Theories for Session-based Governance for Large-scale Distributed Systems

Tzu-chun Chen
Department of Computer Science
Queen Mary, University of London

A thesis submitted for the degree of

Philosophiae Doctor (PhD)

2013, March

Supervised by: Dr Kohei Honda
Abstract

Large-scale distributed systems and distributed computing are the pillars of IT infrastructure and society nowadays. Robust theoretical principles for designing, building, managing and understanding the interactive behaviours of such systems need to be explored. A promising approach for establishing such principles is to view the session as the key unit for design, execution and verification.

Governance is a general term for verifying whether activities meet the specified requirements and for enforcing safe behaviours among processes. This thesis, based on the asynchronous $\pi$-calculus and the theory of session types, provides a monitoring framework and a theory for validating specifications, verifying mutual behaviours during runtime, and taking actions when non-compliant behaviours are detected. We explore properties and principles for governing large-scale distributed systems, in which autonomous and heterogeneous system components interact with each other in the network to accomplish application goals.

This thesis, incorporating lessons from my participation in a substantial practical project, the Ocean Observatories Initiative (OOI), proposes an asynchronous monitoring framework and the process calculus for dynamically governing the asynchronous interactions among distributed multiple applications. We prove that this monitoring model guarantees the satisfaction of global assertions, and state and prove theorems of local and global safety, transparency, and session fidelity. We also study and introduce the semantic mechanisms for runtime session-based governance and the principles of validation of stateful specifications through capturing the runtime asynchronous interactions.
Acknowledgements

My greatest thanks go to my supervisor Prof. Kohei Honda, who has been without doubt the person with the greatest influence in my life. He constantly encouraged and supported me not only for my doctoral research but also for my living in London. He advised me almost every day, tirelessly, dedicating more time and effort than anyone could ask from a supervisor. Because of his great supports, I had an invaluable PhD life. He was always cheerful, approachable, supportive, and put my doctorate studies as his first priority. For me, he is the model of a great computer scientist. He has endless loves and enthusiasm for computer science. He is so dedicated to it and so willing to communicate with people and to listen to different opinions. Kohei, thank you so much. Thank you for your cares, supports, and advices on both professional and personal issues. There are no words to express the full measure of my gratitude. How lucky I am to know you, to be your PhD student, and to share all the happy moments with you in the past few years.

Also, my warmest thanks go to my second supervisor, Prof. Nobuko Yoshida (Imperial College London). I learned from Nobuko both as a student and a co-author. She has a mind of steal and, at the same time, has the softest and warmest heart. After Kohei’s sudden passed away, she supported me and worked extremely hard to help me to complete my thesis even though herself is in a great sadness. Thank you Nobuko. Thank you so much for your valuable advices, efforts, and cares. Kohei and you both give me great impacts on my research life.

My thanks also go to Prof. Edmund Robinson (Queen Mary, University of London), who gave me the precious help to proof read the thesis, especially when he, as the head of the department, was extremely busy. Thank you
Edmund. Thank you for your patience and encouragements to help me go through the difficult period.

I would like to express my gratefulness that I have worked with, and learned from, Dr. Romain Demangeon (Queen Mary, University of London), Dr. Luca Fossati (Queen Mary, University of London), Dr. Laura Bocchi (University of Leicester), Dr. Pierre-Malo Denielou (Royal Holloway, University of London), and Dr. Raymond Hu (Imperial College London). Thank you so much for your helps and guidances. Especially, thank you Romain, Laura and Luca. Your advices and comments make this thesis completed.

Last but not least, my special thanks go to my families, my beloved parents, my dearest brother Chun-ting and cousin Yuju, and my friends Dr. Mu-yan Wang, Dr. Tzu-ching Horng, Pelin Yilmaz, Yvonne Chi, Dr. Kurosh Meshkat, Dr. Yuk-Chien Liu, Faris Abou-Saleh, and all of my colleagues. Thank you for accompanying me to overcome the most difficult time after the sudden death of Kohei, a great sadness for all people who know him. Before this, I did not know how important and how precious my families, my loved ones, and my friends are. You made me understand how lucky I am. Thank you all. You are all my angels.

Most important, thanks to the funding body of EPSRC grants EP/G015481/1 and Queen Mary, University of London. Without your support, I cannot even have the chance to study abroad to pursue a doctoral degree and to know those people who are so important and so valuable for me.

_I dedicate this work to my parents. I believe there are no parents like them devoting their loves to their children so much. Without their loves and unconditional supports, I cannot finish this thesis, and I cannot have the chance to continue my research works._

_I also dedicate it to my supervisor Prof. Kohei Honda, who died of a stroke on Thursday 4 December 2012. I still have not taken it in, and I think I will never do. Kohei, you had promised me that I will have a great adventure of computer science. And I promise you that I will continue it._
Contents

List of Figures

1 Introduction
1.1 Motivations and Objectives
1.2 Contributions
1.3 Publications & Detailed Contributions of the Author
1.4 Synopsis

2 Background and Theoretical Foundations
2.1 Large-scale Distributed Systems
2.2 Ocean Observatories Initiative (OOI)
2.3 Theory Foundations
  2.3.1 The $\pi$-calculus
    2.3.1.1 The Syntax and Semantics
    2.3.1.2 Mobility
  2.3.2 The Asynchronous $\pi$-calculus
    2.3.2.1 Synchrony v.s. Asynchrony
  2.3.3 Session Types
    2.3.3.1 Multi-party Session Types
    2.3.3.2 Multi-party Session Assertions

3 Related Works and Comparisons
3.1 Specification and Verification for Concurrent Programs
3.2 Specification and Verification for Conversations
3.3 Runtime Verification for Sharing Memory among Multiple Participants
3.4 Dynamic Monitoring Frameworks
## CONTENTS

3.4.1 Inlined Monitoring .................................................. 36  
3.4.2 Outline Monitoring .................................................. 37  
3.4.3 Monitoring for Conversations ................................. 38  
3.5 Governance .............................................................. 39  
3.5.1 Service-oriented Architecture (SOA) Governance .......... 39  
3.5.2 Law-governed Interactions ....................................... 40  
3.6 Endpoint Access Control ............................................. 40  
3.7 The Related Calculi .................................................... 42  
3.7.1 The Spi-calculus .................................................... 42  
3.7.2 Policy for Sessions in the Ambient Calculus .............. 43  

4 Assumptions and Terminologies ........................................ 45  
4.1 Principals, Processes, and Endpoints in Systems .............. 45  
4.2 Communications and Interactions ................................... 48  
4.3 Names, Sessions, Shared Channels, and Session-roles ........ 49  
4.4 More Illustrations for Shared Names ............................. 51  

5 The Capability-passing $\pi$-calculus ..................................... 55  
5.1 Motivating Example ................................................... 55  
5.2 Use Case: OOI Instrument Commands ............................. 57  
5.2.1 The Overview of OOI Instrument Commands ................. 58  
5.2.2 Specifying Protocols for Instrument Commands .......... 58  
5.2.3 Asynchronous Session Creation for Instrument Commands . 59  
5.2.4 The Complete Formal Processes of Instrument Commands .... 61  
5.3 The Calculus of Local Processes .................................... 62  
5.3.1 The Syntax of Local Processes ................................ 63  
5.3.2 The Structural Congruence of Local Processes .......... 68  
5.3.3 The Semantics of Local Processes ............................. 69  
5.4 The Calculus of the Network ......................................... 72  
5.4.1 The Syntax of the Network ...................................... 72  
5.4.2 The Structural Congruence of the Network ................. 75  
5.4.3 The Semantics of the Network ................................. 76  
5.4.4 Well-formedness .................................................... 78  
5.4.5 Global Queue v.s. Local Queue ............................... 80
## CONTENTS

7.4 Safety, Transparency, and Session Fidelity ........................................... 138
  7.4.1 Local Safety and Transparency .................................................. 138
  7.4.2 Global Safety, Transparency and Session Fidelity ....................... 139

7.5 Global Environment $\mathcal{E}$ ......................................................... 147
  7.5.1 Motivating Example ....................................................................... 148
  7.5.2 The Syntax of $\mathcal{E}$ ............................................................... 149
  7.5.3 The Semantics of $\mathcal{E}$ ........................................................... 150
  7.5.4 The Typing Rules of $\mathcal{E}$ ....................................................... 154
  7.5.5 The Coherence of $\mathcal{E}$ ............................................................ 155

8 Specifying Stateful Asynchronous Properties for Distributed Programs157
  8.1 Motivating Example .......................................................................... 158
    8.1.1 Using State in Specifications .................................................... 158
    8.1.2 Synchrony v.s. Asynchrony for Stateful Specifications ............... 160
    8.1.3 Capturing Causality Using Sets in Stateful Specifications .......... 161
    8.1.4 Analysis of Capturing Causality: $G_{assign}$ .............................. 163
  8.2 The Language of Stateful Specifications: SP ...................................... 165
    8.2.1 The Syntax of SP ..................................................................... 165
    8.2.2 Consistency Principles and Well-formedness .............................. 166
    8.2.3 The Projection from a Global SP to Local SPs ............................ 169
  8.3 Specifications Composed by SP ......................................................... 170
    8.3.1 The Syntax of Stateful Specifications ....................................... 170
    8.3.2 The Semantics of Stateful Specifications .................................... 171
  8.4 Traces of Local Actions ...................................................................... 173
    8.4.1 Permutation of Stateful Protocols .......................................... 174
    8.4.2 Permutation of Local Actions ................................................... 175
  8.5 Theory for Stateful Specifications ..................................................... 178
    8.5.1 Satisfaction ............................................................................. 178
    8.5.2 Asynchronously Verifiable Specifications ................................... 179
    8.5.3 Commutativity ......................................................................... 184
## 9 Conclusions and Future Topics

### 9.1 Conclusions and Discussions

- **9.1.1 The Capability-passing $\pi$-calculus**
- **9.1.2 The Calculus of Dynamic Asynchronously Monitoring**
- **9.1.3 Specifying Asynchronous Stateful Specifications**
- **9.1.4 Concluding Remarks**

### 9.2 Future Topics

- **9.2.1 The Development of Scribble and Monitoring**
- **9.2.2 Exploring Structures of Asynchronous Specifications**
- **9.2.3 Sharing Memory in Stateful Asynchronous Specifications**
- **9.2.4 Governance with Stateful Policies**

## Appendixes

### A Appendix for Capability-passing Calculus

- **A.1 Notes for the Syntax with or without Session Creation Rule**
- **A.2 Notes for the Design of $I$- / $O$-mode Shared Names**

### B Appendix for Dynamic Asynchronously Monitoring

- **B.1 Proofs for Local Safety and Transparency**
- **B.2 Proofs for Global Safety**
- **B.3 Proofs for Global Transparency**
- **B.4 Proofs for Session Fidelity**
- **B.5 Proofs for $E$ Coherence**

### C Appendix for Specifying Stateful Asynchronous Properties for Distributed Programs

- **C.1 Auxiliary Theorems and Proofs for Strongest Specifications**
- **C.2 Proofs for SPs’ Commutativity**

## References
### List of Figures

2.1 A Simplified Schematic Representation of Endpoints’ Interactions ........................................ 13
2.2 The Difference between Sequential and Session-based Abstractions of Interactions ............................... 23
2.3 The Grammar of Global \((G)\) and Local \((T)\) Types ................................................................. 25
2.4 The Syntax of Global \((G)\) and Local \((T)\) Assertions .............................................................. 26
3.1 The Different Approaches of the Representation of the Relationships of Events ............................... 30
4.1 The Relationships between Principals, Processes, and Endpoints .................................................. 47
4.2 The Relationship between Input- and Output-modes Shared Names ............................................. 50
4.3 Endpoints Represented by I-mode Shared Names in a Principal .................................................. 52
4.4 Using Shared Name to Represent Endpoints .................................................................................. 53
5.1 Delivering Information Through a Broker to Proper Targets ....................................................... 56
5.2 Illustration of the Global Protocol for OOI Instrument Commands ............................................. 58
5.3 The Syntax of Local Processes .................................................................................................... 65
5.4 The Labelled Transition System of Asynchronous Local Processes ........................................... 73
5.5 The Syntax for the Network ......................................................................................................... 73
5.6 The Reduction Rules of the Network .......................................................................................... 77
5.7 The Labelled Transition System of the Global Transport .......................................................... 79
6.1 Global Specifications: \(G\) ........................................................................................................ 93
6.2 Well-formedness for Global Specifications .................................................................................. 98
6.3 Local Specifications: \(T\) ........................................................................................................ 100
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>The Relationships between the Global Specifications, Local Specificaitons, and the Projection</td>
<td>102</td>
</tr>
<tr>
<td>7.1</td>
<td>Monitoring Architecture</td>
<td>112</td>
</tr>
<tr>
<td>7.2</td>
<td>Monitoring for One Session $s$ with the Specification: OO Instrument Commands</td>
<td>113</td>
</tr>
<tr>
<td>7.3</td>
<td>Monitors ($M$)</td>
<td>114</td>
</tr>
<tr>
<td>7.4</td>
<td>The Labelled Transition System of Monitors</td>
<td>116</td>
</tr>
<tr>
<td>7.5</td>
<td>The Labelled Transition System of Monitor-off</td>
<td>119</td>
</tr>
<tr>
<td>7.6</td>
<td>The Syntax of the Monitored Network</td>
<td>121</td>
</tr>
<tr>
<td>7.7</td>
<td>The Reduction Rules of the Monitored Network</td>
<td>124</td>
</tr>
<tr>
<td>7.8</td>
<td>The Labelled Transition System of the Monitored Network as Actions are Valid</td>
<td>125</td>
</tr>
<tr>
<td>7.9</td>
<td>The Labelled Transition System of the Monitored Network as Actions are Invalid</td>
<td>126</td>
</tr>
<tr>
<td>7.10</td>
<td>The Labelled Transition System of Configurations</td>
<td>145</td>
</tr>
<tr>
<td>7.11</td>
<td>The Labelled Transition System of $\mathcal{E}$</td>
<td>152</td>
</tr>
<tr>
<td>8.1</td>
<td>The Valid Traces of Asynchronous and Synchronous Interactions w.r.t. $G_{assign}$</td>
<td>162</td>
</tr>
<tr>
<td>8.2</td>
<td>The Grammar of Stateful Protocols</td>
<td>165</td>
</tr>
<tr>
<td>8.3</td>
<td>The Labelled Transition System of Specifications</td>
<td>172</td>
</tr>
</tbody>
</table>
Introduction

1.1 Motivations and Objectives

Motivations Governance is the collection of activities of governing. The purpose of governance for a large system is to ensure that independent system components (e.g. system agents, normal users, endpoint devices, etc.) can securely achieve their respective goals and, at the same time, the overall performance of the system is maintained and consistent. The related topics for achieving this purpose include access control mechanisms (e.g. access control matrix (105), DAC, MAC (53), and RBAC (62, 141), etc.), information flow control (28, 29, 65, 126, 140, 162), and policy languages for describing laws and regulations or specifying contracts and commitments (17, 54, 144).

Over the last two decades, we have witnessed computing systems evolve from isolated machines to network environments, from the centralised to the distributed; such evolution gives systems the benefits of performing tasks through densely coordinated actions among multiple heterogeneous components with distributed resources (19, 74, 112, 127). Communication in distributed components is becoming crucial for building large-scale applications, aided by a rapidly developing infrastructural support for portable distributed devices through technologies such as cloud computing, messaging and distributed stores. While distribution leads to such virtues as scalability, sharing and resilience (12, 125), specifying and ensuring the diverse correctness properties that individual applications demand poses new technical challenges.
1. INTRODUCTION

In order to understand and formalise interactive behaviours among communicating processes, robust theoretical foundations for such systems are needed. Without capturing the interactive behaviours, we can not judge the safety and reliability of target applications, and hence can not even set the baseline that our governance systems must meet. The traditional framework of sequential computing, such as objects and functions, does not enable us to effectively apprehend the behaviours and properties of distributed computing as a whole, since the central mode of computation in this new context is communication rather than, for example, assignment and function application.

In the concrete engineering setting of a large-scale distributed system, for example, the large IT infrastructure for ocean sciences (129), which is our leading example, applications are predominantly built as asynchronous interactions among heterogeneous distributed components. To cater for scalability and flexibility (23), it must be possible for each component to be implemented in a different programming language, and likewise for some of its components to be contributed by a third party, and these may be buggy or untrusted; moreover, it is also possible that the properties of services provided by contributors are dynamically discovered and changed. With the issues mentioned above and the problems addressed in (152, 153, 154), foreign components may not have been statically checked and runtime behavioural checks must be enforced.

In reality, most modern large-scale systems are distributed, but their governance relies on ad-hoc monitoring, complex safety enforcement mechanisms, centralised protocols, and expensive testing. And they still fail. Therefore, there is both a practical and theoretical need for the dynamic adjustment of a global specification in order to protect endpoints from malicious attacks and, at the same time, prevent them from producing malicious messages that pollute the network. Session-based governance, in which session types direct the computing, promises to offer a completely distributed, asynchronous governance framework for real-life systems, from fine-grained capability-passing $\pi$-calculus, to the semantics of stateful specifications.

Objectives  This thesis aims to identify principles to harness the complexity of asynchronous interactions among distributed heterogeneous components through capturing processes’ runtime behaviours. With this purpose in mind, we propose the formalism of a session-based dynamic-asynchronous monitoring framework:
1.1 Motivations and Objectives

1. The framework consists of *external* observers or monitors. The prototype of a monitor adopted in this thesis is similar to the one defined in [111, 103, 104]. A monitor acts as an endpoint guard, rather than a central mediator.

2. The observers or monitors in the framework *asynchronously* and *distributively* verify interactions among endpoints, which may come from heterogeneous domains.

3. The monitoring and verification mechanisms of this framework ensure, during runtime, the safe interactions of endpoints in a session through session-type-based local specifications, which are obtained by projection from global protocol specifications.

This framework is general enough to represent most large-scale distributed systems. With this framework, we introduce and prove *governance theories* for safety, transparency, session-fidelity, and the validation of stateful specifications.

One critical issue is how to deal with *asynchrony*. Two difficulties arise when this framework is applied. The first comes from adopting external monitors, which is common in practice, because inserting system internal monitors at every endpoint is expensive and they might be polluted by malicious local processes. This setting however results in *asynchronous interactions* between endpoints and their corresponding monitors since one monitor may economically guard more than one endpoint process. To deal with asynchrony, the mechanism of *permutation* is proposed and formalised.

The second difficulty comes from the desire to specify the endpoint state in specifications. A monitor, for guarding interactions, relies on a specification as a judgement base when it evaluates whether local process behaviour fulfill the intended requirements through observing the asynchronous messages passing from one process to another. In large-scale distributed systems, the use of *state* is omnipresent in specifications to capture real-life scenarios, where the (expected) states of participants in applications, such as the credit of a client for on-line shopping or the booking number for a transaction, play a critical role in specifications. A specification language for dynamic observations becomes non-trivial when *states* and asynchrony are both counted. An issue in the *semantics* of a specification language arises. The issue is that a monitor may be in asynchronous communication with the endpoint it monitors, and some interactions may update the endpoint’s state. For example, assume a local specification specifies that a ticket allocation server, with a state called *counter*, should assign a fresh ticket whose
value is equal to the value of \texttt{counter} for a client’s request and the value of \texttt{counter} is increased by one after every assignment. Thus, the server is required to assign ticket numbers as a sequence 1,2,3,4,5,.... Intuitively, the local specification of the server can assert that the output ticket value, say \( x \), should be equal to the current value of state \texttt{counter} i.e. \( x = \texttt{counter} \), and can stipulate the update of state as \( \texttt{counter} := \texttt{counter} + 1 \) once an output takes place. We call this kind of specification a \textit{stateful} specification. It seems natural that a monitor can use such \textit{stateful} specification to judge if the server manages state \texttt{counter} according to the specification. However, when the interaction between a monitor and its corresponding local process is asynchronous, the monitor may see ticket assignments out of order and hence some \textit{stateful} specifications, particularly the one in the above example, may lead a monitor to a wrong judgement in determining whether a local process is well-behaved or not. This issue poses a fundamental challenge to the endeavour to provide a consistent specification-verification framework.

In summary, this thesis presents the following contributions for governance of large-scale distributed systems:

1. We provide dynamic monitoring of runtime endpoint behaviour and prove that it guarantees the satisfaction of global specifications.

2. We state and prove the following properties:
   
   \begin{itemize}
   
   \item \textit{Dynamic global safety assurance} ensuring endpoint communication conformance (communication safety in (86)) and stating that a fully monitored network behaves well with respect to the given global specification.
   
   \item \textit{Dynamic global transparency} (43, 143) ensuring that if every endpoint program conforms to its local specification, the presence of monitors do not change the global interactions.
   
   \item \textit{Session fidelity} (86) ensuring that interactions in a session always follow stipulated global specifications step by step.
   \end{itemize}

3. We introduce the semantics of specifications for dynamic adjustment and prove the properties of satisfaction and validation of \textit{stateful} specifications for a formalism.

   Ongoing and future work addresses the development of policy languages and the properties for commitments.
1.2 Contributions

This dissertation focuses on the theories of dynamic distributed monitoring and specifying stateful specifications. It covers a wide range of specifications and semantics, while presenting a complementary approach for runtime verification. The main contributions of this thesis are divided into three parts:

**Capability-passing $\pi$-calculus.** This part is covered in Chapter 5, which contributes:

1. The introduction of a multi-party session-based $\pi$-calculus with new capability passing primitives for fine-grained control of endpoint behaviour through *session creation*.
2. The presentation of an exact semantic account of how a session can be initiated linearly with our calculus.
3. The introduction of a framework with an accurate view of the reality of distributed systems through formalising session-roles, name-passing, and asynchronous messaging.
4. The presentation of an abstraction of asynchronous operational semantics for both endpoint processes (locally) and the network (globally).

**Dynamic distributed monitoring.** This part is covered in Chapters 6 and 7, which contribute:

1. A model of dynamic *asynchronous* monitoring for distributed systems featuring the following elements:
   - The endpoints which are interacting with one another may come from heterogeneous domains, each of which may have different data structure, interface, typing compiler, or authentication policies. The endpoint code contributed by a heterogeneous domain may be written in a different language or possibly malicious.
   - The external monitors, each of which may guard more than one endpoint, protect endpoints from malicious attacks in the network and, at the same time, prevent endpoints from polluting the network. This practical setting results in asynchronous interactions between endpoints and their corresponding monitors.
1. INTRODUCTION

- The global specifications [22] enable concise application-level multi-party protocols, and local monitoring guarantees overall network conformance to stipulated global protocols at runtime.

2. The required permutation mechanism for external monitors. Due to asynchrony, the order of messages is not preserved during runtime; the permutation mechanism is therefore needed for monitors to capture the real-world asynchronous messagings.

3. The formalisation and establishment of properties of the monitored network, including:

- **Local and global safety.** Local safety (Theorem 7.4.3) states that a monitored process always behaves well with respect to the specification. Global safety (Theorem 7.4.16) states that a fully monitored network behaves well with respect to the given global specifications.

- **Local and global transparency** [43] [143]. Local transparency (Theorem 7.4.5) states that a monitored process behaves as an unmonitored process when the latter is well-behaved (e.g., it has been statically checked). Global transparency (Theorem 7.4.17) states that a monitored network and an unmonitored network have equivalent behaviour when the latter is well-behaved with respect to the same collection of local specifications, which are projected from well-formed global specifications.

- **Session fidelity** [86] (Theorem 7.4.28) states that, if all session message exchanges in a monitored/unmonitored network behave well with respect to the specifications (as communications dynamically unfold), then this network exactly follows the original global specifications.

- **Conformance with respect to the global observables** (Proposition 7.5.7) states that, whenever the global observable behaviours are coherent, as every possible endpoint action takes place, the resulting global observable behaviours, after the transition, are still coherent. Note that, the global observable behaviours are those which can be witnessed globally (introduced in Section 7.5). We formalise it because, during runtime, there is always a time lag due to asynchrony making the local specifications for the sender and the receiver inconsistent.
1.3 Publications & Detailed Contributions of the Author

**Specifying stateful specifications.** This part is covered in Chapter 8, a full version of my paper (40), which contributes:

1. An introduction of an intuitive stateful specification, which is suitable for describing asynchronous stateful behaviours among multi-party sessions, and enriches (22) with set-based stateful operations (Sections 8.1 and 8.2 in Chapter 8).
2. An identification of a *semantic* issue when specifying asynchronous interactive behaviour combined with updatable states.
3. A formal analysis of the issue through *asynchronous trace semantics*. We reach several criteria for asynchronous verifiability of specifications (healthiness conditions (81)), including a decidable one which can express a rich set of specifications.
4. The properties of stateful specifications, which include the definition and analysis of the strongest asynchronous specification w.r.t a given synchronous one, and the theorems of safety satisfaction and the validation of stateful specifications.

1.3 Publications & Detailed Contributions of the Author


**Author’s contribution:** The Scribble language was first developed by Dr Kohei Honda and Dr Gary Brown. My contribution was part of the theoretical foundation for Scribble. This work was majorly carried out under the advice and the support of Dr Kohei Honda. The development of Scribble, which is not in the scope of this thesis, is ongoing (87).

**Corresponding Part:** Chapter 9

Author’s contribution: Parts of theories and ideas. The ideas and formulations of asynchronous linear session establishment, the permutation mechanism of specifications and global observables, paper’s writing (mainly for the theory parts).

Corresponding Part: Chapters 5, 6, and 7.


Author’s contribution: The ideas, theories, writings, and proofs. This is a paper of my own.

Corresponding Part: Chapter 8.


Author’s contribution: Parts of theories and writings. The complete proofs of local/global safety, local/global transparency, and session fidelity.

Corresponding Part: Chapters 5, 6, and 7.

1.4 Synopsis

The dissertation is divided into 9 chapters, covering the background and related works, the main theories, and the future directions.

Chapter 2 introduces the background of large-scale distributed systems, our leading example, and the asynchronous π-calculus and the multi-party session types, which are the theoretical foundations of this thesis.

Chapter 3 gives an overview of related works and the comparisons of our work with those related ones.

Chapter 4 gives the assumptions and defines the terminologies used in this thesis. This chapter provides an overall picture of the system and framework that we are interested in, and the assumptions supporting our formalisms and theories.
1.4 Synopsis

Chapter 5 introduces the capability-passing $\pi$-calculus. This chapter, although does not include any main theory, gives the basis for the design of governance specifications and the calculus of dynamic asynchronously monitoring.

Chapter 6 introduces the syntax and semantics of the session-type based global/local specifications. This chapter grounds the specifications used in the following chapters and introduces the consistency principles and several useful mechanisms for working with specifications, such as the projection and the permutation rules.

Chapter 7 introduces the dynamic asynchronously monitoring calculus on the base established in Chapter 5 and 6. Several main theorems, such as local/global safety, local/global transparency, and session fidelity, are established here.

Chapter 8 extends the specifications, introduced in Chapter 6, to stateful specifications. It addresses the semantic issue while the stateful specifications are applied to external monitors in asynchronous monitoring environments. Also, it proposes theories and several properties of satisfaction of the sequence of actions and the validation of stateful specifications.

Chapter 9 concludes the dissertation by summarising the main theory chapters (i.e. Chapters 5, 6, 7, and 8). It also focuses on important future work which can pave the way to design session-based policy languages useful in practice based on the fundamental theories developed in the main parts.

Appendix includes three parts: Part A contains the notes of Chapter 5. Part B contains all proofs of the theorems introduced in Chapter 7 and their auxiliary definitions and lemmas. Part C contains the proofs of results from Chapter 8 which are not proved directly there.
Background and Theoretical Foundations

2.1 Large-scale Distributed Systems

Tanenbaum and Steen (155) define a distributed system as “a collection of independent computers that appears to its users as a single coherent system.”; while Leslie Lamport (12) says “you know you have a distributed system when the crash of a computer you’ve never heard of stops you from getting any work done”. According to them, a distributed system is a collection of computing tasks that sometimes goes very wrong because of its complexity and the difficulties of its maintenance. In this dissertation, we are concerned with large-scale distributed systems from the point of view of their usage. From our perspective, the key property is:

people residing in different domains want to conveniently and efficiently enjoy cooperation on tasks across domains.

Here “people” can be replaced by system components or any electronic devices. The reference to “different domains” implies that they may have different system policies, access control rules, and different verification mechanisms. The requirement of “conveniently and efficiently” implies that time and spatial limitations should be minimised. And “cooperation on tasks across domains” implies that if a user wants to access cooperative data in another domain, he or she should be able to do so through proper authentication. In a large-scale distributed system, participants may be geographically remote
2. BACKGROUND AND THEORETICAL FOUNDATIONS

and the system must be scalable enough to cater for heterogeneous remote components joining or leaving the system.

Jean Bacon carried out an extensive survey of large distributed systems and concluded that they are hard to maintain [14]. The particular challenges that she identified include concurrency, naming, and failure recovery. The same issues are also prominent in the analysis of Anderson [12]. This thesis, based on the \( \pi \)-calculus, takes concurrency of processes as the norm, uses names to denote endpoints, and equips primitives for name passing to control mobility. For failures (i.e. errors), the monitoring mechanism proposed in this thesis straightforwardly stops the ill-behaved process and drops it off. As the first step in governing asynchronous interactions with a session-based approach, this thesis does not cover the issue of a failure recovery mechanism.

2.2 Ocean Observatories Initiative (OOI)

The Ocean Observatories Initiative (OOI), the model of a large-scale distributed system that this thesis based on, is a major project funded by the US NSF. One of its goals is to realise the cross-domain inter-networks and inter-cooperations. The OOI’s intention is not to produce a private cloud, unlike Google [70] and Amazon [8], it aims to provide a public cloud integrating more than one cloud to serve researchers and the public with persistent and interactive capabilities for observing the oceans over a period of more than 30 years [36, 129], and, at the same time, enjoys scalability and consistency. It therefore presents a general architecture which has all the attributes a large-scale distributed system should have. The governance theories in this thesis are mainly based on OOI’s requirements and attributes.

With our ongoing cooperation, the governance theories proposed in this thesis are going to be adopted as the theoretical foundation for OOI’s design. The key element is a comprehensive cyberinfrastructure (i.e. CI), whose design is based on loosely-coupled distributed services and agents throughout the OOI observatories, from seafloor instruments to on-shore research stations, communicating through a common messaging infrastructure. Most of the use case scenarios focus on distributed and structured conversations among endpoints which may be a thousand miles apart.

In conclusion, for OOI’s system, OOI wishes to provide a communication and data transformation platform for ocean science, connecting observation, data collection, and
modelling under a mechanism, that includes a suitable governance system to guarantee stability and integrity. A traditional data-centric CI has a central data management system that ingests data and serves it to users on a query basis. This however is not sufficient to accomplish the range of tasks ocean scientists will engage in when the OOI is implemented. Instead, a highly distributed set of capabilities is required.

Figure 2.1 describes possible relationships among OOI organizations (Orgs). Each ellipse delineates an Org, corresponding informally to a community of participants. Orgs may be nested within, be disjoint from, or partially overlap with other Orgs. Org OOI is the root Org in that it defines the identities for the participants involving in and provides the rules to monitor and enforce contracts among its participants (41).

2.3 Theory Foundations

In this section, we give a brief overview of the two fundamental theoretical bases of this thesis: the asynchronous π-calculus (24, 84) and session types (30, 69, 85, 86, 157), which structure communications. Since the asynchronous π-calculus is built upon the π-calculus (117, 118), we start from introducing the π-calculus to give readers an
over view. The \( \pi \)-calculus is a process algebra for modeling communications. There are many formalisms for describing concurrent communications besides the \( \pi \)-calculus. They include the actor model (76), CSP (communicating sequential processes) (79, 80), CCS (communication and concurrency system) (115), and the Ambient Calculus (33). This thesis is based on the asynchronous \( \pi \)-calculus for two main reasons:

1. Like the \( \pi \)-calculus, it has the virtue providing a neat and sufficient expressive model for identifying and formalising interactive behaviours among participants in distributed systems. This virtue is elegantly captured in its syntax and semantics, which will be reviewed below.

2. It identifies concurrent and asynchronous behaviours, and mobility of processes through message passing with a simple but expressive syntax and semantics.

We also make substantial use of the theory of session types (22, 30, 31, 57, 69, 86, 89). Session types, the types typing conversations, are simple and expressive formal languages for describing protocols. When we use a session type to define a session, although the interactive behaviours in an individual session may be sequential, different sessions can interleave, which makes the overall interactions behave concurrently. Thus the attribute of concurrency of processes in distributed systems is captured in our theory. Since the focus of this thesis is to establish a foundation for governing processes’s interactions in large-scale distributed systems, applying the ideas of protocols, which define and specify the behaviours of session participants who agree on it, is thus practical, expressive, and effective.

2.3.1 The \( \pi \)-calculus

As noted by (134), the \( \pi \)-calculus (117, 118) is a core calculus of message-based concurrency. It was inspired by Nielsen and Engberg (57), and formulated and introduced by Robin Milner, Joachim Parrow and David Walker (118). There are many studies about the \( \pi \)-calculus, including the works of (82, 116, 117, 121). The defining feature of the \( \pi \)-calculus is its ability to model interactive behaviours among participants by message passing. As three main attributes of activities in large-scale distributed systems are: (I) interactions, including sending-receiving pair-wise communications via passing messages among processes, are the norm, and (II) the behaviours of those interactions
are majorly concurrent, and (III) the processes can be mobile in the network. The π-calculus, with its conciseness and expressiveness for concurrency and name passing, provides for this thesis an ideal basis.

2.3.1.1 The Syntax and Semantics

Here we briefly introduce the action labels and the grammar of the π-calculus.

**Action Prefixes**

The action prefixes $\alpha$ of the π-calculus includes both observable and internal ($\tau$) actions. An action prefix represents either sending or receiving a message (a name), or making a silent transition. The syntax is

$$
\alpha ::= x(y) \text{ receiving (input) of name } y \text{ via channel } x \mid \pi(y) \text{ sending (output) of name } y \text{ via channel } x \mid \tau \text{ internal (silent) action}
$$

**Processes**

The set of the π-calculus processes, $P, Q, \ldots$, is defined by the grammar

$$
\text{Process } P ::= \sum_{i \in I} \alpha_i.P_i \mid P_1|P_2 \mid \nu xP \mid !P,
$$

where $I$ is any finite indexing set. The process $\sum_{i \in I} \alpha_i.P_i$ is called summation or sum. It represents guarded choice. Generally speaking, $P_i$ is guarded by $\alpha_i$, since the action represented by $\alpha_i$ must occur before $P_i$ becomes active. 0 (inactive) is used to represent the empty sum, $\alpha.P$ (prefix) is used to represent sum on one element only, and $P + Q$ is for the binary sum. The symbols $|$ and $!$ are respectively the parallel and the replication operator. The restriction $\nu x$ and the input $y(x)$ both bind the name $x$, i.e. in the processes $\nu xP$ and $y(x).P$, the occurrences of $x$ in $P$ are considered bound with the usual rules of scoping. On the other hand, $x$ is free on the output $y\langle x \rangle$ action. The set of free names of $P$, i.e. those names which do not occur in the scope of any binder, is denoted by fn($P$). The set of bound names is denoted by bn($P$), and n($P$) is used to denote all the names which occur in $P$. The renaming (or substitution) $P(y/x)$ is defined as the result of replacing all free occurrences of $x$ in $P$ by $y$.

**Process Contexts**
2. BACKGROUND AND THEORETICAL FOUNDATIONS

The set of process contexts $C$ is given by the syntax:

$$C ::= [ ] | \alpha.C + M | \nu xC | C|P | P|C | !C.$$

$C[Q]$ denotes the result of filling the hole $[ ]$ in the context $C$ with the process $Q$. The elementary contexts are $\alpha.[ ] + M$, $\nu x[ ]$, $[ ] | P$, $P | [ ]$, and $! [ ]$.

**Process Congruence**

Let $\equiv$ be an equivalence relation over the set of all the $\pi$ processes. The $\equiv$ is said to be a process congruence if it is preserved by all elementary contexts; that is, if $P \equiv Q$, then

$$\begin{align*}
\alpha.P + M & \equiv \alpha.Q + M \\
\nu xP & \equiv \nu xQ \\
P | R & \equiv Q | R \\
R | P & \equiv R | Q \\
!P & \equiv !Q
\end{align*}$$

**Structural Congruence**

Two process expressions $P$ and $Q$ in the $\pi$-calculus are structurally congruent, written $P \equiv Q$, if we can transform one into the other by using the following equations (in either direction)

- Change of bound names (alpha-conversion)
- Reordering of terms in a summation
- $P | 0 \equiv P, P | Q \equiv Q | P, P | (Q | R) \equiv (P | Q) | R$
- $\nu x(P | Q) \equiv P | \nu xQ$ if $x \notin \text{fn}(P)$
- $\nu x0 \equiv 0, \nu xyP \equiv \nu yxP$
- $!P \equiv P | !P$

**Reduction**
The reduction rules are define below:

\[ \begin{align*}
\text{TAU} & : \quad \tau.P + M \rightarrow P \\
\text{REACT} & : \quad (x(y).P + M) \mid (\overline{\pi}(z).Q + N) \rightarrow P[z/\tau] \mid Q \\
\text{PAR} & : \quad \frac{P \rightarrow P'}{P|Q \rightarrow P'|Q} \\
\text{RES} & : \quad \frac{P \rightarrow P'}{\nu xP \rightarrow \nu xP'} \\
\text{STRUCT} & : \quad \frac{P \rightarrow P'}{Q \rightarrow Q'} \quad \text{if} \ P \equiv Q \text{ and } P' \equiv Q'
\end{align*} \]

We use the following example to illustrate reduction rules. A reduction is a silent action (\(\tau\) action). This example is extracted from Robin Milner’s *Communicating and Mobile Systems: The \(\pi\)-calculus* [117]. Let

\[ P = \nu z((\overline{\pi}(y) + z(w).\overline{\pi}(y)) \mid x(u).\overline{\pi}(v) \mid \overline{\pi}(z)). \]

\(x, y,\) and \(v\) are the free names in \(P\). A pair of positive and negative actions using the same channel, such as \(\overline{\pi}(y)\) and \(x(u)\) are complementary. If both are unguarded and not in the same summation (i.e. not alternatives to each other) then they constitute a *redex*: this redex constitutes a reduction \(P \rightarrow P'\), which invokes a substitution-here \(\{y/\tau\}\). In the example, \(P\) has two redexes; the pair \(\overline{\pi}(y), x(u)\) and the pair \(x(u), \overline{\pi}(z)\). By the rule \(\text{REACT}\), there are two possible reductions \(P \rightarrow P_1\), where \(P_1 = \nu z(0 \mid \overline{\pi}(v) \mid \overline{\pi}(z))\), or \(P \rightarrow P_2\), where \(P_2 = \nu z((\overline{\pi}(y) + z(w).\overline{\pi}(y)) \mid \overline{\pi}(v) \mid 0)\). There is no further reduction in \(P_1\), but by rule \(\text{REACT}\) there is one in \(P_2\):

\[ P_2 \rightarrow P_3, \text{ where } P_3 = \nu z(\overline{\pi}(y) \mid 0 \mid 0) \]

This example also shows the non-determinism of concurrent processes.

*Labelled Transition System*
The labelled transition system (LTS) is defined as follows:

\[ \text{Actions } \ell ::= x(y) | \tau(y) | \bar{\tau}(y) \]

**I-SUM**

\[ \Sigma_i \alpha_i . P_i \xrightarrow{x(z)} P_j \{z/y\} \quad \alpha_j = x(y) \]

**O/\tau-SUM**

\[ \Sigma_i \alpha_i . P_i \xrightarrow{\alpha_j} P_j \quad \alpha_j = \bar{\tau}(y) \text{ or } \alpha_j = \tau \]

**OPEN**

\[ P \xrightarrow{\bar{\tau}(y)} P' \]

\[ (\nu y) P \xrightarrow{\bar{\tau}(y)} P' \]

**RES**

\[ P \xrightarrow{\tau} P' \]

\[ (\nu y) P \xrightarrow{\tau} (\nu y) P' \]

\[ y \not\in n(\ell) \]

**PAR**

\[ P \xrightarrow{\tau} P' \]

\[ P | Q \xrightarrow{\tau} P' | Q \]

\[ \text{fn}(Q) \cap \text{bn}(\ell) = \emptyset \]

**COM**

\[ P \xrightarrow{\bar{\tau}(y)} P' \]

\[ Q \xrightarrow{x(y)} Q' \]

\[ P | Q \xrightarrow{\bar{\tau}(y)} (\nu y)(P' | Q') \]

**CLOSE**

\[ P \xrightarrow{\bar{\tau}(y)} P' \]

\[ Q \xrightarrow{x(y)} Q' \]

\[ y \not\in \text{fn}(Q) \]

**REP**

\[ P \parallel P \xrightarrow{\tau} P' \]

\[ \nu P \xrightarrow{\tau} P' \]

**CONG**

\[ P_1 \equiv P_2 \]

\[ P_2 \xrightarrow{\ell} Q_2 \]

\[ Q_2 \equiv Q_1 \]

\[ P_1 \xrightarrow{\ell} Q_1 \]

Note that \( n(\ell) \) means the collection of free and bound names occurring in \( \ell \). \( n(\ell) \) does not include the channel name. For example, \( n(\bar{\tau}(y)) = n(x(y)) = y \). \( \text{bn}(\ell) \) means the name bound by channel, e.g. \( \text{bn}(x(y)) = \text{bn}(\bar{\tau}(y)) = y \), but \( \text{bn}(\bar{\tau}(y)) = \text{bn}(\tau) = \emptyset \). And, on the contrary, \( \text{fn}(\ell) \) means the name free to channel, e.g. \( \text{fn}(\bar{\tau}(y)) = y \), \( \text{fn}(x(y)) = \text{fn}(\bar{\tau}(y)) = \text{fn}(\tau) = \emptyset \). Rules I-SUM and O/\tau-SUM are straightforward: When the action of an input (resp. output) process fires, the process executes the input (resp. output) action; while \( \tau \) action is for reduction of processes. The only action different from the prefix (i.e. \( \alpha \)) is \( \bar{\tau}(y) \), which means a bound output. It is introduced to model scope extrusion, which is corresponding to transition rule OPEN. Scope extrusion is
2.3 Theory Foundations

outputting a secret, say a private name \( y \) (through bound output \( \overline{x}(y) \)). If there is no corresponding receiver to get this private name (see rule CLOSE), then this private name becomes non-private. Rule RES says, when the action has nothing to do with the private names possessing by process \( (\nu y)P \), after the fire of this action, \( (\nu y)P' \) still has this name as private. If the channel of \( \ell \) is exactly the private name \( y \), it means the message is delivered internally. Rule PAR says the action will not affect the concurrent process \( Q \) if \( fn(Q) \cap bn(\ell) = \emptyset \), e.g. it will not result in a communication, as rule COM defines. Rule COM corresponds to the reduction rule REACT: When there synchronously exist an output \( x\langle y \rangle \) and an input \( x(y) \), a communication happens. While rule CLOSE, which seems similar to COM, is a dual to rule OPEN. It says when the sender sends a secret (by sending a private name via bound output \( x(y) \)) and at the same time, there is a receiver ready to input this secret, then this secret is shared only by the sender and the receiver, denoted by \( (\nu y)(P' \mid Q') \), saying the name is private in the scope of \( (P' \mid Q') \).

2.3.1.2 Mobility

As Milner’s work (117) states, in the \( \pi \)-calculus, link is used as the connectivity for describing mobility. The movement of a process can be represented entirely by the movement of its links, which is called as link mobility. According to Milner’s observation, what distinguishes the \( \pi \)-calculus from earlier process calculi, in particular to Calculus of Communicating Systems (CCS) (115) and Tony Hoare’s similar work on Communicating Sequential Processes (CSP) (79, 80), is the capability to change the links of a network of processes.

In the \( \pi \)-calculus, that is the name-passing makes mobility possible:

\[
\overline{x}(y).P \mid x(z).\overline{z}(10).Q \longrightarrow P \mid \overline{y}(10).Q\{y/z\}
\]

the \( \pi \)-calculus

\[
\overline{x}(10).P \mid x(z).\overline{y}(z).Q \longrightarrow P \mid \overline{y}(z)\{10/z\}.Q\{10/z\} = \overline{y}(10).Q\{10/z\}
\]

the CCS\(_{vp}\)

In the \( \pi \)-calculus, a name \( y \) is passed as a message, from process \( \overline{x}(y) \) via channel \( x \) to another concurrent process \( x(z).\overline{z}(10).Q \). As reduction happens (i.e. \( x(z).\overline{z}(10).Q \) receives \( y \), \( y \) becomes a channel, \( \overline{y}(10) \), for sending out value 10. While in the CCS\(_{vp}\) (i.e. value-passing CCS), a name cannot be passed, but only a value can be passed. Thus in the \( \pi \)-calculus, when a name is passed as a message, it can later become a channel. This simple idea realises the mobility through the change of links, which dynamically
2. BACKGROUND AND THEORETICAL FOUNDATIONS

change the computing configurations. Palamidessi in [33] analysed that link mobility is a very powerful feature for coordination of distributed activities, since it allows two remote processes, originally not directly connected, to establish a direct communication link and to take decision together via synchronous exchange of information along that link. Palamidessi proved that the link mobility makes the \( \pi \)-calculus strictly more powerful than CCS\(_{vp}\).

2.3.2 The Asynchronous \( \pi \)-calculus

Asynchrony is inherent in distributed systems because it takes time for a message to travel from one system component to another. The asynchronous \( \pi \), proposed by Honda and Tokoro in 1991’s [84] and, independently by Boudol in 1992’s work [24], contains no explicit operators for choice and output-prefixing. Due to the lack of output prefix, an output action is non-blocking and can only be written "in parallel" with other activities. With the \( \pi \)-calculus introduced above, here we address the main different grammars for the asynchronous \( \pi \)-calculus.

**Asynchronous Processes**

The set of the asynchronous \( \pi \)-calculus processes, \( P, Q, \ldots \), is defined by

\[
\text{Process } P ::= \overline{\pi}(y) \mid x(y).P \mid \sum_{i \in I} P_i \mid P_1P_2 \mid \nu x \ P \mid !P,
\]

The main difference is, in the asynchronous \( \pi \)-calculus, there is no output-prefix guarding a process. The output is unattached to the process producing it but exists in parallel with it. This design allows the sender to output without waiting for the synchronisation of the receiver side.

**Labelled Transition System**

The main rules different from the LTS rules of the \( \pi \)-calculus are listed below. Let \( \overline{\pi}y ::= \overline{\pi}(y) \mid \overline{\pi}(y)\):

\[
\text{OUT } \quad \overline{\pi}y \xrightarrow{\text{OUT}} 0
\]

\[
\text{COM } \quad \overline{\pi}y, x(z).P \xrightarrow{\text{COM}} P\{y/z\}
\]

Rule OUT states that \( \overline{\pi}y \) is able to be outputted at anytime and is independent to other processes at one location. In rule COM, "\( \cdots \)" is used to separate two processes inside one
2.3 Theory Foundations

location i.e. \( \overline{xy} \) and \( x(z).P \) are both at one location. The calculus proposed in this thesis uses different notation for "\( , \)" and "\( | \)". We use \( | \) for "\( , \)" to denote that a local process can consist of multi-threads in parallel; while use \( || \) for "\( | \)" to represent that the local processes existing in the network in parallel.

The attributes and benefits of the asynchronous \( \pi \)-calculus can be observed as making the communication between a sender and a receiver becomes asynchronous through having the sender to be able to fire its output at every possible execution time.

2.3.2.1 Synchrony v.s. Asynchrony

In concurrent and distributed computations, communications are dominant. Communication is a process for delivering messages, exchanging opinions, negotiation, and achieving agreements. There are many kinds of communication models, for example, synchronous, asynchronous, one-to-one, or one-to-many communication models. Two main models are discussed: The synchronous \( \pi \)-calculus, denoted by \( \pi \), and the asynchronous \( \pi \)-calculus, denoted by \( \pi_a \). We study the distinction between the synchronous and the asynchronous \( \pi \)-calculus with Palamidessi’s work (133). Note that the \( \pi \)-calculus itself is a synchronous paradigm which contains an "asynchronous" fragment (Boudol, 1992; Honda and Tokoro, 1991).

In the \( \pi \)-calculus, we write \( P = \overline{xy}.P' \) to represent a process \( P \) that performs an output of name \( y \) on channel \( x \) and continues as \( P' \), and we write \( Q = x(z).Q' \) to represent a process \( Q \) that performs an input on channel \( x \) and continues as \( Q' \{ y/z \} \) after replacing every \( z \) in \( Q' \) with \( y \). By using these operators, the synchronisation of \( P \) and \( Q \) on \( x \) is enforced: Only when the communication along \( x \) takes place, these two processes can proceed. On the contrary, in the asynchronous \( \pi \)-calculus, we write a process that performs an output in the form \( P = \overline{xy} \mid P' \), where \( \overline{xy} \) is an output to send \( y \) through channel \( x \) and \( \mid \) is the operator representing parallel composition. Since they are in parallel, the output process does not have to wait until a reception with corresponding primitive, say \( x(z) \), appears. In other words, the output action does not suspend the continuous process, i.e. \( P' \), and there is no crucial notion of continuation point. \( \overline{xy} \mid P' \) is a process which performs an output on \( x \) at some unspecified moment and of the handshaking between \( \overline{xy} \) and \( x(z).Q' \) as the moment in which the message is received by a reception. The reception enables the continuation point \( Q' \{ y/z \} \) in the receiver, but it does not cause any resumption of activity in the sender.
2. BACKGROUND AND THEORETICAL FOUNDATIONS

In conclusion, a synchronous communication is usually understood as the simultaneous exchange of information between the partners, for example, the telephone. In contrast, in an asynchronous communication, the action of sending a message and the action of receiving it usually take place at different times, for example, the e-mail. \cite{133} has proved that there does not exist any uniform, fully distributed translation from the \( \pi \)-calculus into the asynchronous \( \pi \)-calculus, up to any "reasonable" notion of equivalence. In other words, the asynchronous \( \pi_a \), is not as expressive as the full \( \pi \)-calculus.

However, the communication model of \( \pi_a \) is powerful enough to simulate output-prefixing, as shown by Honda and Tokoro 1991 and by Boudol 1992, and input-guarded choice, as shown by Nestmann and Pierce 2000’s work \cite{128}.

2.3.3 Session Types

A session type is a type for structuring a conversation, or called a “session”, which consists of more than one related interaction and multiple participant. It forms and specifies a unit of series of interactions which generally involve multiple participants, called endpoints in this thesis. The interactions can be sequential interactions, parallel interactions, or sub-interactions (which are formally called sub-sessions in \cite{19}). A session type is a protocol-like specification with formal shape.

Traditionally, viewing a computation as a sequence of actions gives a basis of the principles for sequential programming. Based on this viewpoint, sessions are done by RPC (remote procedure call). Every RPC is viewed as a single pair of interactions that starts with a request from a client to a server and ends with the response from the server to the client. The main difference between the concept of RPC and the one of sessions is that a session describes a structured flow of interactions which may include one or more, possibly an unbounded number of, interactions. For example, creating a new bank account is naturally abstracted as a scenario involving a sequence of interactions contacting with other services such as authentication components. From the viewpoint of RPC, both at the programming level and at runtime, such a sequence of interactions are not treated as forming a meaningful scenario as a whole since each call-return constitutes a single, isolated session. Figure \ref{fig:2.2} shows these two concepts as they both capture a common sequence of interactions but result in different representations of the behaviours. For the 4 interactions among Alice and Bob, they can be viewed
2.3 Theory Foundations

Figure 2.2: The Difference between Sequential and Session-based Abstractions of Interactions

as two independent RPCs (with two different RPC identities) or can be viewed as one session. The advantage of viewing these 4 interactions as one session is that it makes the relationships between endpoints trackable. For example, if some issue happens at the second RPC interaction, which is however caused by the first RPC interaction, without understanding that they are in fact related, the system cannot track through these interactions and resolve the problem. Viewing a session as a unit of executions makes it possible to clarify the patterns of interactive behaviours as a semantic entity.

2.3.3.1 Multi-party Session Types

The works of multi-party session types (MPSTs) \cite{32,86} present a formal approach to the local validation of globally specified protocols, which assure that the session names are used linearly (i.e. linearity) and the interactions are deadlock-free in a single session (i.e. progress). Overall, session types ensure communication safety, protocol fidelity.
2. BACKGROUND AND THEORETICAL FOUNDATIONS

and progress. Here we introduce its grammars of global and local types, and use one example in (86) to illustrate the use of session types.

The Syntax of Global and Local Types

In Figure 2.3, $U$ is for value types which denote interaction message types. $T@p$ is a located type, representing a local type $T$ assigned to participant $p$. $S$ is for standard value types, such as `bool`, `int`, `string`, etc., and the types for channels. $G,G',...,$ range over global types, $T,T',...,$ range over local types, and $p_1,p_2,...$ range over session participants, and $k$ is the variable for a channel. The rule of values for $G$ says participant $p_1$ should send a message with type $U$ to $p_2$ through channel $k$, then both participants should continue interactions guided by $G'$. From the local view point, participant $p_1$ has a corresponding local type, $k!⟨U⟩;T'$, to guide it to send a message of type $U$ through channel $k$, and continues the behaviour w.r.t. $T'$; while participant $p_2$ has a corresponding local type, $k?⟨U⟩;T'$, to guide it to receive a message of type $U$ through channel $k$, and continues the behaviour w.r.t. $T'$. The rule of branching for $G$ says participants $p_1$ and $p_2$ should use channel $k$ to interact through selecting a label from the branching pool (i.e. label pool). From the local viewpoint, participant $p_1$ has a corresponding local rule, called selection, to guide it to select a label, say $l_j$, and continues the actions specified by $T_j$; while participant $p_2$ has a corresponding local rule, called branching, to guide it to receive possible labels which may be chosen by the sender, and continues the actions specified by $T_k$ if the label $k$ has been chosen. The rule of recursion for global type, $µt.G$, is the type for defining a recursion, where $G$ is the recursion body. When we project it on the local endpoints, we have the corresponding recursion rule, $µt.T$, where $t$ is a type variable for either $G$ or $T$. It is used as a recursion point when it is involved in a recursion. $\text{end}$ is the termination of interactions. In summary, a global type $G$ layouts the interactions among session participants globally. When we project a global type to all session participants, a set of local types are generated to guide the interactive behaviours of endpoints.

Classic Example

The following example shows a scenario that a session is established for three participants, `Buyer`, `Broker`, and `Seller`, in which `Buyer` sends a request to `Broker`, and
2.3 Theory Foundations

Broker classifies this request should belong to either catalog buy or service. Then Broker informs Seller the catalog (i.e. branch label) she chooses. If label buy is chosen, both Broker and Seller’s interactions should follow $G_{buy}$’s guidance, otherwise they should follow $G_{service}$’s guidance.

We use global type $G$ to formally represent this scenario:

$$G = \text{Buyer} \rightarrow \text{Broker} : a\langle\text{string}\rangle, \text{Broker} \rightarrow \text{Seller} : b\{\text{buy} : G_{buy}.\text{end}, \text{service} : G_{service}.\text{end}\}$$

Note that, $G$ indicates that channel $a$ is used for Buyer to communicate with Broker, who is responsible for delivering the request of type string, from Buyer to Seller; while the communication between Broker and Seller is done through channel $b$.

For the endpoints, they respectively have the following local types:

$$T_{Buyer} = a!\langle\text{string}\rangle; \text{end}$$

$$T_{Broker} = a?\langle\text{string}\rangle; b \oplus \{\text{buy} : T_{buy}^{\text{Broker}}; \text{end}, \text{service} : T_{service}^{\text{Broker}}; \text{end}\}$$

$$T_{Seller} = b \& \{\text{buy} : T_{buy}^{\text{Seller}}; \text{end}, \text{service} : T_{service}^{\text{Seller}}; \text{end}\}$$

$T_{buy}^{\text{Broker}}$ is the local type for participant Broker when label buy is selected, while $T_{service}^{\text{Broker}}$ is for this participant when label service is selected. Similar, $T_{buy}^{\text{Seller}}$ and $T_{service}^{\text{Seller}}$ are the local types for participant Seller when label buy and label service are selected, respectively. This example shows that session types structure multiple interactions to an organised interaction flow and guide endpoints to behave well as what global scenario expects.
2. BACKGROUND AND THEORETICAL FOUNDATIONS

\[
\begin{align*}
L & ::= \{p, p', ..., \} & \text{Location} \\
S & ::= \text{bool} \mid ... \mid \langle G \rangle & \text{Sort} \\
G & ::= p_1 \rightarrow p_2 : k(\bar{v} : \bar{S}) \{A\}.G' & \text{values} \\
& \mid G \mid G' & \text{branching} \\
& \mid \mu t(\bar{e})(..., \bar{v}_i : \bar{S}_i @ L_i) \{A\}.G & \text{recursive} \\
& \mid t(\bar{e}) & \text{variable} \\
& \mid \text{end} & \text{end}
\end{align*}
\]

Figure 2.4: The Syntax of Global (G) and Local (T) Assertions

2.3.3.2 Multi-party Session Assertions

Multi-party session assertions (MPSAs) \cite{22} further allow, by extending MPSTs with logical formulae, fine-grained specifications of interactive behaviour including message contents, runtime choices of conversation paths and recursion invariants. By projecting a global assertion (i.e. global protocol specification) onto endpoints, we get endpoint assertions (i.e. local protocol specifications), each of which specifies endpoint in the protocol. Thus the local validations which automatically ensure global correctness are obtained.

The Grammar of Global and Local Assertions

Figure 2.4 shows the syntax of MPSAs, which extend MPSTs with logical formulae. The syntax of MPSAs is similar to the one of MPSTs, except that the interaction predicate \(A\) is introduced at every interaction to guard interactions. Note that, \(T@p\) in MPSTs is replaced by \(v : S@L\) (particularly defined in recursion for global types) with definition of locations \(L ::= \{p, p', ..., \}\). Also note that \(\bar{v}\) is defined in rule of values, send, receive, and recursion because \(\bar{v}\) should be specified in interaction predicate \(A\) to bind \(A\). As for the type of global recursion, since it defines the recursion variables known by all endpoints involving in the recursion, in \((..., \bar{v}_i : \bar{S}_i @ L_i, ...),\) \(\bar{v}_i : \bar{S}_i @ L_i\) indicates the types of contents for a particular location \(L_i\); while for the type of local recursion, since it has been located, only \(\bar{v} : \bar{S}\) is enough.
Related Works and Comparisons

To represent our focus without confusion, here we only mention the most related works having significant impact to the subjects that we are interested in. As a brief summary of comparisons, the following two points are noted here:

1. In the literature, the works of dynamic monitoring mostly rely on inlined monitors. In other words, in these works, they monitored the asynchronous interactions among endpoints through embedding monitoring code besides the variables and procedures which should be protected; however, as an external monitor is adopted for economic and scalable settings, we shall consider the asynchronous interactions between an endpoint and its corresponding monitor.

2. In the literature, most works of runtime monitoring do not provide the theoretical foundation to state and prove that their mechanisms enjoy the properties of safety and transparency, which are necessary for governing large-scale distributed systems. This thesis gives both. To cater for the asynchronous monitoring, we provide the semantics and the permutation mechanism of specifications for monitoring, which determines the endpoint behaviours based on these specifications, to capture the effects of actions whose order may not be preserved due to concurrency and asynchrony.
3. RELATED WORKS AND COMPARISONS

3.1 Specification and Verification for Concurrent Programs

Specifications are the rules for statically regulating endpoint programs and system structures or dynamically verifying runtime behaviours of processes and systems. In Alfred V. Aho et al.’s book (5), a specification is as an articulation of the request of a compiler. In Pierce’s book (135), a specification is defined by a type inference system. In general, a specification is a concise description which formally specifies the intended computation outcomes and makes verification of programming code or runtime processes possible. A proper specification should make verification effective. When the verification follows the semantics of a specification, it can at least judge an invalid code or process as incorrect, and can at most judge a valid code or process as correct.

There are two aspects of formal verification: One is to statically inspect the structure of programming code, the other is to dynamically check the behaviours of processes. Leslie Lamport’s opening in (101) says “a large body of research on formal verifications can be characterised as state-based or assertional”. A state-based verification is an automata-like approach, where the “state” means the “status” of a program or a process. An assertional verification is an approach with proof system and the construction of invariants, which are logical formulae whose value never change (100, 131).

The following history of specification and verification for concurrent programs is a summary from Lamport’s note (101), which reviewed the works having significant contributions and advocates specifying programs with mathematics (e.g. the proposal of TLA (temporal logic of actions)). In 1967, Floyd in (64) introduced the modern concept of correctness for sequential programs. In every program, there are control points, called annotations, attached with assertions, which are written in logical formulae. Partial correctness is proved by verifying if the control point is annotated “true” whenever control is at the point. A formula in Hoare’s logic, proposed in 1969’s work (77), has the form \{P\}S\{Q\}, denoting that if the assertion \(P\) is true before initiation of program \(S\), then the assertion \(Q\) will be true upon \(S\)’s termination. The state-based approach viewed a program as a state transformer, which can be verified by checking whether every control point satisfies the attached assertions.

Ashcroft in 1975 (13) adopted the state-based approach to concurrent programs, where concurrency is expressed by fork and join operations. In concurrent programming, a control can be at multiple control points at the same time: At every moment,
the annotation of a control is not unique, but rather as a collection of annotations of controls representing that the assertions are true. This collection is viewed as *invariance*, which should be true after every execution. The idea of invariance gives a fundamental principle to specify concurrent programs: Instead of only considering what is true before and after executing the program, one must consider what remains true throughout the execution.

In 1976, Owicki and Gries ([131]) attempted to reason about concurrent programs by generalising Hoare’s method with the following additional proof rule:

\[
\begin{align*}
\{P_1 \cap \ldots \cap P_n\} &\mathrm{cobegin}\ S_1 \parallel \ldots \parallel S_n \mathrm{coend} \{Q_1 \cap \ldots \cap Q_n\} \\
\end{align*}
\]

provided \(\{P_1\}S_1\{Q_1\}, \ldots, \{P_n\}S_n\{Q_n\}\) are interference-free.

Unlike Ashcroft’s method, the assertions in the Owicki-Gries method do not mention the control state but only introduce auxiliary variables to capture the control information. Ashcroft’s invariance is actually hidden inside the machinery of the Owicki-Gries method: This proof rule is as a general summary of valid concurrent programs without specifying how to share variables among concurrent programs to achieve invariance. To achieve \(\{P_1 \cap \ldots \cap P_n\} \mathrm{cobegin} S_1 \parallel \ldots \parallel S_n \mathrm{coend} \{Q_1 \cap \ldots \cap Q_n\}\), \(P_i\) and \(Q_j\) \((i \neq j)\) should have some hidden relationships which are not fully addressed.

Lamport in ([99]) indicates that a module in a concurrent program must be specified in terms of its behaviour, rather than the values it returns because, in a concurrent program, input and output actions are no more sequentially executed in one process but could be called by different processes. With the reality of concurrency, temporal logic is a useful tool to reason about the behaviour of concurrent programs ([132], [137]). In ([99]), Lamport introduced temporal assertions to make the specifications simpler and easier to understand. In ([27]), distributed temporal logic (DTL) was proposed for formalising properties of concurrent, communicating agents. It is a modal temporal logic with modalities referring to events, which are mapped to corresponding actions. ([27]) also introduced communication points to realise the asynchrony between a sender and a receiver through two phases of synchronisations: Synchronising the sender and a shared channel (i.e. sending a content to the communicating channel), and then synchronising the channel and the receiver (i.e. receiving the content from the communicating channel).
To compare the session-type-based approach and the temporal logic-based one, we use Figure 3.1 to illustrate that the session-type-based approach gives a cleaner and more uniform specification for verification. Assume there are three principals, Alice, Bob, and Carly in the system. Each of them has a unique identity. Assume Alice has a communication with Bob: Alice orders a book from Bob. Here Alice plays role client and Bob plays role store. Also, assume Alice has another communication with Carly: Carly sends a task request to Alice. Here Alice plays role server and Carly plays role client. For simplicity, here we only show the one-way events (i.e. no corresponding responses). In the figure, a horizontal solid line is the life time of a principal, and a black spot is an event. These two interactions are concurrent. As we apply the temporal logic-based approach, we have at least 6 different possible temporal assertions to describe these two concurrent interactions. As we apply the session-type-based approach, since unrelated sessions, e.g. the interaction of Alice and Bob and the one of Alice and Carly are unrelated, can interleave, only two session types (i.e. Session 1 and Session 2)
are needed. As one session starts, the corresponding session identity is generated for the system to track and maintain the overall endpoint behaviours. The advantage of session-type-based specifications is that session types concisely and uniformly represent all necessary information for concurrent interactions.

