast G) \) and \( \text{var}(\psi) = \text{var}(\ast G) \). Hence, \( (b_G \land \varphi)C^*(\lnot b_G \land \varphi) \) is precise for \( \ast G \).

Parallel Composition

Consider \( S = S_1 \parallel S_2 \). By the induction hypothesis, we can derive \( S_1 \text{sat } \varphi_1 \) and \( S_2 \text{sat } \varphi_2 \) with \( \varphi_1 \) and \( \varphi_2 \) precise for \( S_1 \) and \( S_2 \), respectively. From preciseness, \( dch(\varphi_i) \subseteq dch(S_i) \) and \( \text{var}(\varphi_i) \subseteq \text{var}(S_i) \), for \( i = 1, 2 \). Then we can apply the General Parallel Composition Rule, obtaining \( S_1 \parallel S_2 \text{sat } \psi \) with \( \psi \equiv (\varphi_1 \land (\varphi_2 \land \psi_1)) \lor (\varphi_2 \land (\varphi_1 \land \psi_2)) \) where \( \psi_1 \equiv \text{inv}(\text{var}(S_2)) \land \square \text{empty}(\text{dch}(S_2)) \) and \( \psi_2 \equiv \text{inv}(\text{var}(S_1)) \land \square \text{empty}(\text{dch}(S_1)) \). We prove that \( \psi \) is precise for \( S_1 \parallel S_2 \).

By the Soundness Theorem 6.3, \( S_1 \parallel S_2 \text{sat } \psi \) is valid. Let \( \sigma \) be a well-formed model such that \( dch(\sigma) \subseteq dch(S_1 \parallel S_2) \) and any program variable \( y \notin \text{wvar}(S_1 \parallel S_2) \) is invariant with respect to \( \sigma \). Let \( \gamma \) be an arbitrary environment. Assume \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \psi \). We show \( \sigma \in \mathcal{M}(S_1 \parallel S_2) \).

By the well-formedness of \( \sigma \), for any \( c \in \text{CHAN} \), for any \( \tau, \text{begin}(\sigma) \leq \tau < \text{end}(\sigma) \), \( \neg(c \in \sigma(\tau).\text{comm} \land c' \in \sigma(\tau).\text{comm}) \) is valid. Suppose \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_1 \land (\varphi_2 \land \psi_1) \). Define \( \sigma_1 \) as \( [\sigma \uparrow \text{var}(S_1)]_{dch(S_1)} \). From \( \langle \sigma, \text{begin}(\sigma) \rangle \gamma \models \varphi_1 \) and \( \text{var}(\varphi_1) \subseteq \text{var}(S_1) \), Lemma 6.10 leads to \( \langle \sigma \uparrow \text{var}(S_1), \text{begin}(\sigma) \rangle \gamma \models \varphi_1 \). By \( dch(\varphi_1) \subseteq dch(S_1) \) and Lemma 6.9, we obtain \( \langle [\sigma \uparrow \text{var}(S_1)]_{dch(S_1)}, \text{begin}(\sigma) \rangle \gamma \models \varphi_1 \), i.e. \( \langle \sigma_1, \text{begin}(\sigma_1) \rangle \gamma \models \varphi_1 \). Since \( \sigma \) is well-formed, \( \sigma_1 \) is also well-formed. By the definition of \( \sigma_1 \), any program variable \( y \notin \text{wvar}(S_1) \) is invariant with respect to \( \sigma_1 \). Together with the preciseness of \( \varphi_1 \) for \( S_1 \) and \( dch(\sigma_1) \subseteq dch(S_1) \), we obtain \( \sigma_1 \in \mathcal{M}(S_1) \).
Next consider \((\sigma, \text{begin}(\sigma)) \gamma \models \varphi_2 \land C \psi_1\). By the definition of \(C\) operator, there exist models \(a_3\) and \(a_4\) such that \(\sigma = a_3 a_4\), \((a_3, \text{begin}(a_3)) \gamma \models \varphi_2\), and \((a_4, \text{begin}(a_4)) \gamma \models \psi_1\). Define \(a_2\) as \([a_3 \uparrow \text{var}(S_2)]_{\text{dch}(S_2)}\). Since \text{var}(\varphi_2) \subseteq \text{var}(S_2)\), Lemma 6.10 leads to 
\((a_3 \uparrow \text{var}(S_2), \text{begin}(a_3)) \gamma \models \varphi_2\). From \text{dch}(\varphi_2) \subseteq \text{dch}(S_2)\) and Lemma 6.9, we obtain 
\([a_3 \uparrow \text{var}(S_2)]_{\text{dch}(S_2)}, \text{begin}(a_3)\) \(\gamma \models \varphi_2\), i.e. \((a_2, \text{begin}(a_2)) \gamma \models \varphi_2\). Since \(\sigma\) is well-formed, so is \(a_2\). By the definition of \(a_2\), any program variable \(y \notin \text{var}(S_2)\) is invariant with respect to \(a_2\). Together with the preciseness of \(\varphi_2\) for \(S_2\) and \(\text{dch}(a_2) \subseteq \text{dch}(S_2)\), we obtain \(a_2 \in \mathcal{M}(S_2)\).