The session-type-based approach uses sessions to partition the interactions among processes. Although interactions are concurrent, because a session has linked all related interactions, there is no interference between different sessions. Thus, inside a session, the interactions are executed step by step, to which the principles of Floyd and Hoare’s works can be applied: Every interaction point attached with assertions (at the sender and the receiver) is viewed as a control point. At the same time, since different sessions concurrently exist in the network, we can focus on exploring and specifying the properties of invariance among sessions. For example, one invariance in our setting is the property of coherence. One rule of coherence states that, in all monitors’ specifications, there is one and only one shared channel with input mode, and, whenever there is a sender, there is a receiver.

Other methods of algebraic approaches, like CCS (115), and functional approaches, like the method of Broy (25), attempt to replace state-based reasoning with other proof techniques. In an algebraic approach, verification is based on applying algebraic transformations. In a functional approach, the rules of function applications are used.

Our approach is an algebraic one. We view a specification as a session-type-based language through formally defining its syntax and semantics. We provide the labelled transition system (LTS) of session-type-based specifications. As the operational specifications advocated by Lam and Shankar (97) and Lamport (99), the LTS makes the specifications efficient to specify parts of concurrent processes.

### 3.2 Specification and Verification for Conversations

In the literature, the purpose of defining specifications for conversations is to coordinate heterogeneous autonomous agents (95, 149). Many works related to this subject are particularly for multi-agent systems (MASs). In general, protocols are specifications for conversations.

There are two purposes of the exploration of conversation specifications: To define policies for conversations and to inspect (statically or dynamically) conversations among
3. RELATED WORKS AND COMPARISONS

multiple participants. To achieve them, one needs to firstly identify the relationships among the multiple system components, which may possibly locate in different domains. According to Singh’s work (149), to figure out distributed coordination of heterogeneous agents, we need to know the skeletons of agents with compact descriptions of the given agents in terms of their events for coordination, and the relationships among the events occurring in these skeletons. They adopted a graphic-approach, Dooley graphs (109), to generate the skeletons and the relationships required for coordination. The skeletons here are specifications, while coordinations in multi-agent systems generally are meant to be interactions among agents. With the use of Dooley graphs, the table recording the histories of agents in conversation is generated and the skeletons of an agent involving in coordination are produced. This work represented a methodology to produce a specification from observations and given requirements.

Other related works are (95, 150) of Smith et al. (150) provided a comprehensive semantics for the conversational policies through using joint intention theory (JI), which prescribes a way to execute actions jointly by a team of agents. In (95), the most important aspect of a conversation protocol is not the set of communicative actions involved in that protocol but the effects or the states that these actions bring about. They proposed a formal analysis of landmark-based approach to view a conversation protocol as partially ordered landmarks. Each landmark defines a set of specifiable semantic properties that must hold of the agents involved. Based on (150), they represented and analysed families of protocols with JI theory. They expressed JI in terms of joint commitment between two agents to bring about a certain state of affairs which results in appropriate individual commitments.

Wooldridge’s work (158) examined the issue of developing semantics for ACL (agent communication languages\(^1\)). It considered verification of conformance to the semantics and had given the first precise definition of what it means for an agent communication framework to be verifiable. Another work of his (159) argued that, for agents in large-scale multi-agent systems to safely communicate to one another, it must be able to determine whether any system that claims to conform to an ACL standard actually does so when agents are possibly built by different organisations using different platforms (136). Particularly, this conformance — the semantics of the language adopting

---

\(^1\)ACL means either KQML or FIPA ACL, proposed by Foundation for Intelligent Physical Agents (FIPA) in 1997.
3.2 Specification and Verification for Conversations

by a system conforms to the standard ACL semantics — can be determined by an independent observer. Koning and Oudeyer in (93) proposed POS (Protocol Operational Semantics), a unification and generalisation of interaction protocols, which allows the design of dedicated ACLs together with policies or constraints of messages.

The motivation behind the issues they addressed are similar to ours. They explored the semantic conformance for standard ACL, while we explored for the session-type-based specification languages. ACL is to cater for the needs of agents to interact in a shared language, hiding the details of their internals and to build communities of agents that can tackle problems that no individual agent can. Session types share the same interest. According to the investigation of (96), the existing semantic approaches for verifying the conformance for ACL standard, however, rely on multi-modal logics that are often non-computable and/or have no efficient implementation. Since session types standardise the sequence of actions (including the permutation of actions to cater for asynchronous environments) of a given protocol and the operational semantic system of specifications is deterministic, the semantic approach for verification of communications proposed in this thesis is decidable and computable.

Meng et al. in (113) explored the synthesis of Reo circuit scenario-based (i.e. session-based) interaction specifications, where Reo is a channel-based coordination language. Although their tool (i.e. Reo circuit) is different from ours, both of us aim to systematically generate runtime monitoring mechanism (i.e. adaptors in their words) to inspect the behaviour of interactions. They argued about session types are for coping with heterogenous descriptions of component interfaces. By applying session types, an adaptor can be automatically generated from the adaptor specification (specified by session types), which establishes a correspondence between messages in different components. They also argued that the adaptor specification based on session types requires implementation details to achieve the correspondences among methods (and their parameters) of different components. Our responses are: (I) We aim to specify interactions and the contents of interaction messages among endpoints, but leave the private tasks, like how to deal with information at different locations, to the local endpoints. (II) Session types are thus useful to cope with runtime verification for the session-level interactions as unexpected runtime endpoint values are generated by endpoints. Our approach focuses on injecting specifications into external monitors, rather than automatically generating endpoint processes which obey specifications. Session-type-based specification gives
3. RELATED WORKS AND COMPARISONS

the freedom for endpoint programmers to design their own interfaces. Through run-
time verification of an external monitor, which is unattached to endpoints, as long as
daypoints’ behaviours obey what the specifications specified, endpoints and the overall
system obey the given global scenario.

3.3 Runtime Verification for Sharing Memory among Multiple Participants

How to specify specifications for multiple participants (e.g. multiple threads) to share
memory in one operation system or in one application, and how to verify the behaviours
of multiple participants to see if they obey the specifications, are important topics in
the area of specification and verification. In these topics, most works consider the
participants and their actions are in one common domain (e.g. one operation system),
which provides the ability for scheduling processes. Thus, when they consider runtime
verification for sharing memory, they are able to design synchronisation mechanism to
achieve data-race freedom. These works include (98, 138, 142), which aim to explore
and propose methods for synchronisation of asynchronous actions (e.g. multi-threads
in their cases). They are briefly described in the follows.

(98) proposed the algorithm for synchronising physical clocks, which should always
imply logical clocks. If one can resolve the problem of synchronising physical clocks at
different domains, then one can apply the similar idea to synchronise the events issued
by different local processes, which require, at least, the partial ordering. However, many
issues arise in practice as those discussed in (66, 91, 102, 114, 139). Even the physical
clocks at different domains can be practically synchronised, preserving the order of
messages (or the actions triggered by messages) costs the overall system inefficient
because the earlier-arrived but later-issued message needs to wait for the later-arrived
but earlier-issued message.

(142) proposed “Eraser” for detecting data races in lock-based synchronisation for
multi-threaded programs by checking that all shared-memory accesses follow a consis-
tent locking discipline. Eraser uses binary rewriting techniques to monitor every shared
memory reference and verify that consistent locking behaviour is observed. (138) fo-
cused on synchronisation for achieving linearisability and refinement to make the use of
sequential specifications for data structure operations.
However, synchronisation is not practical in large-scale distributed systems because no scheduler can schedule the events of processes in different independent/dependent domains at the same time. Thus we adopt a different way: Directly cope with the issues of asynchrony and concurrency in large-scale distributed systems, rather than designing synchronisation mechanism.

In Chapter 8 we address the issue of sharing memory among multiple heterogeneous parties and realisation of asynchronous monitoring in large-scale distributed systems. Due to the nature of asynchrony, the order of floating messages is not preserved, which implies that the order of actions, which are corresponding to these messages, is not preserved. Although our governance framework focuses on the safety of the session-level by regulating the interactions through runtime monitoring, we also consider the effects when the states of endpoints are specified in the specifications of monitors, which may make runtime monitoring ineffective due to the nature of asynchrony. When the states of endpoints are specified, sharing memory in sessions is stipulated. The formal syntax and semantics of stateful specifications and the theorems for asynchronous specifications are introduced in Chapter 8.

### 3.4 Dynamic Monitoring Frameworks

Works (73, 107) gave a brief view of dynamic monitoring or runtime monitoring. According to Havelund and Goldberg’s work (73), specification-based runtime verification consists of monitoring a program’s execution against a user-provided specification of intended program behaviour. In (107), Leucker and Schallhart defined runtime verification as the discipline of dealing with the detection of violations (or satisfactions) of correctness properties. They pointed out the use of runtime verification for contract enforcement.

Schneider in (143) introduced security automata for specifying exactly that class of security policies. It is a runtime monitoring mechanism for enforcing safety properties. (143) characterised that the set of executions for a security policy which is enforceable by security automata is a safety property. This work provided a general picture for runtime monitoring based on specifications or policies. As Deniénlou and Yoshida in (511) addressed, every well-formed global session type can be represented by a multi-party session automata (MSA), i.e. it implies that session types are enforceable.
3. RELATED WORKS AND COMPARISONS

The earliest mechanism of monitors are introduced in the 1972 U.S. Air Force report (11), which was based on the works of Lampson (104). Hoare in (78) invented the name monitor based on Brinch-Hansen and Dijkstra’s concept (58, 72) and defined it as a collection of local administrative data, together with some procedures and functions which are called by programs wishing to acquire and release resources. It targeted to avoid data races by using lock to realise monitor’s mutual exclusion, which means at each time, at most one thread may occupy a monitor.

The monitoring check proposed in (78) is for static-checking: Detecting data races during compile time through reasoning about the semantics of programs. (106) pointed out the limitations when people want to dynamically allocate shared variables. Dynamic monitoring is able to monitor such an environment where (I) a process (e.g. an object, which may allocate new variables) can be created; and (II) there is a monitor for every instance of an object. Each of these monitors shares the same code but has its own lock for process.

In summary, dynamic checking, compared to static checking, enjoys (I) dynamic verification making the whole system becomes scalable with the assurance of correctness even when untrusted components exist, and (II) the floating messages delivered during runtime have no chance to pollute local source code because evil messages have been blocked by a corresponding monitor.

3.4.1 Inlined Monitoring

In inlined monitoring, monitors run during runtime and exactly keep the status of monitored process and make the communication overhead significantly reduced. However, since the monitoring code is written in the code which should be protected by replacing the annotations containing specifications at every control point, an inlined monitor cannot detect the unexpected interruptions.

Since an inlined monitor positions at every local process, the interactions between an endpoint and its corresponding inlined monitor are synchronous; therefore, formalising the interactive behaviours among endpoint processes and the corresponding monitors and the external is not a challenge. The works for inlined monitors, such as (6, 71, 100), aimed to provide a policy specification language for policy written in monitors and certify the specifications generated by inlined monitors satisfy the original policy. However, inlined monitors may suffer from the code pollution of malicious endpoints and
become expensive especially when thousands of new and possibly untrusted participants are joining a large-scale distributed system every hour.

(6, 11) introduced a formalisation of monitoring and monitor inlining for the Java Virtual Machine. They specified monitor inlining correctness using annotations, which are based on Floyd’s work. Their monitors are security automata, as the one of Schneider’s. The monitoring code is embedded into the local code which need protection. They also analysed and specified the synchronisation check point.

Falcone et al. in (61) introduced a generic formalism for runtime enforcement based on the concepts of Hoare’s monitor and Schneider’s security automata for analysing properties. They studied the problem of enforcement relatively to the so-called Safety-Progress hierarchy of regular properties, which provides a finer-grained classification of enforceable properties. They showed how to generate an enforcement monitor in a systematic way. Although their goal is different from ours, they provided a good summary and explored the composition, synthesis, and enforcement abilities of monitors.

3.4.2 Outline Monitoring

Another spectrum of monitoring framework is outline (or offline) monitoring (37, 38, 107), in which monitors are external to application code. Outline monitoring implementation, which may work on a finite set of recorded executions, is decoupled from application code or execution. It represents a desirable feature in untrusted environments, and is commonly used for distributed infrastructures. Outline monitoring better supports decentralised monitor configuration.

Chen and Rosu in (37) introduced monitoring-oriented programming (MoP), a paradigm for combining formal specification with implementation. It provided an outline monitoring framework and light-weighted formal method to check conformance of implementation to specification at runtime. The monitoring code using the same target language for the implementation is automatically generated during a pre-compilation stage. The generated code has the same effect as a logical checking of requirements. In outline monitoring, the monitoring code is executed within a different process, potentially on an independent component (e.g. external monitor). This kind of monitoring allows one monitor to guard multiple endpoint processes. In (38), Chen and Rosu extended their previous work to allow the specifications have parameter, together with
an implementation of JavaMOP that supports parameters. With this extension, it can state and monitor safety properties referring to two or more related objects.

In the above works, since they are not designed to monitor interactive behaviours among endpoints, their formal syntax and semantics of specifications are directly written in past time linear temporal logic, thus logic experts, domain experts, requirement analysers, software designers and programmers are needed to cooperate for generating the monitoring code. On the contrary, session types represent the causal relations, the timing, the steps of taking actions of sending, receiving, and passing messages in a straightforward way, and at the same time, elegantly express the scenario which may be very difficult to be described in temporal logic. Our session-type based specifications can thus be used for generating monitoring code more easily and directly. As an implementation of our formal specifications, Scribble (145), a completely session-type-based description language, is developed to give program developers a clear and easy-to-read endpoint behaviour guidance.

Against to the shortage of inlined monitoring mentioned above, outline monitoring, positioning externally against to endpoint processes, can ideally provide economic and robust monitoring solutions. However, since this setting results in asynchronous interactions among local processes and external monitors, it is rather hard to capture and formalise the interactive behaviour, which is the key for designing effective specifications for monitors. One main contribution of this thesis is that we capture and formalise the asynchronous interactive behaviour for dynamic monitoring based on the outline monitoring setting.

3.4.3 Monitoring for Conversations

The main related works include (10, 148). The runtime monitoring of (148) is based on MSCs (message sequence charts). They adopted MSCs as their specification language to represent the global scenario, and transformed these diagrams to automata to enable conformance checking of finite execution traces against the specifications. Because their monitoring is based on MSCs, every action at endpoints is strictly ordered (i.e. total order), which means, when one endpoint, say $p$, is waiting for inputs from $q_1$ and $q_2$ which are specified as $p$ should firstly input $q_1$’s message then $q_2$’s even though the messages from $q_1$ and $q_2$ have no any causal relation, when $q_2$’s message arrives at $p$ earlier than $q_1$’s due to asynchrony, the monitor at $p$ needs to refuse $q_2$’s message. Our
monitoring is more advanced by having \textit{permutation} mechanism to make $p$’s monitor to accept $q_2$’s message if these two messages have no causality. One main contribution of their monitoring is that it ensures liveness for finitely terminating behaviours. But, note that, liveness property generally is not monitorable because interactive behaviours may not terminate.

(110) proposed dynamic monitoring framework based on MPSTs for MASs (multi-agent systems) to guard interactions between local agents and the environments. They gave a procedure for automatically deriving a self-monitoring MAS by the Jason agent oriented programming language to verify that a MAS implementation is compliant with a given \textit{global session type}, which can naturally be represented as cyclic Prolog terms. Another work of theirs (9) proposed global types, which are very similar to global session types for multi-party interactions for dynamic checking without projections.

Compared to ours, the similarity is for guarding interactions during runtime based on session types. But their monitoring is centralised and inlined while ours is completely distributed and outline; and therefore, their monitoring can only realise synchronous monitoring rather than asynchronous one. Most important, (110) focused on implementation of monitors, while we aim to establish a theoretical foundation for dynamic monitoring. The implementation of dynamic monitoring based on the theorems proposed in this thesis can be found in (39), contributed by Pierre-Malo Deniélou. Although (9) investigated the theorems for their framework, they do not have the theorems of local and global safety, local and global transparency, and session fidelity, which are contained and thoroughly proved in this thesis.

3.5 Governance

3.5.1 Service-oriented Architecture (SOA) Governance

Service-oriented Architecture (SOA) (92, 94) is a method of designing and managing systems which are characterised by coarse-grained services and service consumers. SOA governance is however too limited compared to large-scale distributed systems, such as OOI, because its ultimate governance goal is to deliver agility and objectives to businesses (41 111), and it is the governance mechanism particularly for an enterprise. In other words, it is for regulating processes in one single domain, which has consistent policies, typing rules, and governance goals: This domain may contain many sub-units,
3. RELATED WORKS AND COMPARISONS

e.g. an enterprise can have many departments, but all these sub-units follow common policies. Our current governance mechanism is general enough for formalising the automatic governance parts of SOA governance.

3.5.2 Law-governed Interactions

The series of works (119, 120, 121, 122, 123, 163), for law-governed interaction mechanism, which regards control/policy mechanism in distributed systems, gave a general picture and concept for governing interactions.

However, these works may not be able to capture the properties and theorems hidden behind the complex facts of interactions. Their formal model, called LGI (law-governed interaction), represented the static relations between laws and interactions: Defining law-governed interactions as those local interactions obeying global law. Their model did not deepen into the effects of concurrency and asynchrony of interactive behaviours which are the norm in distributed systems. They did not provide formalism based on process algebra to represent the dynamics of interactions among the local endpoints, their corresponding monitors, and the network.

Compared to these works, we represent the dynamic relations among endpoints, system monitors, and the network for runtime monitoring, and the formalisation of the dynamics of monitor’s specifications. We also explore the issues that, for some intuitive sensible specifications, asynchronous interactions will result them in becoming insensible, and we characterise the specifications which are proper for asynchronous environments.

3.6 Endpoint Access Control

The access of users to shared objects at endpoint is a basic operation in distributed systems. Though certainly many of the works are worth mentioning, one of the early clear statements on access control mechanisms and policies is found in Lampson’s (105), which introduced two notions, Protection Domain and Access Control Matrix (ACM). Protection Domain is the environment defining a set of objects (e.g. processes) and the types of operations that can be invoked on each object. An ACM is a matrix saying who can access which with what operations.
3.6 Endpoint Access Control

We do not provide formalism for detailed access control mechanism for the local, but we formalise a session-level endpoint capability control: We specify the capability of a role involving in a session, which is specified under a particular protocol defining the behaviours of session-roles (the roles in a specific session). Only the endpoint playing a particular session-role can output (resp. input) messages to (resp. from) other particular session-roles. The related works in this category include Lampson et al. (103) and Abadi et al. (2), safeDpi (75), typing system for a higher-order $\pi$ calculus (160), and the series of works of Klaim (46, 47, 48). The frameworks of (103) and (2), are based on logical approach, in which they introduced the logics in access control and the famous “say” authentication logic; while others are based on process algebraic approach as which this thesis adopts. Others provided formalism for access control by assigning types, i.e. capabilities, to located processes (according to (48, 160)) in distributed systems to express and enforce policies that control access to resources and data. In work (160), they proposed a typing system for a higher-order $\pi$-calculus. The typing system is used as an access control for an endpoint to judge the accessibility of processes for protecting local resources.

safeDpi (75), proposed by Hennessy et al., modelled filtering for migrating processes with channel dependent types. With the similar concept of processes migration, Ferrari et al. (63) proposed an ambient-based runtime monitoring formalism, called guardians, which aims for the rights of access control of network processes.

The series works of Klaim (46, 47, 48) advocated a hybrid (dynamic and static) approach to access-control against capabilities including resources and data: The aim is to provide a static checking that is integrated within a dynamic access-control procedure controlling data communication and processes migration. These works (46, 47, 48, 63, 75) also addressed access-control for mobility.

Other related works such as those of Dezani-Ciancaglini et al. (55, 56) provided a type system for the $Xd\pi$ calculus (67), proposed by Gardner and Maffeis, which is a calculus for describing a network of locations, each of which consists of data tree and processes. For a well-typed $Xd\pi$-network, every process properly controls its data (e.g. update or copy) and it can access the data at other locations only when whose security level is equal to or less than its security level.

Our work realises an endpoint capability control in every session by passing a session-role, denoted by $s[p]$, viewed as a capability, to every process participating in session.
3. RELATED WORKS AND COMPARISONS

$s$ to identify (i.e. a session identity plus a role) the endpoint process, and embed assertions \(22\) into monitors. This embeddedness of assertions enables external monitors to not only verify the interaction messages, but also check if the access requester has the capability (e.g. authority) to access the resource. In our governance framework, interactions in distributed systems are partitioned into sessions, thus is called session-based governance. Viewing inter-related interactions as one session unit enjoys governance benefits: (I) It reduces the tasks for endpoint access control. Originally an endpoint inlined monitor needs to check and authenticate thousands of input or output access permissions, with session-based outline monitoring, the session-level (i.e. interaction level) check firstly filters most ill-behaved input or output actions, then leaves those obeying global protocol but critical tasks, e.g. request to access confidential data, to endpoint static checking system. (II) Through passing capabilities, delegation and migration can be realised in our calculus.

In summary, compared to these works, our contributions are the formally founded enforcement of global invariants, such as global safety and session fidelity, and the proposal of decentralised session-level runtime monitoring for interactive behaviours among components written in possibly different programming languages. By incorporating protocols and conversations as two formally founded abstractions for programming and runtime, our framework offers formal assurance of clearly articulated properties for distributed applications.

3.7 The Related Calculi

3.7.1 The Spi-calculus

Abadi and Gordon in 1997 [3] introduced the Spi-calculus, an extension of the $\pi$-calculus designed for the description and analysis of cryptographic protocols by embedding encryption libraries into the $\pi$-calculus. They represented protocols as processes in the Spi-calculus: When all the processes are combined, a protocol is represented. They also stated the security properties in terms of coarse-grained notions of protocol equivalence.

We adopt the $\pi$-calculus and session types rather than the Spi-calculus is because we want to focus on governing conversations but leave the authentication tasks to each endpoint in different domains. Since in large-scale distributed systems, every domain may have their own authentication systems which are different from one to another,
applying the Spi-calculus would however hinder the flexibility we want to give to the endpoints, and may make our formalism and analysis become complicated. For example, when two endpoints in different domains interact, different domains may have different encryption libraries or different keys. Using the calculus with encryption and decryption primitives make us hard to describe and analyse the critical interactive behaviours among multiple participants.

Another reason is, to explore fundamental theories for governing conversations, the best way is to start from the original theories with the clearest form (e.g. the π-calculus and session types). This reason also applied for the following related calculus.

### 3.7.2 Policy for Sessions in the Ambient Calculus

The ambient calculus (33), introduced by Cardelli and Gordon in 1998, is a calculus for describing the mobility of concurrent processes. It introduced a paradigm of mobility where computational ambients are hierarchically structured. It describes where agents are connected to ambients and where ambients move under the control of agents. As a note in (110), the ambient calculus is a useful tool to construct mathematical models for security problems because of its facilities in expressing hierarchies of locations and their mobility.

Garralda et al. in (68) introduced BACI (Boxed Ambients with Communication Interfaces), an ambient calculus with flexible communication policies. BACI makes different communication policies with different parents during computation possible. Moreover, BACI makes communication and mobility become explicit by separating the channels of communication between ambients. Our work, to BACI, is for its session-level’s governance. It is a promising future work to integrate our session-based governance for conversations into BACI.
3. RELATED WORKS AND COMPARISONS
Assumptions and Terminologies

As the bases for the later chapters, the assumptions and terminologies of system participants and the communicating instances are introduced, and their relations are explained.

4.1 Principals, Processes, and Endpoints in Systems

Since the term “system participant” can be for any entity involving in systems, it is vague for representing entities with particular tasks. Therefore, more specific terms like principals, processes, endpoints are distinctly used here, and each of them is explained as follows:

1. Principals: A system consists of principals, which are system components involving in the system. The activities of principals include having interactions with other principals: With system’ agents, e.g. accessing data storage through a system agent, or dealing with system-level operations, e.g. scheduling, monitoring, updating policies for systems. In summary, a principal can be a user (e.g. a service contributor, a server, or a client, etc.), a system agent (e.g. a monitor or a database agent, etc.), or an electronic device, etc.

Since interactions among principals are the norm in large-scale distributed systems, principals should be abstracted to realise communications. A principal may have many names for different activities, but is identified with a unique identity
4. ASSUMPTIONS AND TERMINOLOGIES

such that (I) it has its own data storage, which may be positioned at the end-
point or at a shared database in the network; (II) it has pre-defined capability of
executing particular activities and communications; (III) it is viewed as local in
distributed systems. All of them can be referred to a unique principal with its
identity.

2. Processes: With standard definition of processes, a process is an instance of a
program of an application that is being executed. A process may interact with
other processes and have multiple threads for executing multiple tasks. A principal
can have more than one process running applications for it, while a process can
concurrently include more than one endpoint by having multiple threads. Since
we focus on the conversations (sessions) among applications, we generally assume
a process involving in sessions have interactions with other processes.

3. Endpoints: An endpoint process is for a local process, and an endpoint is for a
session participant, which is represented by a shared channel (name) linking con-
nections to it. Although many works use “endpoints” for “endpoint applications”,
in distributed systems, an application may concurrently run more than one system
component. In this thesis, an endpoint is abstractly represented by a shared name
with the assumption that a unique input-mode shared channel connects commu-
nications to it. A process can have more than one endpoint by having distinct
shared names. Thus, a process can execute more than one activity simultaneously
through different session endpoints.

Figure 4.1 illustrates the relationships between principals, processes, and endpoints,
which are connected by shared channels $a, b, c, d, e$ and $f$.

(i) There are Principals $A$ and $B$. A principal can have more than one process. In the
figure, Principal $A$ has an Application $A_a$, which has two processes Process $A_1$ and
$A_2$ running concurrently. Principal $B$ has two applications, which are Application
$B_a$ and $B_b$. Each of them has one process. Application $B_a$ has Process $B_1$, and
Application $B_b$ has Process $B_2$.

(ii) A process can have more than one endpoint. In the figure, Process $A_1$ uses three
endpoints, connected by shared names $a, b$ and $c$. These shared names represent
Figure 4.1: The Relationships between Principals, Processes, and Endpoints
4. ASSUMPTIONS AND TERMINOLOGIES

the endpoints. Process $A_2$ also uses these three endpoints but running separately in three concurrent threads. Process $B_1$ uses three endpoints $d$, $e$ and $f$ separately for running in three concurrent threads. Similarly, Process $B_2$ uses endpoints $e$ and $d$ separately for running two concurrent threads. Note that Process $A_2$ and $B_1$ are in one session where interactions are linked by endpoints $a$, $b$, $c$ of Process $A_2$, and $d$, $e$, $f$ of Process $B_1$.

(iii) An endpoint is represented by a shared name which realises a connection for this endpoint and represents the usage of this endpoint. For example, Principal $A$ has endpoints represented by names $a$, $b$, and $c$ for different activities in two different processes. $a$ in Process $A_1$ is used for running an activity, while $a$ in Process $A_2$ is used for participating in a session (to interact with Process $B_1$). Similarly, Principal $B$ has endpoints represented by names $d$, $e$ and $f$.

In summary, a system principal may run several network applications (executed by processes) concurrently, where each application can possibly have more than one proxy endpoint for communications. Those applications belong to the same principal identity.

4.2 Communications and Interactions

1. Communications: A “communication” is a piece of interactive behaviours in a session, which can be realised by a system component’s one-way activity to another system component, e.g. sending a message with particular content(s) to another system component, or receiving a message from another system component.

2. Interactions: An “interaction” is a pair of communications. It at least consists of two activities which are dual to each other among two system components communicating to each other. In other words, while a system component (as a sender) sends a message to another system component (as a receiver), the recipient always receives it (synchronously) or is going to receive it (asynchronously). Note that system components are local processes with multiple (session) endpoints.
4.3 Names, Sessions, Shared Channels, and Session-roles

1. Names: We use a name for a communication channel. In this thesis, we classify channels to two kinds: A session name and a shared name. Generally a session name is for identifying a session, but widely speaking, a session-role is also a kind of name for representing a session endpoint’s communication capability. A shared name is for a shared point. An input-mode shared name (introduced later) links connections to an endpoints.

2. Sessions: A session, also called a conversation, is a sequence of interactions. In our system, it is identified by a session name, and specified under a particular protocol, which can be represented by a session-type-based specification. A session links related interactions from pieces to a whole. One virtue of using session as a unit for formalising thousands of interactive behaviours among endpoints is that a session structures interactive behaviours and, based on this structure, provides a basis for analysing and verifying runtime behaviours. When a session name is created, a session with a new session identity is created in systems.

3. Shared names: A shared name denotes a shared channel, which is identified by a particular name. It abstractly represents a communication endpoint. It has three kinds: I is for input-mode, O is for output-mode, and IO is for both input- and output-modes. With the explanation of the definition of endpoints, a shared name with input-mode, a mode containing mode I, connects input communications to a unique session endpoint, thus, in this thesis, such a shared channel abstracts an endpoint. As a process has an endpoint connected by input-mode shared channel, this process listens to incoming messages through this channel but does not send out messages through it; as a process is connected by a shared name, say a, with output-mode O, we say this process uses channel a to send out messages to the process having common shared channel a but with mode I or IO. The relationship between I-, O-, and IO-mode shared names is illustrated in Figure 4.2. Note that, a shared name with mode I or IO represents an endpoint of a process; it locates this process and makes others be able to send messages (i.e. output messages) to it (i.e. input message from others). On the other hand, when a process has a shared name with mode of 0 or IO, the shared name represents a knowledge about where
4. **ASSUMPTIONS AND TERMINOLOGIES**

(i.e. to whom) it can output a message to the target receiver; this process itself is driven by other endpoints represented by other input-mode shared names. Note that, for flexibility, a shared name representing an endpoint can have both modes I and O, called IO-mode, denoting that this endpoint is able to communicate internally through itself. For example, the endpoint $b : IO$ in Figure 4.2 can output a message to itself. Also note that, an input-mode (i.e. I- or IO-mode) shared name locates an endpoint at a particular location (e.g. at a principal) in the network.

4. **Session-roles**: A session-role is played by an endpoint with the shared name that abstractly represents this endpoint. A session generally includes more than one endpoint, and a local process can participate in more than one session by having
4.4 More Illustrations for Shared Names

multiple endpoints in it. For example:

\[ P = s_1[buyer, seller]\langle 10 \rangle \mid s_2[trader, bank]?(x).P' \]

process \( P \) plays role \( buyer \) in session \( s_1 \) by an endpoint, say \( a \), and concurrently, plays role \( bank \) in session \( s_2 \) by another endpoint, say \( b \). Since a session is specified by a particular protocol, which defines roles playing in this protocol and confines the behaviours of roles for interactions, every role in a session is \textit{pre-defined}. A role in a session is generally called a \textit{session-role}. As an endpoint driven by a process \textit{involves} (i.e. joins) in a session, it plays one particular session-role connected by a shared channel.

4.4 More Illustrations for Shared Names

By the assumption, an I- or IO-mode shared name locates an endpoint and abstractly represents the endpoint. More illustrations below concretely explain how an input-mode shared name connects communications to an endpoint.

Figure 4.3 shows that a process can use an input-mode shared name to participate different activities, but can not use an \( O \)-mode shared name for this purpose. An \( O \)-mode shared name in a process is a knowledge telling the process where to output a message. In Figure 4.3

- Process \( A \) uses IO-mode shared name \( a \) to play role \( Bank \) specified under the protocol \( G_1 \) and has the knowledge of where to output to \( Bank \) specified under protocol \( G_2 \) by having \( c : 0(G_2[Bank]) \), and the knowledge about the \( Buyer \) specified under protocol \( G_3 \) by having \( b : 0(G_3[Buyer]) \). For convenience, we say Process \( A \)'s endpoint is represented by \( a \), or simply say its endpoint is \( a \). Note that, although shared names \( b \) and \( c \) also appear in Process \( A \), they are output-mode shared name and can not represent an endpoint process.

- Process \( B \) uses I-mode shared name \( b \) to play role \( Buyer \) specified under protocol \( G_3 \). As explained above, the \( O \)-mode shared name \( d \) for role \( Bank \) specified under protocol \( G_1 \) can not represent an endpoint in Process \( B \). Since Process \( A \) has \( O \)-mode shared name \( b \) with \( b : 0(G_3[Buyer]) \), Process \( B \) and \( A \) can communicate to each other through channel \( b \). Although Process \( A \) has IO-mode shared name \( a \) of
4. ASSUMPTIONS AND TERMINOLOGIES

Figure 4.3: Endpoints Represented by I-mode Shared Names in a Principal

playing role Bank specified under protocol $G_1$ and Process $B$ has 0-mode shared name $d$ of role Bank specified under the same protocol, they cannot interact with each other because they do not have a common shared name; in other words, they cannot be in one session.

- Process $C$ uses I-mode shared name $c$ to play role Bank specified under protocol $G_1$. Process $C$ also uses I-mode shared name $d$ to play role Bank specified under the same protocol. Thus Process $C$ has two endpoints represented by $c$ and $d$ respectively. Note that the same role specified under a common protocol can be played by different I-mode shared names. Also note that, Processes $C$ and $B$ have interactions through shared channel $d$, while Processes $C$ and $A$ cannot have interactions through $c$ because they are bound to different protocols.

The follows give the example of showing the relationships between an input-mode and an output-mode shared name. Assume an email server providing mailing service
4.4 More Illustrations for Shared Names

![Diagram illustrating communication between Buyer and Seller]

**Figure 4.4:** Using Shared Name to Represent Endpoints

can be abstracted by $a : \texttt{I}(G[\texttt{Server}])$, which denotes the server, playing role \texttt{Server}, specified under protocol $G$, is using shared name $a$ as an endpoint to input communications. When a client has a knowledge denoted by $a : \texttt{O}(G[\texttt{Server}])$, this client can send a request (output) to this server via channel $a$. Assume clients $C_1,\ldots,C_n$ have I-mode shared channels $c_1,\ldots,c_n$, e.g. $c_1 : \texttt{I}(G[\texttt{Client}]),\ldots,c_n : \texttt{I}(G[\texttt{Client}])$, playing role \texttt{Client} with mode I, specified under the common protocol $G$, to receive the server’s responses. A server can response to them because it knows “where the clients are” by having knowledge of $c_1 : \texttt{O}(G[\texttt{Client}]),\ldots,c_n : \texttt{O}(G[\texttt{Client}])$, with mode O under the matched protocol $G$.

Figure 4.4 illustrates another example where endpoint seller uses I-mode shared name $b$ to play role \texttt{Seller} in session 1 and session 2. For role \texttt{Seller}, channel $b$ is \textit{uni-direction}, which is used for inputting messages from the outside. The role \texttt{Buyer} in session 1 and the role \texttt{Buyer} in session 2 are run by different endpoints represented by different shared names: One is run by I-mode shared name $a$, another is run by
4. ASSUMPTIONS AND TERMINOLOGIES

I-mode shared name $c$. Both of them have $O$-mode shared name $b$, which means they both know where the Seller is. Similarly, in order to let the Seller know where they are, they provide their $O$-mode shared names $a$ and $c$ when they established sessions.

In the network, an $O$-mode shared name can appear in more than one principal, but an $I$- or $IO$-mode shared name can only appear in one principal. If we allow an $I$-mode shared name to appear in more than one principal, it makes the routers hard to route service requests to different principals who have common input-mode shared names but are located in different domains. Also, the security issue arises because the principals with common input-mode shared names are not specified and makes it hard to realise who should take responsibility when something goes wrong with a cooperative common task. If we want to describe that a common task can be done by more than one agent, this scenario can be realised by delegating the task to agents with different shared names (see Example 5.3.1). For simplicity, this thesis assumes that a shared name having mode $I$ or $IO$ can only appear in one principal in the network. More discussions about the design of $I$-, $O$-, or $IO$-mode shared name to cater for monitoring and routing purposes can be found in Appendix A.2.
The Capability-passing $\pi$-calculus

Overview  In this chapter, we introduce the formal syntax and semantics of the capability-passing $\pi$-calculus. It is a process calculus for dynamic governance for large-scale distributed systems, where basic interaction steps are asynchronous message exchanges, and interactions are concurrent. With the primitive nature of operations, the calculus leads to a clear monitoring mechanism, introduced in Chapter 7.

We start from Section 5.1 with a motivating example. In Section 5.2, we introduce a real-life use case from OOI, an under-construction large-scale distributed system, to show the expressiveness of the proposed calculus. The calculus is formally introduced in Sections 5.3 and 5.4. Section 5.3 provides the syntax and semantics for local processes; while Section 5.4 provides the syntax and semantics for the network. Local processes and the network together compose large-scale distributed systems that we target.

5.1 Motivating Example

The capability-passing $\pi$-calculus has fine-grained primitives for system entities to activate or deliver capabilities via a session in which they involve.

This calculus has two main concepts. One is viewing a type of session as a template so that participants can reuse it, e.g. participants can do tradings by establishing a Buyer-Seller-Broker type session where roles Buyer, Seller and Broker are defined and the interactions among those roles are described in such a session. A Buyer-Seller-Broker type session can be realised as a session that follows Buyer-Seller-Broker protocol.
session is a collection of structured interactions and the roles, generally called session-roles, involving in those interactions. Another concept is viewing a role defined in a session type as a capability. When a participant can play a session-role, he or she has the capability to execute the series of behaviours defined in this session.

These concepts come from the observation of activities of system entities in large-scale distributed systems, where the activities may be only available to some particular participants, e.g., when a user only registers himself/herself as a role Buyer, in some activities, he/she can only behave as a Buyer but not as a role Seller. As for an entity identified by a particular system ID, it should always be able to flexibly communicate with others through joining different session-roles concurrently, or delegating/delivering its capabilities to others for playing these session-roles.

A session-role arises as a basic syntactic entity in this calculus. The mechanism for playing different roles in different sessions concurrently makes system entities be able to flexibly and simply represent various forms of multi-party session establishment. Before
formally introducing the syntax and semantics of our calculus, we use Figure 5.1, a message sequence chart, to show that the benefits as a session can be established through asynchronously linking each session-role. Assume there are five system participants, who join a conversation, which involves activities among session-roles InfoAdmin, Broker, CollegeA, CollegeB and Institute. As Figure 5.1 illustrates, InfoAdmin is for information announcement, Broker is for delivering information from InfoAdmin to proper colleges, which are classified into two levels: CollegeA is for a level-A college, and CollegeB is for a level-B college. Broker will send InfoInstitute to InfoAdmin once it receives the message from InfoAdmin. Then InfoAdmin will send a message to Institute. The symbol ⊕ in the figure means alternative branches which are the choices at Broker: if the information is for CollegeA, Broker sends to CollegeA by selecting branch TypeA, and sends to CollegeB by selecting branch noTypeB with no content.

Assume, participants playing roles InfoAdmin, Broker and Institute are ready for interactions, but not participants of CollegeA and CollegeB, which means roles CollegeA and CollegeB have not yet been played by any participant. If a conversation can only be established through synchronously binding each session-role, then InfoAdmin, Broker and Institute cannot start their interactions (even if they are ready) because they are linked in a session and can only start when this session exists; however, this session does not exist if session-roles CollegeA and CollegeB are not ready. It makes participants playing InfoAdmin, Broker and Institute become idle and inefficient. On the contrary, if a session can be established through asynchronously linking session-roles one by one, then the interactions among InfoAdmin, Broker and Institute can set up to start interactions without waiting for participants of CollegeA and CollegeB getting online. The next section will use a real-life example represented by the formal syntax of the capability-passing π-calculus.

5.2 Use Case: OOI Instrument Commands

Examining real-life examples is useful for clarifying the requirements and providing a shape for the formalism. This section uses OOI instrument commands as a use case and applies the formal syntax of the capability-passing-π calculus (introduced in Section 5.3.1) to represent it.
5. THE CAPABILITY-PASSING $\pi$-CALCULUS

5.2.1 The Overview of OOI Instrument Commands

Consider a scientist, who registers in OOI, may wish to use a remote instrument, say a seabed camera which is realised following a specific application level protocol (i.e. global protocol). To simplify and generalise this scenario, assume the interactions are realised following the protocol, instrument commands, which is illustrated by Figure 5.2 as a message sequence chart. This protocol is specified as a global specification $G_{IC}$, which allows a user to perform operations on a remote instrument. $G_{IC}$ models a session which involves roles User, Register, Agent and Instrument. The formal syntax of global specification $G$ will be introduced in Chapter 6. Note that, as explained in Chapter 4, a session participant is a session endpoint, also called a session-role.

5.2.2 Specifying Protocols for Instrument Commands

In Figure 5.2, User performs one or more commands on a remote Instrument. Register is used to retrieve information on the instrument’s usage, e.g., to determine the maximum number of commands allowed in the current session depending on the system load. Agent interfaces the communications with the actual Instrument. Full arrows represent interactions where one party sends a branch label and a message content (or just one of the two) to another party. The labels carry information on the branch to follow. Arrows linked by $\oplus$ represent alternative branches.
5.2 Use Case: OOI Instrument Commands

The conversation proceeds as follows: (i) User sends Register a message \(\text{x}_{\text{int}}\) of type \text{InterfaceId}. (ii) Register replies with an integer \(\text{x}_n\) which determines the number of commands that User will be allowed to perform on the instrument. The predicate annotating this interaction specifies an obligation for Register to send a value for \(\text{x}_n\) satisfying \(\text{x}_n > 0\); dually User can rely on this fact. (iii) User sends Agent a priority \(\text{x}_p\) (e.g., \text{low}, \text{high}), and \(\text{x}_n\) that he or she received from Register. We assume that there is a public key inserted in \(\text{x}_n\) and Agent can verify if it is a correct value sent from Register. (iv) Agent sends User a label which is either \text{accept} or \text{reject}. In case of \text{reject}, Agent sends also an error message \(\text{x}_e\) of type \text{errData} and the protocol terminates. The predicate for this branch ensures that a request will not be rejected due to the fact that the instrument is busy if the priority is high. In case of \text{accept} the protocol continues with a recursion \(\mu(\text{x}_n)(\text{y} : \text{Int})\) where \(\text{y}\) is a parameter initialised to \(\text{x}_n\), \(\text{y} \geq 0\) is an invariant and \(\text{y}\) is used to enforce User to perform at most \(\text{x}_n\) commands on the instrument. (v) User selects either branch \text{more} and sends a new command to Agent, or \text{quit} and terminates. The predicate for this branch ensures that a request will not be rejected due to the fact that the instrument is busy if the priority is high. In case of \text{accept} the command (vi) or the \text{quit} notification (vii) are forwarded by Agent to Instrument. In the former case, Instrument responds to Agent (who forwards the message to User).

5.2.3 Asynchronous Session Creation for Instrument Commands

Based on the scenario described in Figure 5.2, an example of session creation of processes is illustrated with formal syntax. The form \(s[p]\), called session-role, means role \(p\) in session \(s\). For example, \(s[\text{User}], s[\text{Agent}], s[\text{Register}]\) are the session-roles representing roles User, Agent and Register in session \(s\) respectively.

Consider the following process \(P_1\) of \text{Principal}_1, which creates a session \(s\) with specification \(G_{IC}\) and sends invitations to others:

\[
\begin{align*}
P_1 &= P_{\text{NEWS}} \parallel P_{\text{INV}} \\
P_{\text{NEWS}} &= \overline{\alpha_2}(s[\text{Register}] : G_{IC}).\text{join}(s[\text{User}]).P_{\text{user}} \\
P_{\text{INV}} &= \overline{\alpha_3}(s[\text{Agent}] : G_{IC}); \overline{\alpha_4}(s[\text{Instrument}] : G_{IC})
\end{align*}
\]

where \(\overline{\alpha_2}(s[\text{Register}] : G_{IC}).\text{join}(s[\text{User}])\) represents that \(P_1\) creates session \(s\) which obeys to global protocol \(G_{IC}\), and will later join the role User defined in \(G_{IC}\); while
s[Register] : G_{IC} specifies that Register is defined in protocol G_{IC} and obeys this protocol. Similarly for s[Agent] : G_{IC} and s[Instrument] : G_{IC}. Their projections, e.g. G_{IC} ↾ Register, G_{IC} ↾ Agent, and G_{IC} ↾ Instrument are viewed as capabilities describing what activities and behaviours can/should have for these roles. The rules of endpoint projection are defined in Definition 6.5.1, Chapter 6.

Since P_1 is the initiator of session s, i.e. currently session s is known and only known by P_1, session s in P_{NEWS} and P_{INV} therefore appear. P_1 sends a bound request (i.e. bound invitation), \pi_2(s[Register] : G_{IC}), to endpoint (connected by) a_2 for playing session-role Register as the first session invitation, and joins the session as User by join(s[User]); she concurrently sends invitations to others through doing

\pi_3\{s[Agent] : G_{IC}\}; \pi_4\{s[Instrument] : G_{IC}\}.

Note that, only the first session invitation is bound, denoted with the shape \pi(s[p] : G) i.e. round bracket, because a session name, s, is newed simultaneously; the later invitations for the same session are free, denoted with the shape \pi(s[p] : G) i.e. angle bracket, because the session name s has been introduced in \pi_2(s[Register] : G_{IC}). Also note that, as \pi_2(s[Register] : G_{IC}) has been sent out (from P_1) to the network,

\pi_2(s[Register] : G_{IC}).join(s[User]).Puser | P_{INV} \xrightarrow{\pi(s[Register]; G_{IC})} (\nu s)(\nu s).Puser | P_{INV},

which means, as it informs the network that new session name s is created by doing \pi_2(s[Register]; G_{IC}), s is no more only known by P_1 but may be known globally; therefore, for this runtime process, now (\nu s) is needed to hide session s for private usage (i.e. s is only shared by those P_1 wants to invite). Principal_1 is inviting other four principals, Principal_2, Principal_3 and Principal_4. Shared channels, e.g. a_2, a_3, ..., determine which invitations each process is entitled to receive, e.g. only Principal_4 and Principal_5 below can accept (by any other process) an invitation s[Instrument], through a_4 and a_5, respectively. Note that, Principal_4, which receives the capability of s[Instrument],
passes this capability to Principal5 who joins this session to play role Instrument:

\[ P_2 = a_2(y_2[Register] : GIC).\text{join}(y_2[Register]).P_{\text{Register}} \]
\[ P_3 = a_3(y_3[Agent] : GIC).\text{join}(y_3[Agent]).P_{\text{Agent}} \]
\[ P_4 = a_4(y_4[Instrument] : GIC).\text{register}(y_4[Instrument] : GIC) \]
\[ P_5 = a_5(y_5[Instrument] : GIC).\text{join}(y_5[Instrument]).P_{\text{Instrument}} \]

With the design of the grammar, system can observe the exchange of capabilities between their endpoint and the network.

### 5.2.4 The Complete Formal Processes of Instrument Commands

We assume Principal1 uses some local functions needmore() (which determines if the user needs to perform more commands) and next() (which returns a command). Noticeably 0, generally omitted, denotes termination. \( \mu X(x_n)(y).P' \) is the recursion where \( X \) is the recursion body defined in \( P' \), and \( x_n \) is the initiation value and \( y \) is the parameter acting as a binder over \( P' \). In \( P_{\text{acc}}^u \), when \( x_n \) is replaced by 10 received from Register, \( y \) is replaced by the value of \( x_n \). If \( \text{needmore}() \cap y > 0 \) is true, the process executes to the recursion call \( X(y - 1) \), then \( X \) leads the process go back to the beginning of the recursion, where parameter \( x_n \) should be replaced by \( v \) if \( y - 1 \downarrow v \). Otherwise, the process executes \( s[\text{User, Agent}]!\text{quit}() \) then terminates.

\[ P_1 = (\overline{a_2}(s[Register] : GIC).\text{join}(s[User]).P_{\text{User}}) \mid P_{\text{INV}} \]
\[ P_{\text{INV}} = \overline{a_2}(s[Register] : GIC); \overline{a_3}(s[Agent] : GIC); \overline{a_4}(s[Instrument] : GIC); 0 \]
\[ P_{\text{User}} = s[User, Register]!!(v_{\text{inv}}); s[Register, User]?(x_n); s[User, Agent]!([\text{High}, x_n]; s[Agent, User]?{\text{accept}().P_{\text{acc}}^u, \text{reject}(x_e).0}) \]
\[ P_{\text{acc}}^u = \mu X(x_n)(y) \text{if needmore}() \land y > 0 \text{ then } s[User, Agent]!\text{more}(\text{next}()); s[Agent, User]?(x_r).X(y - 1) \text{ else } s[User, Agent]!\text{quit}(); 0 \]

It follows the process of Principal2 who defines channel \( a_2 \), receives an invitation and joins the session as Register. Assume Principal2 returns always 10 allowing all participants to perform at most 10 commands on the instrument.

\[ \text{new } a_2 : I(GIC[Register]).P_2 \]
5. THE CAPABILITY-PASSING $\pi$-CALCULUS

\[ P_2 = a_2(y_2[\text{Register}] : G_{IC}) \cdot \text{join}(y_2[\text{Register}]).P_{\text{register}} \]
\[ P_{\text{register}} = y_2[\text{User, Register}]?((x_{\text{init}}).y_2[\text{Register, User}]!!(10) ; \emptyset) \]

Below, Principal$_3$ defines channel $a_3$, receives an invitation and joins the session as Agent. Assume Principal$_3$ relies on a local function $\text{error}(\cdot)$ returning an error data. The agent simply forwards the command and the response between the user and the instrument.

\[ \text{new } a_3 : I(G_{IC}[\text{Agent}]).P_3 \]
\[ P_3 = a_3(y_3[\text{Agent}] : G_{IC}) \cdot \text{join}(y_3[\text{Agent}]).P_{\text{agent}} \]
\[ P_{\text{agent}} = y_3[\text{User, Agent}]?((x_p, x_n) . \text{if } x_p = \text{High then } y_3[\text{Agent, User}]!\text{accept}() ; P_{\text{acc}}^a \]
\[ \text{else } y_3[\text{Agent, User}]!\text{reject}() ; \emptyset) \]
\[ P_{\text{acc}}^a = \mu X. (x_n)[\emptyset].y_3[\text{User, Agent}]?\{\text{more}(x_{\text{com}}).P_{\text{com}} \}
\]
\[ \text{quit}().y_3[\text{Agent, Instrument}]!\text{quit}() ; \emptyset \}
\[ P_{\text{com}}^a = y_3[\text{Agent, Instrument}]!\text{more}(x_{\text{com}}) ; y_3[\text{Instrument, Agent}]?((y_r).y_3[\text{Agent, User}]!\langle y_r \rangle ; X(y - 1) \}

Below, Principal$_4$ and Principal$_5$ define shared channels through which they receive an invitation for role Instrument. Principal$_4$ forwards the invitation to Principal$_5$ and terminates. Principal$_5$ joins the session and recursively listening to the message sent from agent. The recursion $\mu X. P''$ means there is no parameter or binder over the recursion body $X$ defined in $P''$, so noticeably there is no parameter of $X$. If branch more is selected, the process (playing instrument) returns response($y_{\text{com}}$) to Agent by relying on a local function response, and then go back to the beginning of the recursion body. Otherwise, it terminates.

\[ \text{new } a_4 : I(G_{IC}[\text{Instrument}]).P_4 \]
\[ \text{new } a_5 : I(G_{IC}[\text{Instrument}]).P_5 \]
\[ P_4 = a_4(y_4[\text{Instrument}] : G_{IC}) \cdot \pi y_4[\text{Instrument}] : G_{IC} ; \emptyset \]
\[ P_5 = a_5(y_5[\text{Instrument}] : G_{IC}) \cdot \text{join}(y_5[\text{Instrument}]).P_{\text{inst}} \]
\[ P_{\text{inst}} = \mu X. y_5[\text{Agent, Instrument}]?\{ \]
\[ \text{more}(y_{\text{com}}).y_5[\text{Instrument, Agent}]!\langle \text{response}(y_{\text{com}}) \rangle ; X, \]
\[ \text{quit}().\emptyset \}\]

5.3 The Calculus of Local Processes

This section introduces the syntax and semantics of the capability-passing $\pi$-calculus for local processes with distributed session primitives. As shown in Section 5.2, the fine-grained scheme calculus is expressive to represent real-world examples, including
5.3 The Calculus of Local Processes

those in \(35\). As synchronous process calculi can not fully identify the properties in distributed systems because the assumptions of synchronous interactions are:

1. A message can be outputted only when its input side (a receiver is ready to receive this outputted message) exists; and

2. An output can be immediately absorbed by the input side, which makes the order of messages floating around networks preserved,

this thesis focuses on the processes in asynchronous environment, which reflects the reality of distributed systems. Note that, considering the interactions between processes are synchronous or asynchronous becomes critical as we consider stipulating states, i.e. the current value of a specific field of an endpoint, in specifications. This issue will be explored in Chapter 8.

5.3.1 The Syntax of Local Processes

The capability-passing \(\pi\)-calculus is defined in Figure 5.3. Let \((P,Q,\ldots)\) denote process variables. Session names are identified by \((k,k',\ldots)\), which represent both session instances and session variables. Shared names are identified by \((u,u',\ldots)\), which represent both shared channels and shared channel variables. Let \((p,q,\ldots)\) range over roles involving in a session, and \((x,y,\ldots)\) range over variables; \((v,v',\ldots)\) range over values, including shared name with I/O type, a boolean, or a constant \(c\). A constant can be a number, a name, an alphabet, or a string; \((e,e',\ldots)\) are for expressions, while \((S,S',\ldots)\) are for sorts, representing data types of expressions. \((U,U',\ldots)\) is a kind of sorts, particularly for representing how a local process is able to use a shared name. Interaction variables are those variables that are exchanged in interactions. There are three modes for shared name: \(I\) for input only, \(O\) for output only, and \(IO\) for both input and output.

Rule \([P\text{-n creation}]\) says a process, with primitive \(\text{new } a : \text{im}(G[p])\), creates a fresh input-mode shared name \(a\) in \(P\). Through \(a\), an endpoint can play role \(p\) specified under global protocol \(G\). When there are runtime monitors, the fresh name with input-mode should be ensured to be new to the systems. A shared name with mode \(O\) can not be created by a process but be propagated from one endpoint process having the common shared name with input-mode to another process. For example, assume there exists
5. THE CAPABILITY-PASSING $\pi$-CALCULUS

A process having shared name $a$ with type $\mathbb{I}(G[p])$. This process can propagate this name by sending it to other processes; but as others receive it, it should be typed by $\mathbb{O}(G[p])$ at these processes. Again, this can be ensured when there are runtime monitors.

When a process creates a new shared name with mode $\mathbb{I}$ or $\mathbb{O}$, it is treated as a bound (hidden) name with the scope including herself and other participants having $a$ with mode $\mathbb{O}$.

The primitives $\mathbb{u}(s[p] : G)$ and $\mathbb{u}(s[p] : G)$, $u(y[p] : G)$ and $u(y[p] : G)$, embedding specification $G$, make the control of session creation possible. The actions of bound request and accept with round bracket introduces a new session to the local process. For example, when $P_1 = a(s[p] : G).P'_1$, $P_1$ creates a fresh name $s$ and simultaneously invites endpoint $a$ for playing role $p$. $\mathbb{u}(s[p] : G)$ introduces new session $s$ to $P'_1$ and $s$ acts as a binder over $P'_1$. Similarly, when $P_2 = a(s[p] : G).P'_2$, session $s$, which is new to $P'_2$, is created and simultaneously $P_2$ accepts the invitation for playing role $p$ in session $s$. The actions of free request and accept with angle bracket mean that $s$ is not fresh to the processes. As the example shown in Section 5.2 only the first request and accept are bound.

$s[p]$ is viewed as a capability of having behaviours of playing role $p$ specified under global specification $G$. Either $u(y[p] : G).P$ or $u(y[p] : G); P$ shows an endpoint has the capability of playing role $p$ specified under $G$ and then behaves as $P$. A special message invitation, denoted by $\mathbb{u}(k[p] : G)$ without “;” attached after it, is either with a local process in parallel, e.g. $P \mid \mathbb{u}(s[p] : G)$ or floating around the network in the global queue (introduced in Section 5.4), e.g. $H \cdot \mathbb{u}(s[p] : G)$. Note that, an invitation is different from an interaction message, which queues in either local or global queue; an invitation only queues in the global queue. Invitations are delivered by applying rules $[P\rightarrow \text{request b/f}]$ or $[P\rightarrow \text{accept b/f}]$ along shared channels $(u,u', \ldots)$. When an invitation is sent out from a local process, it implies that the local process takes action of free/bound request; while an invitation enters a local process, it implies the local process takes action of free/bound accept.

As mentioned above, $[P\rightarrow \text{accept b/f}]$ do not mean a process has joined a session-role. An endpoint uses $[P\rightarrow \text{join}]$ to claim to join a session-role in a particular session. This syntax together with $[P\rightarrow \text{request b/f}]$ and $[P\rightarrow \text{accept b/f}]$ give the calculus the flexibility for realising delegation.
5.3 The Calculus of Local Processes

\[ u ::= a,b \mid x,y \]  
\[ k ::= s,s' \mid x,y \]  
\[ v ::= a \mid true \mid false \mid c \]  
\[ e ::= v \mid x \mid e + e' \mid e \cap e' \mid \neg e \cdots \]  
\[ S ::= int \mid string \mid bool \mid G \mid T \mid U \]  
\[ U ::= mode(T[p]) \]  
\[ im ::= I \mid IO \]  
\[ mode ::= im \mid 0 \]  
\[ P ::= new a : im(G[p]).P \mid \pi(k[p] : G).P \mid \pi(k[p] : G); P \mid u(y[p] : G).P \mid u(y[p] : G); P \mid join(s[p]).P \mid if e then P else Q \mid k[p,q]!l(e); P \mid k[p_1,p_2]?\{l_i(x_i).P_i\}_{i \in I} \mid P \mid Q \mid P_{rt} \mid 0 \mid \mu X(e)(x).P \mid X(e) \mid P_{rt} \]  
\[ P_{rt} ::= (\nu s)P \mid (\nu a)P \]  
\[ h ::= \emptyset \mid m \cdot h \]  
\[ m ::= s(p,q,l(v)) \mid \pi(s[p] : G) \]  

Figure 5.3: The Syntax of Local Processes
Example 5.3.1 (accept, join, and delegation). Assume there is a web-service, who is able to play role Server in session \( s \) guided by protocol \( G \). Assume the server needs to deal with many requests from clients concurrently, the server thus delegates these tasks to the trusted agents, i.e. its deputies, who can as well play role Server in protocol \( G \). Assume process \( P_{server} \) has a list of the shared names of the trusted agents. Let \( agent \) be the variable of shared name of the trusted agent. Let \( P'_{server} \) be

\[
P'_{server} = \mu X(\langle agent \rangle(u).\text{if } agent \neq \emptyset \text{ then } a(y[Server] : G).\pi(y[Server] : G); X(\text{selectAgent()} ) \text{ else } 0 \text{ recursively accepts a new session, say } s, \text{ to replace } y \text{ and then delegates session-role } s[Server] \text{ to agent } agent, \text{ which is private to } P_{server}, \text{ by replacing } u \text{ with } agent. \text{ A process } P' \text{ may be in parallel with the recursion for assigning an initial value of } agent \text{ to the recursion. Also, function selectAgent() selects an agent from the list, then put the selected one into the recursive body. We can specify the recursion ends when } X(\emptyset).
\]

Every process for an agent should have the shape

\[
P_{agent} = agent(y'[Server] : G).Join(y'[Server]).P''
\]

which says that endpoint \( agent \) will join session-role \( Server \) specified under \( G \), by applying \( \text{join}(y'[Server]) \), when such an invitation happens.

Definition 5.3.2 (the set of indexes). Define \( I \) as the set of indexes.

\[
\begin{align*}
[P - \text{selection}] \text{ and } [P - \text{branching}] \text{ are for session interactions}, \text{ which are communications through an established session } k. \text{ We make the sender } p_1 \text{ and receiver } p_2 \text{ in session } k \text{ explicit by the notation } k[p_1, p_2]. \text{ } [P - \text{selection}] \text{ defines a process involving in session } k \text{ for sending value } v \text{ with chosen label } l \text{ from } p_1 \text{ to } p_2. \text{ Dually, } [P - \text{branching}] \text{ defines a process ready to receive whatever label } l_i, i \in I = \{1, ..., n\} \text{ has been chosen and behaves as } P_j\{v/x_j\} \text{ after replacing every } x_j \text{ in } P_j \text{ with } v \text{ if label } l_j \text{ has been chosen}. \text{ For brevity, write } k[p_1, p_2]?l(x).P \text{ or } k[p_1, p_2]?(x).P \text{ for a single branch, and omit trailing } 0. \text{ Conditional, parallel composition and inaction are standard. The recursion } \mu X(e)(x).P \text{ defines a recursion where } X \text{ is the recursion body defined in } P \text{ with parameter } x \text{ which is initiated to } e. X(e) \text{ is the corresponding recursion call.}
\end{align*}
\]

Some arguments arise from the necessity of embedding protocol \( G \) in the process calculus. The reasons are as follows: (I) Ensuring deadlock-free of processes in a session since behaviours are safely guided by the specifications, and (II) providing system the information about the structure that a session obeys. Without knowing to which protocol a session obeys, system can hardly guard/monitor the interactions in this session.
5.3 The Calculus of Local Processes

Once a session is created, the runtime syntax \( P_{rt} \) (not accessible to programmers) is used. To model the asynchronous interactions between a local process and its external monitor during runtime, a local queue, \( s[p] : h \), created when \( \text{join}(s[p]) \) takes place and designed particularly for the endpoint playing session-role \( s[p] \), is used as a bridge between them to buffer incoming (resp. outgoing) messages for which the endpoint is going to receive from (resp. send to) the network. Although the global queue (defined in Section 5.4) can realise the asynchronous interactions among processes, it is not enough for realising the ones between a process and its external monitor. Through buffering, a monitor can efficiently guard the incoming (to the local processes) and outgoing (to the network) messages for more than one endpoint.

The set of bound names in \( P \) is denoted by \( \text{bn}(P) \), the set of free names in \( P \) is denoted by \( \text{fn}(P) \), and the set of names in \( P \) is denoted by \( \text{n}(P) \). We view a session-role, say \( k[p] \), as a composite of a session name and a role. Note that, a role \( p \), specified under a global protocol, represents a pre-defined capability of an endpoint; therefore, it is not a name but is there for pattern-matching of capability. Below we illustrate the set of names, bound names, and free names of each process:

**Definition 5.3.3 (the set of names, free/bound names of a process).** \( \bigcup \) is standard union set operation in set theory.

1. For \( P = \overline{\alpha}(k[p] : G) ; P' \), \( \text{n}(P) = \{a, k\} \cup \text{n}(P') \), \( \text{fn}(P) = \{a\} \cup \text{fn}(P') \), and \( \text{bn}(P) = \{k\} \cup \text{bn}(P') \).

2. For \( P = \overline{\alpha}(k[p] : G) ; P' \), \( \text{n}(P) = \{a, k\} \cup \text{n}(P') \), \( \text{fn}(P) = \{a, k\} \cup \text{fn}(P') \), and \( \text{bn}(P) = \text{bn}(P') \).

3. For \( P = a(k[p] : G) . P' \), \( \text{n}(P) = \{a, k\} \cup \text{n}(P') \), \( \text{fn}(P) = \{a\} \cup \text{fn}(P') \), and \( \text{bn}(P) = \{k\} \cup \text{bn}(P') \).

4. For \( P = a(k[p] : G) . P' \), \( \text{n}(P) = \{a, k\} \cup \text{n}(P') \), \( \text{fn}(P) = \{a, k\} \cup \text{fn}(P') \), and \( \text{bn}(P) = \text{bn}(P') \).

5. For \( P = k[p, q]!l(e) ; P' \), \( \text{n}(P) = \{k\} \cup \text{n}(e) \cup \text{n}(P') \), \( \text{fn}(P) = \{k\} \cup \text{n}(e) \cup \text{fn}(P') \), and \( \text{bn}(P) = \text{bn}(P') \).

6. For \( P = k[p, q]?(x) . P' \), \( \text{n}(P) = \{k, x\} \cup \text{n}(P') \), \( \text{fn}(P) = \{k\} \cup \text{fn}(P') \), and \( \text{bn}(P) = \text{n}(x) \cup \text{bn}(P') \).
5. THE CAPABILITY-PASSING π-CALCULUS

7. For \( P = \text{new } a : \text{im}(G[p]).P' \), \( n(P) = \{a\} \cup n(P') \), \( \text{fn}(P) = \text{fn}(P') \), and \( \text{bn}(P) = \{a\} \cup \text{bn}(P') \).

8. For \( P = \text{join}(k[p]).P' \), \( n(P) = \{k\} \cup n(P') \), \( \text{fn}(P) = \text{fn}(P') \), and \( \text{bn}(P) = \{k\} \cup \text{bn}(P') \).

9. For other processes, the names and free/bound names of them are standard.

Convention 5.3.4 (Barendregt convention). In every process (and in every sequence of actions), bound names are different from each other and different from free names.

Convention 5.3.5. We call a process initial when a process does not contain any free variable and a runtime syntax. An initial process is thus always closed because it has no free variables.

5.3.2 The Structural Congruence of Local Processes

For convenience, we define the prefix of a process as two kinds:

Definition 5.3.6. Define two kinds of prefixes as follows:

\[
\begin{align*}
\alpha_1 & ::= \pi(k[p]:G) \mid u(k[p]:G) \mid k[p_1,p_2]?l(x) \mid \text{join}(s[p]) \mid \text{new } a : \text{im}(G[p]) \\
\alpha_2 & ::= \pi(k[p]:G) \mid u(k[p]:G) \mid k[p_1,p_2]!l(e)
\end{align*}
\]

Definition 5.3.7 (the laws of congruence). Let \( \mathcal{R} \) be an equivalence relation over process. Then \( \mathcal{R} \) is said to be a congruence relation

- if it is preserved by all elementary contexts over open process; that is, if \( P_1 \mathcal{R} P_2 \), then

\[
\begin{align*}
\alpha_1.P_1 & \mathcal{R} \alpha_1.P_2 \\
\alpha_2;P_1 & \mathcal{R} \alpha_2;P_2 \\
P_1 \mid Q & \mathcal{R} P_2 \mid Q \\
Q \mid P_1 & \mathcal{R} Q \mid P_2 \\
(\nu n)P_1 & \mathcal{R} (\nu n)P_2
\end{align*}
\]

- and, if \( P \mathcal{R} Q \), then \( \forall x,v, P\{v/x\} \mathcal{R} Q\{v/x\} \).

Definition 5.3.8 (processes structural congruence). The structural congruence is the smallest binary relation \( \equiv \), which
1. is a congruence, i.e. abides to the law defined in Definition 5.3.7 and

2. satisfies the following axioms

1. \( P \equiv Q \) whenever \( P \) is an alpha-conversion of \( Q \).

2. \( P | 0 \equiv P \), \( P_1 | P_2 \equiv P_2 | P_1 \), \( (P_2 | P_3) \equiv (P_1 | P_2) | P_3 \).

3. \((\nu n)(P_1 | P_2) \equiv P_1 | (\nu n)P_2 \) if \( n \notin \text{fn}(P_1) \), \((\nu n)P_1 | (\nu n)P_2 \equiv (\nu n)(P_1 | P_2) \).

4. \((\nu n)0 \equiv 0 \).

5. \( s[p] : h \cdot s\langle p, p_1, l\langle v \rangle \rangle \cdot s\langle p_2, p, l'(v') \rangle \cdot h' \equiv s[p] : h \cdot s\langle p_2, p, l'(v') \rangle \cdot s\langle p_1, p, l(v) \rangle \cdot h' \) if \( p_1 \neq p_2 \).

6. \( s[p] : h \cdot s\langle p, p_1, l\langle v \rangle \rangle \cdot s\langle p, p_2, l'(v') \rangle \cdot h' \equiv s[p] : h \cdot s\langle p, p_2, l'(v') \rangle \cdot s\langle p, p_1, l(v) \rangle \cdot h' \) if \( p_1 \neq p_2 \).

In the definition of structural congruence, besides the standard rules defined in Definition 5.3.7, Rules 5 and 6 are the rules for rearranging messages. Rule 5 says that, when two messages are received from different senders, these two messages can be permuted; while rule 6 says that, when two messages are going to send to different receivers, these two messages can be permuted.

5.3.3 The Semantics of Local Processes

In this section, we introduced the labelled transition system (LTS) and reductions rules (the \( \tau \) rules in LTS) of local asynchronous processes. Equation 5.1 is the full version of action labels. The LTS includes the following action labels, which are also used in Chapters 7 and 8. Labels consist of \( \tau \)-action (i.e. \( \tau \)), session bound/free request and accept (i.e. \( \pi(s[p] : G) / \pi(s[p] : G) \), \( a(s[p] : G) / a(s[p] : G) \)), shared channel creation \( \text{new} \ a : \text{im}(G[p]) \), join session-role \( s[p] \) and two actions for session interactions: selection and branching (i.e. \( s[p_1, p_2]!l(x) \), \( s[p_1, p_2]?l(x) \)). Request and selection (resp. accept and branching) are often collectively called output (resp. input). Note, when a process announces to join a session-role \( s[p] \) through a join label, only at this moment, the session-role becomes active and the local queue \( s[p] : \emptyset \) is generated.

In Chapters 8 the action labels will be simplified by taking off \( \text{join}(s[p]) \) and \( \text{new} \ a : \text{im}(G[p]) \) to only focus on session interaction actions.
5. THE CAPABILITY-PASSING $\pi$-CALCULUS

$$
\ell \ ::= \ \tau \mid a(s[p] : G) \mid a(s[p] : G) \mid a(s[p] : G) \mid \text{new } a : \text{im}(G[p]) \\
\mid \text{join}(s[p]) \mid s[p_1, p_2]|_{u} \mid s[p_1, p_2]|_{u}(v)
$$

(5.1)

Below we illustrate the set of names, bound names, and free names of each action:

**Definition 5.3.9 (the set of names, free/bound names of an action).** $\cup$ is standard union set operation in set theory.

1. For $\ell = \pi(k[p] : G)$, $n(\ell) = \{a, k\}$, $fn(\ell) = \{a\}$, and $bn(\ell) = \{k\}$.
2. For $\ell = k[p] : G$, $n(\ell) = \{a, k\}$, $fn(\ell) = \{a, k\}$, and $bn(\ell) = \emptyset$.
3. For $\ell = a(k[p] : G)$, $n(\ell) = \{a, k\}$, $fn(\ell) = \{a\}$, and $bn(\ell) = \{k\}$.
4. For $\ell = k[p] : G$, $n(\ell) = \{a, k\}$, $fn(\ell) = \{a, k\}$, and $bn(\ell) = \emptyset$.
5. For $\ell = k[p, q]|_{l}(e)'$, $n(\ell) = \{k\} \cup n(e)$, $fn(\ell) = \{k\} \cup n(e)$, and $bn(\ell) = \emptyset$.
6. For $\ell = k[p, q]|_{l}(x)$, $n(\ell) = \{k, x\}$, $fn(\ell) = \{k\}$, and $bn(\ell) = n(x)$.
7. For $\ell = \text{new } a : \text{im}(G[p])$, $n(\ell) = \{a\}$, $fn(\ell) = \emptyset$, and $bn(\ell) = \{a\}$.
8. For $\ell = \text{join}(k[p])$, $n(\ell) = \{k\}$, $fn(\ell) = \emptyset$, and $bn(\ell) = \{k\}$.

Note that, according to Convention [5.3.4] (i.e. Barendregt convention), in every sequence of actions, bound names are different from each other and different from free names.

**Example 5.3.10.** Consider a sequence of actions:

$$
\ell_1 \cdot \ell_2 \cdot \ell_3 \cdot \ell_4 = a(k[p] : G) \cdot k[p, q]|_{l}(v) \cdot a(k[q] : G) \cdot k[q, r]|_{l'}(v')
$$

It is wrong because it does not follow Barendregt convention as $a(k[p] : G)$ and $a(k[q] : G)$ have common bound name $k$. It should be revised to:

$$
\ell_1 \cdot \ell_2 \cdot \ell_3 \cdot \ell_4 = a(k[p] : G) \cdot k[p, q]|_{l}(v) \cdot a(k[q] : G) \cdot k'[q, r]|_{l'}(v')
$$

Then we have $\ell_1$ binds $\ell_2$ and $\ell_3$ binds $\ell_4$.

**Definition 5.3.11 (subject of an action).** Define $\text{sbj}(\ell)$ as the subject of $\ell$:
1. If it is an action for session interaction, its subject is the endpoint, represented by a session-role, who fires the action. For example, \( \text{sbj}(s[p, q]!l(v)) = s[p] \) and \( \text{sbj}(s[p, q]?l(v)) = s[q] \).

2. If it is an action for request or accept, its subject is the initial shared name. For example, \( \text{sbj}(a(s[p] : G)) = \text{sbj}(a(s[p] : G)) = a \) and \( \text{sbj}(a(s[p] : G)) = \text{sbj}(a(s[p] : G)) = a \).

3. \( \text{sbj}(\tau) = \emptyset \).

4. Others are not defined.

The definition of subject of actions for session interaction is an abstraction of the viewpoint of a local process who takes the action. Thus, for action \( s[p, q]!l(v) \), the endpoint that takes this action is the process playing the session-role \( s[p] \); similarly, for action \( s[p, q]?l(v) \), the endpoint takes this action is the process playing the session-role \( s[q] \). For request and accept actions, \( a \), as a shared point, fires the action; while \( s[p] \) in a request or an accept is not counted as a subject because it is for pattern-matching of capability, and this pattern-matching check is only done when the content is delivered to the endpoint.

**Definition 5.3.12.** The evaluation of an expression, denoted by \( e \downarrow v \), is always possible whenever the initial process is closed and the logic of the boolean expressions is decidable.

Figure 5.4 lists the LTS rules of local processes, including the \( \tau \) action. Each output is performed in two steps: (I) a local action spawns the message (i.e. invitations remain local and interaction messages are inserted in a local queue, say \( s[p] \)) and (II) a visible action sends out the message. Inputs are dual. For the first five rules, the output and input at local endpoints are globally invisible: \( [\text{Arq } f, \text{Aac } b/f] \) respectively spawn and receive an invitation along a shared name. \( [\text{Sel}] \) puts a message in a local queue, after evaluating \( v \) from expression \( e \); dually, \( [\text{Bra}] \) gets a message from a local queue with label \( l_j \), so that the \( j \)-th process \( P_j \) receives value \( v \) and becomes \( P_j \{v/x_j\} \) after replacing every \( x_j \) in \( P \) with \( v \). \( [\text{Iv}] \) is standard. The rest models actions which can be observed globally: \( [\text{New}] \) is for shared name creation. Through this action, the monitor learns this freshly created shared name is able to play role \( p \) with behaviour defined in protocol \( G \). Note that, there are two ways for a process to get a shared name: (I) One
is when it creates a new name by applying rule \([\text{New}]\). This process always hides the shared name and makes it private. (II) Another is, without loss of generality, a process announces the shared name it knows to the public so that other processes can access this name by having the 0-mode common shared name.

\([\text{Join}]\) is for an endpoint to join a session by activating capability \(s[p]\) and creating the corresponding local queue. \([\text{REQ-OUT} B/F]\) sends out an invitation, its duality \([\text{ACC-IN} B/F]\) receives an invitation from the outside. Note that \([\text{REQ-OUT} B]\) (resp. \([\text{ACC-IN} B]\)) simultaneously creates the session \(s\) and requests (resp. accepts) the session role \(s[p_j]\) at the endpoint represented by the shared name \(a\). \([\text{SEL-OUT}]\) (resp. \([\text{BRA-IN}]\)) sends (resp. receives) a message from (resp. into) its local queue. Rules \([\text{RES}], [\text{PAR}],\) and \([\text{STR}]\) are standard according to (II).

5.4 The Calculus of the Network

In this section, this thesis introduces the formalism, including syntax and semantics, for the network, which can be an un-monitored, monitored, or a mixed network, where processes asynchronously interact with each other. The calculus considers both the aspects of the marginal and the global of the network.

5.4.1 The Syntax of the Network

The syntax of the network is given in Figure 5.5, where every notation, representing a network component, is separated by “\(|\)”.

A process may have more than one endpoint. During runtime, these endpoints are driven by this process. A process \(P\), residing locally, is a part of the network. “\(|\)” is used to represent that each network component exists in parallel. Let \(N_s\) denote the static network, which does not include the global queue; and let \(N\) denote the dynamic network which contains all components (including local processes and the global queue with messages).

**Definition 5.4.1.** Let \(\text{ep}(N)\) be the set of endpoints residing in \(N\). As \(N = P\), \(\text{ep}(P)\) is the set of endpoints in process \(P\).

**Definition 5.4.2 (network composability).** Two networks \(N_1 \overset{\text{def}}{=} N_{s1} \parallel H_1\) and \(N_2 \overset{\text{def}}{=} N_{s2} \parallel H_2\) are composable if and only if
5.4 The Calculus of the Network

The Labelled Transition System of Figure 5.4:

\[ H ::= m \mid N \]  
\[ N ::= \emptyset \mid m \cdot H \]  
\[ m ::= s(p, q, l(v)) \mid \overline{\pi}(s[p] : G) \]

\[ \pi(s[p] : G) \mid a(y[p] : G).Q \xrightarrow{r} Q\{s/y\} \]  
\[ \pi(s[p] : G) \mid a(s[p] : G); Q \xrightarrow{r} Q \]

\[ s[p, q] l(c); P \mid s[p_1]; h \xrightarrow{r} P \mid s[p_1]; h \cdot s[p_1, p_2, l(v)] \]  
\[ s[p_1, p_2]\{l_i(x_i).P_1\}_{i \in I} \mid s[p_2]; s[p_1, p_2, l_j(v)] \cdot h \xrightarrow{r} P_j\{v/x_j\} \mid s[p_2]; h \]

if \( b \) then \( P_{true} \) else \( P_{false} \xrightarrow{r} P_b \) (\( b \in \{true, false\} \))

new \( a : \text{im}(G[p]).P \xrightarrow{new a: \text{im}(G[p])} (\nu a)(P) \]

\[ \overline{\pi}(s[p] : G) \mid a(s[p] : G); Q \xrightarrow{r} Q \]

\[ 0 \mid P \xrightarrow{a(s[p] : G)} (\nu s)(\overline{\pi}(s[p] : G) \mid P) \]  
\[ 0 \mid P \xrightarrow{a(s[p] : G)} \overline{\pi}(s[p] : G) \mid P \]

\[ s[p_1]; s(p_1, p_2, l(v)) \cdot h \xrightarrow{s[p_1, p_2] l(v)} s[p_1]; h \] (\( p_1 \neq p_2 \))

\[ s[p_2]; h \xrightarrow{s[p_1, p_2] l(v)} s[p_2]; h \cdot s(p_1, p_2, l(v)) \] (\( p_1 \neq p_2 \))

\[ P \xrightarrow{\ell} P' \quad \text{fn}(Q) \cap \text{bn}(\ell) = \emptyset \]
\[ P \xrightarrow{\ell} P' \quad n(\ell) \notin n \]
\[ P \equiv Q \quad Q \xrightarrow{\ell} Q' \quad Q' \equiv P' \]

Figure 5.4: The Labelled Transition System of Asynchronous Local Processes

\[ N_s ::= P \mid N_{s1} \parallel N_{s2} \mid \emptyset \mid (\nu n)N_s \quad n \in \{u, k\} \quad \text{static network} \]
\[ N ::= N_s \mid H \mid N_1 \parallel N_2 \mid (\nu n)N \quad n \in \{u, k\} \quad \text{dynamic network} \]
\[ H ::= \emptyset \mid m \cdot H \quad \text{global queue} \]
\[ m ::= s(p, q, l(v)) \mid \overline{\pi}(s[p] : G) \quad \text{message} \]

Figure 5.5: The Syntax for the Network
1. \( \text{ep}(N_{s1}) \cap \text{ep}(N_{s2}) = \emptyset \).

2. There is no common message existing in \( H_1 \) and \( H_2 \).

Note that, we define the composability of monitored network as same as the above.

**Definition 5.4.3 (composition of global queues).** For any \( H_1 = m_1 \cdot m_2 \cdot \ldots \cdot m_n \) and \( H_2 = m'_1 \cdot m'_2 \cdot \ldots \cdot m'_m \), the composition of two global queues is denoted by \( H_1 \cdot H_2 = m_1 \cdot m_2 \cdot \ldots \cdot m_n \cdot m'_1 \cdot m'_2 \cdot \ldots \cdot m'_m \).

**Definition 5.4.4 (parallel composition of \( N_1 \parallel N_2 \)).** Assume \( N_1 \overset{\text{def}}{=} N_{s1} \parallel H_1 \) and \( N_2 \overset{\text{def}}{=} N_{s2} \parallel H_2 \). When \( N_1 \) and \( N_2 \) are composable, write the parallel composition of \( N_1 \) and \( N_2 \) as \( N_1 \parallel N_2 = N_{s1} \parallel N_{s2} \parallel H_1 \cdot H_2 \).

The global queue \( H \) is an abstract global transport among all network participants i.e. all endpoints share one common global queue. \( H \) consists of a sequence of messages \( m_1 \ldots m_n \), where a message has the shape of either \( \pi(s[p] : G) \) or \( s(p_1, p_2, l(v)) \), ranged over \( m \), which represents an in-transit-message, i.e. the message which has been sent from some sender but has not yet been received by its corresponding receiver. Abstracting a global queue is important, especially for asynchronous interactions, because

1. it captures the dynamics of the network by carrying floating messages from one endpoint to another, and

2. it illustrates that floating messages are interleaving in different sessions.

Consider, during runtime, in a session, a sender sends a message to a receiver. As the message enters the network, under the asynchronous environment, the receiver may not get the message immediately due to asynchrony. Because some local processes may be untrusted, the receiver is expecting an input but does not know if the corresponding sender has sent out a message to her. Since the message has been sent out, there is no message left at the sender side, the only place that a global observer (if there is any) can check is the global queue. Under the asynchronous environment, a message for session-interaction purpose should always be at three places: the sender’s local queue, the global queue, or the receiver’s local queue. The global queue abstracts the asynchronous interactive behaviours. Note that, for asynchronous interactions, the order of messages in the network is generally not preserved, except the messages from
5.4 The Calculus of the Network

a common session or two common session-roles, e.g. \( s(p_1, p_2, l(v)) \cdot s(p_1, p_2, l'(v')) \) (as in a TCP connection).

For synchronous environments, a message can only be outputted when its receiver is ready to receive it; while the receiver is ready, the outputting and inputting of a message are done *synchronously*. Thus there is no need to have a global queue in the network.

5.4.2 The Structural Congruence of the Network

**Definition 5.4.5 (the laws of the network congruence).** Let \( \equiv_N \) be an equivalence relation over \( N \). Then \( \equiv_N \) is said to be a network congruence if it is preserved by all elementary contexts; that is, if \( N_1 \equiv_N N_2 \), then

\[
N_1 \parallel N \equiv_N N_2 \parallel N \\
N \parallel N_1 \equiv_N N \parallel N_2 \\
(\nu n)N_1 \equiv_N (\nu n)N_2
\]

**Definition 5.4.6 (network structural congruence).** The structural congruence over networks is the smallest binary relation \( \equiv_N \), which

1. is a \( \equiv_N \), i.e. abides to the law defined in Definition 5.4.5, and
2. satisfies the following axioms

\[
1 \quad N_1 \equiv_N N_2 \text{ if } N_1 \text{ is an alpha-conversion of } N_2. \\
2 \quad N \parallel 0 \equiv_N N, N_1 \parallel N_2 \equiv_N N, N_1 \parallel (N_2 \parallel N_3) \equiv_N (N_1 \parallel N_2) \parallel N_3. \\
3 \quad (\nu n)(N_1 \parallel N_2) \equiv_N N_1 \parallel (\nu n)N_2 \text{ if } n \notin fn(N_1). \\
4 \quad (\nu n)0 \equiv_N 0. \\
5 \quad H \cdot s(p, q, l(v)) \cdot s'(p', q', l'(v')) \cdot H' \equiv_N H \cdot s'(p', q', l'(v')) \cdot s(p, q, l(v)) \cdot H' \text{ if } s \neq s' \text{ or } p \neq p' \text{ or } q \neq q'.
\]

In the definition of structural congruence of the network, rule 5 is the rule for rearranging messages. It says, globally, as long as two adjacent messages belong to different sessions, or they have different senders or receivers, they can be permuted.
5. THE CAPABILITY-PASSING $\pi$-CALCULUS

5.4.3 The Semantics of the Network

Based on the labels defined in Equation 5.1, let $\ell^0$ be the output action labels, $\ell^I$ be the input action labels.

$$\ell^0 ::= \overline{a}(s[p] : G) | \overline{a}(s[p] : G) | s[p_1, p_2]!l(v)$$

$$\ell^I ::= a(s[p] : G) | a(s[p] : G) | s[p_1, p_2]?l(v)$$

(5.2)

To have a general definition of network reduction rules, several mapping functions are defined below to make the description of reduction rules simple. Define $\text{msg}$ as a function mapping an action to the message which it has outputted or is going to input:

$$\text{msg} ::= \overline{a}(s[p] : G) \mapsto \overline{a}(s[p] : G) | \overline{a}(s[p] : G) \mapsto \overline{a}(s[p] : G)$$

$$| a(s[p] : G) \mapsto a(s[p] : G) | a(s[p] : G) \mapsto a(s[p] : G)$$

$$| s[p_1, p_2]!l(v) \mapsto s[p_1, p_2, l(v)] | s[p_1, p_2]?l(v) \mapsto s[p_1, p_2, l(v)]$$

(5.3)

other actions are not defined. Note that as $\overline{a}(s[p] : G)$ is viewed as a message, it is an invitation. Also, define $\text{dest}$ as a function mapping an action, if it is for input and output, to this action’s destination as:

$$\text{dest} ::= \overline{a}(s[p] : G) \mapsto a | \overline{a}(s[p] : G) \mapsto a$$

$$| a(s[p] : G) \mapsto a | a(s[p] : G) \mapsto a$$

$$| s[p_1, p_2]!l(v) \mapsto s[p_2] | s[p_1, p_2]?l(v) \mapsto s[p_2]$$

(5.4)

other actions are not defined.

The operational semantics of the network is a duality of the semantics of local processes. The actions happening at local processes are marginal actions to the network. From the global viewpoint, those marginal actions are invisible, and are treated as silent actions ($\tau$), which can be viewed as reductions happening in the network. On the other hand, the messages sent across network can be globally observed. For example, as a message is sent from one local endpoint, say Alice, to another, say Bob, for whom are in different local domains, this message is outputted from Alice to the global queue, then absorbed (inputted) by Bob from the global queue. When a message is outputted into
5.4 The Calculus of the Network

\[
\frac{P \xrightarrow{\ell^0} P'}{P \parallel H \rightarrow P' \parallel H \cdot \text{msg}(\ell^0)} \quad \text{[N-OUT]}
\]

\[
\frac{P \xrightarrow{\ell^1} P' \quad \text{dest}(\ell^1) \in \text{ep}(P)}{P \parallel \text{msg}(\ell^1) \cdot H \rightarrow P' \parallel H} \quad \text{[N-IN]}
\]

\[
\frac{P \xrightarrow{\text{new } a \cdot \text{im}(G[p])} (\nu a)(P')}{P \parallel H \rightarrow (\nu a)(P') \parallel H} \quad \text{[N-NEW]}
\]

\[
\frac{\text{join}(s[p]).P \xrightarrow{\text{join}(s[p])} P \mid s[p]; \emptyset}{\text{join}(s[p]).P \parallel H \rightarrow P \mid s[p]; \emptyset \parallel H} \quad \text{[N-JOIN]}
\]

\[
\frac{N_1 \rightarrow N'_1 \parallel N_2 \rightarrow N'_2 \parallel N_2}{N \rightarrow N'} \quad \text{[N-PAR]}
\]

\[
\frac{(\nu \tilde{n})N \rightarrow (\nu \tilde{n})N'}{N \equiv_N N_0 \rightarrow N'_0 \equiv_N N'} \quad \text{[N-STR]}
\]

Figure 5.6: The Reduction Rules of the Network

The global queue, we say this message, from the global viewpoint, enters the network; then this message can be observed through watching the global queue. Conversely, when a message is inputted by an endpoint, we say this message leaves the network.

Figure 5.6 shows the reduction (\(\tau\) actions) rules for the network. Remember, the rules are based on the global viewpoint. Rule [N-OUT] says, when a local process \(P\) outputs a message with action label \(\ell^0\), globally it is a marginal invisible action putting the message (corresponding to \(\ell^0\)) into global queue \(H\). Rule [N-IN] is the duality of [N-OUT]. A local process \(P\) inputs a message with action label \(\ell^1\), which can be finally absorbed by \(P\) since dest\((\ell^1)\) is in ep\(\)\((P)\). Globally, it is a marginal invisible action absorbing the message (corresponding to \(\ell^1\)) from global queue \(H\). Rule [N-NEW] represents that newing a shared name happens locally. Since we restrict that an im-mode shared name is unique in the network, to satisfy this restriction, in practice and in monitoring, one can assume that there are distributed routing tables in the global queue, \(H\), for recording every created name. Rule [N-JOIN] says joining a session-role is locally decided and it will inform the routing mechanism if there is any. Rule [N-PAR] says a reduction of a part of the network does not affect other parts in the network.
Rule \([\text{N-res}]\) says that if a network \(N\) can be reduced to \(N'\), the bound network \((\nu n)N\) can be reduced to \((\nu n)N'\). Rule \([\text{N-str}]\) is standard.

Figure 5.7 illustrates the rules of LTS of the network, represented by the observable global transport. Note that, \(\ell \rightarrow_g\) is particularly used to denote the transitions which are globally observable through observing the global queue. \(N \rightarrow_g N'\) represents the global observability of the network. By watching the transitions happening in the global queue, where actions are visible via inputting and outputting messages, the rules are as the dual of the reduction rules, which generalise the LTS of local processes. Rules \{\text{Req-b/f}\} and \{\text{Sel}\} are summarised as the general output rule \{\text{Out}\}, which is the dual of reduction rule \([\text{N-in}]\); while rules \{\text{Acc-b/f}\} and \{\text{Bra}\} are summarised as the general input rule \{\text{In}\}, which is the dual of reduction rule \([\text{N-out}]\). Note that, \(H/\text{msg}(\ell)\) means taking off message \(\text{msg}(\ell)\) from the set of messages in \(H\). Rule \{\text{Req-b}\} says that, as action \(\overline{a}(s[p] : G)\) takes place, it implies that there exists a local process in the network taking this action for newing a session, and rule \{\text{req-out b}\} defined in Figure 5.4 is applied.

As a message leaves the global queue, there should be exist local process receiving it as an input. Rule \{\text{Out}\} means there is a local process in \(N_s\) outputting a message to the global queue, thus the destination of action \(\ell\) should not be inside \(N_s\) but outside it. Rule \{\text{In}\} means local process \(P\) is going to receive a message from the global queue, thus \(N_s\) does not change its configuration. Rule \{\text{tau}\} summarise the reduction rules defined in Figure 5.6. Rule \{\text{res}\} and \{\text{str}\} are standard according to (117). Rule \{\text{par}\} says that, the bound names of action \(\ell\) should not be any free name appearing in network \(N_2\), and it should not be absorbed by any process in network \(N_2\) (i.e. its destination is not in \(N_2\)). The global transport in the network is used to abstract the network dynamics. The LTS of the network (Figure 5.7), which describes the observable actions via the LTS of global transport, and the LTS of local processes (Figure 5.4) together illustrate that the actions happening in the global queue and those happening in the endpoints are dual.

**Remark 5.4.7.** The actions happening in local processes are the dualities of those happening in the network, and vice versa.

### 5.4.4 Well-formedness

A network \(N\) which satisfies the following conditions is called well-formed: (I) it contains at most one global queue. (II) Two local processes never have the same shared name.
Figure 5.7: The Labelled Transition System of the Global Transport
5. THE CAPABILITY-PASSING $\pi$-CALCULUS

with input mode (i.e. I or IO). We write $\prod_i P_i$ to denote $P_1 \parallel P_2 \cdots \parallel P_n$. Note that well-formedness is preserved by reduction.

As for (II), it means that, let mode be a function mapping a shared name to its I/O mode whenever $a \in n(P)$ and $a \in n(Q)$ where $P \neq Q$, if $a \in n(P), \text{mode}(a)=I$ or $\text{mode}(a)=IO$, then for any $a \in n(Q)$, its mode should be 0 (for output only). This restriction comes from the setting that there is only one input mode for a common shared channel in the network; a shared channel can be used by several endpoints as an output channel to communicate to one and only one target, who has the same shared channel with input mode. If $N$ does not contain a global queue and has no hiding, then $N$ is static, i.e. $N_s$, because it has no dynamic. A network is called initial if the local processes do not contain operator for new name hiding and if the message queue $H$ is empty.

5.4.5 Global Queue v.s. Local Queue

A “queue”, which is in between processes, is there for abstracting asynchronous behaviours through buffering messages which cannot be immediately absorbed by an expected receiver. In the proposed calculus, we design both global queue, which is unique in the network, and local queues, which belong to specific endpoints, to realise asynchronous interactions. If the purpose is only for realising asynchronous processes, we only need one of them. But for asynchronous monitoring, we need both of them: Use the global queue to represent asynchronous interactions among concurrent processes, and use local queues to capture asynchronous interactions between an external monitor and its, more than one, corresponding local processes. Having local queues in the monitoring framework also makes our model closer to the reality: in real-life systems, local processes generally use buffers to manage interaction messages. When we have local queues, having a global queue is to make interleaving messages, which corresponding to interleaving actions in different sessions, become explicit and observable globally.
5.5 The Functionalities of the Capability-passing $\pi$-Calculus

5.5.1 Mobility

As this thesis claims that the capability-passing $\pi$-calculus is based on the asynchronous $\pi$-calculus, thus it should be able to represent not only concurrent interactions but also mobility. Note that, in the $\pi$-calculus,

$$x(y) \mid x(z).\tau(10) \rightarrow y(10),$$

the mobility is realised by name passing shown above; although the capability-passing $\pi$-calculus has the similar name-passing mechanism shown below, the mobility is not done by replacing variable $u$ by the received name $a$, but is done by passing capability $s[q_2]$ to $a$ through $\pi(s[q_2] : G)$:

$$s[p,q]!(a); Q' \parallel s[p,q]?(u).\pi(s[q_2] : G); P'$$

in which a process playing session-role $s[q_1]$ receives the knowledge about where shared point $a$ is, and then passes the endpoint represented by $a$ the capability for playing session-role $s[q_2]$ specified under $G$.

The mobility will be explained by using the scenario of "mobile phones" example for explaining how the $\pi$-calculus is powerful enough to realise mobility.

The follows illustrate some key points which make the representation of mobility of the capability-passing $\pi$-calculus different from the original asynchronous $\pi$-calculus:

1. Every shared channel at every endpoint is specifically I/O typed with mode $I$, $IO$, or $O$ to declare their I/O capability.

2. When a name, say $a$, is transmitted by a session interaction action, say $s[p,q]!(a)$, from endpoint playing $s[p]$ to endpoint playing $s[q]$, it is viewed as a propagation rather than name passing (introduced in (117)) such that the endpoint playing $s[p]$ still knows $a$ through either of the following ways:

(a) If $a$ is with input mode, $I$ or $IO$, at the endpoint playing $s[p]$, then this endpoint still binds $a$ with mode $I$ or $IO$. $a$ with mode $I$ or $IO$ is alive since it is created by a process (i.e. an endpoint), and it will die until this process terminates.
5. THE CAPABILITY-PASSING $\pi$-CALCULUS

(b) If $a$ is with output mode, $\text{O}$ or $\text{IO}$, then this endpoint still has the knowledge about $a$ with mode $\text{O}$ or $\text{IO}$, which means the endpoint knows where to communicate with $a$.

And, the endpoint playing $s[q]$ has the knowledge about $a$ with mode $\text{O}$ because action $s[p,q]!\langle a \rangle$ passes $a$ to the endpoint playing $s[q]$.

3. By applying $[P\text{-request } b/f]$, an endpoint loses a session-role $s[p]$ by delegating it to another endpoint, i.e. by requesting another endpoint to play this session-role. If the endpoint is represented by a specific shared name $b$, then the delegation is

$$\bar{b}(s[p] : G)$$

which means giving up for playing $s[p]$ and requesting shared chanel $b$ to bind $s[p]$ for playing this role.

Although it seems some restrictions are attached to this calculus, this session-based calculus can realise mobility with a high-level language. The following section with a whole example illustrates this point.

In (117), it uses example “mobile phones” to demonstrate the mobility that the $\pi$-calculus provides. Its scenario is described as follows: Assume a user uses mobile phone in a car. When the car runs from one area to another, say from area $A$ to area $B$, the mobile phone transmitter of area $A$ will be correspondingly changed to the one of area $B$. This is controlled by a control center, which is responsible for switching the mobile phone’s connection of the transmitter in area $A$ to the connection of the transmitter in area $B$.

From this example, we learn that the mobility is represented by the ability of possessing a channel. When a process possesses or knows a channel, it has the ability to use it for sending or receiving messages. Recall that, based on our assumptions (see Chapter [4]), there are two kinds of names (or channels), which are session channel and shared channel. A session channel is designed for interactions, while a shared channel is viewed as a shared point linking connections to a specific endpoint. Particularly, a session-role inside a session channel is as important because it is a kind of name, which represents the capability of interactive behaviours. With the similar idea, but different representation, the capability-passing $\pi$-calculus mainly applies session-roles passing
to show the change of *possessing a capability* from one process to another process to represent the mobility.

Here we use the capability-passing $\pi$-calculus to represent the mobility of example "mobile phones". In the session-based calculus, every process is viewed as a session-role involving in a session. In this example, there are three session-roles: Role *car* as a car, role *trans* as a transmitter, and role *control* as a control center. Once a session is established, the interactions are done by passing messages among the session-roles. Even though the car will move from one area, covered by a transmitter, to another area, covered by another transmitter, only the shared channel of the transmitter will change, but the session-role *trans* is still the same.

Let $P_{\text{trans}_i}$ be the process for a transmitter $i$, using shared name $a_i$ for playing role *trans*, specified under protocol $G$, in session $y_i$, which is a session variable for $P_{\text{trans}_i}$:

$$P_{\text{trans}_i} = a_i(y_i[\text{trans}] : G).\mu X.y_i[\text{control, trans}]?\{\text{talk}().P_{\text{talkcar}}.X, \text{lose}(tn).P_{\text{idtrans}}\}$$

where $i = \{1, 2\}$, and $tn$ is the variable of name for a transmitter. A transmitter is recursively waiting for the command from *control*. If the command from *control* is "talk" i.e. branch "talk" has been chosen, then it executes $P_{\text{talkcar}}$ and then keeps listening. If the command from *control* is "lose$(tn)$", then it executes $P_{\text{idtrans}}$. $P_{\text{idtrans}}$ is a process to idle the transmitter $P_{\text{trans}_i}$, by removing the capability of $P_{\text{trans}_i}$ of playing role *trans*, and, at the same time, requests shared channel $tn$, informed from *control*, to play session-role $s[\text{trans}]$.

$$P_{\text{idtrans}} = \overline{tn}(y_i[\text{trans}] : G); P_{\text{trans}_j} \rightarrow \overline{tn}(y_i[\text{trans}] : G) \mid P_{\text{trans}_j}$$

where $j \in \{1, 2\}$ and $i \neq j$. There can be many $P_{\text{trans}_j}$, other transmitters, positioning in parallel after the request $\overline{tn}(y_i[\text{trans}] : G)$. If the *control* assigns the shared channel $tn$ correctly, there must exist some $P_{\text{trans}_j}$ having a shared channel that matches $tn$, i.e. $tn = a_j$ so that it can accept this request.

Note that, with the capability-passing $\pi$-calculus, there is no need to inform the process who plays role *car*, as what the "mobile phones" example in (117) did. It is because the process playing *car* only needs to know how to communicate with other session-roles. Every session-role is bound to some shared channel during communications, and these bindings are decided by the actions of request and accept. When action
5. THE CAPABILITY-PASSING $\pi$-CALCULUS

\( \overline{\text{tn}}(s[\text{trans}] : G) \) in \( P_{\text{trans}} \), takes place, it means the shared channel \( a_i \) in \( P_{\text{trans}} \), for binding session-role \( s[\text{trans}] \) has given up the capability of playing role \( s[\text{trans}] \); when some \( P_{\text{trans}} \), accepts this request, its shared name \( a_j \) will take this capability by binding to the session-role \( s[\text{trans}] \).

If there is a routing table for routing messages among session-roles, the routing table will change the record from \( s[\text{trans}] \mapsto a_i \) to \( s[\text{trans}] \mapsto a_j \). It implies that, the session-role \( s[\text{car}] \) will not feel there is a change because its communications with \( s[\text{trans}] \) are still there even though the shared name of \( s[\text{trans}] \) is changed from \( a_i \) to \( a_j \).

To complete this example, let process \( P_{\text{talkcar}} \) be the process to communicate with process \( P_{\text{car}} \), which plays role \( \text{car} \) in the session:

\[
\begin{align*}
P_{\text{talkcar}} &= \text{if } \text{info} = \text{true} \text{ then } y_i[\text{trans,car}]!\text{info}(\text{info}) \text{ else } y_i[\text{trans,car}]!\text{error}(\text{errMsg}) \\
P_{\text{car}} &= c(y_{\text{car}}[\text{car}] : G).\mu X.y_{\text{car}}[\text{trans,car}]? \\
&\quad \{ \text{info}(x).y_{\text{car}}[\text{car,trans}]!\text{reply}(\text{message}_1), \\
&\quad \quad \text{error}(y).y_{\text{car}}[\text{car,trans}]!\text{report}(\text{message}_2) \}
\end{align*}
\]

\( P_{\text{talkcar}} \) is a process to communicate with role \( \text{car} \). It can be any kind of interactions with \( \text{car} \). Here it assumes that when there is a new information, which is denoted by \( \text{info} = \text{true} \), role \( \text{trans} \) sends \( \text{car} \) the coming information. Similarly, when there is an error happening, role \( \text{trans} \) sends \( \text{car} \) the error message. As for \( P_{\text{car}} \), it firstly accepts to join a session to play role \( \text{car} \), specified under protocol \( G \). Then it recursively waits for messages from \( \text{trans} \). If it is for "info", it replies \( \text{trans} \) with \( \text{message}_1 \). If it is for "error", it reports to \( \text{trans} \) with \( \text{message}_2 \).

The process of control center, playing role \( s[\text{control}] \), is described below:

\[
P_{\text{control}} = \text{if } \text{sig} > \text{bottle} \text{ then } s[\text{control,trans}]!\text{talk()} \text{ else } s[\text{control,trans}]!\text{lose}(\text{tn})
\]

It assumes that when the signal, denoted by \( \text{sig} \), is strong enough, represented by \( \text{sig} > \text{bottle} \), \( \text{control} \) asks role \( \text{trans} \) to continue using the same channel to communicate with \( \text{car} \) by selecting branch "talk"; otherwise, it selects branch "lose" to ask it to lose the current channel and to grab another channel, \( \text{tn} \), to continue playing role \( \text{trans} \) for communicating with \( \text{car} \).
5.5 The Functionalities of the Capability-passing π-Calculus

5.5.2 Pattern-matching

Primitives \( \pi(k[p] : G) \) (or \( \pi\langle k[p] : G \rangle \)) and \( u(y[p] : G) \) (or \( u\langle y[p] : G \rangle \)) compose a pair for pattern-matching. Pattern-matching mechanism is a kind of access control through identifying endpoints for playing each session-role asynchronously and linearly one by one. When a session is created through linear invitations, linearity is automatically satisfied, which means there is no conflict (racing) at session-roles. When an invitation comes from session \( k \), which is fresh to the recipient, primitive \( u(y[p] : G) \).P is used to match this request with \( u, p, \) and \( G \). If it is matched, this request is accepted by replacing variable \( y \) with session \( k \). When \( k \) is not fresh to the recipient, the primitive \( u\langle y[p] : G \rangle \).P is used for pattern-matching. Note that, since \( y \) should has been replaced by some session, say \( s \), the invitation should match not only \( u, p, \) and \( G \), but also \( s \).

Example 5.5.1 (access control through pattern-matching). Assume a process \( P \), defined as below,

\[
P = \pi(s[p_1] : G) \mid \pi\langle s[p_2] : G \rangle
\]

wants to invite endpoints \( a \) and \( c \) for playing roles \( p_1 \) and \( p_2 \) in session \( s \), specified under \( G \). Assume there are two processes \( P_{rev1} \) and \( P_{rev2} \),

\[
P_{rev1} = a(y[p_1] : G).P'_{rev1}
P_{rev2} = c(y[p_3] : G).P'_{rev2}
\]

then only \( P_{rev1} \) can accept \( P \)'s invitation for playing role \( p_1 \) specified under \( G \) because \( P_{rev2} \) is only eligible for playing role \( p_3 \) but not \( p_2 \).

Another example is, assume, for the same \( P \), there are two processes \( P_{rev3} \) and \( P_{rev4} \),

\[
P_{rev3} = a(y[p_1] : G).b(y[q] : G)
P_{rev4} = a(y[p_1] : G').b(y[q] : G')
\]

both of them can play role \( p_1 \) but defined under different protocols \( G \) and \( G' \). Then only \( P_{rev3} \) matches the pattern to accept the invitation from \( P \). Note that, in \( P_{rev3} \), when invitation \( \pi(s[p_1] : G) \) matches \( a(y[p_1] : G) \), the process of recipient becomes

\[
b(y[q] : G')\{s/y\} = b(s[q] : G)
\]

so that the next invitation for endpoint \( b \) should match \( b, q, G \) and \( s \).
Access control is also realised through runtime monitoring where monitors have specifications with logical predicate.

Example 5.5.2 (pattern-matching for preventing information leakage). Assume a network has the following local processes in parallel:

\[(\nu s)(\pi(s[p] : G); P) \parallel H \parallel a(y[p] : G).Q \parallel b(y'[p] : G).Q'\]

where \(a(y[p] : G).Q\) and \(b(y'[p] : G).Q'\) are two local processes in the network. As \(a \neq b\), the process of \(b(y'[p] : G).Q'\) cannot match the invitation \(\pi(s[p] : G)\) to get it. Moreover, when monitoring is on, \(a = b\) is not allowed because, in the network, there is one and only one endpoint having \(a\) with input mode (based on the assumptions defined in Chapter 4).

5.5.3 Propagation

As a shared name, say \(a\), is passed from one endpoint to another, the endpoint (driven by a process) who sends it will not lose \(a\) and the endpoint who receives it will only get \(a\) with output mode, which means it only has the knowledge about \(a\) but cannot use \(a\) to play any session-role. The modes of input and output distinguish the capability of a shared channel, and therefore distinguish the capability of a process who has the channel. When a process has a shared channel with input mode, it can use it to bind a session-role for playing this role because it can listen (i.e. input) the requests from the outside; while a process has the same shared channel but with O-mode (i.e. not including IO-mode), it can only send (i.e. output) messages through this channel with her knowledge about this channel.

Thus passing a shared name in our calculus is different from the standard name-passing mechanism in which, when a process passes a name to another, the sender loses the name, while the receiver gains it. For this difference, we say passing a shared name as a propagation: to propagate the knowledge about a shared name.

The propagation is realised by the following mechanism, which is controlled by the change of configurations of specifications (introduced in Chapter 6):

1. When a process creates a new name, say \(a\), the specification guarding this process will add \(a\) with input mode. It means that whenever a process creates a new name, the process has this name for input.
2. When a specification guarding a process (i.e. an endpoint) has a shared name, say \(a\), this process can send out name \(a\).

3. When a process receives a name, say \(a\), from another process, the specification for this process will add \(a\) with output mode.

As it comes to the calculus of monitoring, every system monitor possesses local specifications, which are projected from the global ones, of the endpoints which she monitors.
Specifications for Governance

Overview  This chapter, as a preparation for Chapter 7, formally introduces the specifications for session-based dynamic monitoring. These specifications are built upon standard MPST and MPSA technologies which bring essential mechanisms such as the global specifications for network-wise interactions, the local specifications for endpoint processes’s behaviours, and endpoint projection from a global specification. Section 6.1 gives two motivating examples. One motivates the effectiveness of session-based specifications, another motivates the desire of permutation mechanism of specifications. Section 6.2 introduces the grammar of global session-based specifications, and Section 6.3 states the consistency principles, together with well-formedness and well-assertedness properties, to validate global specifications. Section 6.4 gives the grammar of local session-based specifications, and Section 6.5 introduces projection mechanism for projecting a global specification to endpoint roles with local specifications. The permutation mechanism is introduced in Section 6.6 which is designed to support a monitor for determining messages passing in asynchronous monitoring environment.

6.1 Motivating Example

This section provides two motivating examples. One gives an illustration that a session-type based specification enjoys conciseness and expressiveness for regulating concurrent interactions. Another shows that, since asynchrony leads to non-deterministic results,
6. SPECIFICATIONS FOR GOVERNANCE

permutation mechanism, introduced in Section 6.6, is designed for specifying asynchronous interactions.

6.1.1 The Effectiveness of a Session-based Specification

Assume an external monitor, guarding the local process representing Principal A, has the following concurrent tasks:

(I) Principal A sends Principal B a request for buying a book with a content “buy War and Peace”. Finish.

(II) Principal A sends Principal C a request for booking a book with a content “book Harry Potter”. Finish.

(III) Principal A gets a feedback as “231342”. Finish.

(IV) Principal A gets a feedback as “B231342”. Finish.

Note that (I) and (II) (resp. (III) and (IV)) may happen concurrently. When the structure of sessions is not applied, at the conversation-level, the monitor watching conversations can not realise if content of “231342” is coming from Principal B or C, neither can she ensure the content of “B231342”. Note that, as we say it is at the conversation-level, or the session-level, we mean that the messages have not yet entered the domain of the receiver’s location. If a message arrives at the endpoint, the endpoint may ask a key from the message to check if the message is valid. The session-type-based specifications are for the conversation-level messages when those messages have not yet arrived at the receivers. Even if Principal A is informed that “B231342” is a feedback from Principal B because the message claims so, she does not know whether the format of the content is correct. In practice, before an interaction starts, they firstly establish a commitment through negotiation to specify the format of transmitted data. It can be done by a negotiation protocol, which in fact can apply the structure of sessions.

With the structure of sessions, a protocol can be easily done with session-based specifications which have specified every step of interactions. The following protocols are represented by session types:

\[
\begin{align*}
\text{Buy Protocol} & \quad G_{\text{buy}} = A \rightarrow B : (\text{string}).B \rightarrow A : (\text{formatB}).\text{end} \\
\text{Book Protocol} & \quad G_{\text{book}} = A \rightarrow C : (\text{string}).C \rightarrow A : (\text{formatC}).\text{end}
\end{align*}
\]
where the formatB is composed by one alphabet plus 6 natural numbers, while formatC is composed by 6 natural numbers. Protocols Buy and Book specify the sequence of interactions and the individual formats for transmitted data. A monitor can clearly realize that case (III) or (IV) coming from which principals and whether their contents are in right format.

6.1.2 Verifying Non-deterministic Results

Historically, most well-known process calculi, like CCS (115), CSP (79, 80), and the π-calculus (117, 118) assume the interactions happening among processes are synchronous. In comparison, the assumption that interactions are asynchronous makes analysis more challenging because (I) communications are hard to harness and (II) asynchronous interactions result in non-determinism. The following example shows the permutation mechanism, defined in Section 6.6, is useful for a monitor to verify non-deterministic results.

Example 6.1.1. Assume there are three processes in the network (introduced in Section 5.4) in parallel, each of which is separated by notation ||:

\[ s[p, q]!\langle 1 \rangle || s[q, r]!\langle 2 \rangle; s[p, q]?\langle x \rangle || s[q, r]?\langle x \rangle \]

Let \( P_1 = s[p, q]!\langle 1 \rangle \), \( P_2 = s[q, r]!\langle 2 \rangle; s[p, q]?\langle x \rangle \), and \( P_3 = s[q, r]?\langle x \rangle \). As the interactions are synchronous, the result of variable \( x \) is deterministic, which is 1. \( P_1 \) with action \( s[p, q]!\langle 1 \rangle \) can not take place until action \( s[q, r]!\langle 2 \rangle \) in \( P_2 \) takes place because its corresponding input \( s[p, q]?\langle x \rangle \) should wait until \( s[q, r]!\langle 2 \rangle \) fires, which is able to fire immediately because \( P_3 \) with action \( s[q, r]?\langle x \rangle \) is ready for it. Therefore, the sequence of actions is

\[ s[q, r]!\langle 2 \rangle \cdot s[q, r]?\langle x \rangle \cdot s[p, q]!\langle 1 \rangle \cdot s[p, q]?\langle x \rangle \]

which is deterministic. When the interactions are asynchronous, \( P_1 \) and \( P_2 \) can take actions in any order or even concurrently. The sequence of actions can be

\[ s[q, r]!\langle 2 \rangle \cdot s[q, r]?\langle x \rangle \cdot s[p, q]!\langle 1 \rangle \cdot s[p, q]?\langle x \rangle \quad \text{or} \quad s[p, q]!\langle 1 \rangle \cdot s[p, q]?\langle x \rangle \cdot s[q, r]!\langle 2 \rangle \cdot s[q, r]?\langle x \rangle \]

Thus the result of \( x \) may be 1 or 2 depending on \( P_2 \) with action \( s[p, q]?\langle x \rangle \) firstly receive the message from \( P_1 \) or \( P_3 \) with action \( s[q, r]?\langle x \rangle \) firstly receive the message from \( P_2 \).
6. SPECIFICATIONS FOR GOVERNANCE

Synchronous interactions, however, make the overall systems inefficient and do not reflect the facts of large-scale distributed systems.

As we focus on asynchronous interactions, to make an external monitor relying on specifications sensible to judge local processes’ runtime behaviours, the permutation mechanism is proposed. The permutation mechanism can verify that both traces

\[
s[q, r]!⟨2⟩·s[q, r]?(x)·s[p, q]!⟨1⟩·s[p, q]?(x) \quad \text{or} \quad s[p, q]!⟨1⟩·s[p, q]?(x)·s[q, r]!⟨2⟩·s[q, r]?(x)
\]

are correct behaviours under asynchronous environment.

6.2 Global Specifications

Before introducing global specification with assertions, firstly the logical language for predicates (i.e. assertions) is defined below:

**Definition 6.2.1 (logical language).** The grammar for logical formulae (i.e. predicate) is:

\[
A ::= \text{true} \mid \text{false} \mid e_1 = e_2 \mid e_1 > e_2 \mid \phi(e_1, ..., e_n) \mid A_1 \cap A_2 \mid \neg A \mid \exists x(A)
\]

where \(e_1, ..., e_n\) are expressions, and \(\phi, ..., \) range over a pre-defined set of predicates with fixed arities and types. \(\exists x(A)\) returns true if there exists \(x\) in \(A\); otherwise it returns false. Write \(\text{var}(A)\) for the set of free variables occurring in \(A\), similarly for \(\text{var}(e)\).

**Convention 6.2.2.** Assume a fixed model for logical formulae satisfying: (I) validity of each closed atomic formula including equality and inequality is polynomially decidable; and (II) validity of closed formulae is decidable.

The syntax of global types, or called *global specifications*, is defined in Figure 6.1. It is based on (22), in which rule “interaction” is divided into the rules of “value” and “branching”. In other words, the syntax in Figure 6.1 is not original but with some minor revision of the syntax of (22).

In Figure 6.1 sessions are described in terms of global specifications, which are called *types* in (86), and are called *assertions* in (22). Because, later in Chapter 8, we extend global/local assertions to embed *endpoint states* for specifying endpoints’ behaviours through observing traces, for generality, from now on, a session type or a session assertion is uniformly called a *session specification* (i.e. global/local specifications).
Definition 6.2.3 (the set of roles in \( G \)). Define \( \text{role}(G) \) as the set of roles occurring in global specification \( G \). Whenever \( p, q \in \text{role}(G) \), \( p \neq q \).

The global specification \( G \) describes a session as a protocol signature among multiple roles with logical formulae. It is an abstract global scenario description which structures multi-party interactions and indicates the steps taken by the roles in the session. The main construct is a labelled message exchange, where \( p \) sends \( q \) a label \( l_i \) (\( I \) is a finite set of integers) and a message \( x_i \) with sort \( S_i \). Sorts include base types and shared name type \( \text{mode}(G[p]) \). In \( \text{mode}(G[p]) \), \( G \) defines the behaviour of role \( p \). \( G_i \) describes the continuation of the session for the selected branch \( i \), and \( A_i \) is a predicate on interaction variables specifying what \( p \) must guarantee and dually what \( q \) can rely on. \( A_i \) expresses a constraint on the choice of branch \( i \) (e.g., a guard that must hold when selecting label \( l_i \)) and on the value of the exchanged message \( x_i \), which we call interaction variable.

We do not fix a specific logic for \( A \), we only assume it is decidable. Interactions bind each \( x_i \) in \( A_i \) and in \( G_i \).

A recursive specification is guarded by an invariant \( A \), and defines a recursion parameter with its initialisation. \( \tilde{e} = e_1, \ldots, e_n \), \( \tilde{x} = x_1, \ldots, x_n \) and \( \tilde{S} = S_1, \ldots, S_n \). and every \( x_i, x_j, i \neq j \) are pairwise disjoint. \( \tilde{x} \) is the binder of predicate \( A \). Note that, the variable of recursion parameter is known by every participant involved in the recursion. For example, in recursion

\[
\mu t(e)(x:S)⟨⟨A⟩⟩.p \to q : (y : \text{int})⟨⟨y > x⟩⟩.t,
\]

\( x \) is not an interaction variable sent from \( p \) to \( q \) but a parameter of this recursion, both \( p \) and \( q \) know \( x \) because they are all involved in the recursion. \( t \) is a variable for specifications. Its formal form is \( t(e) \) because it may be a specification for a recursion.
6. SPECIFICATIONS FOR GOVERNANCE

which has parameters. Branching and recursion describe potential choices and repeated
interactions. Each message exchange/branching is annotated with a predicate specifying
a constraint on the message value or the choice of a branch. end ends the session. Parallel
composition is written as $G_1 \mid G_2$ in rule parallel. When a session follows $G_1 \mid G_2$, there
are multi-threads running concurrently in this session. Note that whenever $G_1 \mid G_2$,
role($G_1$) $\cap$ role($G_2$) = $\emptyset$ holds. This structure provides the language flexibility, and
benefits programers to write tasks in a readable structure.

Example 6.2.4 (OOI Instrument Commands - global specification). The fol-
lowing specification is the global specification for the example introduced in Chapter 5
(see Figure 5.2). A branch without predicate means its accompanying predicate is true.
We sometimes omit labels when there is a single branch.

$$G_{IC} = \text{User} \rightarrow \text{Register} : (x_{int} : \text{Intefaced}).$$
$$\text{Register} \rightarrow \text{User} : (x_n : \text{Int}) \langle x_n > 0 \rangle. \text{User} \rightarrow \text{Agent} : (x_p : \text{Priority}).$$
$$\text{Agent} \rightarrow \text{User} : \{\text{accept}(). G_{acc}, \text{reject}(x_E : \text{ErrData}) \langle x_p = \text{high} \supset x_e \neq \text{busy} \rangle. \text{end}\}$$

$$G_{acc} = \mu(x_n)(y) \langle y \geq 0 \rangle.$$  
$$\text{User} \rightarrow \text{Agent} : \{\text{more}(x_{com} : \text{Command}) \langle y > 0 \land x_{com} \neq \text{switch-off} \rangle. G_{com},$$
$$\text{quit}(). \text{Agent} \rightarrow \text{Instrument} : \text{quit}(). \text{end}\}$$

$$G_{com} = \text{Agent} \rightarrow \text{Instrument} : (y_{com} : \text{Command}).$$
$$\text{Instrument} \rightarrow \text{Agent} : (y_r : \text{Response}). \text{Agent} \rightarrow \text{User} : (x_r : \text{Response}). t(y - 1)$$

The scenario modelled by $G_{IC}$ has already been described informally in Section 5.2
Chapter 5.

6.3 Consistency Principles

Based on (22 [86]), this thesis addresses the consistency principles, well-formedness and
well-assertedness for global specifications. For detailed theories and proofs, please see
(22 [86]).

The consistency principles of global specifications for ensuring the consistency of
overall network behaviours are introduced in (22). This thesis, for completion reason,
also mentions these principles which are defined on the basis of (22). The principles
addressed are history sensitivity and temporal satisfiability. The well-formedness and
well-assertedness of global specifications which are also very similar to those in (22),
except the minor changes of the syntax of global specifications, are reviewed. Note, when
we go to stateful specifications, Chapter 8 the revised stateful well-formedness for global
specifications will be introduced, while the well-assertedness for global specifications is still the same. Also note that the principle of locality, which is discussed in \( (22) \), is not addressed in this thesis because this thesis combines actions “interaction” and “branching” to be one action; which means, every action of “interaction” is one kind of action of “branching”. Moreover, the principle of temporal satisfiability directly implies locality according to \( (22) \)'s Proposition B.10.

History sensitivity says, for every interaction,

1. the sender must know the variables/names he or she is going to send, and knows the variables/names deciding the result of the interaction predicate;
2. the receiver must know the variables/names, except those variables carried through the interaction (which are new to the receiver), deciding the result of the interaction predicate.

In other words, the interaction predicate of a participant must be defined only on those interaction variables introduced in the preceding interactions in which the participant is involved. Note that, according to the syntax of global specification shown in Figure 6.1, an interaction predicate is for both the sender and the receiver involved in this interaction. The variables carried through this interaction, which should be known by the sender, may be new to the receiver. The receiver knows these variables when he receives them.

**Example 6.3.1 (history sensitivity).** The following global specification violates history sensitivity

\[
p \rightarrow q : (x : \text{int})  \langle\langle x > 5 \rangle\rangle.
\]
\[
r \rightarrow q : (y : \text{int})  \langle\langle y > x \rangle\rangle.
\]

because \( r \) does not know variable \( x \), which is only shared by roles \( p \) and \( q \).

It can be easily revised to the global specification below

\[
p \rightarrow q : (x : \text{int})  \langle\langle x > 10 \rangle\rangle.
\]
\[
q \rightarrow r : (x : \text{int})  \langle\langle \text{true} \rangle\rangle.
\]
\[
r \rightarrow q : (y : \text{int})  \langle\langle y > x \rangle\rangle.
\]

to respect history sensitivity.
Well-formedness conditions for global specifications introduced later (Section 6.3.1) ensures a global specification satisfies history sensitivity.

As for temporal satisfiability, this principle says

Every participant involved in an interaction should always find a valid path to proceed (in that interaction) unless he or she meets end.

Note, when interaction predicates do not attach to global specifications, like the ones in (86), a global specification always satisfies temporal satisfiability. When predicates are attached to interactions, they restrict the paths for interaction participants to go forward: Only the valid paths, according to the predicate, can forward the process.

The following example illustrates how a global specification violates temporal satisfiability principle, and how it can be revised to satisfy this principle.

Example 6.3.2 (temporal satisfiability). The global specification below violates temporal satisfiability

\[
\begin{align*}
p \rightarrow q & : \text{len}(x : \text{int}) \langle x > 5 \rangle. \\
q \rightarrow p & : \{ \text{walk}(y : \text{int}) \langle x < y < 10 \rangle, \\
& \qquad \text{run}(y : \text{int}) \langle x < y < 50 \rangle \}
\end{align*}
\]

because, when \( x \) is bigger than 50, which is actually possible since the predicate at role \( p \) only ensures \( x > 5 \), neither branch "walk" nor "run" can be selected for sending a proper \( y \) from role \( q \) to role \( p \) to satisfy the predicates specified at role \( q \) and \( p \).

A revised one that respects temporal satisfiability can be

\[
\begin{align*}
p \rightarrow q & : \text{len}(x : \text{int}) \langle 49 > x > 5 \rangle. \\
q \rightarrow p & : \{ \text{walk}(y : \text{int}) \langle x < y < 10 \rangle, \\
& \qquad \text{run}(y : \text{int}) \langle x < y < 50 \rangle \}
\end{align*}
\]

where \( x : \text{int} \text{ and } 49 > x > 5 \) ensures the possible values of \( x \) are from 6 to 48. Even when a value in the range of 8 to 48 is sent from role \( p \) to role \( q \), \( q \) can select branch "run" to send \( y \) in the range of 9 to 49 to satisfy the predicate \( x < y < 50 \).

When the local endpoint states are embeded into specifications, the consistency principles are revised, which are discussed in Section 8.2.2. Chapter 8.
6.3 Consistency Principles

6.3.1 Well-formedness

The well-formedness of global specifications stipulates the principle of history sensitivity, which can be ensured linearly through a syntactic checker (for details, please see \(22\)). Before introducing well-formedness, a convention and definitions are stated as follows.

**Convention 6.3.3.** This thesis assumes the standard bound name convention for all syntactic entities with bindings.

\[ I(G) \] is defined as the one in \(22\):

**Definition 6.3.4.** Define \( I(G) \) as the set of interaction variables occurring in \( G \). \( p \in \text{role}(G) \) knows an interaction variable \( u \in I(G) \) when \( p \) sends \( u \) or receives \( u \), or when \( u \) is a parameter of a recursion where \( p \) involves.

**Definition 6.3.5 (projection of interaction variables, \( I(G) \mid p \)).** Define \( I(G) \mid p \), where \( p \in \text{role}(G) \), as the set of variables that role \( p \) knows.

**Definition 6.3.6.** Let \( \tilde{S} = S_1, ..., S_i, ..., S_n \). Define \( t : \tilde{S} \) for representing that the sort of \( i \)th parameter of \( t \) is \( S_i \).

**Definition 6.3.7 (shared environments).** Let \( \Gamma \) be the shared environments, defined by the following grammar:

\[ \Gamma ::= \emptyset | \Gamma, x : S | \Gamma, u : \text{mode}(G[p]) | \Gamma, t : \tilde{S} \]

where \( x \) is a variable for integer, string, and boolean, etc., while \( u \) is a variable for shared name, and \( t \) is for specification variable, When it is used to handle a recursive specification, it has the corresponding parameters to the recursion specification. Note that, \( \Gamma \vdash e \) if for every \( x \in \text{var}(e) \), \( \Gamma \vdash x \).

As the one defined in \(22\), the well-formedness for global specifications is defined in Figure 6.2 with some revisions to cater for the syntax of our global specifications.

The key rule [WF-interaction] requires that interaction participants must know all the variables appearing in predicate \( A \).

\[ \forall x.((x \in \bigcup_{i \in I} \text{var}(A_i) \cap x \notin \{x_i\}_{i \in I}) \supset x \in (I(G) \mid p \cap I(G) \mid q)) \]

means that for any \( x \) which is in the assertions \( \{A_i\}_{i \in I} \) but not as an interaction variable, it should be known by both roles \( p \) and \( q \). In rule [WF-rec], \( t : S_1, ..., S_n \)
6. SPECIFICATIONS FOR GOVERNANCE

∀i ∈ I, Γ, xi : Si ⊢ Gi
∀x.((x ∈ ∪i∈I\text{var}(A_i) \cap x \notin \{x_i\}_{i \in I} \supset x \in (J(G) \downarrow p \cap J(G) \downarrow q)) \quad \text{[WF-interaction]}

Γ ⊢ p → q : \{i_i(x_i : S_i)∥A_i∥G_i\}_{i \in I}

Γ ⊢ G' \quad Γ ⊢ G
Γ ⊢ G | G'
\quad \text{[WF-par]}

Γ ⊢ \text{end}
\quad \text{[WF-end]}

Γ ⊢ e_1 : S_1, ..., Γ ⊢ e_n : S_n
\quad Γ, t : S_1, ..., S_n ⊢ t(e_1, ..., e_n)
\quad \text{[WF-rec]}

Γ' = Γ, t : S_1, ..., S_n
Γ' ⊢ G
\quad \text{dom}(Γ') \supseteq \text{var}(A)
\quad ∀i.Γ ⊢ x_i : S_i, e_i : S_i
\quad \text{[WF-def]}

\Gamma ⊢ \mu t(e_1, ..., e_n)(x_1 : S_1, ..., x_n : S_n)∥A∥G

Figure 6.2: Well-formedness for Global Specifications

means the parameters of recursive variable t has types S_1, ..., S_n. This knowledge is known by the participants involved in the recursion. [WF-def] says that, if the shared environment can prove the value of each parameter follows the specified type, i.e. ∀i.Γ ⊢ x_i : S_i, e_i : S_i, and prove the recursion body G, i.e. Γ' ⊢ G where Γ' = Γ, t : S_1, ..., S_n, which implies that the invariant A is true, then it can prove the recursive specification μt(e_1, ..., e_n)(x_1 : S_1, ..., x_n : S_n)∥A∥G. Other rules are straightforward. According to (22), the rules are purely syntactic, and the validation of G is a linear time problem.