Notice that \(\text{end}(\sigma) = \text{end}(a_3 a_4) \geq \text{end}(a_3) = \text{end}(a_2)\) and \(\text{end}(\sigma) = \text{end}(\sigma_1)\), hence \(\text{end}(\sigma) = \max(\text{end}(\sigma_1), \text{end}(\sigma_2))\). Using the definition of \(\sigma_1, \sigma_2, \text{inv},\) and \(\text{empty}\), we can derive that, for \(i = 1, 2,\)

\[
[s]_{\text{dch}(S_2)}(\tau).\text{comm} = \begin{cases} 
\sigma_i(\tau).\text{comm} & \text{begin}(\sigma_i) \leq \tau < \text{end}(\sigma_i) \\
\emptyset & \text{end}(\sigma_i) \leq \tau < \text{end}(\sigma)
\end{cases}

(\sigma \uparrow \text{var}(S_i))(\tau).\text{state} = \begin{cases} 
\sigma_i(\tau).\text{state} & \text{begin}(\sigma_i) \leq \tau \leq \text{end}(\sigma_i) \\
\sigma_i(\text{end}(\sigma_i)).\text{state} & \text{end}(\sigma_i) < \tau \leq \text{end}(\sigma)
\end{cases}
\]

Thus \(\sigma \in \mathcal{M}(S_1||S_2)\).

Similarly, if \((\sigma, \text{begin}(\sigma)) \gamma \models \varphi_2 \land (\varphi_1 \land \psi_2)\), we can also prove that \(\sigma \in \mathcal{M}(S_1||S_2)\).