6.3.2 Well-assertedness

Well-assertedness is defined in terms of principle of temporal satisfiability. Temporal satisfiability requires that for every possible value sent and branch selected in the past, it is always possible to make a choice that satisfies the current predicate. The most trivial violation of temporal satisfiability is an interaction with one single branch and predicate false. The intuition for realising temporal satisfiability is to ensure that, for every interaction predicate A, there exists an interaction predicate A' just appearing after A such that A implies A', i.e. A ⊃ A'. Below the checker for temporal satisfiability, a boolean function GSat, is defined based on (22).

Definition 6.3.8 (well-assertedness for global specifications). Assume at the beginning A = true. We define a recursively boolean function GSat(G, A) as follows:
6.3 Consistency Principles

(i) If $G = p_1 \rightarrow p_2 : \{l_i(x_i : S_i)\langle A_i \rangle.G_i\}_{i \in I}, I = \{1, ..., n\}$ then $\text{GSat}(G, A)$ returns

$$\begin{cases} 
\text{GSat}(G_1, A \cap A_1) \cap \ldots \cap \text{GSat}(G_n, A \cap A_n) & \text{if } A \supset \bigcup_{i \in I} (\exists x_i(A_i)) \\
false & \text{otherwise}
\end{cases}$$

(ii) $G = G_1 \mid G_2$ then $\text{GSat}(G, A)$ returns $\text{GSat}(G_1, A) \cap \text{GSat}(G_2, A)$.

(iii) $G = \mu \langle \tilde{e} \rangle \langle \tilde{x} : S \rangle \langle A' \rangle.G'$ then $\text{GSat}(G, A)$ returns

$$\begin{cases} 
\text{GSat}(G', A \cap A') & \text{if } A \supset A'\{\tilde{e}/\tilde{x}\} \\
false & \text{otherwise}
\end{cases}$$

(iv) $G = t_{\langle \tilde{x}, A' \rangle}(\tilde{e})$ then $\text{GSat}(G, A)$ returns $true$ if $A \supset A'\{\tilde{e}/\tilde{x}\}$ and $false$ otherwise.

(v) $G = \text{end}$ then $\text{GSat}(G, A)$ returns $true$.

Write an annotation of type variable $t$ as $t_{\langle \tilde{x}, A' \rangle}(\tilde{e})$ to represent that type variable $t$ has a predicate $A'$ (i.e. recursion invariant) associated to this recursion and parameters $\tilde{x}$. This annotation is always possible if $t$ is bound in a whole global specification, i.e. if the whole global specification is closed.

In (i), it requires that there exists at least one branch, say label $j$, that can be chosen such that $\exists x_j(A_j)$ is true whenever $A$ is true. For example,

$$ p \rightarrow q : \{(x : \text{int})\langle x < 10 \rangle.G'_1, (x : \text{int})\langle x \geq 10 \rangle.G'_2\}$$

is well-asserted because if the first branch fails, the second branch can be chosen, and vice versa. Also,

$$ p \rightarrow q : \{(x : \text{int})\langle x > 10 \rangle.G'_1, (y : \text{int})\langle y > 10 \rangle.G'_2\}$$

is well-asserted when it starts from $A = true$ because $p$ is able to send valid values for variables $x$ and $y$. In (ii), a parallel composition is satisfiable if both of them are satisfiable. (iii) and (iv) require $A$ to imply the predicate $A'$ of the recursion after replacing variables $\tilde{x}$ with $\tilde{e}$ in the recursion body (i.e. initiation parameters). (v) says a session termination $\text{end}$ always returns true.
6. SPECIFICATIONS FOR GOVERNANCE

\[ T ::= p\{l_i(x_i:S_i)\langle\langle A_i\rangle\rangle.T_i\}_{i\in I} \text{ selection} \]
\[ | \quad p?\{l_i(x_i:S_i)\langle\langle A_i\rangle\rangle.T_i\}_{i\in I} \text{ branch} \]
\[ | \quad \mu t(e)(x:S)\langle\langle A\rangle\rangle.T \mid t(e) \mid \text{end rec/var/end} \]

Figure 6.3: Local Specifications: \( T \)

6.4 Local Specifications

For runtime monitoring, every local process is associated a dedicated monitor that manages its interactions with the network (hence with other peers) by inspecting outgoing and incoming messages.

The endpoint specifications, \( T \), are defined in Figure 6.3. They are local specification used by monitors to represent which interactions are acceptable for an endpoint. A local specification describes a session from the perspective of a role.

Rule selection expresses the transmission to role \( p \) of a label \( l_i \) taken from a label pool \( \{l_i\}_{i\in I} \), where \( I \) is a set of indexes, together with an interaction variable \( x_i \) of sort \( S_i \) and that the remaining interaction in the session is \( T_i \). Branching is its dual. Others are similar to the global version.

Based on Example 6.2.4, Example 6.4.1 shows the endpoint specifications (which can be automatically projected from \( G_{IC} \). The projection algorithm is introduced in Section 6.5).

Example 6.4.1 (OOI Instrument Commands - the user endpoint).

\[ T_{\text{user}} = \text{Register!(}x_{\text{int}}:\text{Interfaceld}).\text{Register?}(x_n: \text{Int})\langle\langle x_n > 0 \rangle\rangle.\text{Agent!(}x_p: \text{Priority}).\text{Agent?}\{\text{accept()}.T_{\text{acc}}^u, \text{reject}(x_c: \text{ErrData})\langle\langle x_p = \text{high} \supset x_c \neq \text{busy}\rangle\rangle.\text{end}\} \]
\[ T_{\text{acc}}^u = \mu t(x_n)(y)\langle\langle y \geq 0 \rangle\rangle.\]
\[ \text{Agent!}\{\text{more}(x_{com}: \text{Command})\langle\langle y > 0 \wedge x_{com} \neq \text{switch-off}\rangle\rangle.T_{\text{com}}^u, \text{quit()}.\text{end}\} \]
\[ T_{\text{com}}^u = \text{Agent?}(x_r: \text{Response}).t(y - 1) \]

Well-assertedness for endpoint specifications is defined in the same way as the one for global specifications:

Definition 6.4.2 (well-assertedness for local specifications). Assume at the beginning \( A = \text{true} \). We define a recursively boolean function \( GSat(T, A) \) as follows:

(i) If \( T = p\{l_i(x_i:S_i)\langle\langle A_i\rangle\rangle.T_i\}_{i\in I} \) or \( T = p?\{l_i(x_i:S_i)\langle\langle A_i\rangle\rangle.T_i\}_{i\in I} \) where \( I = \)

100
{1, ..., n}, then $GSat(T, A)$ returns
\[
\begin{cases}
    GSat(T_1, A \cap A_1) \cap ... \cap GSat(T_n, A \cap A_n) & \text{if } A \supset \bigcup_{i \in I} (\exists x_i(A_i)) \\
    \text{false} & \text{otherwise}
\end{cases}
\]

(ii) $T = \mu t(\tilde{e})(\tilde{x}: S)(A')$. Then $GSat(T, A)$ returns
\[
\begin{cases}
    GSat(T', A \cap A') & \text{if } A \supset A'\{\tilde{e}/\tilde{x}\} \\
    \text{false} & \text{otherwise}
\end{cases}
\]

(iii) $T = t(\tilde{x}, A')(\tilde{e})$ then $GSat(T, A)$ returns true if $A \supset A'\{\tilde{e}/\tilde{x}\}$ and false otherwise.

(iv) $T = \text{end}$ then $GSat(T, A)$ returns true.

In (i), it is required that, either for sending or receiving, there exists at least one branch, say label $j$, that can be chosen such that $\exists x_j(A_j)$ is true whenever $A$ is true. Other definitions for well-assertedness for local specifications are for same reasons as the ones defined for the case of global specifications.

Together with the calculus defined in Chapter 5, a monitor with $T$ can specify the behaviours of local processes. Once a process joins a session, the corresponding monitor is activated and enforces conformance to the scenario of the subsequent interactions prescribed for the process to follow.

### 6.5 Projection from the Global to the Local

In this section we define the projection from a global specification to endpoint specifications. Projectability is a structural property from the underlying type and well-assertedness is a property on predicates ensuring it is always possible for an endpoint to satisfy its own obligations. This thesis assumes these properties for specifications. Figure 6.4 illustrates the relationships between global specifications and local specifications linked by projection. A local specifications is projected to a role specified in a global specification. It is either used for runtime monitoring or for static type checking. An endpoint projection or often simply projection, denoted by $G \upharpoonright p$, projects $G$ onto $p$ returning an endpoint specification. The projection in this thesis is defined similarly.
### 6. SPECIFICATIONS FOR GOVERNANCE

![Diagram showing the relationships between specifications and projection](image)

**Figure 6.4:** The Relationships between the Global Specifications, Local Specifications, and the Projection

...to the one proposed in [22]. Some rules are revised according to the combination of actions of “interaction” and “branching”.

With Definition 6.3.4, \( \mathcal{I}(G) \) is the set of interaction variables exchanged and recursion parameters in \( G \). We let \( \mathcal{I}(G) \upharpoonright p \) be the set of variables known by \( p \) which are either: (I) the variables that \( p \) sends or receives in \( G \), or (II) the parameter of recursions e.g., \( \mu t(e)(y)\langle A \rangle \langle \langle \alpha \rangle \rangle \). \( p \) knows all the variables in the expression \( e \) and \( p \) knows all variables in \( e' \) for all \( t(e') \) in \( P \). We define the projection of a predicate on a participant as \( A \upharpoonright p = \exists V_{ext}.A \) with \( V_{ext} = \text{var}(A)/\mathcal{I}(G) \upharpoonright p \) (i.e., closing with the existential quantifier the free variables of \( A \) that \( p \) does not know).

Based on [22], the projection of a global specification onto each role with an endpoint specification is defined as a recursive function \( \text{Proj} \). It is also extended to the mergeability studied in [50]. We use annotation \( t_x \) for recursive call where \( x \) is the recursion parameter for \( t \) (i.e., in \( \mu t(e)(x : S)\langle A \rangle \langle \langle \alpha \rangle \rangle \)).

**Definition 6.5.1 (Projection).** Assume \( p \in G, p_1 \neq p_2 \). Let \( A \upharpoonright \text{true} \). The projection of \( G \) on \( p \), written \( \text{Proj}(G, A, p) = G \upharpoonright p \), is defined as follows.
6.5 Projection from the Global to the Local

1. \( \text{Proj}(p_1 \rightarrow p_2 : \{ l_i(x_i : S_i) \langle A_i \rangle . G_i \}, A_{\text{proj}}, p) = \)

\[
\begin{cases}
  p_2!\{ l_i(x_i : S_i) \langle A_i \rangle . G^i_{\text{proj}} \} & \text{if } p = p_1 \neq p_2, \\
p_1?\{ l_i(x_i : S_i) \langle (A_i \cap A_{\text{proj}}) \rightarrow p \rangle . G^i_{\text{proj}} \} & \text{if } p = p_2 \neq p_1, \\
\sqsubset_{i \in I} G^i_{\text{proj}} & \text{if } p \neq p_1, p \neq p_2
\end{cases}
\]

with \( G^i_{\text{proj}} = \text{Proj}(G_i, A_i \cap A_{\text{proj}}, p) \).

2. \( \text{Proj}((G_1 \mid G_2), A_{\text{proj}}, p) = \)

\[
\begin{cases}
  \text{Proj}(G_i, A_{\text{proj}}, p) & \text{if } p \in G_i \text{ and } p \notin G_j, i \neq j \in \{1, 2\} \\
\text{end} & \text{if } p \notin G_1 \text{ and } p \notin G_2.
\end{cases}
\]

3. \( \text{Proj}(\mu t(v)(x : S) \langle A \rangle . G, A_{\text{proj}}, p) = \)

\[
\begin{cases}
  \mu t(v)(x : S) \langle A \rightarrow p \rangle \cdot \text{Proj}(G, A \cap A_{\text{proj}}, p) & \text{if } x \in J(G) \rightarrow p \\
\mu t(A \rightarrow p) \cdot \text{Proj}(G, A \cap A_{\text{proj}}, p) & \text{if } x \notin J(G) \rightarrow p \text{ and } p \in \text{role}(G) \\
\text{end} & \text{if } p \notin \text{role}(G)
\end{cases}
\]

4. \( \text{Proj}(t_x(v), A_{\text{proj}}, p) = \)

\[
\begin{cases}
  t_x(v) & \text{if } x \in J(G) \rightarrow p \\
  t_x & \text{otherwise}
\end{cases}
\]

5. \( \text{Proj}(\text{end}, A_{\text{proj}}, p) = \text{end}. \)

where \( \sqsubset_{i \in I} G^i_{\text{proj}} = G^1_{\text{proj}} \sqcup G^2_{\text{proj}} \sqcup \ldots \sqcup G^n_{\text{proj}} \) if \( I = \{1, \ldots, n\} \). The mergeability, \( T_1 \sqcup T_2 \), is defined by \( T \sqcup T = T \) and the following axiom based on (60). Let \( \hat{\dagger} \in \{!, ?, \}. \)

\[
q \hat{\dagger} \{ l_i(x_i : S_i) \langle A_i \rangle . T_i \} \in I \sqcup q \hat{\dagger} \{ l'_j(x'_j : S'_j) \langle A'_j \rangle . T'_j \} \in J = \]

\[
q \hat{\dagger} \{ l_k(x_k : S_k) \langle A_k \rangle . T_k \} \in k \in I \sqcup q \hat{\dagger} \{ l'_k(x'_k : S'_k) \langle A'_k \rangle . T'_k \} \in k \in J \sqcup \]

\[
q \hat{\dagger} \{ l_k(x_k : S_k) \langle A_k \cap A'_k \rangle . T_k \sqcup T'_k \} \in k \in I \cap J
\]

when \( \forall k \in I \cap J, S_k = S'_k \). Then we close the local specification context, defined in Definition 6.6.7 \( \mathcal{J}[T_1] \sqcup \mathcal{J}[T_1] = \mathcal{J}[T_1 \sqcup T_2] \).

In rule 1 for an output the projection of a predicate \( A \) consists of \( A \) itself. Note that if \( G \) is well-formed then \( p_1 \) knows all variables in \( A \). For a receiver, it is not sufficient to verify the non-violation of the current predicate only. Consider the following global
specification:

\[ \text{Seller} \rightarrow \text{Buyer} : (\text{cost} : \text{Int}) \langle \langle \text{cost} > 10 \rangle \rangle \]
\[ \text{Buyer} \rightarrow \text{Bank} : (\text{pay} : \text{Int}) \langle \langle \text{pay} \geq \text{cost} \rangle \rangle \]

The predicate \( \text{pay} \geq \text{cost} \) is meaningless to \( \text{Bank} \) since \( \text{Bank} \) does not know \( \text{cost} \); rather the projection on \( \text{Bank} \) should be \( \text{Buyer}? (\text{pay} : \text{Int}) \langle \langle \exists \text{cost}(\text{cost} > 10 \land \text{pay} \geq \text{cost}) \rangle \rangle \), which incorporates the constraint between \( \text{Buyer} \) and \( \text{Seller} \). Thus rule 1 projects all the past predicates while hiding incorporating the constraints on interactions \( p_2 \) does not participate through existential quantification.

In rule 3, the case when \( p \notin \text{role}(G) \), then it returns \text{end} for ending this session. For example, as we project \( \mu_t.p \rightarrow q : (x : \text{int}).t \) to role \( r \), and \( r \neq p \) and \( r \neq q \), the recursion should terminate by denoting with \text{end}. Other rules are straightforward.

According to (22), the projections of a well-formed global assertion are also well-asserted. In Example 6.2.4 global specification \( G_{IC} \) is well-formed and well-asserted, then it is projectable and the endpoint specifications projected from \( G_{IC} \) are all well-asserted. The lemma proposed and proved in (22) is mentioned below:

**Lemma 6.5.2.** If \( G \) is well-formed then, for all predicates \( A_G, A_T \) such that \( A_T \supset A_G \) and all \( p \in \text{role}(G) \),

\[ GSat(G, A_G) \supset GSat(G \upharpoonright p, A_T) \]

### 6.6 Permutation of Specifications

The permutation mechanism is introduced for runtime monitoring, which needs to verify a non-deterministic sequence of actions due to the asynchronous interactions among processes and monitors.

In this section, we formalise the notion of minimum permutations for monitors. The key idea is to “permute up” an action which is in effect not suppressed by another action to the top, without affecting other actions. Such an action which eventually moves to the top can originally occur in many places in an assertion: These occurrences are merged into one when a sequence of permutations are applied. Here firstly introduces several preliminary notions.

**Definition 6.6.1 (global specification context).** A global specification context \( T \)
6.6 Permutation of Specifications

is a global specification with a hole, whose grammar is defined as:

\[
\mathcal{S}[] ::= [ ] | \mathcal{S}[] | G' | \mathcal{S}]
\]

Then \(\mathcal{S}[G]\) denotes the result of filling the hole in the global specification context \(\mathcal{S}\) with global specification \(G\). Whenever write \(\mathcal{S}[G]\), \(\mathcal{S}[G]\) is assumed well-formed. Note that \([ ]\) defines the identity function, i.e. \([ ] = G\).

Note that there is no need for having \(\mu_t.\mathcal{S}[ ]\) because such a recursion can always be unfolded into each component.

**Definition 6.6.2.** Define a closed global specification \(G\) is prime if \(G \neq \text{end}\) and \(G = G_1 | G_2\) implies one of \(G_i, i = \{1, 2\}\) is end. If \(G\) is a prime specification, then the initial action of \(G\) is the action at the top of \(G\). For a non-prime \(G\), its initial actions are those of its prime components. The initial action of a closed local specification \(T\) is defined similarly.

**Example 6.6.3.** Let

\[G = p_1 \rightarrow q_1 : \{l_i(x_i : S_i)\langle A_i\rangle\}.p_2 \rightarrow q_2 : \{l_j'(x_j' : S_j')\langle A_j'\rangle.G_j'\}_j \in I\].\]

The initial action of \(G\) is \(p_1 \rightarrow q_1 : \{l_i(x_i : S_i)\langle A_i\rangle\}_i \in I\). Another example is, let \(G = G_1 | G_2, G_1 = p_1 \rightarrow q_1 : \{l_i(x_i : S_i)\langle A_i\rangle.G_i\}_i \in I\), and \(G_2 = p_2 \rightarrow q_2 : \{l_j'(x_j' : S_j')\langle A_j'\rangle.G_j'\}_j \in I\). The initial actions of \(G\) are \(p_1 \rightarrow q_1 : \{l_i(x_i : S_i)\langle A_i\rangle\}_i \in I\) and \(p_2 \rightarrow q_2 : \{l_j'(x_j' : S_j')\langle A_j'\rangle\}_j \in I\).

The idea of marking actions in global/local specifications is introduced, so that the effect of each permutation can be tracked. Hereafter, the specification context also includes the marked actions.

**Definition 6.6.4 (specifications with marked actions).**

1. A global specification with marked actions or for brevity, a marked global specification, is a global specification some of whose action occurrences are underlined actions, denoted by underlining the initial part of the action. Write \((G, \ldots)\) for marked global specifications. The underlined actions in \(G\) are called permutation candidates of \(G\), e.g. \(\mathcal{S}[p \rightarrow q : \{l_i(x_i : S_i)\langle A_i\rangle.G_i\}_i \in I]\) is a marked global specification, and \(p \rightarrow q\) is its permutation candidate.
2. Similarly, define marked local specifications (\(T_i\ldots\)) as e.g.

\[T[p\{l_i(x_i:S_i)\langle\langle A_i\rangle\},T_i\}_{i\in I}],\]

where \(p\) is its permutation candidate.

First define a unit permutation, which is a permutation of two nested branchings defined only when they are independent, i.e. there is no causal order between two interactions (no causality through either ordered actions from the same sender to the same receiver, or ordered actions linked by a receiver becoming a sender in the second action).

**Definition 6.6.5 (global unit permutation).** A unit permutation of marked global specifications is defined by the axiom below:

\[\mathcal{G}[p_1 \rightarrow p_2 : \{l_i(x_i:S_i)\langle\langle A_i\rangle\},G_{ij}\}_{i\in I} \sim^{-1} \mathcal{G}[p_3 \rightarrow p_4 : \{l'_j(x'_j:S'_j)\langle\langle A'_j\rangle\},G_{ij}\}_{j\in J} \rightarrow p_1 \rightarrow p_2 : \{l_i(x_i:S_i)\langle\langle A_i\rangle\},G_{ij}\}_{i\in I} \}_{j\in J}\]

with the following conditions: if \((p_2 = p_4)\) then \((p_1 \neq p_3)\); if \((p_1 = p_4)\) then \((p_2 \neq p_3)\); if \((p_1 = p_3)\) then \((p_2 \neq p_4)\); or \(p_i\) pairwise distinct.

**Remark 6.6.6 (unit permutation of global specifications).**

1. Definition 6.6.5 demands each specification under permutation candidate, \(G_{ij}\), to be unmarked specifications (note the symbol \(G_{ij}\) is for an unmarked specification).

2. In the same definition, the inner actions to be permuted up, should have precisely the same branching labels. This condition is automatically ensured by projectability.

The second point above is significant in that, whenever there is no causality among actions, they automatically enable a unit permutation: An inner, nested but causally unsuppressed action can automatically be permuted up over another action which happens to be above it.

**Definition 6.6.7 (local specification context).** A local specification context \(\mathcal{T}[]\) is a local specification with a hole, whose grammar is defined as:

\[\mathcal{T}[] ::= [ ] | p?\{l_i(x_i:S_i)\langle\langle A_i\rangle\},T_1,\ldots,l_i(x_i:S_i)\langle\langle A_i\rangle\},T_i\}_{i\in I} \ldots, l_i(x_n:S_n)\langle\langle A_n\rangle\},T_n\} \]

\[| \quad p!\{l_i(x_1:S_1)\langle\langle A_1\rangle\},T_1,\ldots,l_i(x_n:S_n)\langle\langle A_n\rangle\},T_i\}_{i\in I} \ldots, l_i(x_n:S_n)\langle\langle A_n\rangle\},T_n\}\]
Then \( \mathcal{T}[T] \) denotes the result of filling the hole in the local specification context \( \mathcal{T} \) with global specification \( T \). Note that \([ ]\) defines the identity function, i.e. \( [T] = T \).

In the same way as for global specifications, define the unit permutations for local specifications. In this case, the causal order only occurs when there are two consecutive sending actions with the same target, or when there is an input action followed by an output action. These conditions precisely correspond to permutability in global specifications through projections.

**Definition 6.6.8 (local unit permutation).** The unit permutation of local (end-point) specifications by the axioms below, assuming \( p_1 \neq p_2 \):

\[
\mathcal{T}[p_1!?\{l_i(x_i : S_i)\langle \langle A_i \rangle \rangle .p_2!?\{l'_j(x'_j : S'_j)\langle \langle A'_j \rangle \rangle .T_{ij}\}_{j \in I}\}_{i \in I}]
\rightleftarrows^1
\mathcal{T}[p_2!?\{l'_j(x'_j : S'_j)\langle \langle A'_j \rangle \rangle .p_1!?\{l_i(x_i : S_i)\langle \langle A_i \rangle \rangle .T_{ij}\}_{j \in I}\}_{j \in I}]
\]

\[
\mathcal{T}[p_1?!\{l_i(x_i : S_i)\langle \langle A_i \rangle \rangle .p_2?!\{l'_j(x'_j : S'_j)\langle \langle A'_j \rangle \rangle .T_{ij}\}_{j \in I}\}_{i \in I}]
\rightleftarrows^1
\mathcal{T}[p_2?!\{l'_j(x'_j : S'_j)\langle \langle A'_j \rangle \rangle .p_1?!\{l_i(x_i : S_i)\langle \langle A_i \rangle \rangle .T_{ij}\}_{i \in I}\}_{j \in I}]
\]

\[
\mathcal{T}[p_1?!\{l_i(x_i : S_i)\langle \langle A_i \rangle \rangle .p_2?!\{l'_j(x'_j : S'_j)\langle \langle A'_j \rangle \rangle .T_{ij}\}_{j \in I}\}_{i \in I}]
\rightleftarrows^1
\mathcal{T}[p_2?!\{l'_j(x'_j : S'_j)\langle \langle A'_j \rangle \rangle .p_1?!\{l_i(x_i : S_i)\langle \langle A_i \rangle \rangle .T_{ij}\}_{i \in I}\}_{j \in I}]
\]

**Remark 6.6.9 (unit permutation of local specifications).**

1. As before, demand each specification under permutation candidate to be unmarked.

2. The inner (lower) actions have precisely the same branching labels, automatically ensured among projected local specifications.

We introduce the minimum permutation relation in the follows. Below write unmark(\( G \)) for the result of taking off marks from the actions in \( G \), similarly for unmark(\( T \)).

**Definition 6.6.10 (minimum permutation).** Let \( G \) and \( G' \) be marked. Then define the minimum permutation from \( G \) to \( G' \), denoted \( G \rightleftarrows G' \), by the following induction.

\[
\text{all and only marked action in } G \text{ is one of its initial actions,}
\]

\[
G \rightleftarrows G' \rangle G \rightleftarrows G'' \rightleftarrows G' \]

107
6. SPECIFICATIONS FOR GOVERNANCE

Then define $G \bowtie G'$ by:

$$G = \text{unmark}(G) \quad G \bowtie G' \quad G' = \text{unmark}(G')$$

Similarly define $T \bowtie T'$ by:

all and only marked action in $T$ is its initial action.

$$T \bowtie T'$$

As before, define $T \bowtie T'$ by unmarking.

Basic properties of the minimum permutations follow. In brief, these results say that marking does not determine minimum permutations.

**Proposition 6.6.11 (minimum permutation to the top).**

1. The minimum permutation to permute a marked action in $G$ to the top is inductively applying Definition 6.6.10 until the marked action is at the top of $G$.

2. Whenever $G \bowtie G'$ and $G' \bowtie G''$, there is always a unique marked action in $G''$, which is one of its initial actions. Similarly whenever $T \bowtie T'$, there is always a unique marked action in $T'$, which is its initial action.

3. If $G \bowtie G_1', G \bowtie G_2', G' \bowtie G_1'$, and $G' \bowtie G_2'$, then $G_1 = G_2$. Similarly if $T \bowtie T_1'$ and $T \bowtie T_2'$, then $T_1 = T_2$.

4. If $G \bowtie G'$ and $\text{unmark}(G) = G$, then there is a unique $G'$ such that $G \bowtie G'$ and $\text{unmark}(G') = G'$. Similarly, if $T \bowtie T'$ and $\text{unmark}(T) = T$, then there is a unique $T'$ such that $T \bowtie T'$ and $\text{unmark}(T') = T'$.

By Proposition 6.6.11 write $G \bowtie p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle.G_i \}_{i \in I}$ to indicate a unique permutation from $G$: Just identifying the resulting top action is enough to determine the minimum permutation.
The Calculus of Dynamic Asynchronous Monitoring

Overview  Based on the calculus proposed in Chapters 5 and the specification language introduced in Chapter 6, this chapter introduces a realistic yet formal model of the monitored network in which strong safety properties result from local runtime verification and enforcement of possibly untrusted endpoints, rather than from static checking. The monitoring model proposed here is proven to guarantee the satisfaction of global specifications, focusing on the following properties: The dynamic local and global safety through stating local and global communication safety (Theorems 7.4.3 and 7.4.16); the external local and global monitoring transparency (Theorems 7.4.5 and 7.4.17); and session fidelity (Theorem 7.4.28) in the presence of possibly ill-behaved processes.

We start from Section 7.1, in which motivating examples and a general framework for monitoring are introduced. Section 7.2 is one main part of this chapter: It introduces the syntax and semantics of external monitors and provides viable and efficient reference semantics for monitor implementers. Then it introduces the syntax and semantics of monitor-off, which can be viewed as a gateway. It finally introduces the syntax and semantics of monitored network, which consists of local monitored processes and the global transport. Section 7.3 provides two use cases to illustrate how monitoring works. As another main part of this chapter, Section 7.4 states and proves (the full proofs are in Appendix B) the theorems of local and global safety, local and global transparency, and session fidelity. Section 7.5 introduces a global observer, denoted by $E$, which formalises the global observable interactions from the global point of view. We can also apply $E$
to ensure global safety and session-fidelity through observing the global transport and
the collection of network monitors.

7.1 Motivating Example and the Framework of Monitoring

Many non-trivial safety properties of distributed applications can only be guaranteed
when the endpoints are reciprocally assured of their cooperation (i.e. after static check-
ing). For example, by the adherence to an application-level protocol (“message choreo-
graphy”), they need to satisfy global invariants over the behaviour of multiple peers. Many global invariants can only be effectively assured through runtime local ver-
ification since a centralised verification is unfeasible in large-scale distributed systems,
due to e.g. latency.

7.1.1 Motivating Example

In this section, two examples are introduced to show the effectiveness of runtime local
verification. One example shows that, based on the specifications defined in Chapter
during runtime, a monitor can easily detect a possible malicious sequence of actions,
which can not be statically checked. Another example shows that centralised runtime
verification can not ensure a sequence of actions meet the intended requirements of local
processes due to the latency of routing.

Assume the global specification satisfying the consistency principles is given below:

\[
G_1 = \begin{array}{ll}
  p \rightarrow p_1 : (x : \text{int})\langle x > 0 \rangle \cdot p_1 \rightarrow p_2 : (x : \text{int})\langle \text{true} \rangle .
  \\
  p \rightarrow p_2 : (y : \text{int})\langle y > x > 0 \rangle .
\end{array}
\]

applying the projection rules defined in Definition 6.5.1, the local specification of the
process playing role \( p \) in session \( s \) is:

\[
s[p] : p_1!(x : \text{int})\langle x > 0 \rangle . p_2!(y : \text{int})\langle y > x > 0 \rangle .
\]

The global invariants of this local specification are (I) the possible sequence of ac-
tions of the local process playing \( s[p] \) is either \( s[p, p_1]!(v_1) \cdot s[p, p_2]!(v_2) \) or \( s[p, p_2]!(v_2) \cdot 
(\cdot s[p, p_1]!(v_1) \rangle \), and (II) the content of message sending to role \( p_2 \) should be bigger than
the one to role \( p_1 \). Although this specification is statically valid according to well-
formedness and well-assertedness, and it can be statically realised that there are two
7.1 Motivating Example and the Framework of Monitoring

such possible sequences of actions, it is not enough for safety assurance. When untrusted components may exist in the network, during runtime, as a monitor observes the trace $s[p, p_2]!\langle v_2 \rangle \cdot s[p, p_1]!\langle v_1 \rangle$ sent from $s[p]$, according to Definition 7.2.2 (defined later in Section 7.2.1.2), it is not valid because $v_2 > x > 0 \downarrow \text{false}$ since $x$ is empty when the monitor observes this action. A monitor should reject it or buffer the content of $y$, which is $v_2$, sent to $p_2$ and wait for the content of $x$ to decide if the first coming interaction $s[p, p_1]!\langle v_1 \rangle$ is valid. Otherwise, if this sequence of actions is sent from a malicious process and monitor does not take off it, it may cause damages to the processes playing role $p_1$ and $p_2$ due to the contents do not meet the agreed conditions.

The following example says that the process playing role $p$ is feeding the process playing role $q$ with numbers:

$$G_2 = p \rightarrow q : (x : \text{int})\langle x > 0 \rangle.p \rightarrow q : (y : \text{int})\langle \text{true} \rangle.p \rightarrow q : (z : \text{int})\langle z > \text{max}(x, y) \rangle.\text{end}$$

The local specification projected from $G_2$ on the endpoint playing role $q$, with the assumption that it joins session $s'$, is

$$s'[q] : p?\langle x : \text{int} \rangle\langle x > 0 \rangle.p?\langle y : \text{int} \rangle\langle \text{true} \rangle.p?\langle z : \text{int} \rangle\langle z > \text{max}(x, y) \rangle.\text{end}$$

Since the order of inputted numbers may affect the computation at the process playing role $q$, e.g. role $q$ inputs data for real-time experiment, this scenario restricts the sequence of actions, each of which can not be permuted. A centralised verification is powerless in this case because even it approves a sequence of actions, e.g. which is

$$s'[p, q]?\langle 3 \rangle.s'[p, q]?\langle 2 \rangle.s'[p, q]?\langle 5 \rangle$$

when these actions arrive at process playing role $q$, due to the possible routing latency, the sequence of actions may become

$$s'[p, q]?\langle 5 \rangle.s'[p, q]?\langle 3 \rangle.s'[p, q]?\langle 2 \rangle$$

which should be rejected by the local monitor guarding the process playing role $q$. This example shows that, in distributed systems, centralised monitor is not reliable because some tasks can only be ensured at local monitors.
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

7.1.2 Monitoring Framework

We propose a monitoring framework as shown in Figure 7.1, which is motivated from the understanding of distributed infrastructures such as those for E-Science \((129)\) and the infrastructure behind large-scale web portals. In this framework, each endpoint is linked to the network through an external monitor, which acts as a unique entry point to the infrastructure. In Figure 7.1, a monitor can guard more than one principal, who may have more than one process or endpoint. As a new comer joins the distributed systems, a monitor is generated by the system to guard it. When principals establish a session, e.g. Principals \(A_1\), \(B\), and \(D\) generate session \(s\) and play roles as \(Buyer\), \(Seller\) and \(Broker\), corresponding local monitors guarding each domain inform this session creation information to distributed routers, which are responsible for global transport. In this thesis, the routers are not abstracted and formalised because our focus is on specifying specifications to verify interactions.

![Monitoring Architecture](image)

Figure 7.1: Monitoring Architecture
7.2 The Calculus of Monitoring

Figure 7.2: Monitoring for One Session $s$ with the Specification: OO Instrument Commands

Figure 7.2 illustrates how global and local specifications are used by monitors to ensure the interactions of the use case of OO Instrument Command introduced in Chapter 5. In this scenario, there are five principals, each of which runs a process, involving in the network. To ensure global safety, monitors use projected endpoint specifications to detect whether or not *asynchronously* incoming and outgoing messages obey the stipulated specification, taking appropriate actions as necessary such as dropping illegal messages.

7.2 The Calculus of Monitoring

This section introduces a calculus for distributed monitoring, where every endpoint process is guarded by a corresponding system monitor. The syntax is divided into two parts: Section 7.2.1 for local monitors $M$ which check the correctness of endpoints’ behaviours through checking the incoming and outgoing messages (w.r.t. a set of endpoint specifications) and drop the wrong ones; and Section 7.2.4 for the distributed network $N$ which consists of one or more monitored local processes $M[P]$ and global queue containing pending messages sent by one monitored process but not yet received by another.
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

\[
M ::= \Gamma, \Delta \quad \text{monitor}
\]
\[
\Delta ::= \emptyset | \Delta, s[p] : T | \Delta, s[p]^* : T \quad \text{session environment}
\]
\[
\Gamma ::= \emptyset | \Gamma, a : \text{mode}(G[p]) \quad \text{shared environment}
\]
\[
\text{mode} ::= I | O | IO \quad \text{I/O mode}
\]

Figure 7.3: Monitors (M)

7.2.1 The Syntax and Semantics of Local External Monitors

Every process is associated with a corresponding external monitor that manages its interactions with the network (hence with other peers) by inspecting outgoing and incoming messages. In the following sections, we define the contents and the dynamic configurations of a monitor. A monitor uses these contents, which are specifications of local processes, as knowledge and follows the semantics of specifications to dynamically judge the behaviours of local processes.

7.2.1.1 The Syntax of Monitors

The syntax of monitors is defined in Figure 7.3. \( \Gamma \) is the same one defined in Definition 6.3.7. A monitor \( M = \Gamma, \Delta \) checks two kinds of messages: (I) Capability exchanges at shared channels through invitations, and (II) session messages transmitted through session channels. The specification for a monitor consists of two specifying environments, one for shared channels (\( \Gamma \)) and one for sessions (\( \Delta \)). In \( \Delta \), let \( s[p] : T \) represent a capability which is owned by the local process but is not active yet (i.e., capability \( s[p] : T \) can be sent to invite another process); while \( s[p]^* : T \) represents an active capability after the monitored process has joined the session with role \( p \) (i.e. playing session-role \( s[p] \)). Note that, as a process joins a session-role, say \( s[p]^* : T \), it can no more delegate this capability of playing \( s[p] \) to another endpoint. \( \Delta \) associates each capability, represented by \( s[p] \), to an endpoint specification \( T \) which specifies the behaviour of a particular role in a session.

For a monitor \( M = \Gamma, \Delta \), to extract the elements governed by it, theoretically we can use \( \text{dom}(\Gamma) \) to extract all shared names \( a, b, ... \) and use \( \text{dom}(\Delta) \) to extract all session-role \( s[p], s'[q], ... \) which are governed by \( M \). They give us sufficient information for what endpoints that \( M \) governs: Shared names \( a, b, ... \) with input mode \( I \), which represent endpoint’s input communication channel, give us the positions of the endpoints; while
7.2 The Calculus of Monitoring

$s[p], s'[q],...$ as session-roles give us which session participants are communicating to each other.

To runtime monitor non-deterministic sequences of actions, define the initial state of variables in a monitor as below:

**Definition 7.2.1.** Assume $M = \Gamma, \Delta$. As an element of $\Gamma$ or $\Delta$ is initiated in a monitor, the value of any variable, say $x$, occurring in this element is empty, denoted by $x \mapsto \emptyset$.

Note that, the elements of a monitor can be $\emptyset$, can have input mode shared names, e.g. $a : \text{im}(G[p])$, or can have public session-roles, e.g. $s[p] : T$. When an endpoint process creates a session instance by doing $\exists(s[p] : G)$ (see Section 5.3.1 in Chapter 5), its corresponding monitor learns that a new session is obeying global specification $G$. At the same time, it also learns the specification of $s[p]$ from the projection of $G$ at role $p$.

The asynchronous transport between a process (as a session role $s[p]$) and its monitor is formalised by (local) queue, denoted by $s[p] : h$. The global transport among monitors for a session is formalised by global queue, denoted simply by $H$.

### 7.2.1.2 The Semantics of Monitors

The semantics of monitors show the dynamic configurations of monitors. It is given as a labelled transition system (LTS) following the standard interpretation of types in process calculi. This system is used to control behaviours of processes. $M \xrightarrow{\ell} M'$ only if $\ell$ is a legal action (i.e., that a process should be allowed to perform by monitor $M$).

The following definition is proposed for a monitor to correctly evaluate an assertion $A$.

**Definition 7.2.2 (evaluable assertion).**

Define $A$ is evaluable whenever $\forall x \in \text{var}(A)$, $x$ is not empty. When $A$ is not evaluable, $A \Downarrow \text{false}$.

Figure 7.4 defines the LTS of monitors. Action labels are as same as those defined in Equation 5.1 in Chapter 5. Rule [New] approves an input-mode (i.e. mode of im) shared name creation with specification $a : \text{im}(G[p]), \text{im} \in \{I, IO\}$ whenever name $a$ is fresh to the monitor. Note that, as $a : \text{im}(G[p])$ is fresh to a local monitor, this name is new to the network. The reason is explained in Convention 7.4.15.

115
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

\[ \frac{\text{im} \in \{1, 10\}, a \notin \text{dom}(M)}{M \xrightarrow{\text{new \ a \ im}(G[p])} M, a : \text{im}(G[p])} \]

\[ s \notin \text{dom}(M), \ \text{om} = \{0, 10\}, \ \forall i \in I, p_i \in \text{role}(G), \ G \text{ is well-formed} \]

\[ M, a : \text{om}(G[p_j]), \ s[p_j] : T \xrightarrow{\pi(s[p_j], G)} M, a : \text{om}(G[p_j]) \]

\[ T = G \mid p_j, \ \text{om} = \{0, 10\} \]

\[ M, a : \text{im}(G[p]), s[p] : T \xrightarrow{\pi(s[p], G)} M, a : \text{im}(G[p]), s[p] : T \]

\[ s \notin \text{dom}(M), \ im \in \{1, 10\} \]

\[ M, a : \text{im}(G[p]), s[p] : T \xrightarrow{\alpha(s[p], G)} M, a : \text{im}(G[p]), s[p] : T \]

\[ M, s[p] : T \xrightarrow{\text{join}(s[p])} M, s[p]^* : T \]

\[ M \vdash v : S_j, A_j \{v/x_j\} \downarrow \text{true}, \ j \in I, T \cap p_j \{l_i(x_i : S_i) \langle A_i \rangle T_i\}_{i \in I} \]

\[ M, s[p_1]^* : T \xrightarrow{\text{join}(x_j)} M, s[p_1]^* : T_j \{a \rightarrow x_j\} \]

\[ M \vdash a : S_j, A_j \downarrow \text{true}, \ j \in I, T \cap p_j \{l_i(x_i : S_i) \langle A_i \rangle T_i\}_{i \in I} \]

\[ M, s[p_1]^* : T \xrightarrow{\text{join}(x_j)} M, s[p_1]^* : T_j \{a \rightarrow x_j\} \]

\[ M \vdash v : S_j, A_j \{v/x_j\} \downarrow \text{true}, \ j \in I, T \cap p_j \{l_i(x_i : S_i) \langle A_i \rangle T_i\}_{i \in I} \]

\[ M, s[p_2]^* : T \xrightarrow{\text{join}(x_j)} M, s[p_2]^* : T_j \{a \rightarrow x_j\} \]

\[ S_j = \text{mode}(G\{p\}), A_j \downarrow \text{true}, \ j \in I, T \cap p_j \{l_i(x_i : S_i) \langle A_i \rangle T_i\}_{i \in I} \]

\[ M, s[p_2]^* : T \xrightarrow{\text{join}(x_j)} M, a : 0(G\{p\}), s[p_2]^* : T_j \{a \rightarrow x_j\} \]

\[ M_1 \xrightarrow{\tau} M'_1 \]

\[ M_1 \parallel M_2 \xrightarrow{\tau} M'_1 \parallel M'_2 \]

**Figure 7.4:** The Labelled Transition System of Monitors
Rule [Req-n] is for newing session \( s \), which is specified under specification \( G \), and at the same time inviting the endpoint represented by shared channel \( a \) to play session-role \( s[p_j] \) specified under the local specification \( G \upharpoonright p_j \). It proves the action \( \pi(s[p_j] \cdot G) \) when \( s \) is fresh to the monitor \( M \) and \( M \) has the knowledge of \( a : \text{om}(G[p]) \), \( \text{om} = \{0,10\} \). Again, the local monitor can ensure this session name is globally new with the same reason explained for rule [New]. As the action is approved, it adds the projections from \( G \) on each role \( p_i \in \text{role}(G) \), endowing the local process with the capability \( s[p_j] : G \upharpoonright p_i \) of having behaviours of the role in \( G \), and remove the capability of session-role \( s[p_j] : T \), where \( T = G \upharpoonright p_j \). Rule [Req-f] is for a free request at \( a \). As a monitor has the knowledge of \( a : \text{om}(G[p]) \) and the capability of \( s[p_j] : T \), the monitor approves this invitation and, since this capability has been sent out, relinquishes the capability of \( s[p_j] : T \); rule [Acc-f] is its dual by asking the capability of \( a : \text{im}(G[p]) \), \( \text{im} \in \{1,10\} \). Rule [Acc-n] is very similar to rule [Acc-f] except that [Acc-n] requires that session \( s \) is fresh to \( M \). Rule [Join] activates the capability of \( s[p] \), denoted by \( s[p]^{\bullet} \). Only as a capability is denoted by \( s[p]^{\bullet} \), it fires and executes actions. In [Sel], [SelN], [Bra] and [BraN], permutation mechanism is applied, denoted by \( T \curvearrowright T' \). A sound permutation changes the order of actions to capture the semantics of asynchronously arriving messages without affecting causally related actions. Consider a well-formed global specification

\[
p_2 \rightarrow p_1 : (x:S)(\langle A \rangle_{T'}) p_3 \rightarrow p_1 : (x':S')(\langle A' \rangle_{T'}).G, \quad p_1 \neq p_2 \neq p_3
\]

In an asynchronous environment, the message carrying \( x' \) may arrive at \( p_1 \) earlier than the message carrying \( x \). Naturally, if \( A \) and \( A' \) have no causal relations in \( x \) and \( x' \), \( p_1 \)'s monitor should be able to accept the messages from \( p_2 \) and \( p_3 \) in any order. \( T \curvearrowright T' \) is therefore useful for helping a monitor to evaluate message passing.

With the mechanism of permutations, [Sel] says that, if the local specification of \( s[p_1]^{\bullet} \) can be permuted to \( p_2 ! \{l_i(x_i:S_i)(\langle A_i \rangle_{T_i})\}_{i \in I} \), the outgoing message with label \( l_j \) sent from \( p_1 \) to \( p_2 \), as far as it satisfies formula \( A_j \{v/x_j\} \), is approved by the monitor which prepares the next (incoming or outgoing) message with local specification \( T_j \).

[SelN] is similar to [Sel] except that it is particularly for sending a shared name \( a \). Note that \( A_j \) should be always true since a name can not be evaluated in a predicate. Rule [Bra] is the symmetric (input) counterpart to [Sel], while [BraN] is the rule for receiving a shared name \( a \). It is dual to the rule [SelN].
Note that, in [BrN], \( a \) is added into a monitor with \( \emptyset \)-mode no matter what the original mode of \( a \) is, i.e. it is never added with \( I \)-mode or \( IO \)-mode. Together with the rule [SaN], they imply that, when a shared name is passed from a sender to a receiver through session interactions, the sender does not lose the capability/knowledge of the shared name with its original I/O mode. Therefore, passing a name in session interactions is a propagation of the knowledge of the name. As Section 5.5.1 explained, the mobility is realised by passing session-roles but not by passing input-mode shared names.

Rule [PB] says that, when a monitor, say \( M_1 \), approves an action and becomes \( M'_1 \), this action is network-wise unique such that no other monitors observe this action at the same time because the session contained in this action is unique to the network.

The next section follows the illustration of the LTS of monitor-off \( M^\circ \), which can be viewed as gateways. Its formalism helps us to deepen the understanding about how floating messages can be routed from one endpoint to another. Compared with the semantics of monitor-off, we can realise the effects of monitors for guarding interactions.

### 7.2.2 The Syntax and Semantics of Monitor-off Gateway

Unmonitored networks are given by erasing the co-domain (sorts and specifications) from each monitor in a monitored network. The result of such erasure, the monitor which 'switches-off' the monitoring activity, acts simply as a gateway with information on local addresses, including a session endpoint, say \( s[p] \). Write \( \text{erase}(M) \) for the monitor-off obtained through this erasure of \( M \). Hereafter denote \( \text{erase}(M) \) as \( M^\circ \). This stripped-off \( M \) is called a monitor-off gateway \((M^\circ, M^\circ_1, \ldots)\). The syntax of monitor-off gateways is defined as follows:

\[
M^\circ ::= \emptyset | M^\circ, a | M^\circ, s[p] | M^\circ, s[p]^* 
\]

A gateway \( M^\circ \) is simply defined as removing the typing area from a \( M \).

The LTS of \( M^\circ \) is obtained by erasing the co-domain from each monitor in each rule in Figure 7.4. Below \( M^\circ, a \) indicates \( a \notin M^\circ \), similarly for \( M^\circ, s[p] \). The illustrations of each rules are as followings:

- [\( M^\circ - \text{tau} \)] \( M^\circ \) does nothing to a silent action \( \tau \).
7.2 The Calculus of Monitoring

Figure 7.5: The Labelled Transition System of Monitor-off

**[M₀-new a]** M₀ unisons a name a no matter it is “new” to M₀ or not. Because there is no monitor to specify the newed shared name is input-mode, even the mode is an output mode, M₀ also accepts the action. Thus **mode** is used here instead of using **im**.

**[M₀-req b/f]** By rule [M₀-req b], M₀ adds all session-roles of session s whether session s is new to M₀ or not. M₀ does not know any specification of capability of the roles in \{s[p]_1\}_i\in I \setminus \{j\}. Rule [M₀-req f] says s[p] is removed from M₀ via channel a when request happens.

**[M₀-acc b/f]** These two rules have same effects for two different actions a(s[p] : G) and a(s[p] : G). s[p] is added into M₀ through channel a with no conditions.

**[M₀-join]** M₀ activates the capability of role p in session s. M₀ announces it to the network that role p in session s is ready to start session interactions.

**[M₀-sel, -selN]** Rule [M₀-sel] and [M₀-selN] both say M₀ allows s[p₁, p₂]!l(v) or s[p₁, p₂]!l(a) when its endpoint is the sender p₁ in s.

**[M₀-bra]** As v is not a name, and M₀’s endpoint is the receiver p₂ in s, it approves.
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

[M°-braN] As M°’s endpoint is the receiver p2 in s, it approves it and adds a into M°.

Example 7.2.3 (M v.s. M°). Let \( M_1 \overset{\text{def}}{=} s[\text{p}_1] : p_2!(x : \text{Int})(x > 0).T \) and \( \ell = s[\text{p}_1, p_2]!(-10) \). Then \( M_1 \xrightarrow{\ell} \) but \( M_1 \not\xrightarrow{\ell} \) since the value -10 does not satisfy the predicate \( x > 0 \) attached to the endpoint specification for the session monitored by \( M_1 \). Similarly, for specification violations, if \( M_2 \overset{\text{def}}{=} s[\text{p}_1] : p_2!(x : \text{String})(\text{true}).T \) and \( \ell = s[\text{p}_1, p_2]!(10) \) then \( M_2 \xrightarrow{\ell} \) but \( M_2 \not\xrightarrow{\ell} \).

7.2.3 The Syntax and Semantics of Monitored Processes

Write \( M[P] \) for \( P \) monitored by \( M \), called monitored process. The syntax of a monitored process is defined as a local process guarded by an external monitor.

**Definition 7.2.4.** Define \( M[P] \) as a monitored local process.

**Definition 7.2.5.** \( M[0] \overset{\text{def}}{=} 0 \).

The semantics of monitored processes is simply defined based on the semantics of local processes and monitors:

**Definition 7.2.6 (LTS of monitored process).** Let \( \ell \) be an action label. Then we define \( M_1[P_1] \xrightarrow{\ell} M_2[P_2] \) as the conjunction of \( P_1 \xrightarrow{\ell} P_2 \) and \( M_1 \xrightarrow{\ell} M_2 \):

\[
\frac{M_1 \xrightarrow{\ell} M_2, P_1 \xrightarrow{\ell} P_2}{M_1[P_1] \xrightarrow{\ell} M_2[P_2]}
\]

The LTS of \( P \) and \( M \) are respectively defined in Figure 5.4 (Chapter 5) and Figure 7.4. A local queue of a local process is abstracted for asynchronous monitoring purpose. During runtime, a local queue is part of a runtime process. Formally, we write

\[
M[P_{rt}] = M[P \mid s_{i_1}[p_j] : h_{i_1} \mid \ldots \mid s_{i_n}[p_k] : h_{i_n}]
\]

where \( s_{i_1}[p_j] : h_{i_1} \mid \ldots \mid s_{i_n}[p_k] : h_{i_n} \) are the local queues generated from participating sessions \( s_{i_1}, \ldots, s_{i_n} \) respectively for playing roles \( p_j, \ldots, p_k \).

**Example 7.2.7.** When a process, say \( P \), involves in a session \( s \) for playing role \( p \), during runtime, its runtime monitored process is

\[
M[P_{rt}] = M[P \mid s[p] : h]
\]
7.2 The Calculus of Monitoring

\[ N_s ::= M | M[P] | N_{s1} || N_{s2} | 0 | (\nu n)N_s\ n \in \{a,s\} \] monitored static network

\[ N ::= N_s | N_1 || N_2 | H | (\nu n)N\ n \in \{a,s\} \] monitored dynamic network

\[ H ::= \emptyset | m \cdot H \] global queue

\[ m ::= s(p,q,l(v)) | \pi(s[p] : G) \] message

Figure 7.6: The Syntax of the Monitored Network

where \( M \) should contain the local specification of \( s[p] \) such that \( M = \Gamma, \Delta, s[p] : T \).

Example 7.2.8. Let \( P = s[p_1, p_2]!(100); P' | s[p_1] : \emptyset \) be a process with an empty queue playing role \( p_1 \) in \( s \). Also let \( M_1 = s[p_1]^* : p_2(x : \text{Int})(x > 0).T \) be its local monitor. The communication happens in two steps. First, the message is spawn into the local queue as \( P \xrightarrow{\tau} P_2 \) with \( P_2 = P' | s[p_1] : s(p_1, p_2, (100)) \) hence, since \( M_1 \xrightarrow{\tau} M_1 \), then \( M_1[P] \xrightarrow{\tau} M_1[P_2] \). Second, the message is forwarded to the global queue as \( P_2 \xrightarrow{\ell} P' \) with \( s[p_1] : \emptyset \) with \( \ell = s[p_1, p_2]!(100) \); hence since \( M_1 \xrightarrow{\ell} s[p_1]^* : T \) then \( M_1[P] \xrightarrow{\ell} (s[p_1]^* : T)[P' | s[p_1] : \emptyset] \).

7.2.4 The Syntax and Semantics of the Monitored Network

Based on the syntax and semantics of the network and monitors introduced in Chapter 6 and Section 7.2.1, this section introduces the calculus of the monitored network.

7.2.4.1 The Syntax of the Monitored Network

The syntax of the monitored network is similar to the one of the un-monitored network but with notation \( N \) rather than \( N \) (i.e. un-monitored network), which is defined in Figure 5.5 Chapter 5. The syntax of the monitored network \((N, N', \ldots)\) is defined in Figure 7.6. The following definitions are for illustrating the syntax of the monitored network defined in Figure 7.6.

Definition 7.2.9 (Monitored Network). Assume a full (dynamic) network \( N \) is given. We say \( N \) is a monitored network coming from \( N \) if and only if \( \forall P \in N, P \) is guarded by a monitor \( M \in N \) such that \( M[P] \in N \).

Based on Definition 7.2.9 we define a monitored process more precisely:

Definition 7.2.10. Assume \( N \) is a monitored network coming from \( N \). \( M[P] \in N \) if and only if \( N \equiv_N (\nu \tilde{n})(M[P] || N') \) for some names \( \tilde{n} \).
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

The structural congruency over the monitored network is defined as same as the one of the network (see Definition 5.4.2).

The composability and the parallel composition of two monitored networks are defined as same as those defined in Definitions 5.4.2 and 5.4.4. A monitored network represents a network of processes and their monitors, together with messages in transit: They are interaction message, i.e. \( s(p, q, l(v)) \), and invitation, i.e. \( \pi(s[p] : G) \). Both \( s(p, q, l(v)) \) and \( \pi(s[p] : G) \) are introduced in Figure 5.5 Chapter 5. Note that, without loss of generality, the global queue is shared by all processes participating in the network.

7.2.4.2 The Reduction Rules of the Monitored Network

Before introducing the reduction rules of the monitored network, one observation is noted:

Remark 7.2.11. The labelled transition systems (LTS) of local monitored processes, which are parts of the monitored network, from the global viewpoint, are reductions rules of the monitored network.

Globally, the actions happening at local processes are marginal, which are network-wise invisible; the visible actions can be and can only be observed by the global transport. Therefore, the actions happening in Figure 7.4 are globally invisible: they are reductions of the network. This observation corresponds to Remark 5.4.7 in Chapter 5.

The reduction rules of the monitored network is defined in Figure 7.7. In each rule except \([\text{Proc}]\), the (else) case is when the monitor detects a violation w.r.t. specifications by the current action; for this case, \( \mathcal{M} \) simply drops such message. Each rule corresponds to a rule of monitor semantics defined in Figure 7.4. Rule \([\text{New}]\) creates a fresh (bound) input-mode shared name, where \( \text{im} \in \{I, IO\} \). In rules \([\text{REQ-B/F -OUT, ACC-B/F -IN}]\), monitor \( \mathcal{M} \) checks outgoing and incoming invitations. \([\text{REQ-B/F -OUT}]\) forwards outgoing invitations, which are still local to a process, to the external environment (dually for \([\text{ACC-B/F -IN}]\) with incoming invitations). Particularly, rules \([\text{REQ-B-OUT}]\) and \([\text{ACC-B-IN}]\) also check if session \( s \) is new to the endpoint process. Note that \([\text{REQ-B-OUT}]\) defines that, as error happens, the process following the bound request \( \overline{u}(s[p] : G) \) is completely taken off:

\[
\mathcal{M}[\overline{u}(s[p] : G).P] \parallel H \rightarrow \mathcal{M}[0] \parallel H
\]
7.2 The Calculus of Monitoring

<table>
<thead>
<tr>
<th>PROC</th>
<th>( \mathcal{M}[P] \rightarrow \mathcal{M}[P'] )</th>
<th>(( P \rightarrow P' ))</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW-A</td>
<td>( \mathcal{M}[\text{new } a : \text{in}(G[p])].P \rightarrow { (a)\mathcal{M}'[P] } \mathcal{M}[0] )</td>
<td>(( \mathcal{M}[\text{new } a : \text{in}(G[p])].\mathcal{M}' )) (else)</td>
</tr>
<tr>
<td>REQ-B-OUT</td>
<td>( \mathcal{M}[\pi(s[p]) : G].P</td>
<td></td>
</tr>
<tr>
<td>REQ-F-OUT</td>
<td>( \mathcal{M}[\pi(s[p]) : G].P</td>
<td></td>
</tr>
<tr>
<td>ACC-B-IN</td>
<td>( \mathcal{M}[0]</td>
<td></td>
</tr>
<tr>
<td>ACC-F-IN</td>
<td>( \mathcal{M}[0]</td>
<td></td>
</tr>
<tr>
<td>JOIN</td>
<td>( \mathcal{M}[\text{join}(s[p]).P] \rightarrow { \mathcal{M}'[P</td>
<td>s[p] : \emptyset] } \mathcal{M}[P] )</td>
</tr>
<tr>
<td>SEL-OUT</td>
<td>( \mathcal{M}[s[p_1] : s(p_1, p_2, l(v)) \cdot h]</td>
<td></td>
</tr>
<tr>
<td>BRA-IN</td>
<td>( \mathcal{M}[s[p_2] : h]</td>
<td></td>
</tr>
<tr>
<td>PAR, RES, STR</td>
<td>( N_1 \rightarrow N'_1 ) ( N_2 \rightarrow N'_2 ) ( (\text{par})N \rightarrow (\text{par})N' ) ( N \rightarrow N' ) ( N_0 \equiv N_0' )</td>
<td>( N_0 \rightarrow N_0' ) ( N_0' \equiv N' )</td>
</tr>
</tbody>
</table>

**Figure 7.7:** The Reduction Rules of the Monitored Network

It is because the following process may contain session \( s \) which is going to be created by \( \pi(s[p]) : G \) (refer to the example in Section 5.2.3 in Chapter 5). Rule [JOIN] creates a local queue particularly for session-role \( s[p] \). In [SEL-OUT], \( \mathcal{M} \) forwards a session message from a local queue \( s[p] \) to the global queue (dually for [BRA-IN]). Other rules are standard.

### 7.2.4.3 The Labelled Transition System of the Monitored Network

As \( \xi_g \) is particularly defined for the LTS of the global transport (see Figure 5.7) to indicate that these actions are globally observable actions, it is also used for the LTS of the monitored network in Figure 7.8 for representing that the transitions are globally observable up to monitoring. Thus we use \( \xi_g \) to describe the actions which can be observed by monitors and can affect the overall network. \( N \rightarrow^* N' \) represents the global observability of the network. Although, as mentioned before, the local actions are
invisible to the network, we can apply monitors’ knowledge to describe these invisible actions (w.r.t the network) as visible ones by using $\ell \rightarrow g$ because these actions actually have been observed by monitors.

**Remark 7.2.12.** A monitor, which positions between local processes and the network, is a *bridge* in between.

Therefore, global observability is the aggregate of what all monitors observe.

**Definition 7.2.13 (global observable transition).** Assume $N$ is a monitored network. $N \xrightarrow{\ell} g N'$ if and only there exists $M \in N$ s.t. $M \xrightarrow{\ell} M'$, $M' \in N'$.

Each rule in Figure 7.7 comes from the rule of LTS of monitored processes, in which a corresponding local monitor approves an action. The actions of monitored processes are globally invisible since they are marginal actions to the network. The dynamics of the monitored network, in particular how messages travel from an endpoint through the network to another, is formalised by the LTS defined in Figure 7.8. In all rules, we assume processes and the network obey the standard binding convention.

The rules in Figure 7.8 are dual to those in Figure 5.7 for the LTS of the global transport. In other words, the action which can be observed through the global transport is the duality of the observable action in the monitored network. Figure 7.8 lists the rules when the actions are valid, i.e. those have been approved by monitors. As the actions are invalid, as those shown in Figure 7.9, if they are output actions, they should be intercepted as they are still at the local; if they are input actions, they should be intercepted as they are still in the global queue. In other words, the reduction rules in Figure 7.7 have concluded every case.

All action rules defined in reduction rules of the monitored network are known by the monitors, and therefore are informed to the network by using $\ell \rightarrow g$. The illustrations of the LTS of the monitored network are as followings.

1. Rules $[\text{MG-REQ-F}]$, $[\text{MG-ACC-B}]$, $[\text{MG-ACC-F}]$, $[\text{MG-SEL}]$, $[\text{MG-BRA}]$, and $[\text{MG-IF-T/F}]$ just re-state the invisible action occurring at the local process. Here we particularly explain rule $[\text{MG-ACC-F}]$: When $\overline{a}(s[p]:G)$ enters the local process and is with the process in parallel, it must have been approved by the monitor; in other words, we should have $a : \text{im}(G[p]) \in M$, $\text{im} \in \{1,10\}$, where $a$ is able to play role $p$ specified under $G$. Therefore, $\overline{a}(s[p]:G) \mid a(s[p]:G)$: $P$ is a pattern-matching, which has already been checked by rule $[\text{MG-ACC-F-IN}]$ and will not affect process $P$. 

124
7.2 The Calculus of Monitoring

\[ \frac{\text{im} \in \{1, 10\}, M \xrightarrow{\text{new } a \xleftarrow{\text{im}(G[p])}} M'} M[P][\text{new } a \xrightarrow{\text{im}(G[p])} G(p)] \xrightarrow{\text{new } a \xleftarrow{\text{im}(G[p])}} \] [MG-new-a]

\[ M[\text{join}(s[p]), P] \xrightarrow{\text{join}(s[p])} M'[P \mid s[p], \emptyset] \] [MG-JOIN]

\[ M[\text{int}(s[p]), G] \xrightarrow{\text{int}(s[p])} M'[G \mid s[p]] \] [MG-REQ-F]

\[ M \xrightarrow{\text{int}(s[p])} M' \] [MG-REQ-B-OUT]

\[ M[P] \xrightarrow{\text{int}(s[p])} M'[P \mid s[p]] \] [MG-REQ-P-OUT]

\[ M[P] \xrightarrow{\text{int}(s[p])} M'[P \mid s[p]] \] [MG-REQ-P]

\[ M[P] \xrightarrow{\text{int}(s[p])} M'[P \mid s[p]] \] [MG-ACC-B]

\[ M[P] \xrightarrow{\text{int}(s[p])} M'[P \mid s[p]] \] [MG-ACC-F]

\[ M[P] \xrightarrow{\text{int}(s[p])} M'[P \mid s[p]] \] [MG-ACC-B-IN]

\[ M[P] \xrightarrow{\text{int}(s[p])} M'[P \mid s[p]] \] [MG-ACC-F-IN]

\[ M[s[p_1, p_2][\ell](v)]; P \mid s[p_1]; h] \xrightarrow{s} M[P \mid s[p_1]; h \cdot s(p_1, p_2, \ell(v))] \] [MG-SEL]

\[ M[s[p_1, p_2][\ell_1(x_1), P_1]; s[p_2]; s(p_1, p_2, \ell_2(v)); h] \xrightarrow{s} M[P \mid s[p_1]; h \cdot s(p_1, p_2, \ell_2(v))] \] [MG-BRA]

\[ M[P \mid s[p_1]; s(p_1, p_2, \ell_2(v)); h] \xrightarrow{s} M'[P \mid s[p_1]; h \cdot s(p_1, p_2, \ell_2(v))] \] [MG-SEL-OUT]

\[ M[P \mid s[p_2]; h \cdot s(p_1, p_2, \ell_2(v)) \cdot H] \xrightarrow{s} M'[P \mid s[p_2]; h \cdot s(p_1, p_2, \ell_2(v)) \cdot H] \] [MG-BRA-OUT]

\[ M[\text{if true then } P \text{ else } P \text{ else } Q] \xrightarrow{s} M[Q] \] [MG-IF-T/F]

\[ N_1 \xrightarrow{\ell} N_1' \text{ bn}(\ell) \cap \text{fn}(N_2) = \emptyset \text{ dest}(\ell) \not\subseteq \text{ep}(N_2) \] [MG-PAR]

\[ N \xrightarrow{\ell} N' \not\subseteq \text{ep}(N) \] [MG-RES, STR]

\[ N \xrightarrow{\ell} N' \not\subseteq \text{ep}(N) \] [MG-RES, STR]
### 7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

\[
\begin{align*}
\text{im} & \in \{I, IO\}, M \xrightarrow{\text{new a : im}(G[p])} M[\text{new a : im}(G[p])] \rightarrow_g M[P] & [\text{MG-new-a-err}] \\
M \xrightarrow{\pi(s[p] : G)} M[\pi(s[p] : G)] \rightarrow_g M[0] & [\text{MG-req-b-out-err}] \\
M \xrightarrow{\pi(s[p] : G)} M[\pi(s[p] : G)] \rightarrow_g M[0] & [\text{MG-req-f-out-err}] \\
M \xrightarrow{\alpha(s[p] : G)} M[P] \parallel \pi(s[p] : G) \cdot H \rightarrow_g M[P] \parallel H & [\text{MG-acc-b-in-err}] \\
M \xrightarrow{\alpha(s[p] : G)} M[P] \parallel \pi(s[p] : G) \cdot H \rightarrow_g M[P] \parallel H & [\text{MG-acc-f-in-err}] \\
M \xrightarrow{s[p_1;p_2]l(v)} M[P \mid s[p_1] : s(p_1, p_2, l(v)) \cdot h] \parallel H \rightarrow_g M[P \mid s[p_1] : h] \parallel H & [\text{MG-sel-out-err}] \\
M \xrightarrow{s[p_1;p_2]l(v)} M[P \mid s[p_2] : h] \parallel s(p_1, p_2, l(v)) \cdot H \rightarrow_g M[P \mid s[p_2] : h] \parallel H & [\text{MG-bra-in-err}] \\
\end{align*}
\]

**Figure 7.9:** The Labelled Transition System of the Monitored Network as Actions are Invalid
2. Rules $[MG\text{-new-a}]$ and $[MG\text{-join}]$ say that actions $\text{new } a : \text{im}(G[p])$ and $\text{join}(s[p])$ are approved/known by the local monitor, and they are the information that the monitor can inform the network.

3. Rule $[MG\text{-req-b-out}]$ says when the action is a bound request approved by the monitor, the session $s$ is newed and an invitation $\pi(s[p] : G)$ is outputted to the network.

4. Rule $[MG\text{-req-f-out}]$ says when the action is a free request approved by the monitor, then the invitation $\pi(s[p] : G)$ positioning inside the local process is permitted to output to the network.

5. Rules $[MG\text{-acc-b-in}]$ and $[MG\text{-acc-f-in}]$ are similar. They say that when the accept action is approved by the monitor, the invitation enters the endpoint process and is in parallel with the process.

6. Rule $[MG\text{-sel-out}]$ says when the monitor approves the interaction message, which is inside the local queue of $s[p_1]$, this message is permitted to output to the network.

7. Rule $[MG\text{-bra-in}]$ is dual to rule $[MG\text{-sel-out}]$.

8. Rule $[MG\text{-par}]$ says that, based on Definition 5.4.1 for network parallel composition, the action happening in one network will not affect another network.

9. Rule $[MG\text{-res}]$ says if an action is valid for a network $N$ and it results in $N'$, and if the name of the action does not occur in the bound names of $(\nu \tilde{n})N$, then this action is also valid for $(\nu \tilde{n})N$ and results in $(\nu \tilde{n})N'$.

10. Rule $[MG\text{-str}]$ says if an action is valid for a network $N_2$, then, if $N_1$ is structural congruent to $N_2$, this action is also valid for $N_2$. Once this action fires thus makes $N_2$ become $N'_2$, as the action fires in $N_1$, it makes $N_1$ become $N'_1$, which should be structural congruent to $N'_2$.

For invalid actions, Figure 7.9 shows that a monitor deals with the exceptions by simply removing the invalid primitives or messages from a local process or the global transport. Here we have one important assumption particularly for $[MG\text{-sel-out-err}]$
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

We assume there is a \emph{timeout} mechanism for $\lfloor \text{MG-sel-out-err} \rfloor$. As a process continue producing wrong outputs up to a default \emph{timeout}, the monitor will broadcast to all session-roles in the session with error message \text{session-failure}.

The \emph{timeout} mechanism can ensure the property of \emph{progress} of local monitored processes. It is specially for output session interaction actions, i.e. $s[p,q]!l(v)$, but not for input actions because, as a monitor approves an input for a local process, an asynchronous local process can always take an input action to get message in even if the process itself is not ready to (or will never) take it: an asynchronous local process can always gets an input by putting it into the local buffer. However, as a local process does not take an output session interaction action obeying to the specification defined in the monitor, the output message will be taken off and the action will be stopped. If there is a corresponding receiver waiting for an input coming from this sender, it may need to wait forever if there is no mechanism of \emph{timeout} or \emph{message-enforcement}. The \emph{timeout mechanism} will inform all the session participants that there is a participant failed since it produces errors up to a default time limit. Then the session will finish and will be closed. The message-enforcement mechanism is to revise the output message to the default right format obeying the specification. For example, revise the wrong receiver to the right destination, or revise the content to the right type or to satisfy the assertions. Both are not in the scope of this thesis but are topics that we should continue to work on.

Also note that, corresponding the error case of rule $\lfloor \text{Req-b-out} \rfloor$ defined in Figure 7.7, $\lfloor \text{MG-req-b-out-err} \rfloor$ also defines that the process following bound request $\overline{a}(s[p] : G)$ should be cleared out.

An unmonitored network is obtained by substituting monitored processes $\mathcal{M}[P]$ with \emph{monitor-off processes} $\mathcal{M}^0[P]$ where a gateway $\mathcal{M}^0$ is used instead of the corresponding monitor $\mathcal{M}$. The semantics for $\mathcal{M}_1^0[P] \xrightarrow{\ell} \mathcal{M}_2^0[P']$ is precisely as the one for $\mathcal{M}_1[P] \xrightarrow{\ell} \mathcal{M}_2[P']$, except that we use $\mathcal{M}_1^0 \xrightarrow{\ell} \mathcal{M}_2^0$ instead of $\mathcal{M}_1 \xrightarrow{\ell} \mathcal{M}_2$.

7.3 Use Case: Monitoring OOI Instrument Commands

Since the endpoints reside in diverse administrative entities, each endpoint needs to expect the use of unsafe codes at (other) endpoints, while protocols need be executed
7.3 Use Case: Monitoring OOI Instrument Commands

Assuring their global correctness. Given that two interacting endpoints may be a thousand miles apart, its architectural design stipulates that this assurance is to be done through the collection of dynamic local verifications. The model is based on these principles. Each principal in the OOI (see Section 2.2 in Chapter 2) is modelled as a local authority executing a local process, where incoming and outgoing messages are controlled by a monitor. As depicted in Figure 7.2, monitors are external to endpoints, since generally they are not located under local authorities: rather monitors are part of the distributed infrastructure, protecting the integrity of global interactions which take place there.

7.3.1 Invitations of the OOI Instrument Commands

Monitors dynamically learn about which protocols to enforce during session establishment. Local verification of incoming/outgoing messages to/from an endpoint are done by a dedicated (external and trusted) monitor. The aim is to ensure the correctness of global interactions, while protecting the endpoint so that it sends/receives only proper messages.

Below we illustrate monitored processes of session creation and invitation (assuming shared names have already been created). $M_i$ is the monitor corresponding to Principal$_i$, $i = 1, 2, 3, 4, 5$, and $M_i^k$ is the status of monitor $M_i$ after the $k$th transition from $M_i^k$.

Let $P_{INV}$ be $\overline{\pi_3}(s[Agent] : GIC) ; \overline{\pi_4}(s[Instrument] : GIC)$
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

[step0]
\[ M_0^1 | \mathcal{P}(s[Register] : G_{IC}).\text{join}(s[User] : (P_{user} | P_{INV})) \parallel H \parallel M_0^2 | a_2(y_2[Register] : G_{IC}).\text{join}(y_2[Register]).P_{register} \parallel \]
\[ M_0^3 | a_3(y_3[Agent] : G_{IC}).\text{join}(y_3[Agent]).P_{agent} \parallel M_0^4 | a_4(y_4[Instrument] : G_{IC}).\mathcal{P}(y_4[Instrument] : G_{IC}) \parallel \]
\[ M_0^5 | a_5(y_5[Instrument] : G_{IC}).\text{join}(y_5[Instrument]).P_{inst} \parallel \]

[step1]
\[ \mathcal{P}(s[Register] : G_{IC})_g \]
\[ (v_8)(M_0^1 | \text{join}(s[User] : s[Register] : G_{IC}).P_{user} \parallel P_{INV}) \parallel H \parallel M_2^1 | a_2(y_2[Register] : G_{IC}).\text{join}(y_2[Register]).P_{register} \parallel \]
\[ M_0^2 | a_3(y_3[Agent] : G_{IC}).\text{join}(y_3[Agent]).P_{agent} \parallel M_0^3 | a_4(y_4[Instrument] : G_{IC}).\mathcal{P}(y_4[Instrument] : G_{IC}) \parallel \]
\[ M_0^4 | a_5(y_5[Instrument] : G_{IC}).\text{join}(y_5[Instrument]).P_{inst} \parallel \]

[step2]
\[ \text{join}(s[User] : s[Register] : G_{IC})_g \]
\[ (v_8)(M_2^1 | P_{user} \parallel s[User] : \emptyset \parallel P_{INV}) \parallel H \parallel M_3^1 | \text{join}(s[Register] : s[Register]).P_{register} \parallel \]
\[ M_3^2 | a_3(y_3[Agent] : G_{IC}).\text{join}(y_3[Agent]).P_{agent} \parallel M_0^3 | a_4(y_4[Instrument] : G_{IC}).\mathcal{P}(y_4[Instrument] : G_{IC}) \parallel \]
\[ M_0^4 | a_5(y_5[Instrument] : G_{IC}).\text{join}(y_5[Instrument]).P_{inst} \parallel \]
7.3 Use Case: Monitoring OOI Instrument Commands

In step 0, the process $s$ by primitive $GIC : \text{Join}(s[\text{User}]) \cdot (P_{\text{User}} | P_{\text{INV}})$ creates a fresh session $s$ by primitive $GIC : \text{Join}(s[\text{User}])$, which creates session $s$ obeying to protocol $GIC$ and, at the same time, requests endpoint $a_2$ to play role $\text{Register}$ in $s$. Then this process concurrently joins session $s$ for playing role $\text{User}$ and continues
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

$P_{\text{user}}$ and invites other endpoints to join session $s$ through $P_{INV}$. Monitored process $M_2^0[a_2(y_2[\text{Register}]) \cdot G_{IC}] \cdot \gamma(y_2[\text{Register}]).P_{\text{register}}$ is ready to receive invitation for playing role $\text{Register}$ obeying to protocol $G_{IC}$ by replacing variable $y_2$ with the session names. As it accepts the invitation, it joins the session as a $\text{Register}$. Monitored process $M_3^0[a_3(y_3[\text{Agent}]) \cdot G_{IC}] \cdot \gamma(y_3[\text{Agent}]).P_{\text{agent}}$ is similar to the one for playing $\text{Register}$. The monitored process

$$M_4^0[a_4(y_4[\text{Instrument}]) \cdot G_{IC}] \cdot \gamma(y_4[\text{Instrument}]) : G_{IC}$$

does not join the session when it accepts the invitation but delegates the capability of playing role $\text{Instrument}$ to endpoint $a_5$. The monitored process

$$M_5^0[a_5(y_5[\text{Instrument}]) \cdot G_{IC}] \cdot \gamma(y_5[\text{Instrument}]).P_{\text{inst}}$$

is similar to those for playing roles $\text{Register}$ and $\text{Agent}$. It will accept the invitation and join the session for playing role $\text{Instrument}$.

Note that, actions in $\gamma(s[\text{User}] | a_2(s[\text{Register}]) : G_{IC})$ are permutable to each other, for example, it can be permuted to $a_2(s[\text{Register}]) : G_{IC} \cdot \gamma(s[\text{User}]).P_{\text{register}}$ because they have no causal relation. Similarly, actions in $\gamma(s[\text{Register}] : G_{IC}) \cdot \gamma(s[\text{Agent}] : G_{IC}) : G_{IC}$, therefore, may be rearranged to $\gamma(s[\text{Register}] : G_{IC}) \cdot H$. Then invitation $\gamma(s[\text{Register}] : G_{IC})$ can be absorbed by the monitored process $M_3^0[a_2(y_2[\text{Register}]) : G_{IC}] \cdot \gamma(y_2[\text{Register}]).P_{\text{register}}$ immediately because there is a process ready to input this invitation. The causal relation of input/output messages, which represent actions, are decided by the endpoint monitors. The transition actions in other steps are permutable for the same reason.

Also note that, after name $s$ is created, from step 1 to step 2 the scope of name $s$ is changed from $(\nu s)(M_1^0[\gamma(s[\text{User}])].P_{\text{user}} | P_{INV}] | H \cdot \gamma(s[\text{Register}]) : G_{IC}))$ to $(\nu s)(M_2^0[P_{\text{user}} | s[\text{User}] : \emptyset | P_{INV}] | H | M_3^0[\gamma(s[\text{Register}]).P_{\text{register}} \{s/y_2\}])$ since endpoint $a_2$ accepts the invitation coming from session $s$. The scope of a session ranges over those processes who currently participate in $s$. Note, as for monitored processes, the scope of $s$ can be controlled by $M$ through checking whether $s \in M$. 

132
7.3 Use Case: Monitoring OOI Instrument Commands

In step 2, the monitored process $\mathcal{M}_1^1[\text{join}(s[\text{User}]).P_{user} \mid P_{INV}]$ joins session $s$ for playing role $\text{User}$ and becomes $\mathcal{M}_1^2[\text{P}_{user} \mid s[\text{User}] : \emptyset \mid P_{INV}]$ in which local queue specifically for session-role $s[\text{User}]$ is created. Also, the monitored process $\mathcal{M}_2^0[a_2(y_2[\text{Register}]) : G_{IC}).\text{join}(y_2[\text{Register}]).P_{register}]$ accepts the invitation for playing role $\text{Register}$ in session $s$ and becomes $\mathcal{M}_2^1[\text{join}(s[\text{Register}]).P_{register}\{s/y_2\}]$ in which every variable $y_2$ is replaced by $s$.

We denote $G_{IC} \mid \text{User}$ as $T_{user}$, $G_{IC} \mid \text{Register}$ as $T_{register}$, $G_{IC} \mid \text{Agent}$ as $T_{agent}$, and $G_{IC} \mid \text{Instrument}$ as $T_{inst}$. We show the configurations of monitors of the above
monitored processes in the follows:

\[ \begin{align*}
\text{[step0]} & \quad M_0^0 = a_1 : I(G_{IC}[User]), a_2 : 0(G_{IC}[Register]), a_3 : 0(G_{IC}[Agent]), a_4 : 0(G_{IC}[Instrument]) \\
\text{[step1]} & \quad M_1^0 = a_2 : I(G_{IC}[Register]) \\
\text{[step2]} & \quad M_2^0 = a_3 : I(G_{IC}[Agent]) \\
\text{[step3]} & \quad M_3^0 = a_4 : I(G_{IC}[Instrument]), a_5 : 0(G_{IC}[Instrument]) \\
\text{[step4]} & \quad M_4^0 = a_5 : I(G_{IC}[Instrument]) \\
\text{[step5]} & \quad M_5^0 = a_5 : I(G_{IC}[Instrument]) \\
\text{[step6]} & \quad M_6^0 = a_5 : I(G_{IC}[Instrument]), s[Instrument] : T_{inst} \\
\end{align*} \]

As for the configurations of monitors, step 0 shows that each monitor should have knowledge about the endpoints who they are going to request. For example, \( M_0^0 \) knows \( a_1 : I(G_{IC}[User]), a_2 : 0(G_{IC}[Register]), a_3 : 0(G_{IC}[Agent]) \) and \( a_4 : 0(G_{IC}[Instrument]) \) so that she can request \( a_2, a_3, \) and \( a_4 \) for playing roles defined in protocol \( G_{IC} \), but she can not request endpoint \( a_5 \) since she does not have the knowledge about it. Among
these monitors, only $\mathcal{M}^0_3$ with the knowledge $a_5 : 0(GIC[Instrument])$ can request $a_5$ for playing role *instrument* specified under $GIC$.

In step 1, since bound request $\pi_2(s[Register] : GIC)$ creates a fresh name $s$ and requests $a_2$ for playing role *Register*, the capabilities of playing roles *User*, *Agent*, and *Instrument* are created and denoted by $s[User] : T_{user}$, $s[Agent] : T_{agent}$, and $s[Instrument] : T_{inst}$, while the capability of playing role *Register* is not there because it has been sent out to endpoint $a_2$. In step 2, the capability of playing role *User* becomes active as $s[User] : T_{user}$ when the process joins session $s$ to play role *User*. And capability of $s[Register] : T_{register}$ is added to monitor $M^1_2$ when it accepts the invitation for playing role *Register*. In step 3, since the capabilities of $s[Agent] : T_{agent}$ and $s[Instrument] : T_{inst}$ have been sent out as requests, they are removed from the monitor. And, as explained above, the monitored process joins role *Register* in $s$ so that it is active as $s[Register]^{\bullet} : T_{register}$. Other operations of the configurations of monitors can be similarly explained.

### 7.3.2 Interactions of the OOI Instrument Commands

It follows an illustration of some actions of the session instrument command. For simplicity, we use $P^k_{role}$ to represent the status after the $k$th action of process $P_{role}$.

#### [step0]

\[
\nu_s(H \parallel s[User] \parallel s[Register] : 0) \parallel s[Agent] \parallel s[Instrument] : 0)
\]

#### [step1]

\[
\nu_s(H \parallel s[User] \parallel s[Register, \langle v_{int} \rangle] : 0) \parallel s[Agent] : 0) \parallel s[Instrument] : 0)
\]

#### [step2]

\[
\nu_s(H \parallel s[User, Register, \langle v_{int} \rangle] \parallel s[User] : 0) \parallel s[Register] : 0) \parallel s[Agent] : 0) \parallel s[Instrument] : 0)
\]
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

In step 0, since it continues with the operations of invitation, $M^0_A[0] \equiv 0$ (based on Definition 7.2.5), $M^0_A$ is neglected. In step 1, $P_{user}$ internally sends an output message $s\langle User, Register, \langle v_{int} \rangle \rangle$ and puts it in its local queue as

$s\langle User \rangle : s\langle User, Register, \langle v_{int} \rangle \rangle$.

Since this internal output action is invisible globally, it is a silent action, i.e. $\tau$ action, of the LTS of the monitored network. Then in step 2, the message is sent out from
the monitored process, thus the visible action \( s[\text{User}, \text{Register}]^!(v_{\text{int}}) \) happens, and the local queue becomes empty as \( s[\text{User}] : \emptyset \), and the message is put in the global queue as \( H \cdot s[\text{User}, \text{Register}, (v_{\text{int}})] \). In step 3, since visible action \( s[\text{User}, \text{Register}]^? (v_{\text{int}}) \) happens, the message \( s(\text{User}, \text{Register}, (v_{\text{int}})) \) is removed from the global queue, which becomes \( H \), and enters the local process \( P_{\text{register}} \), thus the monitored process of playing role \( \text{Register} \) becomes \( M_3^0[\text{Register} \mid s[\text{Register}] : s(\text{User}, \text{Register}, (v_{\text{int}}))] \). In step 4, message \( s(\text{User}, \text{Register}, (v_{\text{int}})) \) is absorbed by process \( P_{\text{register}} \). Thus \( P_{\text{register}} \) becomes \( P_{\text{register}}^1 \) and its local queue becomes empty as \( s[\text{Register}] : \emptyset \). Other operations of the following steps are similar.

Up to now, \( \text{User} \) and \( \text{Register} \) finish their first interaction: \( \text{User} \) sends \( v_{\text{int}} \) to \( \text{Register} \), then \( \text{Register} \) returns 10 back to \( \text{User} \). Other value-passing and branching interactions afterwards are similar. Recall that we denote \( G_{\text{IC}} \upharpoonright \text{User} \), \( G_{\text{IC}} \upharpoonright \text{Register} \) as \( T_{\text{user}} \), \( G_{\text{IC}} \upharpoonright \text{Register} \) as \( T_{\text{reg}} \), \( G_{\text{IC}} \upharpoonright \text{Agent} \) as \( T_{\text{agent}} \), and \( G_{\text{IC}} \upharpoonright \text{Instrument} \) as \( T_{\text{inst}} \). For convenience we let \( T_{\text{role}}^k \) to represent the \( k \)th action of endpoint assertion \( T_{\text{role}} \).

### 7.3 Use Case: Monitoring OOI Instrument Commands

- **Step 0**
  \[
  M_1^0 = a_1 : I(G_{\text{IC}}[\text{User}]), a_2 : 0(G_{\text{IC}}[\text{Register}]), a_3 : 0(G_{\text{IC}}[\text{Agent}]), a_4 : 0(G_{\text{IC}}[\text{Instrument}]), \\
  s[\text{User}]^* : T_{\text{user}} = \text{Register}!(x_{\text{int}} : \text{InterfaceId}).T_{\text{user}}^1
  \]

- **Step 1**
  \[
  M_2^0 = a_2 : I(G_{\text{IC}}[\text{Register}]), \\
  s[\text{Register}]^* : T_{\text{reg}}^1(v_{\text{int}}/x_{\text{int}}) = \text{Register}?(x_n : \text{Int})\langle x_n > 0 \rangle.T_{\text{reg}}^2(v_{\text{int}}/x_{\text{int}})
  \]

- **Step 2**
  \[
  M_3^0 = a_2 : I(G_{\text{IC}}[\text{Register}]), \\
  s[\text{Register}]^* : T_{\text{reg}}^2(v_{\text{int}}/x_{\text{int}}) = \text{User}!(x_n : \text{Int})\langle x_n > 0 \rangle.T_{\text{reg}}^3(v_{\text{int}}/x_{\text{int}})
  \]

- **Step 3**
  \[
  M_4^0 = a_2 : I(G_{\text{IC}}[\text{Register}]), \\
  s[\text{Register}]^* : T_{\text{reg}}^3(v_{\text{int}}/x_{\text{int}})\{10/x_n \} = \text{end}(v_{\text{int}}/x_{\text{int}})\{10/x_n \} = \text{end}
  \]

- **Step 4**
  \[
  M_5^0 = a_1 : I(G_{\text{IC}}[\text{User}]), a_2 : 0(G_{\text{IC}}[\text{Register}]), a_3 : 0(G_{\text{IC}}[\text{Agent}]), a_4 : 0(G_{\text{IC}}[\text{Instrument}]), \\
  s[\text{User}]^* : T_{\text{user}}^2(v_{\text{int}}/x_{\text{int}})\{10/x_n \}
  \]

In step 0, monitor \( M_1^0 \) has active capability \( s[\text{User}]^* \), which is able to send a message to role \( \text{Register} \) with content of type \text{InterfaceId}, then local specification \( T_{\text{user}}^1 \) is ready for
the next action. Similarly, monitor $M_2$ has active capability $s[\text{Register}]^\bullet$, which is able
to receive message of type of $\text{InterfaceId}$ from role $\text{User}$, then local specification $T_1^{\text{register}}$
is ready for the next action. Step 1 describes when action $s[\text{User}, \text{Register}]!(v_{\text{int}}) \langle x_{\text{int}} \rangle$ takes
place, then $\text{Register}!(x_{\text{int}} : \text{InterfaceId})$ is removed, and $T_1^{\text{user}}$ becomes $T_1^{\text{user}}\{v_{\text{int}}/x_{\text{int}}\}$, which becomes $\text{Register}? (x_n : \text{Int}) \langle x_n > 0 \rangle . T_2^{\text{user}}\{v_{\text{int}}/x_{\text{int}}\}$ for the next input action
from role $\text{Register}$. Other operations of configurations of monitors above are similar
and they all obey the LTS of the monitors, defined in Figure 7.4.

7.4 Safety, Transparency, and Session Fidelity

This section states and proves the key theorems, including the receivability and coherence
of the network, properties of local and global safety, local and global transparency,
and session fidelity. They are the properties that our monitoring mechanism can enforce.

7.4.1 Local Safety and Transparency

We first list the properties that monitors guarantee for local configurations. Hereafter,
we write $\mathcal{L}$, a located process, for either a monitored process $M[P]$ or a monitor-off
process $M^\circ[P]$.

**Definition 7.4.1.** Define $\mathcal{L} \xrightarrow{\ell} M$ as $\mathcal{L}$ approves the action $\ell$ and it implies $\exists \mathcal{L}'$ such that
$\mathcal{L} \xrightarrow{\ell} \mathcal{L}'$. Similarly, define $M \xrightarrow{\ell} \mathcal{M}$ as $M$ approves the action $\ell$ and it implies $\exists \mathcal{M}'$ such that
$\mathcal{M} \xrightarrow{\ell} \mathcal{M}'$.

**Definition 7.4.2 (conformance).** A relation $\mathcal{R}$ between a located process $\mathcal{L}$ and its
monitor $M$ is a conformance if whenever $\mathcal{L} \xrightarrow{\ell} M$, we have

1. Given an output $\ell$, if $\mathcal{L} \xrightarrow{\ell}$ then $M \xrightarrow{\ell}$.
2. Given an input $\ell$, if $M \xrightarrow{\ell}$ then $\mathcal{L} \xrightarrow{\ell}$.
3. For any $\ell$, if $\mathcal{L} \xrightarrow{\ell} \mathcal{L}'$ and $M \xrightarrow{\ell} \mathcal{M}'$ then $\mathcal{L}' \xrightarrow{\ell} \mathcal{M}'$.

If $M \xrightarrow{\ell} \mathcal{L}$ for a conformance $\mathcal{R}$, we write $M \models \mathcal{L}$, and say $\mathcal{L}$ conforms to $M$.

Conformance says that a located process is a process that only sends "good" messages
and can at least receive "good" messages (which have been approved by its own monitor).
The following theorem says every monitored process conforms to the specification given
by its own monitor.
Theorem 7.4.3 (local safety (local conformance)). \( M \models M[P] \) for all \( M \) and \( P \).

Proof. The proof and auxiliary theorems are in Appendix [B.1]

Definition 7.4.4. Let \( R \) be a relation between a monitor and a pair of located processes. Then \( R \) is a monitored strong bisimulation if the following holds for each \( M, L_1 \) and \( L_2 \) related by \( R \). Below we assume \( i \neq j \), with \( i, j \in \{1, 2\} \).

1. If \( L_i \xrightarrow{\ell} L'_i \) s.t. \( \ell \) is an output/\( \tau \) then \( M \xrightarrow{\ell} M', L_j \xrightarrow{\ell} L'_j \) and \( (M', L'_i, L'_j) \in R \).

2. If \( L_i \xrightarrow{\ell} L'_i \), \( M \xrightarrow{\ell} M' \) s.t. \( \ell \) is an input then \( L_j \xrightarrow{\ell} L'_j \) and \( (M', L'_i, L'_j) \in R \).

If \( M, L_1 \) and \( L_2 \) are in a monitored strong bisimulation then \( L_1 \) and \( L_2 \) are bisimilar under \( M \), denoted \( M \models L_1 \sim L_2 \).

The following states that a monitored-process and a monitor-off process behave precisely in the same way if the latter already conforms to the monitor’s specification.

Theorem 7.4.5 (local transparency). If \( M \models M^\circ[P] \), then \( M \models M^\circ[P] \sim M[P] \).

Proof. The proof and auxiliary theorems are in Appendix [B.1]

Note that a process \( P \) that can be validated by \( \Gamma \vdash P \triangleright \Delta \) (in the sense of (22)) is guaranteed to behave correctly and thus satisfies \( M \models M^\circ[P] \) for \( M = \Gamma, \Delta \).

7.4.2 Global Safety, Transparency and Session Fidelity

This section shows that global message flows inside the monitored network are safe in spite of untrusted endpoints. To make exact the notion of global correctness, \( \xrightarrow{\ell_g} \) is used for describing \( N \xrightarrow{\ell_g} N' \) by following the transitions for the monitored network in Figure 7.8. Note that both \( N \) and \( N' \) are the monitored network.

Definition 7.4.6 (receivable network). We say \( N \) is receivable if there exist a sequence of actions \( \ell_1 \ldots \ell_k \) consisting of all the inputs corresponding to the pending messages in \( N \) and joins, such that \( N \xrightarrow{\ell_1 \ldots \ell_k} N' \).

Lemma 7.4.7 (receivability). Let \( N \) be a monitored network and \( \ell \) be an input action. If \( N \) is receivable and \( N' \xrightarrow{\ell} N' \), then \( N' \) is receivable.

Proof. It is proved in Appendix [B.2]

Definition 7.4.8. Define \( s[p]^\circ \) stand for either \( s[p] \) or \( s[p]^\bullet \).
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

Definition 7.4.9 (\(T' \subseteq T\) w.r.t a session-role). We say \(T' \subseteq T\) w.r.t \(s[p]\) if, for some \(M\) containing \(s[p]\), we have either (I) \(s[p] \triangleright \ell_1 \ldots \ell_n \vdash T'\) or (II) \(T \bowtie T'\).

Note that, when \(T, T'\) are clearly for the same session-role, we simply write \(T' \subseteq T\).

Here we define a group of monitors which are parts of the network as follows:

Definition 7.4.10 (a group of monitors). Define a group of monitors as

\[ \mathcal{M} = \prod_{i \in I} M_i = M_1 \parallel \ldots \parallel M_k, I = \{1, \ldots, k\} \]

the monitors existing in parallel in the network.

Remark 7.4.11. Since every monitor contains specifications \(\Gamma, \Delta, \mathcal{M}\) can also be viewed as a set of specifications.

Definition 7.4.12 (consistency of a group of monitors). Let \(\mathcal{M}\) be a group of monitors. Let \(\forall M_i \in \mathcal{M}, M_i = \Gamma_i, \Delta_i\). If all of the following conditions hold,

1. (a) \(\forall M_i \in \mathcal{M}, \text{if } a : \text{im}(G[p]) \in M_i, \text{then there is no other } a : \text{io}(G[p]) \in M_j, M_j \in \mathcal{M}.\)
    
   (b) \(\forall M_i \in \mathcal{M}, \text{if } \forall s, s[p] \circ T \in M_i, \text{then } s[p] \circ T \notin M_j, j \neq i, M_j \in \mathcal{M}.\)

2. If \(a : \text{io}(G[p]) \in M_i, \text{then there exists } M_j \text{ such that } a : \text{im}(G[p]) \in M_j.\)

3. Assume \(p_1 \neq p_2\). As \(\Delta_i(s[p_1]^{\circ}) = T\) and
   
   \[ p_2! \{l_k(x_k : S_k) \langle \langle A_k \rangle \rangle, G_k \upharpoonright p_2 \}_{k \in I} \subseteq T, \]
   
   there exists \(j\) such that \(\Delta_j(s[p_2]^{\circ}) = T'\) and
   
   \[ p_1? \{l_k(x_k : S_k) \langle \langle A'_k \rangle \rangle, G_k \upharpoonright p_1 \}_{k \in I} \subseteq T' \]
   
   with \(A_k \{v/x_k\} \downarrow \text{true}\) iff \(A'_k \{v/x_k\} \downarrow \text{true}\) for some \(v.\)

4. \(\bigcup_i \Delta_i = \bigcup_{1 \leq j \leq n} \{s_j[p_{j1}] : T_{j1}, \ldots, s_j[p_{jk}] : T_{jk}, \ldots, s_j[p_{jm_j}] : T_{jm_j}\} \) where, for each \(s_j\), there is \(G_j\) such that \(G_j \upharpoonright p_{jk} = T_{jk}\) for \(1 \leq k \leq m_j.\)

then the group of monitors, \(\mathcal{M}\), is consistent.
7.4 Safety, Transparency, and Session Fidelity

Note that for rule 3, we only ask that, whenever there is an output, there is a corresponding input because the monitors should at least ensure that the outputs from local processes will not output unexpected messages to the network. By considering the following global specification,

\[ G = p_1 \rightarrow p_2 : \{ l_i(x_i : S_i)\langle\langle A_i\rangle\rangle.p_2 \rightarrow p_3 : \{ l'_j(x'_j : S'_j)\langle\langle B_j\rangle\rangle.G'_{ij} \}_{j \in I} \}_{i \in I} \]

assume \( s \) follows \( G \). After applying projection rules defined in Definition 6.5.1, we have

\[
\begin{align*}
    s[p_1] : & \quad p_2\{ l_i(x_i : S_i)\langle\langle A_i\rangle\rangle.G'_{ij} | p_1 \}_i \in I \\
    s[p_2] : & \quad p_1?\{ l_i(x_i : S_i)\langle\langle A'_i\rangle\rangle.p_2\{ l'_j(x'_j : S'_j)\langle\langle B_j\rangle\rangle.G'_{ij} | p_2 \}_j \in I \}_i \in I \\
    s[p_3] : & \quad p_2?\{ l'_j(x'_j : S'_j)\langle\langle B'_j\rangle\rangle.G'_{ij} | p_3 \}_j \in I 
\end{align*}
\]

where sending to \( p_3 \) at \( s[p_2] \) is not permutable to receiving from \( p_1 \). Since the consistency of monitors requires that an output should correspond to an input, rule 3 requires that, when a sending action is in a monitor’s specification, a corresponding receiving action is in some monitor’s specification. Moreover, when a sending action is ready to send a message, there exists a corresponding receiving action at some monitor to input this message.

**Definition 7.4.13 (monitored network coherence).** \( N \) is coherent if all of its pending messages are receivable up to permutation of actions \( \bowtie \) and, after these messages have been received, the resulting group of monitors which guard all local processes in \( N \), say \( M \), is consistent.

The coherence above states that, after all messages are cleared out of the network, the monitors of the network satisfy the following rules: rule 1: An input mode shared name with particular specification is unique to the network (see Lemma 7.4.15), and similarly, a session-role is unique to the network such that no two different locations share a common role in a common session; rule 2: As long as an \( O \)-mode shared name exists, its dual mode (i.e. \( I/\text{IO}\)-mode) shared name co-exists; rule 3: Each output action in a specification has its corresponding input action in some other specification; rule 4: For each session name, the local specifications for the roles of its participants is the result of projecting a common global specification on their roles.

**Convention 7.4.14.** We say an element is unique to the network \( N \) whenever \( M_i \in N \), \( M_i \) has one and only one of this element, and \( \forall M_j \in N, j \neq i, M_j \) does not have this element.
Compared to Definition 5.4.2 of composability, the composable network, say \( N_1 \parallel N_2 \) may not be coherent when they are composed in parallel. The rule 1 of Definition 7.4.12 implies that the \( a : \text{im}(G[p]) \) is unique to the network, which is proved by the following Lemma:

**Lemma 7.4.15 (global uniqueness of names).** Assume every local domain has a network-wise unique identity, which will be attached to a local name when the name is created. If \( a : \text{im}(G[p]) \) is unique to a local monitor guarding a local domain, which means there is no more \( a : \text{I}(G[p]) \) or \( a : \text{IO}(G[p]) \) in that monitor, then it is unique to the network. Similarly, if \( s \) is unique to a local monitor, it is unique to the network.

*Proof.* As Figure 7.1 shows, there is a routing mechanism in the network. Distributed routers are responsible for both routing and registering individual components in different domains. As long as a local monitor approves name \( n \), which is either a shared name or a session name, it is fresh to the local domain, say \( A \). When this name is announced to the network (with rules \( \lfloor \text{MG-new-a} \rfloor \) and \( \lfloor \text{MG-req-b-out} \rfloor \) in Figure 7.8), theoretically we can assume the identity of the domain is attached to this name, e.g. \( n.A \), where \( A \) is unique in the network. Therefore, this name (i.e. \( n.A \)) is unique globally. With the same reasoning above, \( s \) is unique to the network as long as it is unique to a local monitor.

Since we want to abstract the actions as simple as possible, we neglect the details of routing mechanism in this thesis.

The property of global safety says that, as, at the very beginning, the network is protected by consistent monitors, the coherence of the monitored network is preserved by the interactions that can happen in a monitored network. In brief, it states that a fully monitored network behaves well with respect to the given global specification.

**Theorem 7.4.16 (global safety).** Let \( N \) be coherent. Then \( N \xrightarrow{\ell} g N' \) implies \( N' \) is coherent.

*Proof.* It is proved in Appendix B.2

\( N \) is **locally conformant** if, for each monitored process \( M_i[P_i] \) in \( N \), we have \( M_i \models \text{erase}(M_i)[P_i] \). If \( N \) is coherent and locally conformant and such that \( N \xrightarrow{\ell_i} g \cdots \xrightarrow{\ell_n} g N' \) then \( N' \) is also coherent and locally conformant. This property is formally defined and proved in Appendix B.3. Let \( \sim \) be the standard strong bisimilarity defined by \( \xrightarrow{\ell} g \). Then we have:
Theorem 7.4.17 (global transparency). Suppose $N$ is coherent and locally confor-
mant. Then $N \sim \text{erase}(N)$.

Proof. It is proved in Appendix B.3.

The property of global transparency states that a monitored network and an unmoni-
tored network have equivalent behaviour when the latter is well-behaved with respect to
the same (collection of) specifications. When a new session is generated, it is associated
with a global protocol $G$. In a monitored network, we expect all message flows for this
session always follow $G$. This notion is called session fidelity [86].

Note as Remark 5.4.7 says, the viewpoints of local and global are dual. Define the
processes that guarded by $M$ as:

Definition 7.4.18. Write $P(M)$ for the set of processes governed by monitor $M$, and
write $P(M)$ to denote the set of processes governed by the group of monitors $M$.

Definition 7.4.19 (labelled transition of $M$). $M \xrightarrow{\ell} M'$ if and only if there exists
$M \in M$ s.t. $M \xrightarrow{\ell} M'$ and $M' \in M'$.

Before introducing the theorem of session fidelity, to simplify and clarify the rela-
tionships between local monitored processes and the global transport, configuration
is introduced. It is the pair of $M$ and $H$, to illustrate the idea of session fidelity.

Definition 7.4.20 (configuration). A configuration is denoted by $\Phi = M; H$, in
which the group of monitors correspond to $H$. In other words, all messages correspon-
ding to the actions guarded by $M$ are in $H$.

A $\Phi$ thus guides and captures the behaviours in the network.

Definition 7.4.21. For any $M_1$ and $M_2$, we write $M_1, M_2$ as a standard union of $M_1$
and $M_2$.

Lemma 7.4.22. Assume $M_1$ corresponds to $H_1$ and $M_2$ corresponds to $H_2$. As long
as $P(M_1) \cap P(M_2) = \emptyset$, there is no common message existing in $H_1$ and $H_2$.

Proof. Based on Definition 7.4.20 for $i \in \{1, 2\}$, if the interactions, including outputs
and their corresponding inputs, are approved by one $M_i$, all messages corresponding to
these actions are in one $H_i$. For $i, j \in \{1, 2\}, i \neq j$, as an output action is approved
by $M_i$ so that its corresponding message is put into $H_i$, and its input, the duality of
the output, if it is approved by $M_j$, then this message will leave $H_i$ and enter $H_j$
and will be absorbed by some monitored process guarded by a monitor in $M_j$. Thus overall
there is no common message existing in $H_1$ and $H_2$. ■
With the definitions and lemma above, we define the parallel composition of configurations:

**Definition 7.4.23 (parallel composition of configurations).** Assume $\Phi_1 = M_1 ; H_1$ and $\Phi_2 = M_2 ; H_2$ are given, we say $\Phi_1$ and $\Phi_2$ are *composable* whenever $P(M_1) \cap P(M_2) = \emptyset$. If $\Phi_1$ and $\Phi_2$ are composable, define the composition of $\Phi_1$ and $\Phi_2$ as: $\Phi_1 \circ \Phi_2 = M_1 , M_2 ; H_1 \cdot H_2$.

$H_1 \cdot H_2$ is defined in Definition 5.4.3. The behaviour of each endpoint in a network is guided by $M$ (specifications), and is observed by $H$ (global transport). We define the LTS of configurations in Figure 7.10. All rules are straightforward from the LTS of monitors (Figure 7.4, Chapter 7) and the one of the dynamic network (Figure 5.7, Chapter 5). The global observable transition $\ell \rightarrow g$ for some action $\ell$ has been introduced in the LTS for the monitored network, defined in Figure 7.8.

- Rule New informs the global transport that a fresh name $a$ is created.
- Rules $[\text{Req-b/f}]$ indicates that when some endpoint monitor approves a bound or free request to go to the network, the configuration inputs this request as an invitation to the global queue. Note that $[\text{Req-b}]$ also creates and hides a fresh session $s$.
- Rules $[\text{Acc-b/f}]$ indicates that, when the invitation has been accepted by an endpoint in the network, the invitation is taken off from the global queue (externally). Note that, we can only observe the invitation leaves the global queue but do not know who accepts it: only $M$ can tell which endpoint accepts this invitation.
- The concepts of rules $[\text{Sel}, \text{Bra}]$ are similar to the concepts of rules $[\text{Req-b/f, Acc-b/f}]$.
- The concepts of rules $[\text{SelN, BraN}]$ are similar to rule $[\text{Sel, Bra}]$, except that they are carrying names.
- Rule Par says if $\Phi_1$ and $\Phi_3$ are composable (see Definition 7.4.23), after $\Phi_1$ becomes as $\Phi_2$, they are still composable.

**Definition 7.4.24 (configurational consistency).** A configuration $\Phi = M; H$ is *configurationally consistent* whenever

1. $H$ is empty and $M$ is consistent, or
7.4 Safety, Transparency, and Session Fidelity

Figure 7.10: The Labelled Transition System of Configurations
2. $H$ is not empty, the sequence of messages in $H$ are receivable to $M$, and after receiving all messages in $H$ with $M \xrightarrow{\ell_1 \ldots \ell_n} M'$, where $\ell_i, i = \{1, \ldots, n\}$ are inputs and, $\forall m \in H, \exists \ell \in \ell_1 \ldots \ell_n$ such that $\ell$ corresponds to $m$, we have $M'$ is consistent.

In other words, $M; H$ is configurationally consistent if, in each of its derivatives, all messages in the transport can be “received” by some monitors in $M$ and, after absorbing all these messages, the resulting $M'$ is still consistent.

As for the satisfaction relation of the partial network $(N_s, N_s', \ldots)$ if $N_s$ is a partial network, $\models N_s : M$ means that monitors in $M$ allow all outputs from the local processes in $N_s$, and all the local processes in $N_s$ are ready to receive the inputs which monitors in $M$ indicate. The output and input satisfactions described above are preserved by transition.

**Definition 7.4.25 (partial satisfaction).** A relation $R$ from partial networks to specifications of monitors in $M$ is a satisfaction when $N_s R M$ implies:

1. If $M \xrightarrow{\ell} M'$ for an input $\ell$ and $\exists P_j \in N_s$ has an input at $sbj(\ell)$, then $P_j \xrightarrow{\ell} P_j'$, which makes $N_s = P_j \parallel \prod_{i \neq j} P_i$ becomes $N'_s = P'_j \parallel \prod_{i \neq j} P_i$ such that $N'_s R M'$.

2. If $\exists P_j \in N_s$ and $P_j \xrightarrow{\ell} P_j'$ for an output $\ell$, which makes $N_s = P_j \parallel \prod_{i \neq j} P_i$ becomes $N'_s = P'_j \parallel \prod_{i \neq j} P_i$, then $M \xrightarrow{\ell} M'$ such that $N'_s R M'$.

3. If $\exists P_j \in N_s$ and $P_j \xrightarrow{\tau} P_j'$, which makes $N_s = P_j \parallel \prod_{i \neq j} P_i$ becomes $N'_s = P'_j \parallel \prod_{i \neq j} P_i$, then $M \xrightarrow{\tau} M'$ such that $N'_s R M'$ (i.e. $N'_s R M$ since $M \xrightarrow{\tau} M$).

When $N_s R M$ for a partial satisfaction $R$, we say $N_s$ satisfies $M$, writing $\models N_s : M$.

Note that, the transitions in the partial network are defined in Figure 5.4, which are invisible globally because a partial network does not include the global queue, which makes the transitions globally visible. Thus we use $\xrightarrow{\ell}$ for representing that there is a local process taking action $\ell$ in $N_s$ instead of using $\xrightarrow{\ell}_g$. Remember, the visible actions can be and can only be observed in the global transport.

**Definition 7.4.26 (conformance to a configuration).** Assume a network $N \equiv N_s \parallel H$ is given. Define $N$ conforms to $M; H$ when:

---

1. The key ideas and concepts of satisfaction for the partial network come from Dr. Kohei Honda. The current version is the result after many discussions and revisions from our works. They also belong to the paper [20] which has been accepted and is going to be published.
7.5 Global Environment \(\mathcal{E}\)

1. \(H\) is empty, \(\models N_s : M\) and \(M\) is consistent, or

2. \(H\) is not empty, and the following conditions hold
   
   \(\begin{align*}
   & (a) \models N_s : M, \\
   & (b) \text{all messages in } H \text{ are receivable to } N_s, \text{ and} \\
   & (c) \text{as } M; H \xrightarrow{\ell_1, \ldots, \ell_n}_{g} M'; \emptyset \text{ so that } N_s \| H \xrightarrow{\ell_1, \ldots, \ell_n}_{g} N_s' \| \emptyset \text{ where each } \ell_i, i = \{1, \ldots, n\} \text{ is an input, } M' \text{ is consistent.}
   \end{align*}\)

Compared to the definition of global observable transition in Definition 7.2.13, which is for the monitored network, here define the global network transition for the unmonitored network.

**Definition 7.4.27 (global network transition).** Assume \(N\) is an un-monitored network and \(N\) conforms to \(M; H\). \(M; H \xrightarrow{\ell}_{g} M'; H'\) if and only if \(N \xrightarrow{\ell}_{g} N'\).

This definition corresponds to the illustration of global observability \(\xrightarrow{\ell}_{g}\) in Section 7.2.4.3. When \(N\), although it is not monitored, conforms to the specifications specified in monitors, they have the same behaviour: When \(N\) takes actions, \(M; H\) takes actions, and vice versa.

**Theorem 7.4.28 (session fidelity).** Assume configuration \(M; H\) is configurationally consistent and \(N \equiv N_s \| H\) conforms to configuration \(M; H\). We say \(N\) satisfies session fidelity, if for any \(\ell\), we have \(N \xrightarrow{\ell}_{g} N'\) such that \(M; H \xrightarrow{\ell}_{g} M'; H'\), it holds that \(M'; H'\) is configurationally consistent and that \(N'\) conforms to \(M'; H'\).

**Proof.** The proof and auxiliary theorems are in Appendix B.3.

### 7.5 Global Environment \(\mathcal{E}\)

The introduction of global observables offers a formal framework to semantically link local behaviour of processes to their global behaviour and to global invariants. Since, in distributed processes, the sending events and the receiving events are decoupled, and because external monitors can only observe asynchronously exchanged messages, the semantic account of global invariants (hence correctness of runtime verification) should take into account temporary discrepancies of the global view. When a sender sends a message correctly, its local view is updated; however, as the receiver has not yet received the message, we cannot update neither the global view nor the receiver’s local view. To
prove the correctness of distributed runtime verification, we here propose to take into account the time lag between the sending and receiving events. Asynchrony also poses a challenge in the treatment of out-of-order asynchronous message monitoring, which we capture through specification-level permutations of actions.

7.5.1 Motivating Example

As Figure 7.7 shows, from the perspective of the global network, all global behaviours of monitored processes become unobservable. To analyse and state properties of monitored networks, we propose to observe the global behaviours through linking global specifications to global interactions among monitored networks, neglecting local interactions inside endpoints. We propose a notion of global observables and define it through two labelled transitions systems: One is for the network and another is for environments (which represent the abstraction of global specifications and message flows).

As for the network, the notation of global observable transition \( \ell \rightarrow^g \) is applied to \( N \rightarrow^g N' \) for \( N \) without hiding, if there exists a monitor in \( N \) having transition \( \ell \) (by the LTS defined in Figure 7.4). We state the global observables, the actions which can be globally observed, is the aggregation of what all monitors observe and what one can observe from the global queue. As for environments, we formalise global observable environments, ranged over by \( E, E', \ldots \), in order to witness the legality of all messages in transit. A global observable environment includes pending messages together with global specifications (for ease of defining its LTS, we also include local specifications). The use of pending messages is motivated as follows.

In the monitored network, we expect that all endpoint processes follow exactly what global specifications \( G \) define. This is the reason that we state that: For all sending and receiving actions, they are dual in the sending-side and receiving-side monitors when the collection of monitors (i.e. the collection of specifications) is consistent (Definition 7.4.12). However, while there are messages in transit, the consistency of monitors may fail: If a message has been sent from a local monitored process, there is no more monitor holds this sending action; but, since this message is in transit, the monitor at the receiver-side still holds the receiving action waiting for the message. Then the sender-side and the receiver-side monitors are not consistent. Here we propose that, the monitor at the receiver-side needs to be compensated not by other monitor specifications.
but by the message in transit in the global queue. The following example illustrates the situation we consider.

**Example 7.5.1.** Assume a simple global protocol specifies that:

\[ p_1 \rightarrow p_2 : (x : \text{int}) \langle\langle x > 5 \rangle\rangle.G_2 \]

At the beginning, the specification of the sender-side monitor is

\[ s[p_1]^* : p_2!(x : \text{int}) \langle\langle x > 5 \rangle\rangle.G_2 \upharpoonright p_1 \]

and the one of the receiver-side is

\[ s[p_2]^* : p_1?(x : \text{int}) \langle\langle x > 5 \rangle\rangle.G_2 \upharpoonright p_2 \]

When the sender-side monitor permits an outgoing message \( s\langle p_1, p_2, 10 \rangle \), (i.e., a legal sending action), its specification immediately changes to \( s[p_1]^* : G_2 \upharpoonright p_1 \) for the next action; however, the specification of receiver-side monitor may not change because it is waiting for the message travelling in the global queue \( H \cdot s\langle p_1, p_2, 10 \rangle \); as long as the message does not arrive, the receiver-side monitor cannot change its specification. In this case, the receiver-side monitor knows the messages will certainly come by looking at the global queue.

### 7.5.2 The Syntax of \( \mathcal{E} \)

In this section, we formalise the notion of the global observable which can witness the legality of all messages in transit. We call \( \mathcal{E} \) a *global environment*, its syntax is defined as follows:

\[
\begin{align*}
\mathcal{E} & ::= \Gamma, \Delta, \Theta \\
\Gamma & ::= \emptyset \mid \Gamma, a : \text{mode}(G[p]) \\
\Delta & ::= \emptyset \mid \Delta, s[p] : T \mid \Delta, s[p]^* : T \mid \Delta, s : m\text{mv} \\
\Theta & ::= \emptyset \mid \Theta, s : G \\
m\text{mv} & ::= s(p, q, l(v))
\end{align*}
\]

where \( \text{mode} = \{1, 0, IO\} \), \( \Gamma \) is for shared environment, \( \Delta \) is for session environment as the one in Figure 7.3, to which we add messages belonging to session \( s \) as \( s : m\text{mv} \), to specify runtime pending messages carrying the information, and \( \Theta \) is a global environment associating sessions to global specifications. All messages of different sessions model a global queue environment where each assignment is of the form \( m\text{v}_1 \ldots m\text{v}_n, n \geq 0 \).
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

\( mv_i \) is a message of shape \( s(p, p', l(v)) \). \( \tilde{mv} \) is a sequence of pending messages, such as \( s_i(p_1, p_2, l_1(10)) \cdot s_j(p_3, p_5, l_2(\text{"hello"})) \cdot s_k(p_1, p_3, l_3(\text{true})) \). Thus the global observable \( \mathcal{E} \) is composed by the standard shared and session environments, global specifications, and global messages in the global queue.

7.5.3 The Semantics of \( \mathcal{E} \)

Before introducing the LTS of \( \mathcal{E} \), define the projection of a sequence of messages to a particular role. The projection results in a sequence of projected messages sent from the role and indicates their destinations. The projected message is in the form \( pl!(v) \), denoted by \( pm \).

**Definition 7.5.2 (projection of messages).** The projection of \( \tilde{mv} \) onto \( p \), written \( \tilde{mv} \restriction p \), is defined as:

\[
\tilde{mv} \restriction p = \begin{cases} 
  p_2!(v) \cdot \tilde{mv}' \restriction p & \text{if } \tilde{mv} = s(p_1, p_2, l(v)) \cdot \tilde{mv}' \text{ and } p = p_1 \\
  \tilde{mv}' \restriction p & \text{if } \tilde{mv} = s(p_1, p_2, l(v)) \cdot \tilde{mv}' \text{ and } p \neq p_1 \\
  \varepsilon & \text{if } \tilde{mv} = \varepsilon
\end{cases}
\]

\( \tilde{mv} \restriction p \) is defined as above because the messages in transit are the source to indicate (so that the receiver-side monitor can refer to) that the corresponding sending actions have taken place.

**Definition 7.5.3 (retrieving a sub-\( T \)).** Let \( pm, pm', \ldots \) range over projected pending messages. Assume \( T \) and \( pm \) are given. We set:

\[
T - pm = \begin{cases} 
  T_j(v/x_j) - pm' & \text{if } T \vdash p!\{l_i(x_i : S_i)\}\langle A_i\rangle.T_i \text{ and } pm = p!l_j(v) \cdot pm', j \in I \\
  T & \text{if } pm = \varepsilon \\
  \text{undefined} & \text{otherwise}
\end{cases}
\]

where \( I \) is the set of indexes.
In Definition 7.5.3, pm indicates the floating messages which are sent from the endpoint whose monitor has specification T. In other words, pm and T are specified at the same endpoint.

Define $E \xrightarrow{\ell} g E'$ when the session environment in $E$ allows $\ell$ and, after the configuration of some specification or the global queue in $E$ changes, results in $E'$. Figure 7.11 defines the labelled transition system for $E$.

In [E-bch], s : G means that session s obeying global specification G. Note that, T is not simply the projection from G (i.e. $T = G \upharpoonright p_2$) but $T = (G \upharpoonright p_2) \{v/x\} - \tilde{mv} \upharpoonright p_2$ which is obtained by removing all outputted actions produced by $p_2$ (e.g., $s(p_2, p, l(v))$ for some $p$) from all actions of $p_2$ (i.e., $G \upharpoonright p_2$). $T_j$ is similarly represented as:

$$T_j = (G_j \upharpoonright p_2) \{v/x\} - \tilde{mv} \upharpoonright p_2$$

obtained by removing outputted actions of $p_2$ from all actions in $G_j$ of $p_2$ and replacing $x_j$ by $v$ in $G_j \upharpoonright p_2$. [E-bchN] is similar to the rule [BraN] defined in Figure 7.4 when a name $a$ is received by $s[p_1, p_2]!l(a), a : 0(G'[p])$ is added into the environment.

The reason of adopting a more complex method instead of simply applying $G \upharpoonright p_2$, is to obtain the appropriate endpoint specification considering the asynchrony nature of interactions while messages may not be received by recipients immediately due to routing delays. We use the following example to show this situation.

**Example 7.5.4.** Assume a global specification

$$p_1 \rightarrow q_1 : (x_1 : \text{int})\langle x_1 > 0 \rangle, p_1 \rightarrow q_2 : (x_2 : \text{int})\langle x_2 > 1 \rangle.$$  \hspace{1cm} (7.1)

$$q_3 \rightarrow p_1 : (x_3 : \text{int})\langle x_3 > 2 \rangle. \text{end}$$

Obviously, as $p_1$ is active, the local specification of monitor at $p_1$ is

$$s[p_1]^* : q_1!(x_1 : \text{int})\langle x_1 > 0 \rangle, q_2!(x_2 : \text{int})\langle x_2 > 1 \rangle, q_3? (x_3 : \text{int})\langle x_3 > 2 \rangle. \text{end} \hspace{1cm} (7.2)$$

It is possible that participants interact in the following order: (I) $q_3$ firstly sends message $s(q_3, p_1, \langle 3 \rangle)$ to $p_1$, (II) then $p_1$ sends messages to $q_1$ and $q_2$ with $s(p_1, q_1, \langle 1 \rangle)$ and $s(p_1, q_2, \langle 2 \rangle)$ respectively. Note that, as the first interaction happens, $p_1$ may not receive
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

\[ \mathcal{E} \xrightarrow{\gamma} \mathcal{E} \]

\[ \mathcal{E} \vdash v : S_j \quad A_j \{v/x_j\} \downarrow \text{true} \quad G \triangleright p_1 \rightarrow p_2 : \{l_i(x_i:S_i)\{A_i\},G_i\}_{i \in I} \]

[\[ \mathcal{E}, s : G, s[p_2] : T, s : s(p_1,p_2,l_j(v)) \xrightarrow{s[p_1,p_2,l_j(v)]} \mathcal{E}, s : G_j \{v/x_j\}, s[p_2] : T, s : \overline{m \nu} \]

[\[ \mathcal{E}, s : G, s[p_2] : T, s : s(p_1,p_2,l_j(a)) \xrightarrow{s[p_1,p_2,l_j(a)]} \mathcal{E}, s : G_j \{a/x_j\}, a : 0(G'[p]), s[p_2] : T, s : \overline{m \nu} \]

[\[ \mathcal{E} \vdash v : S_j \quad A_j \{v/x_j\} \downarrow \text{true} \quad T \triangleright p_2! \{l_i(x_i:S_j)\{A_i\}.T_i\}_{i \in I} \]

[\[ \mathcal{E}, s[p_1] : T, s : \overline{m \nu} \xrightarrow{s[p_1,p_2,l_j(a)]} \mathcal{E}, s[p_1] : T \{v/x_j\}, s : \overline{m \nu} \cdot s(p_1,p_2,l_j(v)) \]

[\[ \mathcal{E} \vdash a : S_j \quad a \in A_j \quad A_j \downarrow \text{true} \quad T \triangleright p_2! \{l_i(x_i:S_j)\{A_i\}.T_i\}_{i \in I} \]

[\[ \mathcal{E}, s[p_1] : T, s : \overline{m \nu} \xrightarrow{s[p_1,p_2,l_j(a)]} \mathcal{E}, s[p_1] : T \{a/x_j\}, s : \overline{m \nu} \cdot s(p_1,p_2,l_j(a)) \]

\[ \text{im} \in \{I,IO\}, \ a \notin \text{dom}(\mathcal{E}) \]

[\[ \mathcal{E} \xrightarrow{\text{new } a: \text{im}(G'[p])} \mathcal{E}, a : \text{im}(G'[p]) \]

[\[ \mathcal{E}, s[p] : T \xrightarrow{\text{join}(s[p])} \mathcal{E}, s[p] : T \]

[\[ s \notin \text{dom}(\mathcal{E}), \ om \in \{0,IO\}, \ p_i \in \text{role}(G), \ G \text{ is well-formed, } \forall k,j \in I, p_k \neq p_j \ (k \neq j) \]

[\[ \mathcal{E}, a : \text{om}(G'[p]) \xrightarrow{\pi(s[p];G)} \mathcal{E}, a : \text{om}(G'[p]), s : G, \{s[p] : (G \upharpoonright p_i) \}_{p_i \in \text{role}(G)}, s : \emptyset \]

[\[ s \in \mathcal{E}, \ G \upharpoonright p = T, \ om \in \{0,IO\}, \ im \in \{I,IO\} \]

[\[ \mathcal{E}, a : \text{om}(G'[p]), a : \text{im}(G'[p]), s[p] : T \xrightarrow{\pi(s[p];G)} \mathcal{E}, a : \text{om}(G'[p]), a : \text{im}(G'[p]), s[p] : T \]

\[ \text{Figure 7.11: The Labelled Transition System of } \mathcal{E} \]

152
this message immediately. Assume before this message arrives, $p_1$ has sent out messages $s(p_1, q_1, \langle 1 \rangle)$ and $s(p_1, q_2, \langle 2 \rangle)$. Therefore, the global queue has
\[ s(q_3, p_1, \langle 3 \rangle) \cdot s(p_1, q_1, \langle 1 \rangle) \cdot s(p_1, q_2, \langle 2 \rangle) \]
and the global specification maintains as Equation (7.1) because no message has been received yet. Note that, the current specification of monitor at $p_1$ is $s[p_1^* : q_3?(x_3 : \text{int})]:(x_3 > 2).\text{end}$ since it has done two output actions. In such case, $G \upharpoonright p_1$, which is still in Equation (7.2) (because $G$ does not change), cannot reflect the reality of $p_1$ due to the asynchrony nature.

Continue with rule $[\xi-bch]$. It says that, if a value is typed with $S_j$ and satisfies $A_j$, and $G$ has a corresponding interaction up to permutations, it allows $s(p_1, p_2, l_j(v))$ to be received, resulting in new local/global specifications.

$G \hookrightarrow G'$ and $T \hookrightarrow T'$ are defined in Definitions 6.6.5 and 6.6.8. The relation $G \hookrightarrow G'$ says specification $G$ can be permuted to $G'$, so that what is not apparently an active action in $G$ becomes active in $G'$ modulo permutation. For example, if both Buyer and Broker are sending a message to Seller:
\[
G = \text{Buyer} \rightarrow \text{Seller} : (x : \text{int}).\text{Broker} \rightarrow \text{Seller} : (x : \text{string}).\text{end}
\]
then Broker’s message may as well arrive at Seller first, hence we permute this to
\[
G' = \text{Broker} \rightarrow \text{Seller} : (x : \text{string}).\text{Buyer} \rightarrow \text{Seller} : (x : \text{int}).\text{end}
\]
where $G \hookrightarrow G'$ and $G'$ is ready to check an appropriate message from Broker to Seller.

Rule $[\xi\text{-sel}]$ states that when $\xi$ approves an output, its global specification is unchanged but put a message to the global queue, indicating that an interaction has partially happened by an output, but the whole interaction is not completed. And, since $T \hookrightarrow p_2!\{l_i(x_i : S_j) : \langle A_j \rangle, T_i\}_{i \in I}$, after output action $s(p_1, p_2, l_j(v))$ takes place, the chosen label $l_j$ leads configuration of local specification to be $T_j(v/x_j)$ as $v$ replaces $x_j$ for the next interaction. Rule $[\xi\text{-selN}]$ is defined similarly to the rule $[\text{SelN}]$ defined in Figure 7.4. $[\xi\text{-new a}]$ says if a shared name $a$ is new to $\xi$, then $\xi$ adds this new shared channel. $[\xi\text{-join}]$ makes a specified session-role $s[p]$ become active. $[\xi\text{-req-b}]$ says if a session $s$ is new to $\xi$, $\xi$ adds the global queue belonging to session $s$ as $s : \emptyset$, the global specification of $s$ as $s : G$, and the session environment which is generated by
7. THE CALCULUS OF DYNAMIC ASYNCHRONOUS MONITORING

the projections of \( G \) to all roles in \( G \), write \( \{ s[p_i] : (G \upharpoonright p_i) \}_{p_i \in \text{role}(G)} \), every \( p_i \) of which involves in \( s \). Since \( E \) watches the global environment containing the information of all local processes, as free request or bound/free accept happens at an endpoint, it does not affect the global environment. \([E_{\text{req-f}}]\) and \([E_{\text{acc-b/f}}]\) state this fact. Note that, for \([E_{\text{req-f}}]\) (or \([E_{\text{acc-b/f}}]\)), if the left-hand side environment violates the rule, the rule \([E_{\text{tau}}]\) is applied.