It is quite obvious that \(\text{dch}(\psi) = \text{dch}(\varphi_1) \cup \text{dch}(\varphi_2) \cup \text{dch}(S_1) \cup \text{dch}(S_2) = \text{dch}(S_1||S_2)\) and \(\text{var}(\psi) = \text{var}(S_1) \cup \text{var}(S_2) = \text{var}(S_1||S_2)\). Therefore we have proved that \(\psi\) is indeed precise for \(S_1||S_2\).
<table>
<thead>
<tr>
<th>Volume</th>
<th>Authors</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>89/1</td>
<td>E.Zs.Lepoeter-Molnar</td>
<td>Reconstruction of a 3-D surface from its normal vectors.</td>
</tr>
<tr>
<td>89/2</td>
<td>R.H. Mak, P.Struik</td>
<td>A systolic design for dynamic programming.</td>
</tr>
<tr>
<td>89/3</td>
<td>H.M.M. Ten Eikelder, C. Hemerik</td>
<td>Some category theoretical properties related to a model for a polymorphic lambda-calculus.</td>
</tr>
<tr>
<td>89/4</td>
<td>J.Zwiers, W.P. de Roever</td>
<td>Compositionality and modularity in process specification and design: A trace-state based approach.</td>
</tr>
<tr>
<td>89/5</td>
<td>Wei Chen, T.Verhoeff, J.T.Udding</td>
<td>Networks of Communicating Processes and their (De-)Composition.</td>
</tr>
<tr>
<td>89/6</td>
<td>T.Verhoeff</td>
<td>Characterizations of Delay-Insensitive Communication Protocols.</td>
</tr>
<tr>
<td>89/7</td>
<td>P.Struik</td>
<td>A systematic design of a parallel program for Dirichlet convolution.</td>
</tr>
<tr>
<td>89/9</td>
<td>K.M. van Hee, P.M.P. Rambags</td>
<td>Discrete event systems: Dynamic versus static topology.</td>
</tr>
<tr>
<td>89/10</td>
<td>S.Ramesh</td>
<td>A new efficient implementation of CSP with output guards.</td>
</tr>
<tr>
<td>89/11</td>
<td>S.Ramesh</td>
<td>Algebraic specification and implementation of infinite processes.</td>
</tr>
<tr>
<td>89/12</td>
<td>A.T.M.Aerts, K.M. van Hee</td>
<td>A concise formal framework for data modeling.</td>
</tr>
<tr>
<td>89/14</td>
<td>H.C.Haesen</td>
<td>ELDA, data manipulatie taal.</td>
</tr>
<tr>
<td>89/15</td>
<td>J.S.C.P. van der Woude</td>
<td>Optimal segmentations.</td>
</tr>
<tr>
<td>89/16</td>
<td>A.T.M.Aerts, K.M. van Hee</td>
<td>Towards a framework for comparing data models.</td>
</tr>
<tr>
<td>89/17</td>
<td>M.J. van Diepen, K.M. van Hee</td>
<td>A formal semantics for Z and the link between Z and the relational algebra.</td>
</tr>
<tr>
<td>Page</td>
<td>Author(s)</td>
<td>Title</td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>-------</td>
</tr>
<tr>
<td>90/2</td>
<td>K.M. van Hee P.M.P. Rambags</td>
<td>Dynamic process creation in high-level Petri nets, pp. 19.</td>
</tr>
<tr>
<td>90/4</td>
<td>A. Peeters</td>
<td>Decomposition of delay-insensitive circuits, p. 25.</td>
</tr>
<tr>
<td>90/5</td>
<td>J.A. Brzozowski J.C. Ebergen</td>
<td>On the delay-sensitivity of gate networks, p. 23.</td>
</tr>
<tr>
<td>90/8</td>
<td>M.B. Josephs</td>
<td>Receptive Process Theory, p. 16.</td>
</tr>
<tr>
<td>90/9</td>
<td>A.T.M. Aerts P.M.E. De Bra K.M. van Hee</td>
<td>Combining the functional and the relational model, p. 15.</td>
</tr>
<tr>
<td>90/10</td>
<td>M.J. van Diepen K.M. van Hee</td>
<td>A formal semantics for Z and the link between Z and the relational algebra, p. 30. (Revised version of CSNotes 89/17).</td>
</tr>
<tr>
<td>90/11</td>
<td>P. America F.S. de Boer</td>
<td>A proof system for process creation, p. 84.</td>
</tr>
<tr>
<td>90/12</td>
<td>P. America F.S. de Boer</td>
<td>A proof theory for a sequential version of POOL, p. 110.</td>
</tr>
<tr>
<td>90/14</td>
<td>F.S. de Boer</td>
<td>A proof system for the language POOL, p. 70.</td>
</tr>
<tr>
<td>90/15</td>
<td>F.S. de Boer</td>
<td>Compositionality in the temporal logic of concurrent systems, p. 17.</td>
</tr>
<tr>
<td>90/16</td>
<td>F.S. de Boer C. Palamidessi</td>
<td>A fully abstract model for concurrent logic languages, p. p. 23.</td>
</tr>
<tr>
<td>90/17</td>
<td>F.S. de Boer C. Palamidessi</td>
<td>On the asynchronous nature of communication in logic languages: a fully abstract model based on sequences, p. 29.</td>
</tr>
</tbody>
</table>
Design and implementation aspects of remote procedure calls, p. 15.

Two Case Studies in ExSpect, p. 24.

The Nature of Delay-Insensitive Computing, p. 18.

Data, Process and Behaviour Modelling in an integrated specification framework, p. 37.


Implication. A survey of the different logical analyses "if..., then...", p. 26.

Parallel Programs for the Recognition of P-invariant Segments, p. 16.

Performance Analysis of VLSI Programs, p. 31.

An Implementation Model for GOOD, p. 18.

SPECIFICATIEMETHODEN, een overzicht, p. 20.

CPO-models for second order lambda calculus with recursive types and subtyping, p.

Terminology and Paradigms for Fault Tolerance, p. 25.

Interval Timed Petri Nets and their analysis, p. 53.

POLYNOMIAL RELATORS, p. 52.

Relational Catamorphism, p. 31.


A note on Extensionality, p. 21.

The PDB Hypermedia Package. Why and how it was built, p. 63.