7.5.4 The Typing Rules of \( E \)

In the following rules, we define \( E \vdash \_g N \) as a network \( N \) is proved under the global observable system, i.e. \( \vdash \_g \), by environment \( E \).

\[
\frac{M = \Gamma_1 \Delta \Delta' \subseteq \Gamma'}{E, \& M[\_g P] \vdash \Gamma, \Delta, \Delta' \Delta_0} \quad \frac{\Gamma \vdash \_g a : \text{im}(G[p]), a : \text{of}(G[p])}{E \vdash H \cdot \pi(s[p] : G)} \quad \text{[E-PM1]}
\]

\[
\frac{H = \emptyset \quad \Gamma, s : H \vdash E}{E, \_g H} \quad \frac{\Gamma, s : \text{mv} \vdash H \quad \Gamma, s : \text{mv} \cdot s(p, p', l(v)) \vdash H \cdot s(p, p', l(v))}{E \vdash H} \quad \text{[E-PM2]}
\]

\[
\frac{\Gamma, \Delta_1, \Delta_2, \Theta \vdash N_i \quad (i = 1, 2) \quad \text{dom}(\Delta_1) \cap \text{dom}(\Delta_2) = \emptyset}{\Gamma, \Delta_1, \Delta_2, \Theta \vdash N_1 \parallel N_2} \quad \text{[E-PAR]}
\]

\[
\frac{\text{E is coherent}}{\text{E \vdash N}} \quad \text{[E-CO]}
\]

Every rule is explained as follows:

[E-M] As the information about monitor \( M \) is known by the global environment, the global environment approves the monitored process \( M[\_g P] \).

[E-PM1] As the shared environment has \( a : \text{im}(G[p]) \), which indicates that \( a \) is capable of playing role \( p \) under the specification \( G \), the invitation message \( \pi(s[p] : G) \), produced by either bound request \( \pi(s[p] : G) \) or free request \( \pi(s[p] : G) \), is proved by the global environment \( \Gamma, E \).

[E-PM2] As the global queue is empty, it is always valid under \( \Gamma, s : H \), for any \( \Gamma \).

[E-PM3] As the global environment \( \Gamma, s : \text{mv} \vdash H \) proves the pending messages \( H \), the additional message \( s(p_1, p_2, l(v)) \) can be proved by \( \Gamma, s : \text{mv} \cdot s(p_1, p_2, l(v)) \) where the message environment contains the additional message.
7.5 Global Environment $\mathcal{E}$

[\mathcal{E}\text{-PAR}] As for $i = 1, 2$, the global environment $\Gamma, \Delta_i, \Theta$ proves the network $N_i$ and $\Delta_1$ and $\Delta_2$ has no common session roles or common message environment, then the global environment $\Gamma, \Delta_1, \Delta_2, \Theta$ proves the composed network $N_1 \parallel N_2$.

[\mathcal{E}\text{-CO}] As the network $N$ can be ensured (i.e. proved) under the system of the global observable environment, we say the network conforms to the global observable $\mathcal{E}$. The coherence of a network to the global observable $\mathcal{E}$ is introduced in the next section.

7.5.5 The Coherence of $\mathcal{E}$

Definition 7.5.5. As long as $s : \text{end}$ is reached, session $s$ is finished and everything related to $s$ is deleted immediately from $\mathcal{E}$. Whenever $s : G$ where $G = \text{end}$, $s : G \notin \mathcal{E}$.

Coherence of $\mathcal{E}$ is defined similarly to the one of the network, taking care of the pending messages in the global queue.

Definition 7.5.6 ($\mathcal{E}$ coherence). Let $\mathcal{E} = \Gamma, \Delta, \Theta$. Then we say $\mathcal{E}$ is coherent when all of the following conditions hold:

1. $\forall a, a : \text{om}(G[p]) \in \Gamma$ implies that $\exists \Gamma', a : \text{im}(G[p]) \in \Gamma'$.
2. If $s[p] \in \Delta$, then $s : G \in \Theta$ and $p \in \text{role}(G)$.
3. $\forall p \in \text{role}(G)$, if $s : G \in \Theta$ and $s : \tilde{m}v \in \Delta$, then $\exists T$ such that $G \parallel p - \tilde{m}v \parallel p = T$ and $\Delta(s[p]) \rhd T$.
4. If $s : G \in \Theta$ and $s : \tilde{m}v_1 \cdot s(p, q, l_j(v)) \cdot \tilde{m}v_2 \in \Delta$ and $\tilde{m}v_1$ does not suppress $s(p, q, l_j(v))$, then

$$G \rhd p \rightarrow q : \{l_i(x_i : S_i)\langle A_i \rangle G'_i\}_{i \in I}$$

where $A_j\{v/x_j\} \downarrow \text{true}$.

The first rule is standard. It says whenever there is an output mode for capability of playing role $p$ specified under $G$, there exists its corresponding input mode in some shared environment $\Gamma'$.

The second rule of $\mathcal{E}$-coherence says: Every session-role $s[p]$ comes from a global specification, which defines this session $s$ and all roles, i.e. $p$, in this session.

In the third rule, $G \parallel p$ represents all interactions defined in $G$ at $p$ and the order of actions that $p$ should fire; similarly, $\tilde{m}v \parallel p$ indicates the targets (i.e. destinations) of
pending messages sent from $p$, and $G \upharpoonright p - \overrightarrow{mv} \upharpoonright p$ together is the left specification after $p$ outputs to targets in $\overrightarrow{mv} \upharpoonright p$. This rule can be read as: For every role in a session, its fully defined actions are exactly the summation of the “happened” actions, which are currently recorded in the global queue, and the “going-to-happen” actions.

The forth rule states the relation between pending messages and its global specification. The existence of a pending message means that the corresponding output has happened, but input has not yet taken place. This rule says: The existence of a pending message implies (I) its corresponding interaction should be defined in global specification, and (II) this interaction can be permuted to the top of its global specification with minimum number of unit permutations (i.e. it is not suppressed by any interaction sequenced ahead of it).

**Proposition 7.5.7** (conformance w.r.t. the global observables). If $\mathcal{E}$ is coherent and $\mathcal{E} \xrightarrow{\mathcal{L}} \mathcal{E}'$, then $\mathcal{E}'$ is coherent.

**Proof.** The proof is in Appendix B.5.

**Definition 7.5.8** ($\mathcal{E} \vdash N$). We write $\mathcal{E} \vdash N$ to state that network $N$ conforms to $\mathcal{E}$ as long as

1. $\mathcal{E}$ is coherent, and
2. the shared and session environments in $\mathcal{E}$ come from the monitors in $N$, and
3. the message environment in $\mathcal{E}$ comes from the pending messages in the global queue of $N$.

If $\mathcal{E}$ is coherent and $\mathcal{E} \vdash N$, then $N$ is coherent. Therefore, with the formalism of global observer, another viewpoint of the property of session fidelity is:

**Theorem 7.5.9** (session fidelity w.r.t. $\mathcal{E}$). If $\mathcal{E} \vdash N$ and $N \xrightarrow{\mathcal{L}} N'$ then $\mathcal{E} \xrightarrow{\mathcal{L}} \mathcal{E}'$ such that $\mathcal{E}' \vdash N'$.

**Proof.** It is proved in Appendix B.5.

The global observable $\mathcal{E}$ maintains all specifications, including the global and the local ones, and together with pending messages. Whenever $N$ is coherent, we can construct a (coherent) $\mathcal{E}$ such that $\mathcal{E} \vdash N$. The version of session fidelity w.r.t $\mathcal{E}$ states that, global interactions in a coherent network never violate the expected network-wise global specifications: The former follows the latter step by step.
Overview Chapter 8 is a full version of the published paper “Specifying Stateful Asynchronous Properties for Distributed Programs” (40). In this chapter, the theorems and properties of stateful specifications for dynamic observations among communicating processes are introduced. They are based on the condition that observations are done asynchronously, where a semantic problem in specifications for distributed systems arises. Consider a general situation described as follows: When an observer (e.g. a trusted monitor) is located at an observee, the order of the observee’s actions the observer sees is exactly the same as what happens at the observee. However, when an observer sits outside the observee, e.g. remotely from the observee, the order of actions that she observes may not be as same as what happens at the observee. The former kind of observation is synchronous, and the latter kind is asynchronous. Although the synchronous observation precisely captures the behaviour of the observee, in real-life distributed systems, asynchronous observation is the norm and often a necessity. To make a remote observer be able to properly verify behaviours of processes against a non-trivial stateful specification, this chapter characterises and validates asynchronously verifiable specifications, or simply called asynchronous specifications. We also propose and prove the properties for them.
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

8.1 Motivating Example

Before formally introducing the syntax and semantics of specifications, this section motivates key ideas through simple examples. Our specification language is based on multi-party session types [18, 86] with annotations by logical formulae, extending [22] with endpoint (local) states. Our focus is on visible asynchronous interactions rather than internal actions. We treat three examples. The first motivates the use of state in protocol specifications through a typical business scenario. The second introduces the semantic issue in specifications in the presence of asynchrony through a simplest possible example. The third example illustrates the use of sets in specifications for asynchrony, linking the specification to the corresponding traces, adumbrating our semantic analysis later.

8.1.1 Using State in Specifications

The first example motivates the use of endpoint state in a stateful protocol, which is a part of a specification. Consider the following purchase-invoice scenario:

(step 1) **Buyer** sends a *product name* (denoted by variable *PName*) to **Seller**, then **Seller** replies with its *price* (denoted by variable *Price*), and **Buyer** decides whether to purchase (then go to step 2) or not (then terminate). We assume shipping is done independently.

(step 2) **Seller** sends **Buyer** an *invoice* for the purchased product.

This scenario can be realised as a single protocol [22, 39, 86] between **Buyer** and **Seller**, consisting of a series of a few message exchanges. The scenario can also be realised using two protocols, one for each step. This form has a merit in flexibility: For example, when **Buyer** and **Seller** finish step 1, both can terminate that transaction. Then an invoice can be issued any time later. Example 8.1.1 presents protocols with logical annotations following the framework of representing one scenario with two separated protocols.
8.1 Motivating Example

Example 8.1.1 (SP for a cross-session Purchase-and-Invoice scenario).

\begin{align*}
G_{pcs} &= B \rightarrow S : \text{Request}(PName : \text{string}) \\
S &\rightarrow B : \text{Confirm}(PNameConf : \text{string}, Price : \text{int}) \\
&\quad \langle\langle PNameConf = PName \land Price \geq \varepsilon \rangle\rangle \\
&\quad \langle\langle \text{true} \rangle\rangle. \\
B &\rightarrow S : \{\text{OK}(UserID : \text{int}) \langle\langle UserID \neq 0 \rangle\rangle \langle\langle \text{true} \rangle\rangle\}. \\
S &\rightarrow B : (PNo : \text{int}) \\
&\quad \langle\langle PNo \notin \text{dom}(PLog) \rangle\rangle \\
&\quad \langle\langle \text{PLog} := \text{PLog} \cup \{PNo \mapsto (UserID, PName, Price)\} \rangle\rangle \\
&\quad \langle\langle \text{true} \rangle\rangle. \\
\text{end} \\
KO().\text{end}
\end{align*}

\begin{align*}
G_{ivc} &= S \rightarrow B : (PNo : \text{string}, Invoice : \text{int}) \\
&\quad \langle\langle PNo \in \text{dom}(PLog) \land Invoice = \text{PLog}(PNo) \rangle\rangle \langle\langle \text{true} \rangle\rangle.\text{end}
\end{align*}

Above $G_{pcs}$ and $G_{ivc}$ denote the global stateful protocols, or SPs from now on for short, corresponding to Steps 1 and 2. Each specifies the behaviour which the participants, $S$ (denoting seller) and $B$ (denoting buyer), should realise at each session. $\langle\langle ... \rangle\rangle \langle\langle ... \rangle\rangle$ are the obligations for sender (the former) and receiver (the latter), respectively. Note that $\langle\langle \text{true} \rangle\rangle$ means no obligation and no state change. We will formally introduce their syntax in Section 8.3. In this example, the state of $S$, represented by the field $PLog$ (the Purchase Log, which we consider to be a key-value store, mapping distinct keys to values), links the two protocols. Both protocols can be read intuitively. First, in $G_{pcs}$,

1. $B$ firstly sends a request (Request is an operator name), with the message value $PName$ of type string, which is a product name.

2. $S$ confirms by sending the same product name and its price, where the latter should be a non-negative integer as annotated.

3. If $B$ says OK by sending its identity, then (in practice, after authenticating the identity) $S$ sends back a fresh purchase number $PNo$ which should be fresh, i.e. it should not be in the domain of $PLog$. As a result, this new key and the corresponding information is added to $PLog$. On the other hand, if $B$ says KO (not OK), then the conversation terminates.
As may be seen from this example, our protocols use a local state to record an abstraction of preceding interactions across sessions, and to constrain future behaviours using this record. Its ultimate aim is to specify visible behaviours of a process: Thus the stipulated state does not (have to) come from an actual state of a process, i.e. we may call it a “ghost state” following JML [1].

8.1.2 Synchrony v.s. Asynchrony for Stateful Specifications

The next example illustrates the central topic of this chapter, asynchrony in specifications, showing how a specification can be “too synchronous” for asynchronous observations. We focus on a part of the previous example, and, as well use stateful protocols, which compose specifications, to indicate the asynchrony issue. The purchase number allocator $S$ will, upon a request from a buyer $B$ at each session, issue a booking number incrementing the previously issued one: $S$ issues e.g. 1, 2, 3, ... in a sequence of sessions. Example 8.1.2 (a) shows a protocol $G_{\text{sync}}$ for such interactions, specifying a simple behaviour that the participants, $S$ and $B$, should realise at each session. $c$ is a local state of $S$, denoting the next booking number.

Example 8.1.2 (Stateful Protocol of purchase number allocator: synchronous v.s. asynchronous).

(a) synchronous spec

$G_{\text{sync}} = B \rightarrow S : \text{req}(\varepsilon).$
$S \rightarrow B : \text{ans}(x : \text{int})$
$\langle \langle x = c; c := c + 1 \rangle\rangle \langle \langle \text{true}; \varepsilon \rangle\rangle.$

(b) asynchronous spec

$G_{\text{async}} = B \rightarrow S : \text{req}(\varepsilon).$
$S \rightarrow B : \text{ans}(x : \text{int})$
$\langle \langle x \notin c; c := c \cup \{x\} \rangle\rangle \langle \langle \text{true}; \varepsilon \rangle\rangle.$

In the first line of $G_{\text{sync}}$, $B$ (for buyer) requests $S$ (for seller) a purchase number by sending req$(\varepsilon)$, where $\varepsilon$ means there is no message value in this request. In the second line, an integer $x$ is sent from $S$ to $B$, for which $\langle \langle x = c; c := c + 1 \rangle\rangle$ specifies the obligation for $S$, while no obligation i.e. $\langle \langle \text{true}; \varepsilon \rangle\rangle$ for $B$. The first part “$x = c$” says that $x$ should be equal to $c$. The second part “$c := c + 1$” says that, after sending, $S$ will increase $c$ by 1, which constrains further behaviours of $S$ in later sessions.

$G_{\text{sync}}$ is an example of a SP which makes sense synchronously but not asynchronously. It seems an intuitively sensible stateful protocol: However, if a remote observer is far away, even if $S$ actually sends the series of booking numbers 1, 2, 3, 4, ... in this order, they may arrive at the observer as e.g. 2, 4, 1, 3, ..., under the assumption that the order
of messages belonging to distinct sessions may not be preserved, which is a practical assumption. In particular, note this remote observer will consider $S$ as being ill-behaved with respect to $G_{\text{sync}}$: The correctness for $S$ (which is synchronous) and the correctness for its observer (which is asynchronous) are not congruent.

As a remedy, we present $G_{\text{async}}$ in Example 8.1.2 (b), which is intended for asynchronous observation. We use the set of booking numbers: $c$, whose type is a set of integers, corresponds to $\text{PLog}$ in Example 8.1.1. The new stateful protocol just says, in brief, that “$S$ always sends a fresh number”. If the behaviour of $S$ satisfies this condition at $S$, then even though messages from $S$ may arrive out-of-order, the remote observer can verify that they are correct w.r.t. $G_{\text{async}}$, so that the actions of $S$ and their asynchronous observation by a remote observer coincide. We shall later verify this statement formally.

### 8.1.3 Capturing Causality Using Sets in Stateful Specifications

While $G_{\text{async}}$ gives a reasonable stateful protocol, it is not the strongest possible one if our target is the server who issues booking numbers incrementally based on the previous number. For example, if the same buyer sequentially repeats a series of request-reply sessions, that buyer (and an observer sitting in-between) will observe $1, 2, 3, 4$, but this point is not captured by $G_{\text{async}}$.

**Example 8.1.3 (a refinement of $G_{\text{async}}$).**

\[
G_{\text{assign}} = \begin{cases}
B \rightarrow S : \text{req}(\varepsilon) \langle \langle \text{true}; \varepsilon \rangle \rangle \langle \langle \text{true}; t := t + 1, c := c \cup \{ t \} \rangle \rangle , \\
S \rightarrow B : \text{ans}(x : \text{int}) \langle \langle x \in c ; c := c \setminus \{ x \} \rangle \rangle \langle \langle \text{true}; \varepsilon \rangle \rangle .
\end{cases}
\]

$G_{\text{assign}}$ in Example 8.1.3 is a refinement of $G_{\text{async}}$ in Example 8.1.2 so that, while still being suitable for asynchronous observations, can capture a stronger causal constraint. It uses two states: $t$, a counter, and $c$, a collection of valid numbers to be issued. $t$ and $c$ are incremented when receiving a request, while the sent value is taken off from $c$.

Assume the server issues the booking numbers starting from 1. The intuition behind the construction is as follows:

1. If $S$ receives $n$ requests, as a whole, the numbers which can be issued are among $\{1, 2, \ldots, n \}$. 

161
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

<table>
<thead>
<tr>
<th>cases</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
</tr>
</thead>
<tbody>
<tr>
<td>(I) actions</td>
<td>$s_1[B,S]?\text{req}(\varepsilon)$</td>
<td>$s_2[B,S]?\text{req}(\varepsilon)$</td>
<td>$s_1[S,B]\text{ans}(1)$</td>
<td>$s_2[S,B]\text{ans}(2)$</td>
</tr>
<tr>
<td>(II) actions</td>
<td>$s_1[B,S]?\text{req}(\varepsilon)$</td>
<td>$s_1[B,S]?\text{req}(\varepsilon)$</td>
<td>$s_1[S,B]\text{ans}(1)$</td>
<td>$s_2[S,B]\text{ans}(2)$</td>
</tr>
<tr>
<td>(III) actions</td>
<td>$s_2[B,S]?\text{req}(\varepsilon)$</td>
<td>$s_2[B,S]?\text{req}(\varepsilon)$</td>
<td>$s_2[S,B]\text{ans}(1)$</td>
<td>$s_1[S,B]\text{ans}(2)$</td>
</tr>
</tbody>
</table>

(I) states $t \mapsto 1, c \mapsto \{1\}$ $t \mapsto 2, c \mapsto \{1, 2\}$ $t \mapsto 2, c \mapsto \{2\}$ $t \mapsto 2, c \mapsto \{\}$

(II) states $t \mapsto 1, c \mapsto \{1\}$ $t \mapsto 2, c \mapsto \{1, 2\}$ $t \mapsto 2, c \mapsto \{1\}$ $t \mapsto 2, c \mapsto \{\}$

(III) states $t \mapsto 1, c \mapsto \{1\}$ $t \mapsto 1, c \mapsto \{\}$ $t \mapsto 2, c \mapsto \{2\}$ $t \mapsto 2, c \mapsto \{\}$

**Figure 8.1:** The Valid Traces of Asynchronous and Synchronous Interactions w.r.t. $G_{\text{assign}}$

2. If $S$ issues a number from this set, the remaining numbers are what it can issue next.

As we shall see later, the stateful protocol has the property that, if $S$ behaves well w.r.t. $G_{\text{assign}}$, then a remote observer also finds it well-behaved.

To understand $G_{\text{assign}}$ as a stateful protocol, consider two sessions following the protocol, $s_1$ and $s_2$. Assume the initial states are $t \mapsto 0$ and $c \mapsto \{\}$. Then $G_{\text{assign}}$ says the traces in Figure 8.1 are valid ones. Figure 8.1 lists the traces together with step-by-step state change: (I,II,III) are categories each stipulating how states will change.

Above, $s_1[B,S]?\text{req}(\varepsilon)$ denotes an input ? from $B$ to $S$ at session $s_1$ carrying a req-message without value; $s_1[S,B]\text{ans}(1)$ is an output ! from $S$ to $B$ at $s_1$ carrying a ans-message with value 1. (I) and (II) are the traces where a remote observer observes that two consecutive inputs have arrived first. Note that, even if $S$ may have indeed outputted immediately after the first input, we can have these traces due to asynchrony. Even then, unlike $G_{\text{async}}$, the observer is always sure, by $G_{\text{assign}}$, that the returned values should be no more than 2, i.e. it is either 1 or 2. In (III), the observer observes the second request only after the answer to the first request. Note the request-answer order.
in each session is preserved because without the request, its answer cannot occur (which is Lamport’s ordering (98)). Note that, the order of two messages inside each session is preserved. Unlike \( G_{async} \), the observer can expect, based on \( G_{assign} \), that the first answer is surely 1, and the second is surely 2.

The above example shows how we can represent causality while still (intuitively) keeping the asynchronous nature of specifications. It also shows how traces of actions can be used to give extensional meaning of specifications. This observation is given a formal account in Section 8.3 later.

8.1.4 Analysis of Capturing Causality: \( G_{assign} \)

Continue with section 8.1.3 from \( G_{assign} \) we have learnt that an observer can be more insightful if she has more information (which are initially established by input actions).

**Convention 8.1.4.** An observer (remote/close) can expect and reasonably guess the behaviours of her observees based on the messages she has observed. Without loss of generality, we assume that the messages delivered by observees can represent the behaviours of observees.

Based on \( G_{assign} \), in which the assigned number to each session (established at each request) is asked to be increased with the coming requests one by one, the following properties say that a remote observer can expect the next outputted value based on what she observes. Let a sequence of actions, called trace, denoted by \( s \). Let \( I(s) \) be the sequence of input actions of \( s \), \( O(s) \) be the sequence of output actions of \( s \), and \( V(s) \) be the sequence of values carried in \( s \). Let \( num(s) \) be the length of \( s \), and \( prefix(s) \) be the set of prefixes of \( s \). Moreover, let \( v(\ell) \) be the value carried by action \( \ell \), and \( ini(t) \) be the initial value of state \( t \in G_{assign} \). Because in the following cases we only discuss one state of an endpoint, we write \( ini(t) \) simply as \( ini \).

For every trace w.r.t role \( S \) (representing server) satisfying \( G_{assign} \upharpoonright S \), it should have the following properties:

\( tq0 \). binding conventions.

\( tq1 \). \( num(I(s)) \geq num(O(s)) \).

\( tq2 \). \( \forall \ell \in s \cap \ell = s[S,B]l(v) \subset \exists \ell' \in s, \ell' = s[B,S]?l(v) \).

163
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

rq3. \( \forall \ell, \ell' \in O(s), \ell \neq \ell', \text{ then } v(\ell) \neq v(\ell'). \)

rq4. \( \forall \ell \in O(s'), s' \in \text{prefix}(s), \text{ini} \leq v(\ell) \leq \text{num}(I(s')) + \text{ini}. \)

The first 3 properties (rq0, rq1 and rq2) ensures the trace satisfies the interaction structure defined in \( G_{\text{assign}} \). In rq1, operation \( I(s) \) extracts the input actions from trace \( s \) as a new trace, and \( \text{num}(I(s)) \) means the length of input actions in \( s \). Similarly, operation \( O(s) \) extracts the output actions from trace \( s \) as a new trace \( \text{num}(O(s)) \) means the length of output actions in \( s \). Overall it states that the number of inputs (i.e. requests from the buyers) should be bigger than the number of outputs (i.e. assignments from the server). rq2 states that only when a request takes place, an assignment takes place. rq3 ensures that every assigned (outputted) value (i.e. \( \ell \in O, (v(\ell)) \) is distinct. The operation \( v(\ell) \) extracts the value carried by action \( \ell \). In rq4, ini is a constant, denoting the initial value of a particular state used for checking outputted values. Here it is the initial value of state \( c \) defined in \( G_{\text{assign}} \). rq4 states that, an outputted value carried by an output action should be smaller than or equal to the number of inputs which positioning ahead of it. rq3 and rq4 together imply that, for a given trace \( s = \ell_1...\ell_n \), the next outputted value has a fixed range: This range can be measured by knowing how many requests from buyers have occurred and how many assignments to buyers have done.

For example, assume \( \text{ini} = 1 \); when an observer observes a trace \( s_1[B,S]?\text{req}(\varepsilon) \cdot s_2[B,S]?\text{req}(\varepsilon) \cdot s_3[B,S]?\text{req}(\varepsilon) \), if the next action is \( s_2[S,B]!\text{ans}(v) \), then \( v \in \{1,2,3\} \); assume \( v = 3 \). After action \( s_2[S,B]!\text{ans}(3) \), if the upcoming one is \( s_1[S,B]!\text{ans}(v') \), then \( v' \in \{1,2\} \) because 3 has been assigned; assume \( v' = 1 \). When a new request comes, says \( s_4[B,S]?\text{req}(\varepsilon) \), currently the overall actions starting from the beginning is

\[
s_1[B,S]?\text{req}(\varepsilon) s_2[B,S]?\text{req}(\varepsilon) s_3[B,S]?\text{req}(\varepsilon) s_2[S,B]!\text{ans}(3) s_1[S,B]!\text{ans}(1) s_4[B,S]?\text{req}(\varepsilon)
\]

the next output action of it can be \( s_n[S,B]!\text{ans}(v'') \), \( n \in \{3,4\} \) and \( v'' \in \{2,4\} \).

These analyses are useful for verifying a trace step by step. For example, assume the following trace is an initial trace: \( s_1[B,S]?\text{req}(\varepsilon) \cdot s_1[S,B]!\text{ans}(2) \cdot s_2[B,S]?\text{req}(\varepsilon) \) is not right immediately at \( s_1[S,B]!\text{ans}(2) \) because the only possible value at the moment when it is assigned is 1.
8.2 The Language of Stateful Specifications: SP

8.2.1 The Syntax of SP

Figure 8.2 summarises the grammar of global stateful protocols \((G,...)\) for specifying the interaction structure of a session from global viewpoints, and local stateful protocols \((T,...)\), projected from the global \(G\), for specifying protocols for local endpoints. Note that the “state” used here means the “fields of data storages”. For example, it can be a field \texttt{counter} in a server for counting the number of visiters, or a field \texttt{credit} in a bank user for indicating the user’s current savings, etc. This syntax enriches (22) with local states update and rich operations on them: By adding simple data update \(E\) and data type \(set\), we obtain a rich class of stateful specifications (which consist of local SPs).

A state variable, denoted by \(f\), consists of zero or more fields. A field gets read in a predicate \(A\) and gets read and written in an update \(E\). We call \(\langle A; E \rangle\) obligation. We use updates instead of post-conditions for usability in runtime verification. \((S,...)\) are sorts (data types), and \((e,...)\) are expressions, where \(op(e_1,...,e_n)\) is the operation \(op\) on parameters \(e_1,...,e_n\). We use data types such as product \(S_1 \times S_2\), set \(set(S)\) and (finite) function \(map(S_1,S_2)\). Sets and functions play important roles in asynchronous specifications. In expressions, \(x\) is a variable, \(v\) is a value, \(f\) is a (mutable) field. In \(E\), \(f := e\) stipulates that when \(e \downarrow v\), \(f\) is updated with value \(v\), which makes the value of \(f\) be \(v\), denoted by \(f \mapsto v\). The grammars of \(G\) and \(T\) are simplified for distilled
presentation. They are similar to the ones defined in Figures 6.1 and 6.3 in Chapter 6, where $G$ specifies the global interactions and $T$ specifies the obligation for every action coming from endpoints. The recursion of $G$ and $T$ can be omitted because, while a recursion is finite, we can unfold the finitely-recursive obligations of the body to several continuous obligations, each of which is defined by $T$. All results are preserved.

In $G$, $p \rightarrow q$ describes the communication (interaction) from sender $p$ to receiver $q$, while $p!$ and $p?$ are endpoint actions for output (to $p$) and input (from $p$) respectively. In $l_i(x_i : S_i)$, $l_i$ is the label for a branch, when $l_j$ is chosen, the interaction variable is $x_j$, and $S_j$ is its type. In $G$-cm, the first obligation $\langle\langle A; E \rangle\rangle$ is for the sender, indicating the sender should guarantee that its message $x$ satisfies $A$ and as a result $E$ is done; the second obligation $\langle\langle A'; E' \rangle\rangle$ is for the receiver, indicating it can expect a message $x$ to satisfy $A'$ and as a result $E'$ is done. Rule G-par particularly asks that $\text{role}(G_1) \cap \text{role}(G_2) = \emptyset$, which means that no role is shared by $G_1$ and $G_2$, where $\text{role}(G)$ denotes the set of roles in $G$. Rule L-sel is for sender’s behaviour, while rule L-bra is for receiver’s behaviour. Parallel composition specifies two interactions in parallel, while end denotes the end of interactions. As a notational convention, if both obligations for the sender and the receiver are trivial (i.e. the predicate is true and the update is $\varepsilon$) then they are omitted.

8.2.2 Consistency Principles and Well-formedness

Before introducing the conditions of well-formedness for stateful global specifications, the set of states of a predicate or an update is defined as follows.

**Definition 8.2.1 (the set of states).** $\text{field}(C)$ denotes the set of states (i.e. fields) occurring in $C$. $C$ can be a predicate (i.e. $A$) or an update (i.e. $E$).

Assume $p \rightarrow q : \{l_i(x_i : S_i)\langle\langle A_i; E_i \rangle\rangle\langle\langle A'_i; E'_{i} \rangle\rangle.G_i \}_{i \in I}$ is inside a context, with possibly preceding interactions. The following conditions of well-formedness for stateful global SPs, based on (22), stipulate the consistency principles of global stateful protocols:

1. (a) $\forall i \in I, \text{field}(A'_i) = \emptyset$; and (b) $\forall i \in I, A_i$ implies $A'_i$.

2. (history sensitivity) $A_i$ and $E_i$ only refer to interaction variables which $p$, the sender, has sent or received before, as well as $x_i$; moreover, $A_i$ and $E_i$ only contain the states of the sender. Similarly, $A'_i$ and $E'_{i}$ are for the receiver. Moreover, $A_i$ and $E_i$ only contain the states of the sender $p$, while $E'_{i}$ only contains the states of the receiver $q$. 

166
3. (temporal satisfiability) At each step, and for any state, there is always a branch with label $l_i$ and a value $x_i$ that satisfy $A_i$  (hence $A'_i$ at each step).

Condition 1.(a) says that a predicate of a receiver is stateless. Two reasons for this requirement: First, if a receiving-side predicate relies on its own local state, then the sender may not be able to find a “proper” value to send; secondly, a sent message, which has been verified by a trusted observer (e.g. a system monitor), should not be judged invalid by the predicate at the receiver-side (or rejected by the receiver-side’s system monitor), otherwise it is inconsistent because it implies that the judgement at the sender-side is incorrect. Condition 1.(b) says that, in every interaction, the predicate at sender always implies the predicate at the receiver: Together with 1.(a), it means that if the sender sends a message that satisfies the sender’s predicate, then automatically the receiver’s predicate is satisfied (the latter is however useful for the receiver to know what to expect).

**Example 8.2.2** (the sender’s predicate always implies the receiver’s). Let state $f_q$ belong to role $q$. Assume $f_q = 5$. Consider the following simple global SP which violates condition 1.(a):

$$p \rightarrow q : (x : \text{int}) \langle \langle \text{true} ; \varepsilon \rangle \langle f_q < x ; f_q := x \rangle \rangle.$$  

When session participants apply this global SP for communication through a session, say $s$, if session-role $s[p]$ sends a message with value less than 5, this action will be rejected and considered invalid by the receiver-side observer. However, it is a valid action according to the sender-side observer who knows nothing about the predicate at the receiver side. Condition 1.(a) prevents this situation because all system monitors should be considered as having the same governance ability: Whenever the sender-side monitor approves an action according to the protocol, the receiver-side monitor should also approve it because the monitor at the sender side is trusted.

For the similar reason, condition 1.(b), which implies 1.(a), ensures that whenever the sender-side observer approves an action, the receiver-side agrees with it. The following global SP violates condition 1.(b):

$$p \rightarrow q : (x : \text{int}) \langle \langle x > 10 ; \varepsilon \rangle \langle x > 20 ; \varepsilon \rangle \rangle.$$  

This SP is not reasonable because, if the sender sends a value of $x$ in the range from 11
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

to 20, from the sender’s viewpoint, she obeys the protocol \( x > 10 \); however, she will be rejected by the receiver because she does not know that the receiver asks a value more than 20.

Conditions 2 and 3 are based on the consistency principles, history sensitivity and temporal satisfiability, introduced in Section 6.3 which are based on (22). The following examples illustrate the conditions 2 and 3, respectively.

Example 8.2.3 (history sensitivity). Let state \( f_q \) belong to role \( q \). The following global SP satisfies history sensitivity with the similar reasoning of Example 6.3.1 in Section 6.3:

\[
\begin{align*}
p \to q : & \quad (x : \text{int}) \langle x > 10 ; \varepsilon \rangle \langle x > 5 ; f_q := x \rangle. \\
q \to r : & \quad (x : \text{int}). \\
r \to q : & \quad (y : \text{int}) \langle y > x ; \varepsilon \rangle \langle y > x ; f_q := y \rangle
\end{align*}
\]

because every participant \( p, q \) and \( r \) knows the variables deciding the predicates.

However, since the state \( f_q \) is only known by role \( q \), when the constraint of \( f_q \) is added to the predicate of \( p \), it violates the principle of history sensitivity:

\[
\begin{align*}
p \to q : & \quad (x : \text{int}) \langle x > f_q ; \varepsilon \rangle \langle x > f_q ; f_q := x \rangle. \\
q \to r : & \quad (x : \text{int}). \\
r \to q : & \quad (y : \text{int}) \langle y > x ; \varepsilon \rangle \langle y > x ; f_q := y \rangle
\end{align*}
\]

Example 8.2.4 (temporal satisfiability). Let state \( f_q \) belong to role \( q \). The global SP below respects temporal satisfiability with the similar reasoning of Example 6.3.2 introduced in Section 6.3:

\[
\begin{align*}
p \to q : & \quad \text{len}(x : \text{int}) \langle 49 > x > 5 ; \varepsilon \rangle \langle 49 > x > 0 ; f_q := x + 10 \rangle. \\
q \to r : & \quad \{ \text{walk}(y : \text{int}) \langle x < y < 10 ; \varepsilon \rangle \langle x < y < 30 ; \varepsilon \rangle, \\
& \quad \text{run}(y : \text{int}) \langle x < y < f_q ; \varepsilon \rangle \langle x < y < 60 ; \varepsilon \rangle \}
\end{align*}
\]

although the state \( f_q \) is involved in the predicate at branch “run”, since there are always integers between \( x \) and \( x + 10 = f_q \) and the seller’s predicate \( \langle x < y < f_q \rangle \) always implies the receiver’s predicate \( \langle x < y < 60 \rangle \) when \( x \) is confined between 5 to 49, and \( f_q \) is updated to \( x + 10 \).

However, when the update of \( f_q \) is changed to \( f_q := x \), the global SP violates temporal
8.2 The Language of Stateful Specifications: SP

satisfiability because there is no path to go forward when the value of \( x \) is more than 9.

\[
p \rightarrow q : \text{len}(x : \text{int}) \langle\langle 49 > x > 5 ; \varepsilon \rangle\rangle \langle\langle 49 > x > 0 ; f_q := x \rangle\rangle.
\]

\[
q \rightarrow r : \{ \text{walk}(y : \text{int}) \langle\langle x < y < 10 ; \varepsilon \rangle\rangle \langle\langle x < y < 30 ; \varepsilon \rangle\rangle,
\]
\[
\text{run}(y : \text{int}) \langle\langle x < y < f_q ; \varepsilon \rangle\rangle \langle\langle x < y < 60 ; \varepsilon \rangle\rangle \}
\]

Note that in Example 8.2.4, in fact, for the update of \( f_q := x + k \), when \( k \leq 2 \), the global SP always violates temporal satisfiability (Condition 3); when \( k > 12 \), it always violates Condition 1.(b).

Note that, all examples treated in this chapter are well-formed. Henceforth we assume all global SPs we treat are well-formed.

8.2.3 The Projection from a Global SP to Local SPs

Global SPs are useful to capture overall interaction scenarios, while local SPs specify exactly what endpoints should do. They are linked by endpoint projection.

The projection rule defined in Definition 8.2.5 is similar to the one defined in Definition 6.5.1 in Chapter 6. Assume \( p, q, r \in G \) and \( p \neq q \). \( \text{var}(G) \mid p \) is the set of variables that \( p \) knows in \( G \).

**Definition 8.2.5.** Assume \( G \) is well-formed. The stateful projection \( \text{Proj}(G, A, r) \) is inductively defined as:

\[
\text{Proj}(p \rightarrow q : \{ l_i(x_i : S_i) \langle\langle A_i ; E_i \rangle\rangle \langle\langle A_i' ; E_i' \rangle\rangle, G_i \})_{i \in I}, \ A^{pj}, \ r) =
\]

\[
\begin{align*}
q!\{ l_i(x_i : S_i) \langle\langle A_i ; E_i \rangle\rangle \langle\langle A_i' ; E_i' \rangle\rangle, G_i \}_{i \in I} & \quad \text{if } r = p \neq q, \\
p?\{ l_i(x_i : S_i) \langle\langle A_i' ; E_i' \rangle\rangle \langle\langle A_i ; E_i \rangle\rangle, G_i \}_{i \in I} & \quad \text{if } r = q \neq p, \\
\sqcup_{i \in I} G_i^{pj} & \quad \text{if } r \neq q \neq p
\end{align*}
\]

with \( G_i^{pj} = \text{Proj}(G_i, A^{pj}, r) \)

\[
\text{Proj}(G_1 \parallel G_2, \ A^{pj}, \ r) =
\begin{cases}
\text{Proj}(G_i, A^{pj}, r) & \text{if } r \in G_i \text{ and } r \notin G_j \ i, j \in \{1, 2\}, \\
\text{end} & \text{else}
\end{cases}
\]

end \parallel r = \text{end}

where \( \sqcup_{i \in I} G_i^{pj} = G_1^{pj} \sqcup G_2^{pj} \ldots \sqcup G_n^{pj} \text{ if } I = \{1, \ldots, n\} \). The mergeability, \( T_1 \sqcup T_2 \), is defined in the end of Definition 6.5.1 in Chapter 6. The application of projection is illustrated by the following example.
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

Example 8.2.6 (endpoint projection). The local SPs projected from \( G_{\text{assign}} \) on role \( S \) and \( B \) respectively are:

\[
\begin{align*}
G_{\text{assign}} \mid S &= T_S = B?\text{req}(\varepsilon)\langle \text{t} := t + 1, c := c \cup \{t\}\rangle. \\
B!\text{ans}(x : \text{int})\langle x \in c ; c := c \setminus \{x\}\rangle. \text{end}
\end{align*}
\]

\[
\begin{align*}
G_{\text{assign}} \mid B &= T_B = S!\text{req}(\varepsilon) . S?\text{ans}(x : \text{int}). \text{end}
\end{align*}
\]

8.3 Specifications Composed by SP

8.3.1 The Syntax of Stateful Specifications

A specification is a triple \( \Theta ::= (\Gamma; \Delta; D) \) which gives a behavioural specification of a local process (endpoint) as its interface. \( \Gamma, \Delta \) and \( D \), separated by “;” in \( \Theta \), are given by:

\[
\begin{align*}
\Gamma &::= \emptyset | \Gamma, a : \text{mode}(G[p]) | \Gamma, f : S \\
\Delta &::= \emptyset | \Delta, s[p]:T \\
D &::= \emptyset | D, f \mapsto v
\end{align*}
\]

We here simplify the modes of shared names as \text{mode} \in \{I, O\}. \( \Gamma \), shared environment, describes several information: The permitted behaviour at each shared channel; and the type of each field. When a process has \( a : I(G[p]) \), it can accept invitations via shared channel \( a \) to play role \( p \) following what \( G \) specifies; while \( a : O(G[p]) \) is its dual. In \( \Delta \), session environment, \( s[p]:T \) describes the session behaviour \( (T) \) in a session \( s \) as \( p \). \( D \) is a set of (ghost) states of a local process (endpoint): The states in \( D \in \Theta \) belong to an endpoint participant in a session. Each \( D \) is a map from fields to values, storing a range of data structure. In formulae, a field \( f \) itself represents its current value.

Example 8.3.1. Based on \( G_{\text{assign}} \) in Example 8.1.3 and its local SPs in Example 8.2.6, we give a local specification \( \Theta_{\text{ass}} \) for server, playing role \( S \), and \( \Theta_{B_1} \) and \( \Theta_{B_2} \) for two buyers \( B_1 \) and \( B_2 \), each playing role \( B \) in \( G_{\text{assign}} \), assuming there are two ongoing
8.3 Specifications Composed by SP

sessions $s_1$ and $s_2$.

\[
T_{\text{ass}} = B?\text{req}(\varepsilon)\langle\text{true}; t := t + 1 \ c := c \cup \{t\}\rangle.T'_{\text{ass}},
\]

\[
T'_{\text{ass}} = B!\text{ans}(x : \text{int})\langle x \in c ; \ c := c \setminus \{x\}\rangle.\text{end}
\]

\[
\Theta_{\text{ass}} = \langle \Gamma'_{\text{ass}}; \text{server} : \text{I}(G_{\text{ass}}[S]); \Delta'_{\text{ass}}, s_1[S] : T_{\text{ass}}, s_2[S] : T_{\text{ass}}; D'_{\text{ass}}, t \mapsto 0, c \mapsto \{\rangle
\]

\[
T_B = S!\text{req}(\varepsilon).T'_B,
\]

\[
T'_B = S?\text{ans}(x : \text{int}).\text{end},
\]

\[
\Theta_{B_1} = \langle \Gamma'_{B_1}, b_1 : \text{I}(G_B[B]), \text{server} : \text{O}(G_{\text{ass}}[S]) ; \Delta'_{B_1}, s_1[B] : T_B; D_{B_1}\rangle
\]

\[
\Theta_{B_2} = \langle \Gamma'_{B_2}, b_2 : \text{I}(G_B[B]), \text{server} : \text{O}(G_{\text{ass}}[S]) ; \Delta'_{B_2}, s_2[B] : T_B; D_{B_2}\rangle
\]

The data storage in $\Theta_{\text{ass}}$ is $D'_{\text{ass}}, t, c$. In this protocol, no state in $D'_{\text{ass}}$ is used. Similarly, no state in $D_{B_1}$ or $D_{B_2}$ is used. Although we do not illustrate the whole procedures of session establishment (by using rules [Acc] and [Req] defined in Figure 8.3), it shows that buyers $B_1$ and $B_2$ are the session inviters requesting $S$ to join session $s_1$ and $s_2$.

### 8.3.2 The Semantics of Stateful Specifications

Figure 8.3 represents the semantics of specifications as a deterministic labelled transition system, of the form $\Theta \xrightarrow{\ell} \Theta'$, which intuitively means $\Theta$ as a specification allows a process to do an action $\ell$, and demands the resulting process to conform to $\Theta'$.

**Definition 8.3.2.**

\[
\Theta \xrightarrow{\ell_1} \Theta_1 \xrightarrow{\ell_2} \Theta_2 \ldots \xrightarrow{\ell_k} \Theta_k \ldots \overset{\text{def}}{=} \Theta \xrightarrow{\ell_1\ell_2\ldots\ell_k} \Theta_k\ldots
\]

For actions labels, here we adopt the simplified version of those defined in Equation 5.1. Because this chapter, for specifying asynchronous specification when endpoints’ states are also stipulated, focuses on the session interactions, actions new $a : \text{im}(G[p])$ and join($s[p]$), which are control actions, are not discussed in the LTS defined in Figure 8.3. The rules of bound/free request and bound/free accept of the semantics are similar to those of the LTS of monitors defined in Figure 7.4, Chapter 7. We do not use $\tau$ since it is irrelevant in the present work (because, in brief, $\tau$ is always possible and has no effects on specifications). The special rules for stateful specifications are rules [Sel/SelN] and [Bra/BraN]. Rule [Sel] is for sending a message inside a session. The premise says that, first, the type $T$ should be a selection type; the passed value $v$ has type $S_j$ from the $j$th branch of $T$ under $\Gamma$ (note that, when $v$ is a name, $\Gamma$ is necessary
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

Actions
\[ \ell ::= \tau | \overline{p}(s[p] : G) | \overline{a}(s[p] : G) | a(s[p] : G) | a(s[p] : G) | s[p] qI(v) | s[p,q] qI(v) \]

[REQ-INT]
\[ s \not\in \text{dom}(\Delta), \forall i \in I, p_i \in \text{role}(G), \ G \text{ is well-formed, } \forall k,j \in I, p_k \not= p_j \ (k \not= j) \]
\[ (\Gamma, a : 0(G[p_j]); \Delta; D) \xrightarrow{\overline{s}[p_j] | G} (\Gamma, a : 0(G[p_j]); \Delta, \{s[p_j] : G \mid p_j \} \in \cap (I); D) \]

[REQ]
\[ p_j \in \text{role}(G) \]
\[ (\Gamma, a : 0(G[p_j]); \Delta, s[p_j] : G \mid p_j; D) \xrightarrow{s[p_j] | G} (\Gamma, a : 0(G[p_j]); \Delta; D) \]

[ACC-B]
\[ s \not\in \text{dom}(\Delta), \ T = G \mid q, \text{field}(T) \in D \]
\[ (\Gamma, a : I(G[q]); \Delta; D) \xrightarrow{\alpha[\{\theta, \{\gamma\}\}]^T} (\Gamma, a : I(G[q]); \Delta, s[q] : T; D) \]

[ACC-F]
\[ s \in \text{dom}(\Delta), \ T = G \mid q, \text{field}(T) \in D \]
\[ (\Gamma, a : I(G[q]); \Delta; D) \xrightarrow{\alpha[\{\theta, \{\gamma\}\}]^T} (\Gamma, a : I(G[q]); \Delta, s[q] : T; D) \]

[SEL]
\[ T \to q\{l_1(x_1 : S_1)\langle A_1, E_1 \rangle T_1\}_{i \in I}, \ \Gamma \vdash v : S_1, \ \Gamma \models A_1(v/x_j), \]
\[ (\Gamma; \Delta, s[p] : T; D) \xrightarrow{\alpha[\{\theta, \{\gamma\}\}]^T} (\Gamma; \Delta, s[p] : T; D \text{ after } E_1(v/x_j)) \]

[SELN]
\[ T \to q\{l_1(x_1 : S_1)\langle A_1, E_1 \rangle T_1\}_{i \in I}, \ \Gamma \vdash a : S_j, \ a \not\in (A_2 \cap E_1), \ A_1 \downarrow \text{true}, \]
\[ (\Gamma; \Delta, s[p] : T; D) \xrightarrow{\alpha[\{\theta, \{\gamma\}\}]^T} (\Gamma; \Delta, s[p] : T; D \text{ after } E_1) \]

[BRA]
\[ T \to p\{l_1(x_1 : S_1)\langle A_1, E_1 \rangle T_1\}_{i \in I}, \ \Gamma \vdash v : S_j, \ \Gamma \models A_1(v/x_j), \]
\[ (\Gamma; \Delta, s[q] : T; D) \xrightarrow{\alpha[\{\theta, \{\gamma\}\}]^T} (\Gamma; \Delta, s[q] : T; D \text{ after } E_1(v/x_j)) \]

[BRA\text{N}]
\[ T \to p\{l_1(x_1 : S_1)\langle A_1, E_1 \rangle T_1\}_{i \in I}, \ S_j = \text{mode}(G'[p']), \ a \not\in (A_2 \cap E_1), \ A_j \downarrow \text{true} \]
\[ (\Gamma; \Delta, s[q] : T; D) \xrightarrow{\alpha[\{\theta, \{\gamma\}\}]^T} (\Gamma, a : 0(G'[p']); \Delta, s[q] : T; D \text{ after } E_i) \]

[PAR]
\[ \Theta_1 \xrightarrow{\delta} \Theta_2, \Theta_3 \xrightarrow{\delta} \Theta_2, \Theta_3 \]

Figure 8.3: The Labelled Transition System of Specifications
8.4 Traces of Local Actions

to have the knowledge of its type, but it is not needed if \( v \) is a non-name value, like \( 3 \) or "hello" because its type is automatically known without \( \Gamma \); and \( A_j \) after substitution is well-typed under \( \Gamma \). In the conclusion, \( T'_j \) substitutes \( v \) for \( x_j \) and prepares for the next (incoming or outgoing) message, and the state is updated by \( D_{\text{after}} E_j \{v/x_j\} \). To illustrate the updating of \( D \) by \( E_j \), assume \( E_j \) is defined as \( f := f \cup \{x_j\} \), and currently \( f \mapsto \{10\} \). After substituting \( 5 \) for \( x_j \), \( D \) is updated to \( f \mapsto \{10, 5\} \). Rule \([\text{SelN}]\) is similar to rule \([\text{Sel}]\) except that it is particularly for sending a name, which should not be in \( A_j \) and \( A_j \) should be evaluated as true. Rule \([\text{Bra}]\) is a symmetric rule of \([\text{Sel}]\). Rule \([\text{BRAN}]\) is for receiving shared channel \( a \). It is dual to rule \([\text{SelN}]\), and similar to the rule defined in \(7.3\).

We define two specifications, say \( \Theta \) and \( \Theta' \), are composable whenever \( P(\Theta) \cap P(\Theta') = \emptyset \), and write \( \Theta, \Theta' \) as a composition of specification \( \Theta \) and specification \( \Theta \). It is defined similarly as Definition \(7.4.23\) which defines the parallel composition of monitors. \([\text{Par}]\) says, If \( \Theta_1 \) and \( \Theta_3 \) are composable, after action happens and \( \Theta_1 \) becomes as \( \Theta_2 \), they are still composable.

8.4 Traces of Local Actions

In this section, the trace of a local process is defined to describe a local process’s runtime behaviour, and define the satisfaction criterion for formally describing a process satisfies a given specification synchronously/asynchronously. Note that, hereafter, when we say a trace, it always means a trace consisting of local actions inputting or outputting from a local process.

**Definition 8.4.1 (trace).** A trace \((s, s', \ldots)\) is a sequence of actions represented by

\[
s = \ell_1 \cdot \ell_2 \ldots \cdot \ell_n ...
\]

in which each action is connected by "·".

Note that, for every \( s \), we assume an accept/request action introducing a session, say \( s \), binds the later occurrences of \( s \).

**Definition 8.4.2 (valid trace according to \( \Theta \)).** A trace \( s \) is valid according to \( \Theta \) if there always exists \( \Theta' \) such that \( \Theta \xrightarrow{s} \Theta' \).
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

8.4.1 Permutation of Stateful Protocols

We formalise the notion of minimum permutations for local $\Theta$, which is similar to the permutation mechanism defined in Definition 6.6.8 in Chapter 6. Having permutation rules for $\Theta$ (see Definition 8.4.4) makes an observer (i.e. system monitor), who observes actions based on $\Theta$, be able to capture the causality relation of actions when the order of actions is not preserved due to asynchrony. For example, in one session, when an endpoint, say $s[p]$, waits for two input actions from different senders, say $s[q_1]$ and $s[q_2]$, the local $\Theta$ at role $s[p]$ is

$$q_1 ? l_1(x_1) \langle\langle A_1; E_1 \rangle\rangle \cdot q_2 ? l_2(x_2) \langle\langle A_2; E_2 \rangle\rangle$$

then the order of actions may be $s[q_1, p] ? l_1(v_1) s[q_2, p] ? l_2(v_2)$ or $s[q_2, p] ? l_1(v_2) s[q_1, p] ? l_1(v_1)$ because there is no way to restrict that the first action should firstly happen and arrive earlier at $s[p]$ than the second one.

The permutation rules for $\Theta$ have different purpose from the definition of commutativity (see Definition 8.5.31). The permutation rules for $\Theta$ are the mechanisms (or tools) that let an observer use them to properly observe actions, whose order is not preserved; while the attribute of commutativity of a $\Theta$ is used to validate whether the $\Theta$ is asynchronous verifiable or not.

Here we define stateful protocol context and local unit permutation. Assume that, whenever we write $T[\ ]$, it always comes from a well-formed global stateful protocol (i.e. $G$). Recall that the well-formedness principles of global stateful protocol is introduced in section 8.2.2. If it is a local $\Theta$ containing the local SP projected from a non-well-formed global SP, it is not meaningful to explore the permutation mechanism when the original global stateful protocol is in a non-reasonable shape. For convenience, let an obligation $\langle\langle A; E \rangle\rangle$ for sender be $\langle\langle \eta \rangle\rangle$, and an obligation $\langle\langle A'; E' \rangle\rangle$ for receiver be $\langle\langle \eta' \rangle\rangle$.

**Definition 8.4.3 (Local SP context).** Let $\dagger := \{?, !\}$. A local stateful-session type context $\mathcal{T}[\ ]$ is a local stateful protocol with a hole, whose grammar is defined as:

$$\mathcal{T}[\ ] := [\ ] | p \dagger : \{l_{i}(x_{i}: S_{i}) \langle\langle \eta_{i} \rangle\rangle \cdot \mathcal{T}[\ ], ..., l_{k}(x_{k}: S_{k}) \langle\langle \eta_{k} \rangle\rangle : \mathcal{T}[\ ], ..., l_{n}(x_{n}: S_{n}) \langle\langle \eta_{n} \rangle\rangle : \mathcal{T}[\ ]\}$$

$\mathcal{T}[T]$ denotes the result of filling the hole in the local SP context $\mathcal{T}$ with local SP $T$. Note that $[\ ]$ defines the identity function, i.e. $[\ ] = T$. 

174
### 8.4 Traces of Local Actions

The causal order occurs when there are two consecutive sending (or receiving) actions with the same target (e.g., \( q!l(v).q!l'(v') \) or \( p?l(x).p?l'(x') \)), or there is an input action followed by an output action.

**Definition 8.4.4 (local unit permutation).** The *unit permutation* of local SP is defined by the axioms below, assuming \( p_1 \neq p_2 \):

\[
\begin{align*}
\&{\mathcal{T}[p_1][l_i(x_i:S_i)(y_i]\cdot[p_2][l_j(x'_j:S'_j)(y'_j):T_{ij}]_{i\in I}\}}\rightleftharpoons
\end{align*}
\]

\[
\begin{align*}
\&{\mathcal{T}[p_1][l_i(x_i:S_i)(y_i]\cdot[p_2][l_j(x'_j:S'_j)(y'_j):T_{ij}]_{j\in I}\}}\rightleftharpoons
\end{align*}
\]

\[
\begin{align*}
\&{\mathcal{T}[p_1][l_i(x_i:S_i)(y_i]\cdot[p_2][l_j(x'_j:S'_j)(y'_j):T_{ij}]_{j\in I}\}}\rightleftharpoons
\end{align*}
\]

\[
\begin{align*}
\&{\mathcal{T}[p_1][l_i(x_i:S_i)(y_i]\cdot[p_2][l_j(x'_j:S'_j)(y'_j):T_{ij}]_{i\in I}\}}\rightleftharpoons
\end{align*}
\]

\[
\begin{align*}
\&{\mathcal{T}[p_1][l_i(x_i:S_i)(y_i]\cdot[p_2][l_j(x'_j:S'_j)(y'_j):T_{ij}]_{j\in I}\}}\rightleftharpoons
\end{align*}
\]

### 8.4.2 Permutation of Local Actions

Since \( \Theta \) is a specification for a local endpoint, the actions concerned here are all *local* actions, which means that they are the actions happening at endpoints. Similarly, all permutations of actions are the permutation of local actions. Example below shows the relations between global actions and local actions.

**Example 8.4.5 (global actions v.s. local actions).** Assume a session \( s \) is given, in which the roles involved in it are \( p_1 \) and \( p_2 \). Assume globally, there are actions among session-roles \( s[p_1] \) and \( s[p_2] \):

\[
\begin{align*}
s[p_1, p_2]!("How are you?") \cdot s[p_1, p_2]?("How are you?") \cdot s[p_2, p_1]!("Fine. Thanks!") \cdot s[p_2, p_1]?("Fine. Thanks!")
\end{align*}
\]

with the scenario: An endpoint playing role \( p_1 \) in session \( s \), denoted by \( s[p_1] \), firstly sends a regard "How are you" to an endpoint playing role \( p_2 \) in session \( s \), denoted by \( s[p_2] \). After \( s[p_2] \) receives this regards, she replies \( s[p_1] \) with "Fine. Thanks!"; then \( s[p_1] \) receives this response. The sequence of actions can be observed by the following messages

\[
\begin{align*}
s[p_1, p_2, \langle "How are you?" \rangle] \cdot s[p_2, p_1, \langle "Fine. Thanks!" \rangle]
\end{align*}
\]

This sequence of messages reflect the meaning of the sequence of actions.

Locally, the sequence of actions for session-role \( s[p_1] \) is

\[
\begin{align*}
s[p_1, p_2]!("How are you?") \cdot s[p_2, p_1]?("Fine. Thanks!")
\end{align*}
\]

175
while the sequence of actions for session-role \( s[p_2] \) is

\[
\text{\( s[p_1,p_2]\):"How are you?"\cdot s[p_2,p_1]\):"Fine. Thanks!"
}\]

A remote observer generally has more than one specifications (for different session-roles). For each session-role, the specification only specifies the local behaviours of that session-role.

To capture the causality among actions, below we define the relation of \textit{dependency}:

\textbf{Definition 8.4.6 (dependency).} We define \( \mathcal{D} \), the dependency relation, such that \( \ell_1 \mathcal{D} \ell_2 \) whenever

(a) \( \ell_1 \) is either \( a(k[p] : G) \) or \( a(k[p] : G) \), and \( k[p] \in \ell_2 \) or \( \text{sbj}(\ell_2) = k[p] \).

(b) \( \ell_1 \) is \( s[p_1,p_2]\)l(x) and \( x \in \ell_2 \).

We say that \( \ell_2 \) depends on \( \ell_1 \) if \( \ell_1 \mathcal{D} \ell_2 \).

The following examples illustrate the cases of dependency relation over action labels.

\textbf{Example 8.4.7.} Assume a sequence of actions \( \ell_1 \cdot \ell_2 \), where

\[
\ell_1 = a(k[p] : G), \quad \ell_2 = \overline{b}(k[p] : G).
\]

Based on Definition \textbf{8.4.6} (a), \( \ell_2 \) depends on \( \ell_1 \).

\textbf{Example 8.4.8.} Assume a sequence of local actions of some local endpoint \( s = s_0 \cdot \ell_1 \cdot \ell_2 \), where

\[
\ell_1 = a(k[p] : G), \quad \ell_2 = k[p',p]l(v)
\]

\( \ell_2 \) does not depend on \( \ell_1 \) because, based on Definition \textbf{8.4.6} (a), \( \text{sbj}(\ell_2) = k[p'] \neq k[p] \).

\textbf{Example 8.4.9.} Assume a sequence of local actions of some local endpoint \( s = s_0 \cdot \ell_1 \cdot \ell_2 \cdot \ell_3 \cdot \ell_4 \), where

\[
\ell_1 = a(k[p] : G), \quad \ell_2 = k[p,q]l(v), \quad \ell_3 = b(k'[q] : G'), \quad \ell_4 = k'[p,q]?l'(v')
\]

\( \ell_2 \) depends on \( \ell_1 \) because, based on Definition \textbf{8.4.6} (a), \( \text{sbj}(\ell_2) = k[p] \). Similarly, \( \ell_4 \) depends on \( \ell_3 \).
Definition 8.4.10 (suppress of local actions). For a sequence of local actions $\ell_1 \cdot \ell_2$ of an endpoint, we say $\ell_2$ is suppressed by $\ell_1$ if

1. $\ell_1 = s[p_1, q]!!(v)$ and $\ell_2 = s[q, p_2]!!'(v')$, or
2. $\ell_1 = s[p, q]!!(v)$ and $\ell_2 = s[p, q]!!'(v')$, or
3. $\ell_1 = s[p, q]!!(v)$ and $\ell_1 = s[p, q]!!'(v')$.

Definition 8.4.11 (causality). We say local actions $\ell_1$ and $\ell_2$ of an endpoint have causality relation if one of them depends or suppresses the other.

Definition 8.4.12 (legal unit permutation of local actions). Let sequence of local actions $\ell_1 \cdot \ell_2$ be a trace of an endpoint. A permutation from $\ell_1 \cdot \ell_2$ to $\ell_2 \cdot \ell_1$ is legal if $\ell_1$ and $\ell_2$ have no causality relation.

We write $s \rightarrow s'$ when $s'$ is the result of applying zero or more legal unit permutations. In this case $s'$ is a permutation variant of $s$ and this permutation is called a legal permutation.

Definition 8.4.13 (valid unit permutation of actions according to $\Theta$). We say $s_1$ is a permutation variant of $s_2$ under $\Theta$, written $\Theta \vdash s_1 \rightarrow s_2$, when $s_1 \rightarrow s_2$, $\Theta \vdash s_1$, and $\Theta \vdash s_2$ hold.

Example 8.4.14 (legal permutations of actions). In Figure 8.1 all traces in (I) and (II) are permutation variants to each other. The traces in (III) can legally permute to any trace in (I) and (II), but not the converse.

Note that, it does not mean that a sequence of legally-permuted actions is always valid to a $\Theta$. The following example explains this point.

Example 8.4.15. Let $\ell_1 = s[p, q_1]!!(\varepsilon)$ and $\ell_2 = s[p, q_2]!!(\varepsilon)$. Then $\ell_1 \cdot \ell_2 \rightarrow \ell_2 \cdot \ell_1$.

Assume that initial value of state $c$ is 1, and that local SP for role $p$ in session $s$ is:

$$s[p] : q_1!!(\langle (\text{true;} \varepsilon) \rangle . q_2!!(\langle c = 1; c := 0 \rangle))$$

Then $\Theta \vdash \ell_1 \cdot \ell_2$, but $\Theta \not\vdash \ell_2 \cdot \ell_1$. 

177
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

8.5 Theory for Stateful Specifications

8.5.1 Satisfaction

The following simple definition of processes is enough for our purpose: We can readily use the \( \pi \)-calculus with session primitives and its weak (\( \tau \)-abstracted) LTS to induce this abstract notion of processes.

**Definition 8.5.1 (process).** A process \( (P, Q, ..) \) is a prefix-closed set of traces.

The following defines the notion of synchronous and asynchronous observables as the set of traces observed by a synchronous observer (i.e. as it is) and by an asynchronous observer (i.e. up to legal permutations).

**Definition 8.5.2 (synchronous and asynchronous observable).**

1. \( \text{Obs}_s(P) \overset{\text{def}}{=} P \).

2. \( \text{Obs}_a(P) \) is the set of all legal permutation variants of the traces in \( P \).

Firstly, recall the LTS rule of SP defined in Figure 8.3: a valid \( \ell \) against a \( \Theta \) is an action which can be verified by a LTS rule such that \( \Theta \xrightarrow{\ell} \Theta' \). Intuitively, a valid trace is a trace that \( \Theta \) approves it.

**Definition 8.5.3 (trace(\( \Theta \)): the set of valid traces of \( \Theta \)).** Define \( \text{trace}(\Theta) \) as the set of valid traces of \( \Theta \):

\[
\text{trace}(\Theta) = \{ s \mid \Theta \xrightarrow{s} \Theta' \}
\]

i.e. \( \text{trace}(\Theta) \) is the maximum set of traces such that \( \forall s \in \text{trace}(\Theta), \Theta \vdash s \).

**Definition 8.5.4 (satisfaction up to observables).** A process \( \text{Obs}_s(P) \) synchronously satisfies \( \Theta \), denoted \( P \models_{\text{sync}} \Theta \), when the following two conditions hold:

1. (output safety) \( \text{Obs}_s(P) \subseteq \text{trace}(\Theta) \).

2. (input consistency) Whenever \( s \in \text{Obs}_s(P) \) and \( s \cdot \ell \in \text{trace}(\Theta) \) where \( \ell = s[p, q]?!(v) \) is an input, \( s \cdot \ell' \in \text{Obs}_s(P) \) and \( \ell' \) is an input with the shape \( \ell' = s[p, q]?!(v') \), then \( s \cdot \ell \in \text{Obs}_s(P) \).

A process \( P \) asynchronously satisfies \( \Theta \), denoted \( P \models_{\text{async}} \Theta \), if, after replacing each \( \text{Obs}_s(P) \) with \( \text{Obs}_a(P) \), it satisfies condition 1. above and the following condition:
2.b (input consistency) Whenever \( s \in \text{Obs}_a(P) \) and \( s \cdot \ell \in \text{trace}(\Theta) \) where \( \ell \) is an input, then \( s \cdot \ell \in \text{Obs}_a(P) \).

Note that, for synchronous process (2.a), it can accept a valid input only when it is ready to receive it; while for asynchronous process (2.b), it can accept and should accept a valid input. Intuitively, Definition 8.5.4 says that a process \( P \) synchronously (resp. asynchronously) satisfies \( \Theta \) if, w.r.t. synchronous (resp. asynchronous) observables, \( P \) always does valid outputs as far as it receives valid inputs.

**Example 8.5.5** (valid/invalid traces according to \( G_{\text{assign}} \)). We consider \( \Theta_{\text{ass}} \) from Example 8.3.1 which uses the local SP, projected from \( G_{\text{assign}} \) (given in Section 8.1.3), for the server side. Then, for example,

\[
s_2[B,S]?\text{req}(\epsilon) \cdot s_2[S,B]!\text{ans}(1) \cdot s_1[B,S]?\text{req}(\epsilon) \cdot s_1[S,B]!\text{ans}(2)
\]

is a valid trace of \( \Theta_{\text{ass}} \), but

\[
s_2[B,S]?\text{req}(\epsilon) \cdot s_2[S,B]!\text{ans}(2) \cdot s_1[B,S]?\text{req}(\epsilon) \cdot s_1[B,S]!\text{ans}(1)
\]

is not its trace (violation is at the second step), because it is not permitted by a remote observer with \( \Theta_{\text{ass}} \) when she observes it.

**Lemma 8.5.6.** \( s \in \text{Obs}_a(P), P \models_{\text{sync}} \Theta \) implies \( s \in \text{trace}(\Theta) \).

_Proof._ Directly from Definition 8.5.4.

**8.5.2 Asynchronously Verifiable Specifications**

We say \( \Theta \) is asynchronous if it is suitable for a remote observer to verify the behaviour of a process. In this case, we do not want the conformance of a trace to change depending on an accidental reordering due to asynchrony, i.e. we want its validity to be robust w.r.t. legal permutations. In the follows, the protocols introduced in Section 8.1.2 are used.

**Definition 8.5.7** (asynchronously verifiable specification). We say \( \Theta \) is asynchronously verifiable or simply asynchronous when \( s \in \text{trace}(\Theta) \) and \( s \leadsto s' \) imply \( s' \in \text{trace}(\Theta) \).

To check violation of asynchrony of a specification, we only have to find a single acceptable trace whose permutation is not acceptable.
Example 8.5.8. This example uses $G_{\text{sync}}$ introduced in Example 8.1.2, Section 8.1.2. Let $T_{\text{sync}}$ be the local SP at server, projected from $G_{\text{sync}}$.

$$
\Theta_{\text{sync}} = (\Gamma'_{\text{sync}}, a : 1(G_{\text{sync}}[S]); \Delta'_{\text{sync}}, \{s_1[S] : T_{\text{sync}}\}_{i \in I}; D'_{\text{sync}}, c)
$$

where $I$ is the set of indexes for the sessions using $G_{\text{sync}}$. This specification is not asynchronous because $\Theta_{\text{sync}}$ can accept trace $s_1[C, S]?\text{req}(\varepsilon) \cdot s_1[S, C]!\text{ans}(1) \cdot s_2[C, S]?\text{req}(\varepsilon) \cdot s_2[S, C]!\text{ans}(2)$

but cannot accept the trace below which is permuted from the trace above $s_1[C, S]?\text{req}(\varepsilon) \cdot s_2[C, S]?\text{req}(\varepsilon) \cdot s_2[S, C]!\text{ans}(2) \cdot s_1[S, C]!\text{ans}(1)$.

On the other hand, checking asynchrony by Definition 8.5.7 means we should verify this property for all traces, which are usually infinitely many. Later we shall introduce the decidable methods by which we can approve the asynchrony of, for example, $\Theta_{\text{ass}}$ and all the corresponding specifications that apply stateful protocols $G_{\text{pcs}}/G_{\text{ivc}}$ and $G_{\text{sync}}$.

The following characterisation says that, if a synchronous observer recognises that $P$ conforms to $\Theta$, i.e. if $P$ conforms to $\Theta$ synchronously, then an asynchronous observer will also do the same.

Proposition 8.5.9. $\Theta$ is asynchronous iff, for each $P$, $P \models_{\text{sync}} \Theta$ implies $P \models_{\text{async}} \Theta$.

Proof. For $(\Rightarrow)$, assume $P \models_{\text{sync}} \Theta$ and $\Theta$ is asynchronous. By definition, $P \models_{\text{sync}} \Theta$ means $\text{Obs}_s(P) \subset \text{trace}(\Theta)$. Since $\Theta$ is asynchronous, by Definition 8.5.7 all legal permutation variants of $\text{trace}(\Theta)$ are in $\text{trace}(\Theta)$. This implies all legal permutation variants of $\text{Obs}_s(P)$, which is $\text{Obs}_s(P)$, are in $\text{trace}(\Theta)$. Thus $P \models_{\text{async}} \Theta$ as required.

For $(\Leftarrow)$, since $\forall P, P \models_{\text{sync}} \Theta$ implies $P \models_{\text{async}} \Theta$, we know

$$
\forall P, \forall s \in \text{Obs}_s(P) \subset \text{trace}(\Theta) \text{ and } s \bowtie s' \text{ implies } s' \in \text{Obs}_s(P) \subset \text{trace}(\Theta).
$$

By Definition 8.5.7 $\Theta$ is asynchronous. ■

Let $I(s)$ be the sequence of input actions of $s$, $O(s)$ be the sequence of output actions of $s$, and $V(s)$ be the sequence of values carried in $s$. Let $\text{num}(s)$ be the length of $s$, and $\text{prefix}(s)$ be the set of prefixes of $s$. Let $\text{ses}(s)$ be the set of sessions occurring in trace $s$, and, similarly, $\text{ses}(\Theta)$ be the set of sessions involving in $\Theta$, i.e. those sessions obeying
8.5 Theory for Stateful Specifications

Θ. Note that, the size of set $\text{ses}(s)$ is increasing when new sessions are created by a local process; similarly, the size of set $\text{ses}(\Theta)$ is increasing when new sessions obeying $\Theta$ are created. Moreover, let $v(\ell)$ be the value carried by action $\ell$.

When a state is declared in a local specification, since a specification can dynamically verify sequence of actions during runtime, the state may be changed with the incoming or outgoing actions according to the update rules defined in the specification. Therefore, the current value of a state in a specification should be defined with actions of a process because these actions may make the value of state change.

**Definition 8.5.10.** Define $\text{field}(\Theta)$ as the set of states declared in $\Theta$. If $c \in \text{field}(\Theta)$, then $c$ is a state declared in $\Theta$.

**Definition 8.5.11 (current value of a state with respect to $\Theta$ and actions).** Let $f \in \text{field}(\Theta)$ and $\text{val}(f, \Theta')$ be the value of state $f$ when the configuration of specification is $\Theta'$. Define the current value of state $f$ as

$$\text{current}(f, \Theta, s) = \text{val}(f, \Theta')$$

where $\Theta \rightarrow \Theta'$.

Based on this definition, $\text{current}(f, \Theta, s)$ is the current value of state $f$ according to $\Theta$, which specifies the initial value of $f$, when actions in $s$ have happened.

**Definition 8.5.12 (initial value of a state w.r.t. $\Theta$).** Define $\text{current}(f, \Theta, \emptyset)$ be the initial value of state $f$ which is declared in $\Theta$.

The initial value of a state should have been declared in $\Theta$. For example, as $f \mapsto \text{ini}$ is declared in $\Theta$, we have $\text{current}(f, \Theta, \emptyset) = \text{ini}$.

**Lemma 8.5.13.** Assume $c \in \text{field}(\Theta_{\text{sync}})$ and $\text{current}(c, \Theta_{\text{sync}}, \emptyset) = \text{ini}$. Assume every session $s_i$ guided by $G_{\text{sync}}$ has been established. $\Theta_{\text{sync}}$ is defined as below:

$$\Theta_{\text{sync}} = \langle \text{ser} : \text{I}(G_{\text{sync}}[S]) :$$

$$\{s_i[S] : C!\text{req}(\varepsilon)\langle\langle \text{true} : \varepsilon \rangle\rangle.C!\text{ans}(x : \text{int})\langle\langle x = c ; c := c + 1 \rangle\rangle \rangle \rangle \rangle \rangle \rangle$$

where $I$ is the set of indexes of sessions. If $s' \in \text{trace}(\Theta_{\text{sync}})$, then for any $s$ resulting from permutations $s' \sim s$, $s$ satisfies the followings:

cond 1. If session $s \in \text{ses}(s)$, then session $s \in \text{ses}(\Theta_{\text{sync}})$. 

181
cond 2. \( \forall s'' \in \text{prefix}(s), \text{num}(I(s'')) \geq \text{num}(0(s'')) \).

cond 3. If \( s_0, \ell \in s \cap \ell = s[S, B]!\text{ans}(v) \), then \( \exists \ell'' \in s_0, \ell'' = s[B, S]？\text{req}(v) \).

cond 4. \( \forall \ell, \ell' \in 0(s), \ell \neq \ell' \), implies \( v(\ell) \neq v(\ell') \).

cond 5. \( \forall \ell \in 0(s''), s'' \in \text{prefix}(s), \text{ini} \leq v(\ell) < \text{num}(I(s'')) + \text{ini} \).

**Proof.** It is proved in Appendix C.1

**Proposition 8.5.14.** Assume \( c', \log \in \text{field}(\Theta_{\text{ass}}) \) and \( \text{current}(c', \Theta_{\text{ass}}, \emptyset) = \text{ini}' = \text{ini} - 1 \), \( \text{current}(\log, \Theta_{\text{ass}}, \emptyset) = \{ \} \). Assume every session \( s_i \) guided by \( G_{\text{assign}} \) has been established. \( \Theta_{\text{ass}} \) is defined below:

\[
\Theta_{\text{ass}} = (\langle \text{ser} : I(G_{\text{assign}}[S]) ;
\{ s_i[S] : C' \text{req}(\epsilon) \langle \text{true} ;
\{ c' := c' + 1, \log := \log \cup \{ c' \} \} \} ;
C!\text{ans}(x : \text{int}) \langle \{ x \in \log ; \log := \log \setminus \{ x \} \} \}_{i \in I} ;
\}
\]

where \( I \) is the set of indexes of sessions. \( s \) satisfies all conditions listed in Lemma 8.5.13 if and only if \( s \in \text{trace}(\Theta_{\text{ass}}) \).

**Proof.** It is proved in Appendix C.1

**Definition 8.5.15 (the strongest asynchronous specification).** Let \( \Theta_1 \) be the strongest asynchronous specification w.r.t \( \Theta_2 \) if

1. \( \Theta_1 \) is asynchronous, and

2. \( \forall P. (s \in \text{Obs}_s(P) \cap P \models_{\text{sync}} \Theta_{\text{ass}}) \) if and only if \( s \in \text{trace}(\Theta_{\text{ass}}) \).

**Proposition 8.5.16.** \( \Theta_{\text{ass}} \) is the strongest specification w.r.t \( \Theta_{\text{sync}} \).

**Proof.** Based on Definition 8.5.15 it is proved directly from Lemma 8.5.13 and Proposition 8.5.14.

**Lemma 8.5.17.** If \( P \models_{\text{sync}} \Theta_{\text{sync}} \), then \( \forall s \in \text{Obs}_s(P) \) implies \( s \in \text{trace}(\Theta_{\text{ass}}) \).

**Proof.** Firstly, \( P \models_{\text{sync}} \Theta_{\text{sync}} \) means that, for any \( s' \in \text{Obs}_s(P) \), we have \( s' \in \text{trace}(\Theta_{\text{sync}}) \), and for any \( s \in \text{Obs}_s(P) \), \( s \) is the result of legal permutations from some \( s' \in \text{Obs}_s(P) \).

In other words, for any \( s \in \text{Obs}_s(P) \), there exists \( s' \) such that \( s' \in \text{Obs}_s(P) \) and \( s' \in \text{trace}(\Theta_{\text{sync}}) \), then \( s \) can be reached from \( s' \cap s \). Based on Lemma 8.5.13 \( s \) satisfies conditions listed there. Since for any \( s \) satisfies these conditions, by Lemma 8.5.14 it implies \( s \in \text{trace}(\Theta_{\text{ass}}) \), thus \( s \in \text{trace}(\Theta_{\text{ass}}) \).
Definition 8.5.18 (input-output alternating sequence). Let $\ell_{in}^i$ be the $i$th input action and $\ell_{out}^i$ be the $i$th output action. $s$ is called an input-output alternating sequence if it is of the shape

$$s = \ell_{in}^1 \cdot \ell_{out}^1 \cdot \ell_{in}^2 \cdot \ell_{out}^2 \cdots$$

where $\ell_{in}^1$ is the first action and the sequence of actions will end up with $\ell_{in}^k$ or $\ell_{out}^k$ for some $k \geq 1$.

Proposition 8.5.19. If $P \models_{async} \Theta_{ass}$, then $P \models_{async} \Theta_{ass}$.

Proof. It can be proved by proving that $\Theta_{ass}$ is asynchronous through proving it is commutative with the definitions and propositions introduced later. Another direct proof without proving that $\Theta_{ass}$ is asynchronous is provided in Appendix C.1.

Proposition 8.5.20. Assume $s$ is an input-output alternating sequence. If $s \in \text{trace}(\Theta_{ass})$, then $s \in \text{trace}(\Theta_{sync})$.

Proof. Please see Appendix C.1.

The additional lemmas for proving Propositions 8.5.19 and 8.5.20 are in Appendix C.

Although Proposition 8.5.20 says that $G_{\text{assign}}$ is an asynchronous verifiable specification that can realise synchronous behaviours w.r.t $\Theta_{sync}$, the other way round is not true. The following example illustrates this point.

Example 8.5.21. Assume the initial value of state $c \in \Theta_{ass}$ is empty set (i.e. $c \mapsto \emptyset$) and the initial value of state $t$ is 1. Also, assume the initial value of $c \in \Theta_{sync}$ is 1.

Consider a trace $s$:

$$s_1[C,S]?\text{req}(\varepsilon) \cdot s_2[C,S]?\text{req}(\varepsilon) \cdot s_1[S,C]!\text{ans}(2)$$

then $s \in \text{trace}(\Theta_{ass})$ but $s \not\in \text{Ob}_a(P)$ where $P \models_{\text{sync}} \Theta_{sync}$ because there does not exist $s' \in \text{trace}(\Theta_{sync})$ such that $s' \cdot s$.

The next result says that asynchronous verifiability is consistent with the asynchronous trace equivalence. Below let $P \approx_{\text{async}} Q$ mean $\text{Ob}_a(P) = \text{Ob}_a(Q)$. In (SS), we have shown how $\approx_{\text{async}}$ (but not its synchronous counterpart) can be used for non-trivial optimising transformation.

Proposition 8.5.22. If $P \approx_{\text{async}} Q$ and $P \models_{\text{async}} \Theta$ then $Q \models_{\text{async}} \Theta$. 

183
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

Proof. Assume $P \approx_{\text{async}} Q$ and $P \models_{\text{async}} \Theta$. We first show $\text{Obs}_{a}(Q) \subseteq \text{trace}(\Theta)$. By assumption we have:

1. If $s \in \text{Obs}_{a}(Q)$, then $s \in \text{Obs}_{a}(P)$ based on $P \approx_{\text{async}} Q$.
2. If $s \in \text{Obs}_{a}(P)$, then $s \in \text{trace}(\Theta)$ based on $P \models_{\text{async}} \Theta$.

Hence if $s \in \text{Obs}_{a}(Q)$, then $s \in \text{trace}(\Theta)$, as required.

We next show input consistency. Suppose $s \in \text{Obs}_{a}(Q)$ and $s \cdot \ell \in \text{trace}(\Theta)$ where $\ell$ is input. $P \approx_{\text{async}} Q$ implies $s \in \text{Obs}_{a}(P)$, and $P \models_{\text{async}} \Theta$ implies $s \cdot \ell \in \text{Obs}_{a}(P)$.

Again by $P \approx_{\text{async}} Q$, we obtain $s \cdot \ell \in \text{Obs}_{a}(Q)$ as required. This concludes the proof. ■

8.5.3 Commutativity

A basic issue in Definition 8.5.7 and its characterisation in Proposition 8.5.9 is that they do not directly mention the (intensional) structure of specifications. Thus it does not offer engineers insights as to how one may design her/his specifications. Extending the usage of the term in (81), we may call a criteria for specifications which a designer can use for ensuring robustness w.r.t. asynchrony, healthiness condition. The following definition is a first step towards such a criteria.

Definition 8.5.23 (confluence). $\Theta$ is confluent if, whenever $\Theta \xrightarrow{s} \Theta'$, if $\Theta' \xrightarrow{\ell_2 \ell_1} \Theta''$ and $\ell_2 \ell_1 \succcurlyeq \ell_1 \ell_2$, then $\Theta' \xrightarrow{\ell_2 \ell_1} \Theta''$ again.

I.e. the specification accepts the same sequence of values regardless of legal permutations and the resulting states are the same. Immediately confluence means asynchrony.

Lemma 8.5.24. $\Theta$ is asynchronous iff $s \cdot \ell_1 \cdot \ell_2 \in \text{trace}(\Theta)$ and $\ell_1 \cdot \ell_2 \succcurlyeq \ell_2 \cdot \ell_1$ imply $s \cdot \ell_2 \cdot \ell_1 \in \text{trace}(\Theta)$ for each $s, \ell_1$ and $\ell_2$.

Proof. For $(\Rightarrow)$, it is trivial by Definitions 8.5.7 and 8.5.23. For $(\Leftarrow)$, we want to prove that all cases should satisfy Definition 8.5.7, thus $\Theta$ is asynchronous. The reasonings are as follows:

1. If $s = \emptyset$, which is not permutable, then $\forall \ell_1 \ell_2 \in \text{trace}(\Theta), \ell_1 \ell_2 \succcurlyeq \ell_2 \ell_1 \in \text{trace}(\Theta)$ satisfies Definition 8.5.7.

2. If $s \neq \emptyset$, several cases are analysed below:

   (1) If $s \not\succcurlyeq$, which means $s$ is not permutable with any other sequence of actions,
8.5 Theory for Stateful Specifications

(a) when neither $\ell_1$ nor $\ell_2$ can permute with $s$, then the only permutable actions in $s \cdot \ell_1 \cdot \ell_2 \in \text{trace}(\Theta)$ is $\ell_1 \cdot \ell_2 \curvearrowleft \ell_2 \cdot \ell_1$, and $s \cdot \ell_2 \cdot \ell_1 \in \text{trace}(\Theta)$. It satisfies Definition 8.5.7.

(b) when there exists $\ell'_1, \ldots, \ell'_j \in s$ such that $\ell_2$ (or $\ell_1$) is permutable with $\ell'_1, \ldots, \ell'_j$. Note that, since permutations are done one by one through legal unit permutation, $s$ should be of the following shape:

$$s = s_0 \cdot \ell'_1 \ldots \ell'_{j-1} \cdot \ell'_j,$$

where $s_0$ is not permutable at all (i.e. it means that $s_0$ is empty, or actions in $s_0$ are not permutable with each other and no action in $s_0$ is permutable with any action of $\ell'_1, \ldots, \ell'_j$.) Assume that is $\ell_2$ can permute with $\ell'_1, \ldots, \ell'_{j-1}$. Then

$$s_0 \cdot \ell'_1 \ldots \ell'_{j-1} \cdot \ell'_j \cdot \ell_1 \cdot \ell_2 \curvearrowleft s_0 \cdot \ell'_1 \ldots \ell'_{j-1} \cdot \ell'_j \cdot \ell_2 \cdot \ell_1$$

Let $s_0 \cdot \ell'_1 \ldots \ell'_{j-1} \cdot \ell_2 = s' \cdot \ell_2$. It is either

(i) $\ell_2$ can permute with some actions in $\ell'_1 \ldots \ell'_{j-1}$ then it is still under the analysis of case 2.(1)(b), or

(ii) $\ell_2$ has permuted to all permutable actions in $s'$ until $s_0$, which is not permutable at all. Then it is case 2.(1)(a) that satisfies Definition 8.5.7.

Similarly, if $\ell_2 \cdot \ell_1 \curvearrowleft \ell_1 \cdot \ell_2$ and $\ell_1$ can permute with some actions in $s$, it is again under the analysis of case 2.(1)(b).

(2) If there exists $s'$ such that $s \curvearrowright s'$, $s$ should be of the following shape:

$$s = s'_1 \cdot \ell''_1 \cdot \ell''_2 \cdot s'_2,$$

where $\ell''_1 \cdot \ell''_2 \curvearrowright \ell''_2 \cdot \ell''_1$ and actions in $s'_2$ are not permutable with each other and no action in $s'_2$ is permutable with any action in $s'_1 \cdot \ell''_1 \cdot \ell''_2$. Then consider

$$s'_1 \cdot \ell''_1 \cdot \ell''_2 \cdot s'_2 \cdot \ell_1 \cdot \ell_2 \curvearrowleft s'_1 \cdot \ell''_1 \cdot \ell''_2 \cdot s'_2 \cdot \ell_2 \cdot \ell_1$$

185
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

It is either

(a) \( \ell_2 \) is not permutable with \( s'_2 \), then we only consider the part \( s'_1 \cdot \ell''_1 \cdot \ell''_2 \), since \( s \cdot \ell_1 \cdot \ell_2 \in \text{trace}(\Theta) \) implies \( s \in \text{trace}(\Theta) \), which again implies \( s'_1 \cdot \ell''_1 \cdot \ell''_2 \in \text{trace}(\Theta) \), so that \( s'_1 \cdot \ell''_1 \cdot \ell''_2 \in \text{trace}(\Theta) \), and this case (i.e. \( s'_1 \cdot \ell''_1 \cdot \ell''_2 \)) is under the analysis of case 2.(1)(b).

(b) \( \ell_2 \) is permutable with \( s'_1 \cdot \ell''_1 \cdot \ell''_2 \cdot s'_2 \). Then it is again in case 2.(1)(b).

Since all situations in 2.(1)(b) will finally go to 2.(1)(b)(ii), which means when the permutation terminates, it satisfies Definition 8.5.7. Overall, all possible cases satisfy Definition 8.5.7, thus \( \Theta \) is asynchronous. ■

**Proposition 8.5.25.** If \( \Theta \) is confluent, then it is asynchronous.

**Proof.** Directly from Definition 8.5.23 and Lemma 8.5.24. ■

Note that the other way round is not true. The example below illustrates this point.

**Example 8.5.26.** Assume the initial values of states \( c \) and \( t \) are both 0, and the local SP for role \( p \) in session \( s \) is:

\[
\begin{align*}
    s[p] : q_1!\text{ans}(\varepsilon)\langle\langle \text{true}; c = 50 \rangle \rangle . q_2!\text{ans}(\varepsilon)\langle\langle \text{true}; t = c + 10 \rangle \rangle
\end{align*}
\]

Let \( \ell_1 = s[p, q_1!]\text{ans}(\varepsilon) \) and \( \ell_2 = s[p, q_2!]\text{ans}(\varepsilon) \). Then \( \ell_1 \cdot \ell_2 \) makes state \( t \) be 60, but \( \ell_2 \cdot \ell_1 \) makes state \( t \) be 10.

One can easily find a specification which is not confluent (for example, if a specification just does the same counting as the one defined with stateful protocol \( G_{\text{sync}} \)). To check confluence, we still need to consider all possible transition derivatives of \( \Theta \). However we can observe that, in such a derivative, the obligations used to check confluence are already present in \( \Theta \). This suggests us to only look at the obligations occurring in \( \Theta \) and check their commutativity w.r.t. their legal unit permutations. This method demands designers to look only at \( \Theta \), so that it clearly helps her/his design process. The method treats a predicate and an update in an obligation as functions (operations) on state, as follows. Let \( \dagger \in \{?,!\} \).

**Definition 8.5.27 (predicate/update functions).** Let \( \xi \overset{\text{def}}{=} r \dagger l(x : S)\langle A; E \rangle \) with the associated state \( D \) whose domain is \( f_1, ..., f_n \). W.l.o.g. we regard \( E \) to be a
8.5 Theory for Stateful Specifications

Simultaneous substitution of the form $f_1 := e_1, ..., f_n := e_n$. Then we define:

$$\text{pred}(\xi) \overset{\text{def}}{=} \lambda x, f_1, ..., f_n.A \quad \text{upd}(\xi) \overset{\text{def}}{=} \lambda x, f_1, ..., f_n.(e_1, ..., e_n)$$

We call $\text{pred}(\xi)$ (resp. $\text{upd}(\xi)$) the *predicate function* (resp. *update function*) of $\xi$.

**Example 8.5.28.** Below we project $G_{\text{sync}}$ and $G_{\text{assign}}$ (all from Section 8.1) to the server. For simplicity we assume its local state only consists of those fields specified in global SP.

$$G_{\text{sync}} \upharpoonright S = B?\text{req}(\epsilon) \langle\langle \text{true}; \epsilon \rangle\rangle . B!\text{ans}(x : \text{int}) \langle\langle x = c ; c := c + 1 \rangle\rangle$$

$$G_{\text{assign}} \upharpoonright S = B?\text{req}(x) \langle\langle \text{true}; t := t + 1 \ c := c \cup \{ t \} \rangle\rangle . B!\text{ans}(x : \text{int}) \langle\langle x \in c ; c := c \setminus \{ x \} \rangle\rangle$$

Then the following table gives the functions induced by obligations in these local types.

<table>
<thead>
<tr>
<th>input</th>
<th>output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_{\text{sync}} \upharpoonright S$</td>
<td>$\xi_0 \overset{\text{def}}{=} B?\text{req}(\epsilon) \langle\langle \text{true}; \epsilon \rangle\rangle$</td>
</tr>
<tr>
<td>$\text{pred}(\xi_0) \overset{\text{def}}{=} \lambda x, c. (\text{true})$</td>
<td>$\text{pred}(\xi_1) \overset{\text{def}}{=} \lambda x, c. (x = c)$</td>
</tr>
<tr>
<td>$\text{upd}(\xi_0) \overset{\text{def}}{=} \lambda x, c. (\epsilon)$</td>
<td>$\text{upd}(\xi_1) \overset{\text{def}}{=} \lambda x, c. (c + 1)$</td>
</tr>
</tbody>
</table>

| $G_{\text{assign}} \upharpoonright S$ | $\xi_2 \overset{\text{def}}{=} B?\text{req}(x) \langle\langle \text{true}; t := t + 1 \ c := c \cup \{ t \} \rangle\rangle$ | $\xi_3 \overset{\text{def}}{=} B!\text{ans}(x : \text{int}) \langle\langle x \in c ; c := c \setminus \{ x \} \rangle\rangle$ |
| $\text{pred}(\xi_2) \overset{\text{def}}{=} \lambda x, c. (\text{true})$ | $\text{pred}(\xi_3) \overset{\text{def}}{=} \lambda x, c. (x \in c)$ |
| $\text{upd}(\xi_2) \overset{\text{def}}{=} \lambda x, c. (t + 1 \ c \cup \{ t \})$ | $\text{upd}(\xi_3) \overset{\text{def}}{=} \lambda x, c. (c \setminus \{ x \})$ |

Once we can treat obligations as operations on state, we can define their commutativity.

Since the commutativity we need is asymmetric (corresponding to asymmetric permutations induced by asynchrony, cf. Definition 8.4.12), we define semi-commutativity, which plays a key role in validating specifications later. A precursor of the following construction in a different setting is found in [52] (see Chapter 9 for discussions).

**Definition 8.5.29 (semi-commutativity).** Assume w.l.o.g., $\xi_i$ and $\xi_j$ use $f$ as the field. Then we say $\xi_i$ commutes over $\xi_j$ if, for any message values $v_i$ and $v_j$ (for $\xi_i$ and $\xi_j$), and any initial state $w$ (for $f$), the following conditions hold: If $\text{pred}(\xi_i)(v_i, w)$ and $\text{pred}(\xi_j)(v_j, \text{upd}(\xi_j)(v_j, w))$ are both true, then

1. $\text{pred}(\xi_j)(v_j, w)$ and $\text{pred}(\xi_i)(v_i, \text{upd}(\xi_j)(v_j, w))$ are both true.
2. $\text{upd}(\xi_j)(v_j, \text{upd}(\xi_i)(v_i, w)) = \text{upd}(\xi_i)(v_i, \text{upd}(\xi_j)(v_j, w))$.

If $\xi_i$ commutes over $\xi_j$ and vice versa, then we say $\xi_i$ and $\xi_j$ are commutative.

Note that the if statement says that it should satisfy the conditions above for any kind of initial values. I will explain the reason with Example 8.5.36 after Definition 8.5.31 and Proposition 8.5.34 are introduced.

Example 8.5.30. We show $\xi_1$ in Example 8.5.28 does not commute over itself. Let $f = c$. Then $\text{pred}(\xi_1)(1, 1)$, $\text{pred}(\xi_1)(2, \text{upd}(\xi_1)(1, 1))$ and $\text{pred}(\xi_1)(2, 2)$ are all true, however $\text{pred}(\xi_1)(2, 1) = \text{false}$. Similarly, $\xi_0$ does not commute over $\xi_1$ (however $\xi_0, \xi_0$ are commutative).

Using this notion, the healthiness condition for asynchronous specification can be concisely stated as follows. Below we say an obligation is usable in $\Theta$ if it occurs in a local SPin $\Theta$ or in the projection of a global SPin $\Theta$ to its potentially local role, where by “potentially local” we mean that the role has a potential to be played locally (e.g. for the global SP carried by an input shared channel type (i.e. $a(s[p] : G)$), only the specified role is potentially local).

Definition 8.5.31 (commutativity). Given $\Theta$, let $\xi_1, ..., \xi_n$ be all the obligations usable in $\Theta$. Then we say $\Theta$ is commutative if the following conditions hold:

1. For (possibly identical) $\xi'_1$ and $\xi'_2$ from $\{\xi_1, ..., \xi_n\}$, if both are inputs or both are outputs, then $\xi'_1$ and $\xi'_2$ are commutative.
2. For distinct $\xi'_1$ and $\xi'_2$ from $\{\xi_1, ..., \xi_n\}$, if $\xi'_1$ is an output and $\xi'_2$ is an input then $\xi'_1$ commutes over $\xi'_2$.

Possibly identical obligations means that it can be two obligations which are exactly the same, e.g. analysing $\xi, \xi$. In particular when there is only one obligation in $\Theta$, this obligation, say $\xi$, should be analysed by itself $\xi, \xi$ to know whether it commutes over itself.

Note that, based on Definition 8.5.29 Definition 8.5.31 states that, $\Theta$ is commutative if, for any kind of initial values in $\Theta$, it satisfies the conditions given above. It is very important that it is for any initial value. Even though, assume a specification $\Theta$ is given with initial value $w$, $\Theta$ satisfies all conditions above with $w$ but not with another initial value, say $w' \neq w$, then $\Theta$ is not commutative. I.e. $\Theta$ is action confluent when
all obligations used in the specifications for the target process commute over each other up to legal permutations.

Before proving “Θ is commutative implies Θ is confluent”, the following lemma is introduced.

**Lemma 8.5.32.** Assume $Θ \xrightarrow{s} Θ'$ for some $s$. If $Θ$ is commutative, then $Θ'$ is commutative.

**Proof.** For $(\Rightarrow)$, because $Θ' \subset Θ$:

1. For any obligation $ξ ∈ Θ'$, $ξ ∈ Θ'$ implies $ξ ∈ Θ$, where $Θ$ is commutative so that $ξ$ itself is commutative.

2. For any two obligations $ξ, ξ' ∈ Θ$ but $ξ' \notin Θ'$ (an obligation may be finished since the conversation is finished. See Figure 8.3, the LTS of specifications), since $ξ$ itself should be commutative due to $ξ ∈ Θ$ and $Θ$ is commutative, $ξ$ is still commutative in $Θ'$ even it is alone.

Thus $Θ'$ is commutative with new values of states resulting from $Θ \xrightarrow{s} Θ'$ if $Θ$ is commutative. ■

Note that the other way round (i.e. $(\Leftarrow)$) is not true because, while $Θ'$ is derived from $Θ$, $Θ$ can have more obligations than what $Θ'$ does. $Θ'$ is commutative cannot imply that $Θ$ is commutative.

**Remark 8.5.33.** Definitions 8.5.27 and 8.5.29 imply every obligation $ξ$ corresponds to a valid action, and vice versa.

We have soundness characterisation for asynchronously verifiable specifications:

**Theorem 8.5.34 (soundness characterisation: commutativity).** If $Θ$ is commutative then it is confluent (hence asynchronous).

**Proof.** Assume that $Θ$ is commutative is given, let $Θ \xrightarrow{s} Θ'$ for some $s$. Assume $Θ' \xrightarrow{ℓ_1, ℓ_2} Θ''$ for some $ℓ_1$ and $ℓ_2$, and $ℓ_1, ℓ_2 \in ℓ_2, ℓ_1$. We will show that $Θ' \xrightarrow{ℓ_1, ℓ_2} Θ'$ and $Θ'' = Θ'''$. Assume the value carried by $ℓ_i$ is $v_i$, $i = \{1, 2\}$. Since $Θ'$ is commutative based on Lemma 8.5.32

1. When both of $ℓ_1$ and $ℓ_2$ are for output (resp. for input), these actions correspond to (possibly identical) obligations $ξ_1$ and $ξ_2$ from $Θ'$, which are both for outputs.
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

(resp. for inputs). Assume the vector of values of states \( \tilde{f} \in \xi_1 \cup \xi_2 \) is \( \tilde{w} \), then because \( \Theta' \) is commutative,

\[
\text{pred}(\xi_1)(v_1, \tilde{w}) = \text{pred}(\xi_2)(v_2, \text{upd}(\xi_1)(v_1, \tilde{w})) = \text{true}
\]

implies

\[
\text{pred}(\xi_2)(v_2, \tilde{w}) = \text{pred}(\xi_1)(v_1, \text{upd}(\xi_2)(v_2, \tilde{w})) = \text{true}
\]

which means \( \Theta' \xrightarrow{\ell_1} \Theta'' \) for some \( \Theta''' \), and moreover,

\[
\text{upd}(\xi_1)(v_1, \text{upd}(\xi_2)(v_2, \tilde{w})) = \text{upd}(\xi_2)(v_2, \text{upd}(\xi_1)(v_1, \tilde{w})) = \tilde{w}'
\]

which means \( \ell_1 \cdot \ell_2 \) and \( \ell_2 \cdot \ell_1 \) consume the same obligations and they reach the same value of states \( \tilde{w}' \), so that we have \( \Theta'' = \Theta''' \).

2. When \( \ell_1 \) is for output and \( \ell_2 \) is for input, these actions correspond to distinct obligations \( \xi_1 \) and \( \xi_2 \) from \( \Theta' \), which are separately for output and for input. Assume the vector of values of states \( \tilde{f} \in \xi_1 \cup \xi_2 \) is \( \tilde{w} \), then

\[
\text{pred}(\xi_1)(v_1, \tilde{w}) = \text{pred}(\xi_2)(v_2, \text{upd}(\xi_1)(v_1, \tilde{w})) = \text{true}
\]

implies

\[
\text{pred}(\xi_2)(v_2, \tilde{w}) = \text{pred}(\xi_1)(v_1, \text{upd}(\xi_2)(v_2, \tilde{w})) = \text{true}
\]

which means \( \Theta' \xrightarrow{\ell_1 \cdot \ell_2} \Theta'' \) for some \( \Theta''' \), and moreover,

\[
\text{upd}(\xi_1)(v_1, \text{upd}(\xi_2)(v_2, \tilde{w})) = \text{upd}(\xi_2)(v_2, \text{upd}(\xi_1)(v_1, \tilde{w})) = \tilde{w}'
\]

which means \( \ell_1 \cdot \ell_2 \) and \( \ell_2 \cdot \ell_1 \) consume the same obligations and they reach the same value of states \( \tilde{w}' \), so that we have \( \Theta'' = \Theta''' \). ■

Note that the other way round is not true. The completeness characterisation is however more difficult because we need to know the invariants of initial value of the state which is asserted by logical formula and stipulated by update rules. The following examples explain the reasons.

Example 8.5.35. Assume \( \Theta \) has the following local SP, called \( T \). The initial value of \( c \in \Theta \) is 2, and \( c \) will only be updated by the actions defined in \( T \). It shows that \( \Theta \) is
confluent but not commutative.

\[ T = B! \{ \text{ans}_1(\varepsilon) \langle \text{true} ; c := c + 1 \rangle , \]
\[ \text{ans}_2(\varepsilon) \langle c < 2 ; c := c + c \rangle \}. \]

end

It is confluent because based on Definition 8.5.23, we assume \( \Theta \) starts from initial value of \( c \), which is 2. Whenever \( \Theta \xrightarrow{s} \Theta' \xrightarrow{\ell_2 \cdot \ell_1} \Theta'' \) and \( \ell_1 \cdot \ell_2 \succ \ell_2 \cdot \ell_1, \Theta \xrightarrow{s} \Theta' \xrightarrow{\ell_2 \cdot \ell_1} \Theta'' \) is true because \( \ell_1 \) or \( \ell_2 \) never be with branch \( \text{ans}_2 \); otherwise it becomes \( \Theta' \xrightarrow{\ell_1 \cdot \ell_2} \), which is not the case considered.

On the other hand, because Definition 8.5.31 asks that \( \Theta \) is commutative if it satisfies the commutativity conditions for any kind of initial value of \( c \), we know that it does not satisfy the conditions immediately when the initial value of \( c \) is smaller than 2 (i.e., 1, 0, -1, -2, ...). Thus \( \Theta \) is not commutative.

The main motivation to have property of commutativity for \( \Theta \) is that commutativity provides a soundness characterisation, and a more easily verifiable way to decide if \( \Theta \) is confluent, which automatically implies it is asynchronous-verifiable.

Comparing Definition 8.5.23 and Definition 8.5.31, readers may feel curious about why commutativity should hold for any possible initial value of a state \( f \). The reason is because, generally, we do not know what the invariants of the initial values of the states of a given \( \Theta \) are. To ensure that a \( \Theta \) is commutative, we need to know if it satisfies all conditions for all possible initial values. The following example illustrates this point:

**Example 8.5.36.** Consider a specification, \( \Theta \), having a state \( c \) with initial value 8 and the following local SP, called \( T \). Assume \( T \) is for endpoint \( s[q] \) and \( c \) will only be updated by the actions defined in \( T \).

\[ T = p_1! \text{req}_1(\varepsilon) \langle c < 10 ; \varepsilon \rangle , \]
\[ p_2! \text{req}_2(\varepsilon) \langle c < 10 ; c := c + 1 \rangle . \]

end

If commutativity is defined only for a particular initial value of \( c \in \Theta \), which is 8, then \( \Theta \) is commutative; however, \( \Theta \) is not confluent. Let \( \ell_1 = s[q,p_1]!\text{req}_1(\varepsilon) \) and \( \ell_2 = s[q,p_2]!\text{req}_2(\varepsilon) \), when several actions in trace \( s \) update \( c \) and \( c \) becomes 9, and

\[ \Theta \xrightarrow{s} \Theta' \xrightarrow{\ell_2 \cdot \ell_1} \Theta'' \]

is achieved, \( \ell_1 \cdot \ell_2 \succ \ell_2 \cdot \ell_1 \), but \( \Theta' \xrightarrow{\ell_1 \cdot \ell_2} \).
This is because the value of \( c \) is changing as actions happen. If Definition 8.5.31 only considers particular initial value of \( c \), then

1. the checking of commutativity is, however, done by a snapshot for any possible pair \( \xi_i, \xi_j \in \Theta \). It can not reflect the real situation of the changes of value of \( c \);
2. or, we know exactly what the invariant of \( \Theta \) is; e.g. the initial value of \( c \) should be bigger than or equal to 10. With this invariant, \( \Theta \) is confluent. But generally, to find out the invariant(s) of a specification is difficult, which will be part of the future works.

Thus, we generate the soundness characterisation with the following concept:

**Remark 8.5.37.** Whenever any possible snapshot is taken with any kind of initial value of \( c \), \( \Theta \) satisfies the conditions defined in Definition 8.5.31 then \( \Theta \) is commutative.

As mentioned in point 2 above, the method of checking commutativity can be strengthened by adding an invariant (including correlation among states) in state and checking that invariant continues to hold at each step. We can now show all our example specifications with the stateful protocols except the one induced by \( G_{sync} \) is asynchronous. Below, let \( \Theta_{async} \)'s shared environment contains server : \( I(G_{async}[S]) \), and let its data storage contains \( c \mapsto \{\} \).

\[
\Theta_{async} = \langle \text{ser : } \langle G_{async}[S] \rangle; \quad \{ s_j[S] : C!\text{req}(\varepsilon)\langle\langle \text{true} \; ; \varepsilon \rangle \rangle.C!\text{ans}(x : \text{int})\langle\langle x \not\in c \; ; c := c \cup \{x\}\rangle \rangle \}_j \in J; \quad c \mapsto \{ \} \rangle
\]

where \( J \) is the set of indexes of sessions obeying \( G_{async} \). Then we have the following proposition:

**Proposition 8.5.38.** \( \Theta_{async} \) and \( \Theta_{ass} \) at server are both commutative, hence asynchronous.

**Proof.** Commutativity of operations in \( \Theta_{async} \) is immediate. For \( \Theta_{ass} \), we use \( \xi_2 \) and \( \xi_3 \) from Example 8.5.28 Then \( \xi_3 \) easily commutes over itself, because if \( \text{pred}(\xi_3)(v, c) = \text{true} \) and \( \text{pred}(\xi_3)(v', \text{upd}(\xi_3)(v, c)) = \text{pred}(\xi_4)(v', c \setminus \{v\}) = \text{true} \), so that

\[
\text{pred}(\xi_3)(v', c) = \text{true}.
\]

When \( v \neq v' \), we clearly have

\[
\text{pred}(\xi_3)(v, \text{upd}(\xi_3)(v', c)) = \text{pred}(\xi_3)(v, c \setminus \{v'\}) = \text{true}.
\]
When \( v = v' \), due to \( \text{pred}(\xi_3)(v, c) = \text{true} \) and \( \text{pred}(\xi_3)(v', c \setminus \{v\}) \) which together imply that \( c \) contains at least two elements whose values are \( v = v' \), we clearly have \( \text{pred}(\xi_3)(v, c \setminus \{v'\}) = \text{true} \). Similarly \( \text{upd}(\xi_3)(v', \text{upd}(\xi_3)(v, c)) = \text{upd}(\xi_3)(v', c \setminus \{v\}) = c \setminus \{v\} \setminus \{v'\} \) which is equal to \( \text{upd}(\xi_3)(v, \text{upd}(\xi_3)(v', c)) = \text{upd}(\xi_3)(v, c \setminus \{v'\}) = c \setminus \{v'\} \setminus \{v\} \). We can similarly check \( \xi_2 \) is commutative over itself, and \( \xi_3 \) commutes over \( \xi_2 \) (but not the converse), as required.

We can similarly check specifications induced by \( G_{pcs} \) and \( G_{ivc} \) are commutative.

Compare the definition of commutativity and the permutation rules of \( \Theta \), as explained in the beginning of Section 8.4.1, they have different usage:

**Remark 8.5.39.** Attribute of commutativity is used for developers to know whether a \( \Theta \) is asynchronous, while the permutation rules (defined in Definition 8.4.4) are used for an observer (e.g. system monitor) to have to observe the incoming and outgoing non-order-preserved actions.

The valuation of commutativity is essentially satisfiability of a formula whose free variables are universally quantified. Thus if the logic (for predicates) we use for our specification language is decidable, commutativity is decidable. In particular:

**Proposition 8.5.40.** With the SP language given in Section 8.2 restricting operations on integers to be the constant, the addition and the subtraction, then the commutativity of specifications is decidable.

**Proof.** By (161), a logic with sets, products and integers with additions is decidable, which subsumes the formulae used in Definition 8.5.29.

We discuss practical implications of these results in the conclusion of Section 9.1.3, Chapter 9.
8. SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS
Conclusions and Future Topics

9.1 Conclusions and Discussions

This thesis provides fundamental theories for governing real-life large-scale distributed systems from the process calculus to the monitoring mechanism, from session types to stateful specifications. We summarise the main theory chapters, which are Chapter 5, 6, 7, and 8, with conclusions and discussions in the following sections.

9.1.1 The Capability-passing $\pi$-calculus

The capability-passing $\pi$-calculus proposed in Chapter 5 extends the asynchronous $\pi$-calculus by additional primitives of request and accept. These can be used to create sessions linearly and enable the authentication of activities through pattern-matching of the capabilities of proposed participants. The calculus enjoys race-freedom at session roles (86) and reduces the tasks of endpoint access control by filtering unmatched capabilities.

Recently dynamic joining mechanisms have been studied in the conversation-calculus (26) (which uses conversation contexts) and (50) (which is based on roles). These formalisms enable the tracking of participants through roles, but do not enable their controls through capabilities. This thesis formalises asynchronous session creation with capability primitives through passing invitations at shared channels, while (26, 50) formalise joining to the existing session and maintain progress by advanced static type
9. CONCLUSIONS AND FUTURE TOPICS

checking. The result is that this thesis focuses on runtime enforcement of global protocol properties rather than static type checking, and on enforcement of properties by local runtime monitoring. Our framework also incorporates logical assertions, offering more fine-grained logical specifications than the bare protocols representable by types. The adequacy of this formalism is demonstrated by the properties we provide in our discussions of the calculus of dynamic asynchronously monitoring.

9.1.2 The Calculus of Dynamic Asynchronously Monitoring

The session-based specification and monitoring framework in which external monitors evaluate behaviours according to these specifications are respectively studied in Chapters 6 and 7. Session-based specifications, introduced in Chapter 6, provide developers with the ability to build up their own security protocols. System developers can program their desired global protocols through an intuitive description language. As an endpoint process starts a session, which generally involves multiple parties, she can select a well-defined protocol from a system library or define a protocol by herself for this session to obey. Then she, as an invitor, invites other parties, called invitees, to join this session playing particular roles defined in the protocol. As an invitee agrees to join the session to play a role, the invitor gives invitees corresponding external monitor guidance of endpoint behaviours, which takes the form of a specification encapsulating a local projection. The endpoint monitor therefore gets the ability to guard invitees’ behaviours against the guidance and determines whether their behaviours obey the protocol or not.

Chapter 7 contains a model of distributed monitoring featuring the following elements: (I) endpoint code is possibly ill-behaved; (II) global specifications enable concise global specifications of application-level multi-party protocols; and (III) conformance to global protocols is guaranteed at runtime through local monitoring. This monitoring framework can be seen as a distributed variant of runtime verification in the sense of (16, 60, 73). It is light-weight, concerned only with the observable executions, and does not aim to give a conclusive analysis about all their possible behaviours. Hence it is applicable to real-world systems, where off-line formal verification and static checking are intractable or impossible due to incomplete information on system components or the dynamic change in requirements.

There are two important principles of the theories of monitoring: soundness (safety), which states that enforcement results in a correct behaviour, and transparency, which
requires behaviour of a correct program not be modified (a principle studied for example in an automata framework (13, 143)). Our monitor suppresses (108) the illegal actions (as seen in (else) case of \( M \xrightarrow{\ell} M' \)) but neither immediately halts the process nor inserts the correct actions. Incorporating more elaborate reactions, as in edit automata (108, 143) is an interesting future topic. None of the above work can ensure the fidelity to application-level multi-party global protocols for distributed applications with logical properties.

9.1.3 Specifying Asynchronous Stateful Specifications

The characterisation results in Chapter 8 (see Section 8.5) offer not only a decision procedure for a rich subset of specifications, but also a basic insight in the design methodology for asynchronous specifications. In particular they shed light on the use of operations on sets in our examples in Section 8.1. Because checking commutativity relies solely on the obligations occurring in protocols, adding recursion to the syntax does not change the nature of commutativity checking nor the resulting guarantee.

If \( \Theta \) is asynchronous and a process behaves properly w.r.t. \( \Theta \) synchronously, an asynchronous observer will also judge the induced (permuted) trace is proper w.r.t. \( \Theta \). It is however easy to see that the converse is not true: for example, consider a server that violates \( \Theta_{as} \) by responding 2 to the first request, 1 to the second, but these are delayed by asynchrony, leading to a valid trace when they arrive at the remote observer.

A key consistency property is that any further legal permutation of this valid trace is again valid. For example, if a system monitor for Server is sitting between Buyer (i.e. as a client) and Server, and if this monitor observes a valid trace of Server against the specification she has, Buyer will observe no worse behaviour. This monotonic attribute gives a basis for an application of the presented framework such as runtime monitoring.

The semantic differences between synchronous and asynchronous communications have been studied for several decades: early works include (7, 45, 84, 90). The permutations associated with asynchronous communication used in Definition 8.4.12 are noted in these works (and implicit in such work as (98)). Their more explicit presentation in the categorical setting is found in (147). There is also a study in component validation based on asynchronous histories such as (130). In spite of these precursors and close technical connection, the existing works (except (21) which however focuses on synchronous specifications and proof rules for their verifications) may not have pointed out
9. CONCLUSIONS AND FUTURE TOPICS

the concrete semantic issues which stateful behavioural specifications and asynchronous
observables can induce, and how these issues can be resolved through the interplay
between synchronous and asynchronous semantics.

As observed in Section 8.5.3, a close analogue of the commutativity of operations
used for our characterisation result (Definition 8.5.29) appears in (52), where the authors
study a method for checking commutativity (called diamond connectivity) of operations
with pre-conditions in object-oriented programs, with a view to preventing the simulta-
taneous issuance of these operations when they are not commutative. They do not
(aim to) determine a class of specifications suitable for asynchronously communicating
processes.

In contrast, we stipulate a general class of specifications for communicating pro-
cesses suitable for asynchronous observations, and identify its subclass amenable for
automatic verification. We use commutativity to capture asymmetry in asynchronous
communications. Moreover, we propose and prove the properties for asserting that an
asynchronously verifiable specification is the strongest while one wishes to transform a
synchronously verifiable specification to an asynchronously verifiable one.

9.1.4 Concluding Remarks

The achievements of this thesis include (I) establishing formal syntax and semantics
for the session-based dynamic monitoring with control capabilities, (II) proposing a
fine-grained process calculus for linear asynchronous session creation, (III) exploring
the differences between monitoring the behaviours of the local and the global, (IV)
enriching theories of session types by embedding endpoints’ states into specifications,
(V) exploring the differences of observable behaviours between stateful asynchronous
and stateful synchronous monitoring, and (VI) proving properties of local and global
safety (soundness), transparency, and session fidelity (completeness) for the monitoring,
and proposing and proving properties for validating asynchronous specifications. As a
cooperative project, the large-scale cyber-infrastructure of OOI (129) is adopting our
theories as a blueprint for designing their governance systems. Also, a session-based
description language, called Scribble (83, 145), is embedding our specifications into its
syntax to realise more controls during programming. For the future, we have important
directions as those discussed in our future works (introduced in Section 9.2 later) to
explore using this work as a basis. We aim at exploring more theoretical results in
stateful specifications, the adaption of stateful specifications to stateful policy languages, commitments, and the applications of Scribble.

9.2 Future Topics

9.2.1 The Development of Scribble and Monitoring

Scribble is a protocol description language where a protocol is an agreement on how participants interact with each other. Developers can use it to easily code meaningful interaction: the communications among participants become effective, since they know when to expect the other parties to send their data, or whether the other party is ready to receive data it is sending. Scribble makes dynamic distributed monitoring straightforward through projecting the global description, written in Scribble, to every local endpoint as a local specification, and then embedding the generated corresponding monitor with this local specification. It also provides developers the ability and freedom to design their desired protocols for governing the products.

As a session-based description language, Scribble is a good subject for us to study the comparisons between it and other policy and protocol languages through discovering the attributes and the semantical behaviours, and the user feedback on using Scribble. Also, embedding assertions (as annotations) and stateful specifications into Scribble to develop a session-based asserted monitoring methodology of industrial strength is one of our ongoing works.

9.2.2 Exploring Structures of Asynchronous Specifications

There are many interesting open questions in the area of verifying asynchronous specifications. Here we outline the topics that we are currently investigating.

One topic is to explore approaches to automatically translating a synchronous proper stateful specification to an asynchronous proper one. In Chapter 8, two asynchronous transformed stateful specifications $\Theta_{async}$ and $\Theta_{ass}$ are proposed for translating $\Theta_{sync}$. However, they are proposed mostly by intuitions instead of formal understandings of $\Theta_{sync}$. More properties are needed to figure out the algorithm for automatic translation.

Also, identifying and formalising the elements of $\Theta$ which make $\Theta$ asynchronously verifiable are important. If these elements can be identified, we can formally describe the requirements to compose an asynchronously verifiable $\Theta$, and we can compare the
expressiveness of different asynchronously verifiable stateful specifications concretely. Some fundamental understanding about the elements in a specification can help us to analyse the relationships among $\Theta_{\text{sync}}$, $\Theta_{\text{async}}$, and $\Theta_{\text{ass}}$.

As Chapter 8 proves the property of soundness characterisation (see Theorem 8.5.34), which says a commutative specification is an asynchronously verifiable specification, we plan to investigate completeness. The difficulty of completeness has been illustrated in Example 8.5.36 of Chapter 8. Also, Example 8.5.35 in Chapter 8 points out that the property of commutativity is stronger than completeness by asking the conditions hold for any possible initial value of a state because we do not know the invariants of a given specification. To explore these invariants, the properties of structures of asynchronously verifiable specifications should be explored and stated.

Currently we aim to explore and analyse concrete forms of asynchronously verifiable specifications with different structures, informed by use cases from (129) as well as our theory, with a view to their usage in monitoring. One challenge is to find a solid asynchronously verifiable specification framework for inherently conflicting operations, such as two consecutive and overwriting updates on the same datum.

9.2.3 Sharing Memory in Stateful Asynchronous Specifications

As we discussed in Chapter 8 when a state is asserted in a predicate and its updating rules are stipulated in a specification, properly specifying the specification under asynchronous environment becomes critical. As a first step of this issue, in this thesis, we confine a state of an endpoint can only be accessed by sessions who are obeying to the same global specification. Moreover, the state is local, which means it can only be accessed by multi-threads of the local process possessing it; it can not be shared across different domains.

One topic here is to analyse and realise sharing a state, which can only be accessed by a local process, among different sessions. In other words, although a state belongs to a particular local process, this process can join different sessions for playing different roles. With this setting, we want to investigate the structures of a specification which ensure that a state can be properly shared.

When we understand the above more complete, we hope to extend the topic to sharing memory in different sessions across different domains. For example, a state is not local to a process, but is a shared memory in the network, which can be accessed by
authenticated session-roles. This topic will explore the session-based memory sharing in cloud computing.

9.2.4 Governance with Stateful Policies

When we adopt a session-based governance framework where dynamic monitoring is based on stateful specifications, it is natural to explore the corresponding stateful policy language for specifying policies and commitments for governance.

A policy should be simply stated by a policy language so that it is readable by general users. With this principle, we are investigating expressive policy languages for policies which can specify traces which imply the changes of an endpoint field, rather than complicated stateful specifications. We have learned from Chapter 8 that it is not easy to specify an asynchronously verifiable stateful specification.

We find that there are elements which compose a specification, and those elements are the requirements should be stated in a policy. For example, if a policy \( r_q \) asks that “in a trace, every value carried by an output action should be unique”, then \( \Theta_{\text{sync}} \), \( \Theta_{\text{async}} \) and \( \Theta_{\text{ass}} \) all satisfy \( r_q \) so that \( r_q \) is one of the elements which compose these specifications.

But when a policy \( r_q \) says “in a trace, every content carried by an output should be one increment larger than the content carried by its previous output”, then only \( \Theta_{\text{sync}} \) can specify, synchronously, this requirement. We say this kind of policy implies the changes of state of a local process, and it is not a proper policy under asynchronous environments.

Currently we are applying temporal logics to formalise the policy language, and wish to further analyse the properties of stateful policies with the results in Chapter 8.
9. CONCLUSIONS AND FUTURE TOPICS
Appendix for Capability-passing Calculus

A.1 Notes for the Syntax with or without Session Creation Rule

As the syntax defined in Figure 5.3 Chapter 5, we do not have a single rule for newing a session; instead, we use bound request to combine session creation and the first invitation. In (39), the rule for session creation, new $s : G.P$, is used. The advantages of using new $s : G.P$ are (I) clearly stating a process creates a fresh session $s$ specified under $G$, (II) enjoying flexibility for representing actions. A process is able to pass a partial capability to another process with this design of primitives. However, this primitive also makes the representation of interleaving actions too cumbersome to analyse.

For example, if the corresponding action of process new $s : G.P$ is new $s : G$, and $T$ is projected from $G$ as well as $T'$ is projected from $G'$, then the sequence of actions has the following six equivalent sequences of actions (represented by action labels):

\[
\begin{align*}
\text{new } s : G \cdot \text{new } s' : G' \cdot \overline{\alpha}(s[p] : T) \cdot b(s'[p'] : T') & \equiv \\
\text{new } s' : G' \cdot \text{new } s : G \cdot \overline{\alpha}(s[p] : T) \cdot b(s'[p'] : T') & \equiv \\
\text{new } s : G \cdot \text{new } s' : G' \cdot \overline{\alpha}(s'[p'] : T') \cdot \overline{\alpha}(s[p] : T) & \equiv \\
\text{new } s' : G' \cdot \text{new } s : G \cdot \overline{\alpha}(s'[p'] : T') \cdot \overline{\alpha}(s[p] : T) & \equiv \\
\text{new } s : G \cdot \overline{\alpha}(s[p] : T) \cdot \text{new } s' : G' \cdot \overline{\alpha}(s'[p'] : T') & \equiv \\
\text{new } s' : G' \cdot \overline{\alpha}(s'[p'] : T') \cdot \text{new } s : G \cdot \overline{\alpha}(s[p] : T) & \equiv \\
\end{align*}
\]
On the contrary, if \( \overline{a}(s[p] : G) \), as an action label, is used to stand for the sequence of actions \( \text{new } s : G \cdot \overline{a}(s[p] : T) \), there are only two equivalent sequences of actions:

\[
\overline{a}(s[p] : G) \cdot \overline{b}(s'[p'] : G') \equiv \overline{b}(s'[p'] : G') \cdot \overline{a}(s[p] : G)
\]

Therefore, using bound request \( \overline{a}(s[p] : G) \) and free request \( \overline{a}(s[p] : G) \) separately can reduce the complexity of the analysis of the sequences of actions.

Another reason is action \( \text{new } s : G \), which corresponds to process \( \text{new } s : G.P_{\text{req}} \), is always an action belonging to a requester, \( P_{\text{req}} \), but never to an acceptor because the command of \( \text{new } s : G \) becomes duplicated when an acceptor, say \( P_{\text{acc}} \), also has process \( \text{new } s : G.P_{\text{acc}} \). Instead, adopting action notation \( a(s[p] : G) \) with consistent meaning with \( \overline{a}(s[p] : G) \) for declaring \( s \) is new to the process can straightforwardly prevent the duplication illustrated above. Similarly, a free accept syntax can represent the following process:

\[ a(s[p] : G).b(s[q] : G') \]

in which there are two endpoints, \( a \) and \( b \), are running for this process. When the first invitation from session \( s \) comes to endpoint \( a \), it is new to the process so that \( a(s[p] : G) \) is applied, while the second invitation from session \( s \) comes to endpoint \( b \), it is not new to the process anymore so that \( b(s[p] : G') \) is applied.

## A.2 Notes for the Design of I- / O-mode Shared Names

The restrictions of creating a shared name and sending a name through interaction actions are reasoned below.

**The existence of input-mode shared name is unique.** Network coherence asks input-mode shared name exists whenever there is an output-mode shared name. It is defined in Definition 7.4.13 for network coherence. If we do not require this, then, as an invitor invites other parties to join a session with the knowledge of output-mode shared name, say \( a : 0(G[p]) \), which guides the invitor who is capable of playing role \( p \) specified under specification \( G \), and guides it where the target is by \( a \). If there is no corresponding input-mode shared name, say \( a : \text{im}(G[p]), \text{im} \in \{\text{I},\text{IO}\} \), because the monitor of an invitor is local, the monitor can not detect that there is...
A.2 Notes for the Design of I- / O-mode Shared Names

no receiver in the network as it approves this request, and may make the invitor wait forever for non-existent response.

Creating output-mode shared name is not allowed. As we require that whenever there is an output-mode shared name, say $a : 0(G[p])$, there exists its corresponding input-mode shared name $a : \im(G[p]), \im \in \{I, IO\}$, if we allow a process to create a new shared name with 0-mode, then this requirement can be easily broken because it is possible that, when output-mode shared name is created, its corresponding input-mode shared name has not existed.

A passed shared name can only be typed with output-mode as it is received. This restriction corresponds to those above. Refer to Figure 7.4 in which the LTS of monitors is defined, the following example illustrates the issue. Assume there is a process, playing session-role $s[p]$, sends a name $a$ with specification $I(G[p])$ to another process playing session-role $s[q]$. For the sender-side, a monitor can ensure whether the sender sends an input-mode shared name with specific specifications, like $s[p, q]!l_j(a)$, a monitor can check if $I(G[p]) = S_j, \Gamma \vdash S_j$ by referring to

$$s[p] : q!\{l_i(x_i : S_i)\langle A_i \rangle:T_i\}_{i \in I}.$$  

For the receiver-side, as label $l_j$ is chosen with an input action, for example, $s[p, q]?l_j(b)$,

$$s[q] : p?\{l_i(x_i : S_i)\langle A_i \rangle:T_i\}_{i \in I}$$

we can specify $S_j$ at the label pool above as $S_j = I(G[p])$; but, the receiver-side monitor cannot detect if $a = b$ because it is local, and we do not wish it takes the tasks of asking all monitors in the network one by one. If $a \neq b$, then, since $a$ is with input-mode and it has been sent out from its original owner, there is no $a$ with input-mode for those $a$ with output-mode. Thus we type every received shared name with output-mode to ensure the network coherence.
A. APPENDIX FOR CAPABILITY-PASSING CALCULUS
Appendix for Dynamic Asynchronously Monitoring

B.1 Proofs for Local Safety and Transparency

For proving Theorem 7.4.3 Local Conformance and Theorem 7.4.5 Local Transparency, auxiliary definitions and lemmas are stated.

Lemma B.1.1. Let $\ell$ be an input action label and $M \xrightarrow{\ell} M$ as $M$ approves label $\ell$. $M \xrightarrow{\ell}$ implies $M[P] \xrightarrow{\ell}$.

Proof. By the definitions of LTS of $M$ and $M[P]$ locally, for any input action $\ell$, if $M \xrightarrow{\ell}$, $M[P] \xrightarrow{\ell}$. ■

Theorem 7.4.3 (local safety). For each monitor $M$ and local process $P$, we have $M \models M[P]$.

Proof. Let

$$\mathcal{R} = \{(M_i[P], M_i) \mid P_i \text{ and } M_i \text{ are arbitrary}\} \quad (\text{B.1})$$

We show that $\mathcal{R}$ is a conformance relation as we defined in Definition 7.4.2.

1. When $\ell$ is an output action, based on Definition 7.2.6, by deduction, $M_0[P_0] \xrightarrow{\ell}$ implies $M_0 \xrightarrow{\ell}$.

2. When $\ell$ is an input action, $M_0 \xrightarrow{\ell}$ implies $M_0[P_0] \xrightarrow{\ell}$ by Lemma B.1.1.

3. If $M_0[P_0] \xrightarrow{\ell} M'_0[P'_0]$ and $M_0 \xrightarrow{\ell} M'_0$, since the relation $\mathcal{B.1}$ asks that $P'_0$ and $M'_0$ are arbitrary, we have $M'_0[P'_0] \mathcal{R} M'_0$ hence done.
Thus $\mathcal{R}$ is a conformance relation. ■

**Definition B.1.2 (LTS of monitor-off processes (addressed processes)).** We define $M\overset{\xi}{\to}P$ as the conjunction of $M\overset{\xi}{\to}M'$ and $P\overset{\xi}{\to}P'$:

$$
\frac{M\overset{\xi}{\to}M', P\overset{\xi}{\to}P'}{M\overset{\xi}{\to}M'[P']}
$$

**Lemma B.1.3 (determinacy of gateway transitions).** If $M\overset{\xi}{\to}M_1$ and $M\overset{\xi}{\to}M_2$ then $M_1 = M_2$. If $M\overset{\xi}{\to}M_1$ and $M\overset{\xi}{\to}M_2$ then $M_1^0 = M_2^0$.

*Proof.* By the definition of LTS of monitors, $M$ is deterministic. Similarly, by the definition of LTS of $M^0$, $M^0$ is deterministic, thus done. ■

**Definition B.1.4.** We write $\text{erase}(M) = M^0$ a monitor-off address obtained by erasing types, predicates and variables in $M$.

**Lemma B.1.5.**

1. If $M\overset{\xi}{\to}M'$, then $\text{erase}(M)\overset{\xi}{\to}\text{erase}(M')$.

2. Given $M^0 = \text{erase}(M)$, if $M\overset{\xi}{\to}M_2$ and $\text{erase}(M)\overset{\xi}{\to}M_2^0$, then $M_2^0 = \text{erase}(M_2)$.

*Proof.*

1. Since $M$ is deterministic, by the definition of $\text{erase}(M)$, $\text{erase}(M)$ is deterministic corresponding to $M$. Thus if $M\overset{\xi}{\to}M_2$, $\text{erase}(M)\overset{\xi}{\to}\text{erase}(M_2)$.

2. Since $M^0$ and $\text{erase}(M)$ are deterministic, if $M^0 = \text{erase}(M)\overset{\xi}{\to}M_2^0$, and together with 1. above, $M\overset{\xi}{\to}M_2$ implies $\text{erase}(M)\overset{\xi}{\to}\text{erase}(M_2)$, thus $M_2^0 = \text{erase}(M_2)$.

**Theorem 7.4.5 (local transparency).** Let $M^0 = \text{erase}(M)$. If $M \models M^0[P]$ then $M \models M^0[P] \sim M[P]$.

*Proof.* By assumption, we have $M \models M^0[P]$. We also have $M \models M[P]$ by Theorem 7.4.3. Let $M^0[P] = L_1$ and $M[P] = L_2$. Let $\mathcal{R}$ be the minimum conformance relation which witnesses $M \models L$, i.e. $(L, M) \in \mathcal{R}$. Define $\mathcal{R}'$ as:

$$
\mathcal{R}' = \{(M, L_i, L_j) | (L_i, M) \in \mathcal{R}, (L_j, M) \in \mathcal{R}\}
$$
B.1 Proofs for Local Safety and Transparency

We show $\mathcal{R}'$ is a monitored strong bisimulation for $i, j \in \{1, 2\}, i \neq j$.

1. Suppose $(M, \mathcal{L}_1, \mathcal{L}_2) \in \mathcal{R}'$, i.e. $(M, M^o[P], M[P]) \in \mathcal{R}'$ and $(M^o[P], M) \in \mathcal{R}$ and $(M[P], M) \in \mathcal{R}$.

I. When $\ell$ is an $\tau$ or an output action, we want to prove that $M^o[P] \xrightarrow{\ell} M'^o[P']$ implies $M \xrightarrow{\ell} M'$ and $M[P] \xrightarrow{\ell} M'[P']$. Suppose $M^o[P] \xrightarrow{\ell} M'^o[P']$:

(a) Since $M \models M^o[P]$ is given, $M^o[P] \xrightarrow{\ell} \text{ implies } M \xrightarrow{\ell}$ by Definition 7.4.2. Assume there exists $M'$ such that $M \xrightarrow{\ell} M'$. Also assume that there exists $M'^o$ such that $M^o[P] \xrightarrow{\ell} M'^o[P']$, which implies $M^o \xrightarrow{\ell} M'^o$ and $P \xrightarrow{\ell} P'$ by deduction. Since $M^o = \text{erase}(M)$ is given, by Lemma B.1.5 if $M \xrightarrow{\ell} M'$, we have $M^o = \text{erase}(M) \xrightarrow{\ell} \text{erase}(M')$. Since the labelled transition system of $M^o$ is deterministic, we should have $M'^o = \text{erase}(M') = M'^o$.

(b) With (a) above and Definition 7.2.6 $P \xrightarrow{\ell} P'$ and $M \xrightarrow{\ell} M'$ together induce $M[P] \xrightarrow{\ell} M'[P']$.

(c) By Definition 7.4.2 we have $(M'^o[P'], M') \in \mathcal{R}$ due to $(M^o[P], M) \in \mathcal{R}$, and by Theorem 7.4.3 we have $(M'[P], M') \in \mathcal{R}$, so that we have $(M', M'^o[P'], M'[P']) \in \mathcal{R}'$.

II. When $\ell$ is an input action, suppose $M^o[P] \xrightarrow{\ell} M'^o[P']$ as well as $M \xrightarrow{\ell} M'$:

(a) With Definition B.1.2 $M^o[P] \xrightarrow{\ell} M'^o[P']$ implies $P \xrightarrow{\ell} P'$ and $M^o \xrightarrow{\ell} M'^o$. $P \xrightarrow{\ell} P'$ and $M \xrightarrow{\ell} M'$ together implies $M[P] \xrightarrow{\ell} M'[P']$.

(b) Since $M \models M^o[P]$ is given, with Definition 7.4.2 whenever $M \xrightarrow{\ell} M'$ and $M^o[P] \xrightarrow{\ell} M'^o[P']$, we have $(M'^o[P'], M') \in \mathcal{R}$. Together with $(M'[P'], M') \in \mathcal{R}$ by Theorem 7.4.3 we have $(M', M'^o[P'], M'[P']) \in \mathcal{R}'$.

2. For the symmetric case, suppose $(M, \mathcal{L}_2, \mathcal{L}_1) \in \mathcal{R}'$, i.e. $(M, M[P], M^o[P]) \in \mathcal{R}'$ and $(M[P], M) \in \mathcal{R}$ and $(M^o[P], M) \in \mathcal{R}$.

I. When $\ell$ is an $\tau$ or an output action, we want to prove $M[P] \xrightarrow{\ell} M'[P']$ implies $M \xrightarrow{\ell} M'$ and $M^o[P] \xrightarrow{\ell} M'^o[P']$. Suppose $M[P] \xrightarrow{\ell} M'[P']$:

(a) $M[P] \xrightarrow{\ell} M'[P']$ implies $M \xrightarrow{\ell} M'$ as well as $P \xrightarrow{\ell} P'$.

(b) Since $M^o = \text{erase}(M)$ is given, by Lemma B.1.5 and $M \xrightarrow{\ell} M'$ in (a), we have $M^o \xrightarrow{\ell} M'^o = \text{erase}(M')$. Together with $P \xrightarrow{\ell} P'$ in (a), we have $M^o[P] \xrightarrow{\ell} M'^o[P']$.

(c) Since we have $(M'^o[P'], M') \in \mathcal{R}$ by Definition 7.4.2 and $(M'[P'], M') \in \mathcal{R}$ by Theorem 7.4.3 we have $(M', M'^o[P'], M'[P']) \in \mathcal{R}'$. 

209
II. When $\ell$ is an input action, suppose $M[P] \xrightarrow{\ell} M'[P']$ as well as $M \xrightarrow{\ell} M'$. Note that the former implies $P \xrightarrow{\ell} P'$.

(a) Since $M^o = \text{erase}(M)$ is given, by Lemma 3.1.5, $M \xrightarrow{\ell} M'$ implies $\text{erase}(M) \xrightarrow{\ell} \text{erase}(M')$ and $M^o \xrightarrow{\ell} M'^o$ so that $M'^o = \text{erase}(M')$.

(b) $M^o \xrightarrow{\ell} M'^o$ and $P \xrightarrow{\ell} P'$ imply $M^o[P] \xrightarrow{\ell} M'^o[P']$. Since $(M'^o[P'][M')] \in R$ by Definition 7.4.2, and $(M'[P'], M') \in R$ by Theorem 7.4.3, we have $(M', M'^o[P'], M'^o[P']) \in R'$.

Thus $R'$ is a monitored strong bisimulation. ■

B.2 Proofs for Global Safety

Before proving global safety (Theorem 7.4.16) and global transparency (Theorem 7.4.17), we introduce the following definitions and lemmas.

Define the set of monitored processes similarly as the one for the set of monitors defined in Definition 7.4.10.

**Definition B.2.1 (a set of monitored processes).** Define a set of monitored processes as

\[ \prod_{i \in I} M_i[P_i] = M_1[P_1] \parallel \ldots \parallel M_k[P_k], I = \{1, \ldots, k\} \]

**Definition B.2.2 (action chain).** Globally, for a sequence of actions $\ell_i \cdot \ell_j$, we say that $\ell_i$ and $\ell_j$ are in one action chain if a group of monitored processes $\prod_i M_i[P_i]$ approves $\ell_i \cdot \ell_j$, denoted as

\[ \prod_i M_i[P_i] \xrightarrow{\ell_i \cdot \ell_j} g, \]

then

\[ \prod_i M_i[P_i] \xrightarrow{\ell_i \cdot \ell_j} g \]

which means $\ell_i$ and $\ell_j$ are not permutable.

Actions in one action chain are not permutable, but actions in different action chains are permutable. There could be several action chains in a sequence of actions. We use two examples to illustrate how an action chain works.
Example B.2.3. Assume a sequence of actions is given below

\[ s'[p_1, p_2]!\langle 4 \rangle \cdot \text{join}(s[p_3]) \cdot s'[p_1, p_2]?(4) \cdot s[p_1, p_3]!(\text{hi}) \cdot s[p_1, p_3]?(\text{hi}) \]

actions \text{join}(s[p_3]), s[p_1, p_3]!(\text{hi}) and \( s[p_1, p_3]?(\text{hi}) \) are in one action chain, we mark them as \((\text{join}(s[p_3]))^{c_1}, (s[p_1, p_3]!(\text{hi}))^{c_1} \) and \((s[p_1, p_3]?(\text{hi}))^{c_1}\) to denote that they are in an action chain called \( c_1 \); actions \( s'[p_1, p_2]!\langle 4 \rangle \), \( s'[p_1, p_2]?(4) \) are in another action chain, we mark them as \( (s'[p_1, p_2]!\langle 4 \rangle)^{c_2}, (s'[p_1, p_2]?(4))^{c_2} \) to denote that they are in an action chain called \( c_2 \). The sequence of actions can be permuted as

\[ (\text{join}(s[p_3]))^{c_1} \cdot (s'[p_1, p_2]!\langle 4 \rangle)^{c_2} \cdot (s[p_1, p_3]!(\text{hi}))^{c_1} \cdot (s'[p_1, p_2]?(4))^{c_2} \cdot (s[p_1, p_3]?(\text{hi}))^{c_1} \]

but cannot be permuted as

\[ (s'[p_1, p_2]?(4))^{c_2} \cdot (s'[p_1, p_2]!\langle 4 \rangle)^{c_2} \cdot (s[p_1, p_3]!(\text{hi}))^{c_1} \cdot (\text{join}(s[p_3]))^{c_1} \cdot (s[p_1, p_3]?(\text{hi}))^{c_1} \]

because \( (s'[p_1, p_2]?(4))^{c_2} \) cannot happen before \( (s'[p_1, p_2]!\langle 4 \rangle)^{c_2} \), and \( (s[p_1, p_3]!(\text{hi}))^{c_1} \) cannot happen before \((\text{join}(s[p_3]))^{c_1}\).

In the above example, there are two sessions \( s \) and \( s' \) involved. The following example shows the action chains in one session.

Example B.2.4. Given a sequence of actions

\[ s[p_1, p_2]!\langle 4 \rangle \cdot s[p_1, p_2]?(4) \cdot s[p_1, p_3]!(\text{hi}) \cdot s[p_1, p_3]?(\text{hi}) \]

actions \( s[p_1, p_2]!\langle 4 \rangle \) and \( s[p_1, p_2]?(4) \) are in one action chain, we mark them as \((s[p_1, p_2]!\langle 4 \rangle)^{c_1}, (s[p_1, p_2]?(4))^{c_1}\) to denote that they are in an action chain called \( c_1 \); actions \( s[p_1, p_3]!(\text{hi}) \) and \( s[p_1, p_3]?(\text{hi}) \) are in another action chain, we mark them as \( (s[p_1, p_3]!(\text{hi}))^{c_2}, (s[p_1, p_3]?(\text{hi}))^{c_2} \) to denote that they are in an action chain called \( c_2 \). The sequence of actions can be permuted as

\[ (s[p_1, p_2]!\langle 4 \rangle)^{c_1} \cdot (s[p_1, p_3]!(\text{hi}))^{c_2} \cdot (s[p_1, p_2]?(4))^{c_1} \cdot (s[p_1, p_3]?(\text{hi}))^{c_2} \]

but cannot be permuted as

\[ (s[p_1, p_2]?(4))^{c_1} \cdot (s[p_1, p_3]!(\text{hi}))^{c_2} \cdot (s[p_1, p_3]?(\text{hi}))^{c_2} \cdot (s[p_1, p_2]!\langle 4 \rangle)^{c_1} \]

because \( (s[p_1, p_2]?(4))^{c_1} \) cannot happen before \((s[p_1, p_2]!\langle 4 \rangle)^{c_1}\).
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

Definition B.2.5 (input action chain). An input action chain is a subset of an action chain. We denote an action \( \ell \), which is either \( s[p_1, p_2]^l(v) \), or \( a(s[p]) \), or \( \text{join}(s[p]) \), in an input action chain \( c \) as \((\ell)^{cin}\).

Lemma B.2.6. Let \( N \) be a monitored network and \( \prod_i M_i[P_i] \in N \). Assume an input action chain \( c = (\ell_0)^{cin} \cdot (\ell_1)^{cin} \cdot \ldots \cdot (\ell_n)^{cin} \) is given and

\[
\prod_i M_i[P_i] \xrightarrow{(\ell_0)^{cin}(\ell_1)^{cin} \ldots (\ell_n)^{cin}} g
\]

if

\[
\prod_i M_i[P_i] \xrightarrow{(\ell_0)^{cin}} \prod_i M'_i[P'_i], \quad \text{then} \quad \prod_i M'_i[P'_i] \xrightarrow{(\ell_1)^{cin} \ldots (\ell_n)^{cin}} g.
\]

Proof. Let \( c = (\ell_0)^{cin} \cdot (\ell_1)^{cin} \cdot \ldots \cdot (\ell_n)^{cin} \) be an input action chain.

\[
\prod_i M_i[P_i] \xrightarrow{(\ell_0)^{cin}(\ell_1)^{cin} \ldots (\ell_n)^{cin}} g
\]

means that the pending messages corresponding to \((\ell_0)^{cin} \cdot (\ell_1)^{cin} \ldots (\ell_n)^{cin}\) can be received by the group of monitored processes \( \prod_i M_i[P_i] \):

\[
\prod_i M_i[P_i] \xrightarrow{(\ell_0)^{cin}} \prod_i M'_i[P'_i] \xrightarrow{(\ell_1)^{cin}} \prod_i M''_i[P''_i] \xrightarrow{(\ell_2)^{cin}} \ldots \prod_i M'''_i[P'''_i]
\]

If \( \prod_i M_i[P_i] \xrightarrow{(\ell_0)^{cin}} \prod_i M'_i[P'_i], \) the input action chain becomes \( c' = (\ell_1)^{cin} \ldots (\ell_n)^{cin}\), where \((\ell_0)^{cin}\) is received, and \((\ell_1)^{cin}\) becomes the first action in \( c' \):

\[
\prod_i M'_i[P'_i] \xrightarrow{(\ell_1)^{cin}} \prod_i M''_i[P''_i] \xrightarrow{(\ell_2)^{cin}} \ldots \prod_i M'''_i[P'''_i]
\]

Thus \( \prod_i M'_i[P'_i] \xrightarrow{(\ell_1)^{cin} \ldots (\ell_n)^{cin}} g \). ■

Lemma 7.4.7 (receivability). Let \( N \) be a monitored network and \( \ell \) be an input action. If \( N \) is receivable and \( N \xrightarrow{\ell} N' \), then \( N' \) is receivable.

Proof. Assume \( \{M_i[P_i]\}_{i \in I} \in N \). That \( N \) is receivable means every pending message floating in the global queue can be absorbed by some monitored process in \( N \). Thus, as \( N \) is receivable, there exists a sequence of actions, say \( \tilde{\ell} \), consisting of \text{join} and those
input actions corresponding to \textit{all} pending messages in the network \(N\), such that
\[
\prod_i M_i[P_i] \xrightarrow{\ell_k} \prod_i M'_i[P'_i],
\]
all the messages are absorbed by some processes in \(\prod_i M_i[P_i]\). Assume the corresponding set of \textit{input action chains} of \(\ell\) is \(\{c_{inj}\}_{j \in J}\), which means that the actions in \(\ell\) can be partitioned into several input action chains. We mark each action \(\ell \in \ell\) as \((\ell)_{c_{inj}}\) to denote that action \(\ell\) belongs to input action chain \(c_{inj}\).

We rewrite the sequence of actions in \(B.2\) as
\[
\ell \equiv (\ell^0)_{c_{inj}} \ldots (\ell^j)_{c_{inj}} \ldots (\ell^N)_{c_{inj}}
\]
by marking each action and collecting actions belonging to the same input action chain together, where \((\ell^j)_{c_{inj}} = (\ell^j_0)^{c_{inj}} \cdots (\ell^j_m)^{c_{inj}}\).

If
\[
\prod_i M_i[P_i] \xrightarrow{\ell_k} \prod_i M'_i[P'_i] \in N',
\]
there exists an input action chain \(c_{ink}\) such that \(\ell \in (\ell^0)^{c_{inj}} = (\ell^0_0)^{c_{ink}} (\ell^0_1)^{c_{ink}} \cdots (\ell^0_m)^{c_{ink}}\); we thus mark \(\ell\) as \((\ell)^{c_{ink}}\). By Definition \(B.2.5\) no action in the action chain is permutable, action \((\ell)^{c_{ink}}\) should be the first action in chain \(c_{ink}\), thus \((\ell)^{c_{ink}} = (\ell^0)^{c_{ink}}\).

By \(B.2\), that action \((\ell^0)^{c_{ink}}\) is removed from \((\ell^0)^{c_{inj}} \ldots (\ell^j)^{c_{inj}} \ldots (\ell^N)^{c_{inj}}\) in \(B.2\), which becomes \((\ell^0)^{c_{inj}} \ldots (\ell^j)^{c_{inj}} \ldots (\ell^N)^{c_{inj}}\). Note that \((\ell)^{c_{ink'}} \equiv (\ell^0_1)^{c_{ink}} (\ell^0_2)^{c_{ink}} \cdots (\ell^0_m)^{c_{ink}}\).

By Lemma \(B.2.6\)
\[
\prod_i M'_i[P'_i] \xrightarrow{(\ell^0)^{c_{inj}} \ldots (\ell^j)^{c_{inj}} \ldots (\ell^N)^{c_{inj}}} g.
\]

By Definition \(7.4.6\) \(N'\) is receivable. \(\blacksquare\)

The definitions of consisteny of group of monitors and monitored network coherence are reminded below:

**Definition 7.4.12** (consistency of a group of monitors). Let \(M\) be a group of monitors, and \(s[p]^0\) stand for either \(s[p]\) or \(s[p]^*\). Let \(\forall M_i \in M, M_i = \Gamma_i, \Delta_i\). If all of the following conditions hold,
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

1. (a) \( \forall M_i \in M \), if \( a : \text{im}(G[p]) \in M_i \), then there is no other \( a : I(G[p]) \in M_j \) or \( a : I0(G[p]) \in M_j, M_j \in M \).

(b) \( \forall M_i \in M \), if \( \forall s, s[p]\triangleright : T \in M_i \), then \( s[p]\triangleright \notin M_j, j \neq i, M_j \in M \).

2. If \( a : 0(G[p]) \in M_i \), then there exists \( M_j \) such that \( a : \text{im}(G[p]) \in M_j \).

3. Assume \( p_1 \neq p_2 \). As \( \Delta_i(s[p_1]\triangleright) = T \) and

\[ p_2 \{ l_k(x_k : S_k) \langle A_k \rangle.G_k \mid p_2 \}_k \subseteq T, \]

there exists \( j \) such that \( \Delta_j(s[p_2]\triangleright) = T' \) and

\[ p_j \{ l_k(x_k : S_k) \langle A'_k \rangle.G_k \mid p_1 \}_k \subseteq T' \]

with \( A_k \{ v/x \} \downarrow \text{true} \) iff \( A'_k \{ v/x \} \downarrow \text{true} \).

4. \( \bigcup_i \Delta_i = \bigcup_{1 \leq j \leq n} \{ s_j[p_j1] : T_j1, \ldots, s_j[p_jk] : T_jk, \ldots, s_j[p_jm_j] : T_jm_j \} \) where, for each \( s_j \), there is \( G_j \) such that \( G_j \mid p_j = T_jk \) for \( 1 \leq k \leq m_j \).

Then the group of monitors, \( M_i \), is consistent.

**Definition 7.4.13 (monitored network coherence).** \( N \) is coherent if all of its pending messages are receivable up to permutation of actions \( \curvearrowright \) and, after these messages have been received, the resulting group of monitors which guard all local process in \( N \), say \( M_i \), is consistent.

Before proving the theorem of global safety, we use the following lemma to show that as a network is coherent and an output action is ready to fire, then its corresponding input is ready for it.

**Lemma B.2.7.** Assume network \( N \) is coherent with its consistent group of monitors, say \( \prod_i M_i \), where \( M_i = \Gamma_i, \Delta_i, \) and \( \exists M_s \in \prod_i M_i \) such that \( \Delta_s(s[p]^{\bullet}) \bowtie q!\{ l_k(x_k : S_k) \langle A_k \rangle.T_k \}_k \subseteq I \), then \( \exists M_r \in \prod_i M_i \) such that \( \Delta_r(s[q]^{\bullet}) \bowtie p!\{ l_k(x_k : S_k) \langle A'_k \rangle.T'_k \}_k \subseteq I \) with \( A_k \{ v/x \} \downarrow \text{true} \) iff \( A'_k \{ v/x \} \downarrow \text{true} \).

**Proof.** We prove it by contradiction. Since \( \Delta_s(s[p]^{\bullet}) \bowtie q!\{ l_k(x_k : S_k) \langle A_k \rangle.T_k \}_k \subseteq I \), we have \( q!\{ l_k(x_k : S_k) \langle A_k \rangle.T_k \}_k \subseteq \Delta_s(s[p]^{\bullet}) \). And since \( N \) is coherent, there exists
some monitor, say $M_r \in \prod_i M_i$, such that $p^i \{ l_k(x_k : S_k) \langle \langle \mathcal{A}_k \rangle \rangle . T_k^m \}_{k \in I} \subseteq \Delta_r(s[q]^*)$ by rule 3. in Definition 7.4.12. If
\[ \Delta_r(s[q]^*) \not\in p^i \{ l_k(x_k : S_k) \langle \langle \mathcal{A}_k \rangle \rangle . T_k^m \}_{k \in I} \]
(note that $T_k'$ and $T_k^m$) based on Definition 6.6.8, it must be an action with the same subject suppressing the permutation:

- **Case (a)** $\Delta_r(s[q]^*) \not\in p^i \{ l'_j(x'_j : S'_j) \langle \langle \mathcal{B}_j \rangle \rangle . T_k^m \}_{j \in J}$, or

- **Case (b)** $\Delta_r(s[q]^*) \not\in p^i \{ l'_j(x'_j : S'_j) \langle \langle \mathcal{B}_j \rangle \rangle . T_k^m \}_{j \in J}$

Case (a) implies that, for specification $\Delta_s(s[p]^*)$, there is another action $q!$ positioning before $q^i$ such that
\[ \Delta_s(s[p]^*) \not\in q^i \{ l'_j(x'_j : S'_j) \langle \langle \mathcal{B}_j \rangle \rangle . T_k^m \}_{j \in J} \]

Similarly, case (b) implies that, for specification $\Delta_s(s[p]^*)$, there is an action $q?$ positioning before $q^i$ such that
\[ \Delta_s(s[p]^*) \not\in q^i \{ l'_j(x'_j : S'_j) \langle \langle \mathcal{B}_j \rangle \rangle . T_k^m \}_{j \in J} \]

Both cases lead to $\Delta_s(s[p]^*) \not\in q^i \{ l_k(x_k : S_k) \langle \langle \mathcal{A}_k \rangle \rangle . T_k \}_{k \in I}$. Therefore, by contradiction, we prove the statement is true.

**Lemma B.2.8.** Let $s[p]^\circ$ stand for either $s[p]$ or $s[p]^*$. Assume $\forall M_i \in N, \forall s, s[p]^\circ : T \in M_i$ implies $s[p]^\circ \not\in M_j$, $j \neq i, M_j \in N$. If $N \xrightarrow{\ell} N'$ and rule 1.(a) in Definition 7.4.12 holds for $N$ and $N'$, we have $\forall M'_k \in N', \forall s, s[p]^\circ : T \in M'_k$ implies $s[p]^\circ \not\in M'_j$, $j \neq k, M'_j \in N$.

**Proof.** As explained in Lemma 7.4.15 as rule 1.(a) in Definition 7.4.12 holds, $a : \mathsf{im}(G[p])$ is unique to the network. Only three rules, $[\mathsf{req-n}]$ and $[\mathsf{acc-b/f}]$, may affect the uniqueness of $s[p]^\circ : T$ as $N \xrightarrow{\ell} N'$. When $\ell = \pi(s[p_j] : G)$, there exists $M_s \in N$ such that $M_s \xrightarrow{\pi(s[p_j] : G)} M'_j$ implying $s$ is new to $M_s$ and $\{ s[p_k] : G \mid p_k \}_{k \in \Gamma \setminus \{ j \} } \subseteq M'_s$, where each $s[p_k] : G \mid p_k$ only exists in $M'_s$ because $s$ is unique to the network (by Lemma 7.4.15), and every role defined in a global specification is unique (Definition 6.2.3); while $s[p_j] : G \mid p_j$, which is sent as an invitation to the endpoint having $a : \mathsf{im}(G[p_j])$, say it is the endpoint guarded by monitor $M_r$. As $M_r$ accepts this invitation by approving action $a(s[p_j] : G)$ or $a(s[p_j] : G')$, $s[p_j] : G \mid p_j$ is added into $M_r$, and it only exists in $M_r$ network-wise because $a : \mathsf{im}(G[p_j])$ only exists in $M_r$: Only a monitor having
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

\[ a : \text{im}(G[p_j]) \] can accept the capability of \( s[p_j] : G \mid p_j \). With the same reasoning, when \( \ell = a(s[p_j] : G) \) or \( \ell = a(s[p_j] : G) \) is approved by some monitor, say \( M_k \), then \( s[p_j] : G \mid p_j \in M_k \), \( s[p_j] : G \mid p_j \) only exists in \( M_k \) because only a monitor having \( a : \text{im}(G[p_j]) \) can accept the capability of \( s[p_j] : G \mid p_j \). In conclusion, no action affects the uniqueness of \( s[p] : T \) to the network as \( N \overset{\ell}{\rightarrow} N' \), thus \( N' \) holds the statement. 

**Theorem 7.4.16 (global safety).** Let \( N \) be coherent. Then \( N \overset{\ell}{\rightarrow} N' \) implies \( N' \) is coherent.

*Proof.* Assume \( N \) is coherent so that the group of monitors, say \( M \), guarding every local process in \( N \) is consistent. Assume \( \prod_i M_i[P_i] \in N \), where \( \prod_i M_i[P_i] \) is the composition of monitored processes in \( N \). Let \( M_i = \Gamma_i, \Delta_i \) and \( \text{im} \in \{1, 10\} \). For convenience, we use \( \prod_i M_i \) to denote the group of monitors corresponding to the group of monitored processes \( \prod_i M_i[P_i] \), and use \( + \) to denote adding (or having) elements in \( \Gamma_i \) or \( \Delta_i \). Note that, by Lemma 7.4.7 if \( N \) is receivable and \( N \overset{\ell}{\rightarrow} N' \) where \( \ell \) is an input, then \( N' \) is receivable. Also note that, by Lemma B.2.8 rule 1.(b) of Definition 7.4.12 is always true when \( N \) is consistent and \( N \overset{\ell}{\rightarrow} N' \) for any \( \ell \), thus we only need to prove rule 1.(a).

If \( N \overset{\ell}{\rightarrow} N' \), we want to prove the following cases of actions still make the resulting group of monitors in \( N' \) consistent. Note that the rules 1.(a), 2., 3., and 4. are referring to the rules defined in Definition 7.4.12.

**case (shared name) -** If \( \ell \) is new \( a : \text{im}(T[p]) \), then rules 2., 3. and 4. of the consistency of group of monitors guarding all local processes in \( N \) are not affected. We analyse the effects for rule 1.(a). There is some \( M_j[P] \in \prod_i M_i[P_i] \) and \( M_j[P] \overset{\text{new } a : \text{im}(G[p])}{\rightarrow} M'_j[P'] \) such that \( N \overset{\text{new } a : \text{im}(G[p])}{\rightarrow} N' \); it implies that, when \( \text{im} = I \), there is no \( a : I(G[p]) \) nor \( a : \text{IO}(G[p]) \) in \( M_j \) so that \( M_j \) allows this action; similarly, when \( \text{im} = 10 \), there is no \( a : I(G[p]) \) nor \( a : \text{IO}(G[p]) \) in \( M_j \). Therefore, for \( \Gamma_j \in M_j \) and \( \Gamma'_j \in M'_j \), \( \Gamma'_j \) is the configuration resulting from \( \Gamma_j + a : \text{im}(G[p]) \), which induces \( \Gamma'_j = \Gamma_j, a : \text{im}(G[p]) \), \( a : \text{im}(G[p]) \notin \Gamma_j \). Thus rule 1.(a) is satisfied.

**case (bound request) -** If \( \ell \) is \( \pi(s[p_k] : G) \), there is some \( M_j[P_j] \in \prod_i M_i[P_i] \) and \( M_j[P_j] \overset{\pi(s[p_k] : G)}{\rightarrow} M'_j[P'_j] \) such that \( N \overset{\pi(s[p_k] : G)}{\rightarrow} N' = (\nu s)(N_1 \parallel H \cdot \pi(s[p] : G)) \). This action combines two parts: creating a fresh session and requesting through sending an invitation. As for the part of newing a session, as a session is newed, \( \{s[p_i] : G \mid p_i \in \Gamma \cup \{k\} \} \) are added into \( \Delta_j \), which becomes \( \Delta'_j = \Delta_j + \{s[p_i] : G \mid p_i \} \). No other \( \Delta_i, i \neq j \) is affected by newing a session, thus rules 1.(a), 2., and 3. are hold for newing a session. For rule 4., since \( N \) is coherent and \( G \) is approved by monitor \( M_j \),
B.2 Proofs for Global Safety

\(G\) is well-formed, thus the group of monitors guarding all local processes in \(N'\) satisfies rule 4. immediately.

As for the part of requesting an invitation to endpoint \(a\), the reasoning is as same as that for case (free request) below.

case (free request) - If \(\ell\) is \(\bar{a}(s[p] : G)\), for receivability, there is some \(M_s[P_s] \in \prod_s M_s[P_s]\) and \(M_s[P_s] \xrightarrow{\bar{a}(s[p] : G)} M'_s[P'_s]\) such that \(N_1 \parallel H \equiv N \xrightarrow{\bar{a}(s[p] : G)} \gamma N' \parallel H \cdot \bar{a}(s[p] : G)\); it implies that, there exists \(M_s \in N\), in which it has \(\Gamma_s(a) = \emptyset(G[p])\). Since \(N\) is coherent, according to rule 2, there must exist some \(M_r, M_r[P_r] \in N\) such that it has \(\Gamma_r(a) = \text{im}(G[p])\), implying \(M_r[P_r]\) is able to receive invitation \(\bar{a}(s[p] : G)\). Since action \(\bar{a}(s[p] : G)\) does not affect the existence of \(a : \text{im}(G[p]) \in \Gamma_r\), \(a : \text{im}(G[p])\) still exists in the resulting network \(N' \equiv N'_1 \parallel H \cdot \bar{a}(s[p] : G)\). Thus \(N'\) is able to receive the additional message \(\bar{a}(s[p] : G)\), and messages \(H \cdot \bar{a}(s[p] : G)\) are receivable to \(N'\).

Below we discuss if \(N'\) satisfies rules 1.(a), 2., 3. and 4. after receiving \(\bar{a}(s[p] : G)\).

\(N \xrightarrow{\bar{a}(s[p] : G)} \gamma N'\) and \(N'\) is receivable, by rules [MG-REQ-F-OUT] and [MG-ACC-B/F-IN], together imply \(\exists M_s[P_s], M_r[P_r] \in N\) such that

\[N = N_0 \parallel M_s[P_s] \parallel M_r[P_r] \parallel H \xrightarrow{\bar{a}(s[p] : G)} N_0 \parallel M'_s[P'_s] \parallel M_r[P_r] \parallel H \cdot \bar{a}(s[p] : G) = N'\]

where \(a : \emptyset(G[p]) \in \Gamma_s\), and

\[N' = N_0 \parallel M'_s[P'_s] \parallel M_r[P_r] \parallel H \cdot \bar{a}(s[p] : G) \xrightarrow{\gamma} N_0 \parallel M'_s[P'_s] \parallel M'_r[P'_r] \parallel H\]

\(\ell'\) is \(a(s[p] : G)\) or \(a(s[p] : G)\), where \(a : \text{im}(G[p]) \in \Gamma_r\). The invitation \(\bar{a}(s[p] : G)\) in \(H \cdot \bar{a}(s[p] : G)\) can be absorbed to the receiver when its monitor approves it. By rules [REQ-F] and [ACC-B/F], no \(a\) is added into / deleted from \(\Gamma_s\) or \(\Gamma_r\), and \(a : \emptyset(G[p]) \in \Gamma_s\) and \(a : \text{im}(G[p]) \in \Gamma_r\) are respectively still in \(\Gamma_s\) and \(\Gamma_r\), and their configurations do not change, thus hold rules 1.(a) and 2.

Let \(\dagger \in \{!, ?\}\) and when \(\dagger = ?\), let \(\dagger = !\); when \(\dagger = !\), let \(\dagger = ?\). Assume in \(M_s\), \(\Delta_s(s[p]^0) = T \bowtie q \{l_k(x_k : S_k) \langle A_k \rangle G_k \downarrow p\}_{k \in I}\). Since \(N\) is coherent, by Lemma B.2.7 there exists \(M_m[P_m]\) who has \(\Delta_m(s[q]^0) \bowtie \overline{p} \{l_k(x_k : S_k) \langle A_k \rangle G_k \downarrow q\}_{k \in I}\) with \(\forall v, \exists k \in I, A_k \{v/x_k\} \downarrow \text{true}\) iff \(A'_k \{v/x_k\} \downarrow \text{true}\).

1. For rule 3., since \(N\) is coherent, \(s[p]^0\) only exists in \(\Delta_s\). When \(s[p]^0\) is removed from \(\Delta_s\) and added into \(\Delta_r\), by Lemma B.2.8 \(s[p]^0\) is still unique in \(N'\) and only exists in \(\Delta_r\). Moreover, there still exists \(M_m[P_m]\) whose \(\Delta_m(s[q]^0) \bowtie \overline{p} \{l_k(x_k : S_k) \langle A_k \rangle G_k \downarrow q\}_{k \in I}\) being ready for the counter action action going to/coming from
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

$s[p]^\circ$.

2. For rule 4., since $N$ is coherent, $s[p]^\circ = G \uparrow p$, which still holds when $s[p]^\circ$ is removed from $\Delta_s$ and added into $\Delta_r$ by rules $\text{[req-f]}$ and $\text{[acc-b/f]}$. Thus the resulting monitors still satisfy rule 4.

case (output) - if $\ell$ is an output action $s[p_1,p_2]l(v)$, assume $N$ approves this action:

$$N \equiv N_1 \parallel H \overset{s[p_1,p_2]l(v)}{\gamma_g} N_1' \parallel H \cdot s[p_1,p_2,l(v)] \equiv N',$$

(B.3)

where $H$ can be empty. Equation (B.3) infers that $\langle p_1,p_2,l(v) \rangle$ is the only additional pending message to the original network $N$.

In the follows, we first prove that $H \cdot s[p_1,p_2,l(v)]$ is receivable to $N'$. Equation (B.3) indicates that $\exists M_s \in N$, $\Delta_s(s[p_1]^\ast) \sim p_2\{l_k(x_k : S_k)\langle A_k\rangle.T_k\}_{k \in I}$ approves action $\ell = s[p_1,p_2]l(v)$, and, due to coherence and Lemma B.2.7 implies $\exists M_r \in N$ such that $\Delta_r(s[p_2]^\ast) \sim p_1\{l_k(x_k : S_k)\langle A'_k\rangle.T'_k\}_{k \in I} \parallel \forall v, \exists k \in I, A_k\{v/x_k\} \downarrow \text{true}$ if $A'_k\{v/x_k\} \downarrow \text{true}$. Assume $\prod_i M_i$ is the group of monitors of monitored processes $\prod_i M_i[P_i] \in N$, which approves to receive all pending messages in $H$.

1. If $M_s \notin \prod_i M_i$, any monitor in $\prod_i M_i$ remains the same after $\ell$ happens. For the messages in $H$, they are receivable to $N'$ (according to $\prod_i M_i$). As for message $s\langle p_1,p_2,l(v)\rangle$, since action $s[p_1,p_2]l(v)$ can fire in $N$:

   (a) If $M_r = M_s$, since action $s[p_1,p_2]l(v)$ does not affect the configuration of $\Delta_s(s[p_2]^\ast) = \Delta_r(s[p_2]^\ast)$, $s\langle p_1,p_2,l(v)\rangle$ is receivable according to $M_r$.

   (b) If $M_r \in \prod_i M_i$, by Lemma B.2.7 the receiving action $p_1$ in $\Delta_r(s[p_2]^\ast)$ is permutable to other receiving actions corresponding to messages in $H$, so that $M_r$ can receive messages in $H$ and $s\langle p_1,p_2,l(v)\rangle$ in any order.

   (c) If $M_r \notin (\prod_i M_i \cup M_s)$, then it is trivial that $s\langle p_1,p_2,l(v)\rangle$ is receivable to $M_r$.

2. If $M_s \in \prod_i M_i$, let $N \equiv N_0 \parallel \prod_i M_i[P_i] \parallel H$, $N \overset{s[p_1,p_2]l(v)}{\gamma_g} N_0 \parallel \prod_{i \neq s} M_i[P_i] \parallel M'_s[P'_s] \parallel H \cdot s\langle p_1,p_2,l(v)\rangle$. As for those in $H$ receivable to $\prod_{i \neq s} M_i$, straightforwardly, they are still receivable to $\prod_{i \neq s} M_i$ after action $s[p_1,p_2]l(v)$ fires. As for those in $H$ receivable to $M_s$ but not received at $\Delta_s(s[p_1]^\ast)$, because action $s[p_1,p_2]l(v)$ has no effect at the configurations of other session-roles, they are still receivable to $M_s$ at other session-roles. As for those in $H$ but receivable at $\Delta_s(s[p_1]^\ast)$, the messages should be in the form: $s\langle p,p_1,l'(v')\rangle$. Since
B.2 Proofs for Global Safety

\[ \Delta_s(s[p_1]) \sim p_2!\{l_k(x_k : S_k)\langle A_k \rangle.T_k\}_{k \in I}, \] by Definition 6.6.8, the configuration of \( \Delta_s(s[p_1]) \) should be

\[ \Delta_s(s[p_1]) \sim p_2!\{l_k(x_k : S_k)\langle A_k \rangle.p?\{l'_j(x'_j : S'_j)\langle B_j \rangle.T'_j\}_{j \in I}\}_{k \in I} \]

which shows that those messages are still receivable at \( \Delta_s(s[p_1]) \) after action \( s[p_1,p_2]!l(v) \) fires. As for message \( s(p_1,p_2,l(v)) \), the reasonings are as same as those above.

Thus the messages in \( H \cdot s(p_1,p_2,l(v)) \) are receivable to network \( N' \).

Then we show that, after receiving all messages in \( H \cdot s(p_1,p_2,l(v)) \), the resulting monitors in \( N' \) are consistent. Since rules of 1.(a) and 2. for the consistency of monitors (see Definition 7.4.12) are not affected by action \( s[p_1,p_2]!l(v) \), only rules 3. and 4. need discussions. With the analyses above, since \( N \) is consistent, \( \exists M_s,M_r \in N, \exists G \) is well-formed and \( G = p_1 \rightarrow p_2 : \{l_k(x_k : S_k)\langle A_k \rangle.G_k\}_{k \in I} \) such that

\[ \Delta_s(s[p_1]) \sim G \mid p_1 \]
\[ \Delta_r(s[p_2]) \sim G \mid p_2 \]

with \( \forall v, \exists k \in I, A_k\{v/x_k\} \downarrow \text{true} \) iff \( A'_k\{v/x'_k\} \downarrow \text{true} \). Assume \( l = l_0 \).

1. If \( M_s,M_r \not\in \prod_i M_i \), after receiving all messages in \( H \cdot s(p_1,p_2,l_0(v)) \), we have

\[ \Delta_s(s[p_1]) \sim G_0 \mid p_1 \]
\[ \Delta_r(s[p_2]) \sim G_0 \mid p_2 \]

2. If \( M_s \in \prod_i M_i \), i.e. \( M_s \) approves receiving some messages in \( H \), assume there is a message \( s(p_1,l'_n(v')) \in H \), then \( \exists M_r \in N' \) and \( \exists G \) is well-formed and

\[ G = p_1 \rightarrow p_2 : \{l_k(x_k : S_k)\langle A_k \rangle.G_k\}_{k \in I} \]
\[ = p_1 \rightarrow p_2 : \{l_k(x_k : S_k)\langle A_k \rangle.p \rightarrow p_1 : \{l'_j(x'_j : S'_j)\langle B_j \rangle.G'_{kj}\}_{j \in I}\}_{k \in I} \]

such that

\[ \Delta_s(s[p_1]) \sim G \mid p_1 = p_2!\{l_k(x_k : S_k)\langle A_k \rangle.p?\{l'_j(x'_j : S'_j)\langle B_j \rangle.G'_{kj}\}_{j \in I}p_1\}_{j \in I}\}_{k \in I} \]
\[ \Delta_r(s[p_2]) \sim G \mid p_2 = p_2?\{l_k(x_k : S_k)\langle A_k \rangle.G'_{km}\mid p_2\}_{k \in I} \]

where \( G'_{km} \mid p_2 = (p \rightarrow p_1 : \{l'_j(x'_j : S'_j)\langle B_j \rangle.G'_{kj}\}_{j \in I}) \mid p_2 \). After \( p_2 \) fires for
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

receiving \( s(p, p_1, l''_n(v')) \in H \), we have

\[
G \xrightarrow{s[p, p_1]l''_n(v')} G' = p_1 \rightarrow p_2 : \{ l_k(x_k : S_k) \langle A_k \rangle. G'_i \}_{k \in I}
\]

and

\[
\Delta_s(s[p_1]) \sim p_2! \{ l_k(x_k : S_k) \langle A_k \rangle. G'_i \mid p_1 \}_{k \in I}
\]

since \( G \) is well-formed, \( G'_i \) is well-formed. Note that \( G'_i \), \( n \) is a constant, only \( k \) is a variable, thus \( G'_i \) can be viewed as \( G''_k \). Also note that, \( G'_i \mid p_2 = G''_k \mid p_2 \) because, after receiving all messages in \( H \), the monitors in \( N \) are consistent (by Definition 7.4.12), there exists a global specification, i.e. \( G' \), such that

\[
\Delta_s(s[p_1]) \sim G' \mid p_1 = p_2! \{ l_k(x_k : S_k) \langle A_k \rangle. G'_i \mid p_1 \}_{k \in I}
\]

If there are other messages in \( H \) which can be received at \( \Delta_s(s[p_1]) \), then permute every such input action, say \( s[p', p_1]!l''_m(v) \), until it positions after action \( p_2! \) such that

\[
G \sim p_1 \rightarrow p_2 : \{ l_k(x_k : S_k) \langle A_k \rangle. p' \rightarrow p_1 : \{ l''_m(x''_j : S''_i) \langle B' \rangle. G''_i \}_{k \in I} \}_{k \in I}
\]

\[
\Delta_s(s[p_1]) \sim p_2! \{ l_k(x_k : S_k) \langle A_k \rangle. p'' \{ l''_m(x''_j : S''_i) \langle B'' \rangle. G''_i \mid p_1 \}_{k \in I} \}_{k \in I}
\]

\[
\Delta_r(s[p_2]) \sim p_1? \{ l_k(x_k : S_k) \langle A_k \rangle. G''_i \mid p_2 \}_{k \in I}
\]

after input \( s[p', p_1]!l''_m(v) \) takes place at \( \Delta_s(s[p_1]) \), we have

\[
\Delta_s(s[p_1]) \sim p_2! \{ l_k(x_k : S_k) \langle A_k \rangle. G''_i \mid p_1 \}_{k \in I}.
\]

note that, again, \( G''_i \mid p_2 = G''_k \mid p_2 \) with the same reasonings above. For every input action positioning after \( p_2! \) at \( \Delta_s(s[p_1]) \), we have a general result such that there exist \( M_s \) and \( M_r \) approving action \( s[p_1, p_2]!l(v) \) to fire and to receive the generated message, and, after receiving messages in \( H \), the resulting configurations of \( \Delta_s(s[p_1]) \) and \( \Delta_r(s[p_2]) \) should be projected from the same global specification.

3. If \( M_r \in \prod_i M_i \), \( \exists G \) is well-formed and

\[
G \sim p \rightarrow p_2 : \{ l''_j(x''_j : S''_i) \langle B_j \rangle. p_1 \rightarrow p_2 : \{ l_k(x_k : S_k) \langle A_k \rangle. G''_i \}_{k \in I} \}_{j \in I}
\]
such that

$$\Delta_r(s[p_2] \cdot) \cap G \upharpoonright p_2 = p?\{l_j'(x_j' : S_j')\langle B_j'\rangle, p_1?\{l_k(x_k : S_k)\langle A_k'\rangle.G_{kj}' \upharpoonright p_2\}k \in I\}.\tag{B.2}$$

When messages in $H$ have been received, action $s[p, p_2]?l_n'(v)$ has happened, we have

$$G \xrightarrow{s[p, p_2]?l_n'(v)} G' = p_1 \rightarrow p_2 : \{l_k(x_k : S_k)\langle A_k\rangle.G_k' \upharpoonright p_2\}k \in I$$

such that

$$\Delta_r(s[p_2] \cdot) \cap G' \upharpoonright p_2 = p_1?\{l_k(x_k : S_k)\langle A_k\rangle.G_{kn}' \upharpoonright p_2\}k \in I$$

and since, after receiving messages in $H$, the monitors in $N$ are consistent, we have

$$\Delta_s(s[p_1] \cdot) \cap G' \upharpoonright p_1 = p_2!\{l_k(x_k : S_k)\langle A_k\rangle.G_k' \upharpoonright p_1\}k \in I$$

where $n$ is a constant.

On the above, we show that, after receiving all messages in $H$, the configurations at $\Delta_s(s[p_1] \cdot)$ and $\Delta_r(s[p_2] \cdot)$ in any case are in the form

$$\Delta_s(s[p_1] \cdot) \cap p_2!\{l_k(x_k : S_k)\langle A_k\rangle.G_k''' \upharpoonright p_1\}k \in I$$

$$\Delta_r(s[p_2] \cdot) \cap p_1?\{l_k(x_k : S_k)\langle A_k\rangle.G_k''' \upharpoonright p_2\}k \in I\tag{B.4}$$

which imply, whenever action $s[p_1, p_2]!l\langle v \rangle$ then action $s[p_1, p_2]?l\langle v \rangle$ happen, i.e. when messages in $H \cdot s(p_1, p_2, l\langle v \rangle)$ are received, there exist $G_k'''$ satisfying rule 4. of Definition 7.4.12. As for rule 3. of consistency of resulting monitors, since Equation B.4 is consistent, according to rule 3. of Definition 7.4.12 if there is an output in $G_k''' \upharpoonright p_2$ or in $G_k'' \upharpoonright p_1$ for $k \in I$, there exists a corresponding input in other monitors, such that when actions $s[p_1, p_2]!l\langle v \rangle$ and $s[p_1, p_2]?l\langle v \rangle$ fire, the left monitors are still consistent. Thus $N'$ is coherent.

**case (input)** - if $\ell$ is $s[p_1, p_2]?l\langle v \rangle$, since $N$ is receivable, by Lemma 7.4.7, $N'$ is receivable. For an input action $s[p_1, p_2]?l\langle v \rangle$, only when $v$ is a shared name, say $a$, will affect rules 1. and 2. Since a received name is always typed with output mode, rule 1.(a) holds. Since $N$ is coherent, when the process who sends $a$ has an output mode $a$, say $a : 0(G[p])$, there exists an input mode $a$, say $a : \text{im}(G[p])$ in some other monitor; when the process who sends $a$ has an input mode $a$, say $a : \text{im}(G[p])$, the sender itself has $a$ with input mode. For both cases, rule 2. holds as long as typing the received
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

name with output mode. For rules 3. and 4. of Definition 7.4.12 the discussions are as follows.

Suppose \( \ell \) is \( s[p_1, p_2]?l(v) \), where \( v \) is either a value or a name, and \( N \) is coherent, when \( N \xrightarrow{\ell} N' \):

1. If there is no pending message in \( N' \), \( N' \) is coherent because \( N \) is coherent and after \( N \) receives \( s(p_1, p_2, l(v)) \) by \( \ell \), it is still coherent, which is \( N' \).

2. If there are pending messages in \( N' \), by Lemma of receivability, \( N' \) is receivable. Let 
\[
N = \prod_{i \neq r} \mathcal{M}_i[P_i] \parallel \mathcal{M}_r[P_r] \parallel H \cdot s(p_1, p_2, l(v)),
\]
where \( \mathcal{M}_r[P_r] \) will receive message \( s(p_1, p_2, l(v)) \).

(a) If all messages in \( H \) are received by the monitored processes in \( \prod_{i \neq r} \mathcal{M}_i[P_i] \) and \( \mathcal{M}_r[P_r] \), then \( N' = \prod_{i \neq r} \mathcal{M}_i[P_i] \parallel \mathcal{M}_r'[P_r'] \parallel H \). The coherence of \( N \) means that, after receiving all messages of \( H \cdot s(p_1, p_2, l(v)) \), the network becomes \( \prod_{i \neq r} \mathcal{M}_i'[P_i'] \parallel \mathcal{M}_r'[P_r'] \parallel \emptyset \), where the group of monitors is consistent; since, after \( N' \) receives all messages in \( H \), the network also becomes \( \prod_{i \neq r} \mathcal{M}_i'[P_i'] \parallel \mathcal{M}_r'[P_r'] \parallel \emptyset \), where the group of monitors is thus consistent, so that \( N' \) is coherent.

(b) If some messages in \( H \) are received by \( \prod_{i \neq r} \mathcal{M}_i[P_i] \) and some are received by \( \mathcal{M}_r'[P_r'] \):

i. The configuration at \( \Delta_r(s[p_2]^\bullet) \) before action \( s[p_1, p_2]?l(v) \) should be in the following form:

\[
\Delta_r(s[p_2]^\bullet) \rightarrow p_1?\{l_k(x_k : S_k)\langle A_k' \rangle\},
\]

\[
p_2?\{l_j(x_j' : S_j')\langle B_j' \rangle\},
\]

\[
p_2'?\{l_i'^i(x_i'^i : S_i'^i)\langle B_i'^i \rangle \ldots \}_{i \in I,j \in I}k \in I
\]

Assume after \( \mathcal{M}_r[P_r] \) receives messages inputting to it through 
\[
\mathcal{M}_r[P_r] \xrightarrow{\ell} \mathcal{M}_r'[P_r'] \xrightarrow{\ell_0 \ldots \ell_m} \mathcal{M}_r''[P_r''],
\]
it becomes \( \mathcal{M}_r''[P_r''] \). The coherence of \( N \) means that, after receiving all messages of \( H \cdot s(p_1, p_2, l(v)) \), the network becomes \( \prod_{i \neq r} \mathcal{M}_i''[P_i''] \parallel \mathcal{M}_r''[P_r''] \parallel \emptyset \), where the group of monitors is consistent. Since we have \( N' = \prod_{i \neq r} \mathcal{M}_i[P_i] \parallel \mathcal{M}_r'[P_r'] \parallel H \), when \( N' \) receives all messages in \( H \), the network also becomes \( \prod_{i \neq r} \mathcal{M}_i''[P_i''] \parallel \mathcal{M}_r''[P_r''] \parallel \emptyset \), where the group of monitors is thus consistent, so that \( N' \) is coherent.

222
for each monitored process

B.3 Proofs for Global Transparency

Let

no monitor does checking. Thus case (tau) - if monitors guarding all local processes in $\text{join}$ is receivable. Action case (join) - If such that

Thus, after $= N$

similar to $=$ $N$

Since $N$ is receivable, by Lemma 7.4.7, $N'$ is receivable. The following reasonings are similar to case (input).

1. If there is no pending message in $N'$, i.e. $H = \emptyset$, $N'$ is coherent because $N$ is coherent and after $N$ receives $s(p_1, p_2, l(v))$ by $\ell$, it is still coherent, which is $N'$.

2. If there are pending messages in $N'$ and some messages in $H$ are received by $\prod_{i \neq r} M_i[P_i]$, while some are received by $M_r[P_r]$, because receiving $\ell$ only depends on the existence of $a : \text{im}(G[p]) \in M_r$, this action does not affect any session input actions, i.e. it does not change other configurations at session endpoints.

Thus, after $\rightarrow_N N'$, $N'$ is coherent.

**case (join)** - If $\ell$ is a join($s[p]$) action, since $N$ is receivable, by Lemma 7.4.7 $N'$ is receivable. Action join($s[p]$) does not affect any rule of the consistency of group of monitors guarding all local processes in $N$, thus $N'$ is coherent.

**case (tau)** - if $\ell$ is a $\tau$, it does not effect the receivability or any $\Delta_i$ or $\Gamma_i$ in $N$ because no monitor does checking. Thus $N'$ is coherent.

Therefore for any action $\ell$, if $N$ is coherent and $N \rightarrow_N N'$, then $N'$ is coherent.

B.3 Proofs for Global Transparency

**Definition B.3.1.** Let $N$ be a monitored network. Then $N$ is locally conformant if, for each monitored process $M_i[P_i]$ in $N$, we have $M_i \models \text{erase}(M_i)[P_i]$. 

223
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

**Proposition B.3.2.** If \( N \) is coherent and locally conformant and \( N \overset{\ell}{\rightarrow}_g N' \) then \( N' \) is also coherent and locally conformant.

**Proof.** By Theorem 7.4.16 \( N' \) is coherent. Assume \( \prod_i M_i[P_i] \) is the composition of monitored processes in \( N \). If \( N \overset{\ell}{\rightarrow}_g N' \), there exists \( M_j[P_j] \in N \) and \( M_j'[P_j'] \) such that \( N = N_0 \parallel \prod_{k \neq j} M_k[P_k] \parallel M_j[P_j] \overset{\ell}{\rightarrow}_g N_0' \parallel \prod_{k \neq j} M_k[P_k] \parallel M_j'[P_j'] = N' \). \( M_j[P_j] \overset{\ell}{\rightarrow}_g M_j'[P_j'] \) also infers that \( M_j \overset{\ell}{\rightarrow} M_j' \) and \( P_j \overset{\ell}{\rightarrow} P_j' \). Since \( N \) is locally conformant, \( M_j \models \text{erase}(M_j)[P_j] \). By Lemma B.1.5, as \( M_j \overset{\ell}{\rightarrow} M_j' \) and \( \text{erase}(M_j) \overset{\ell}{\rightarrow} \mathcal{L} \), we have \( \mathcal{L} = \text{erase}(M_j') \); thus we have \( \text{erase}(M_j)[P_j] \overset{\ell}{\rightarrow} \text{erase}(M_j')[P_j'] \). Together with Definition 7.4.2 of conformance, we have \( M_j' \models \text{erase}(M_j')[P_j'] \). Note that, except \( M_j \), any other monitor in \( N \) does not change its configuration; the composition of monitored processes in \( N \) is \( \prod_{k \neq j} M_k[P_k] \parallel M_j'[P_j'] \), and every \( M_k[P_k] \in N', k \neq j \) satisfies \( M_k \models \text{erase}(M_k)[P_k] \). Thus \( N' \) is locally conformant. ■

**Definition B.3.3 (network erasure).** Assume \( N = N_1 \parallel N_2 \) is given. Then we have

\[
\text{erase}(N) = \text{erase}(N_1 \parallel N_2) = \text{erase}(N_1) \parallel \text{erase}(N_2).
\]

**Theorem 7.4.17 (global transparency).** Suppose \( N \) is coherent and locally conformant. Then \( N \sim \text{erase}(N) \).

**Proof.** For a network \( N \) which is coherent and locally conformant, we define relation \( \mathcal{R} \) to be:

\[
\mathcal{R} = \{(N, \text{erase}(N)) \mid N \text{ is coherent and locally conformant}\}
\]

We prove that \( \mathcal{R} \) is a standard strong bisimilar relation over \( \overset{\ell}{\rightarrow}_g \). Since \( N \) is locally conformant, \( \forall M_i \in N, M_i \models \text{erase}(M_i)[P_i] \), so that by Theorem 7.4.5 we have

\[
\forall M_i \in N, M_i \models \text{erase}(M_i)[P_i] \sim M_i[P_i].
\]

1. As \( N \overset{\ell}{\rightarrow}_g N' \), it implies there is \( M_j[P_j] \in N \) and \( M_j'[P_j'] \) such that \( N = N_0 \parallel M_j[P_j] \overset{\ell}{\rightarrow}_g N_0' \parallel M_j'[P_j'] = N' \). \( M_j[P_j] \overset{\ell}{\rightarrow}_g M_j'[P_j'] \) also infers \( M_j \overset{\ell}{\rightarrow} M_j' \) and \( P_j \overset{\ell}{\rightarrow} P_j' \). Note that \( N_0 \) is changed to \( N_0' \) because \( N_0 \) contains the global queue, the message corresponding to \( \ell \) may enter or leave the global queue. All monitored processes in \( N_0 \) are not affected. By Definition 7.4.4, when \( \ell \) is an input action, \( M_j[P_j] \overset{\ell}{\rightarrow} M_j'[P_j'] \) and \( M_j \overset{\ell}{\rightarrow} M_j' \) imply \( \text{erase}(M_j)[P_j] \overset{\ell}{\rightarrow} \text{erase}(M_j')[P_j'] \), so that, based on Definition B.3.3, \( \text{erase}(N) \equiv \text{erase}(N_0) \parallel \text{erase}(M_j)[P_j] \overset{\ell}{\rightarrow}_g \).
B.4 Proofs for Session Fidelity

The theorem of session fidelity states that, whenever a network conforms to specifications in monitors, i.e., its all local processes (partial network) which are in $P(N)$ conform to specifications contained in $M$, all of its derivatives conform to the specifications of
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

In the follows, we firstly formally define *receiving, consistency and conformance* based on LTS of configurations. Recall that a *configuration* is the pair of $M$ and $H$:

**Definition 7.4.20** (configuration). A configuration is denoted by $\Phi = M; H$, in which the group of monitors correspond to $H$. In other words, all messages corresponding to the actions guarded by $M$ are in $H$.

**Definition B.4.1** (receivable configuration). Define $M; H$ is receivable by the following induction.

1. If $H$ is empty then $M; H$ is receivable.
2. If $H \equiv m \cdot H'$, then $M; H$ is receivable when we have $M; m \cdot H' \Rightarrow_M M'; H'$, where $\ell$ corresponding to $m$, and $M'; H'$ is receivable.

A configuration $M; H$ is *configurationally consistent* if all of its multi-step global input transition derivatives are receivable and the resulting $M$ is consistent. The consistency of a group of monitors is defined in Definition 7.4.12.

**Lemma B.4.2.** Assume $N \equiv N_s || \emptyset$ and $\models N_s : M$. If $N \Rightarrow_M N' \equiv N_s' || H'$ and $M \Rightarrow_M M'$, then $\models N_s' : M'$.

**Proof.** Directly from Definition 7.4.25.

Session fidelity says: assume a network $N \equiv N_s || \emptyset$ is given, and suppose that $N_s$ satisfies $M$. If $M$ is consistent, then we say $N$ *conforms to* $M$. If this holds, then, with the messages which $N$ exchanges follow the specification containing in $M$, the dynamics of the network witnesses the validity of $M$.

**Theorem 7.4.28** (session fidelity). Assume configuration $M; H$ is configurationally consistent, and network $N \equiv N_s || H$ conforms to configuration $M; H$. We say $N$ satisfies session fidelity, if for any $\ell$, we have $N \Rightarrow_M N'$ such that $M; H \Rightarrow_M M'; H'$, it holds that $M'; H'$ is configurationally consistent and that $N'$ conforms to $M'; H'$.

**Proof.** Assume $N \equiv N_s || H$ and $N$ conforms to $M; H$, which is configurationally consistent. Prove the statement by the inspection of each case. (In most cases, the proofs are similar to those for Theorem 7.4.16 proved in Appendix B.2).

**Sel** Let $\ell = s[p_1, p_2]_{l_j(v)}$, $N_s || H \equiv N \Rightarrow_M N' \equiv N_s' || H \cdot m$ and $M; H \Rightarrow_M M'; H \cdot m$, where $m = s(p_1, p_2, l_j(v))$. Since $M$ allows $\ell$ and $M$ is consistent, $\exists M_s, M_r \in M$,
\[ \exists G \text{ is well-formed such that} \]
\[ G = p_1 \rightarrow p_2 \{ l_i(x_i : S_i)_i(A_i)_i.G_i \}_{i \in I}, \]
and
\[ \begin{align*}
\Delta_s(s[p_1]\star) & \sim G \upharpoonright p_1 = p_2 \{ l_i(x_i : S_i)_i(A_i)_i.G_i \upharpoonright p_1 \}_{i \in I}, \\
\Delta_r(s[p_2]\star) & \sim G \upharpoonright p_2 = p_1 \{ l_i(x_i : S_i)_i(A_i)_i.G_i \upharpoonright p_2 \}_{i \in I}. \tag{B.5}
\end{align*} \]

where \( l_j \in \{ l_i \}_{i \in I} \), \( I \) is the set indexing labels. Note that, the configuration of \( \Delta_r(s[p_2]\star) \) is not changed by action \( \ell \), thus \( \Delta_r(s[p_2]\star) \) remains the same in \( M' \).

Consider (case 1: \( H \) is empty). Since \( M' \) has \( \Delta_r(s[p_2]\star) \sim p_1 \{ l_i(x_i : S_i)_i(A_i)_i.G_i \upharpoonright p_2 \}_{i \in I} \), \( m \) is receivable to \( M' \), and thus \( m \) is receivable to \( N_s' \) due to \( \models N_s' : M' \), according to Lemma B.4.2. After receiving \( m \), say \( M' \sim s[p_1,p_2]\!l_j(v) \rightarrow M'' \), according to Equation B.5 \( M'' \) has \( \Delta_s(s[p_1]\star) \sim G_j \upharpoonright p_1 \) and \( \Delta_r(s[p_2]\star) \sim G_j \upharpoonright p_2 \), and action \( s[p_1,p_2]\!l_j(v) \) does not affect any other configuration in \( M' \), \( M'' \) is consistent by Definition 7.4.12. Therefore, \( N' \) conforms to \( M'; m \).

Consider (case 2: \( H \) is not empty). Since \( N \equiv N_s \parallel H \) conforms to \( M; H \), all messages in \( H \) are receivable to \( N_s \). With the same reasonings of the proof for output in Theorem 7.4.16 for global safety, whenever \( M; H \sim s[p_1,p_2]\!l_j(v) \), \( M' ; H \cdot s(p_1,p_2,l_j(v)) \) are receivable to \( M' \) thus to \( N' \). Therefore, \( N' \) conforms to \( M' ; H \cdot s(p_1,p_2,l_j(v)) \).

(SelN) When \( \ell = s[p_1,p_2]\!l_j(a) \), where \( a \) is a name, by the LTS of monitors defined in Figure 7.4 this case is as same as the case of (Sel).

(Bra) Let \( \ell = s[p_1,p_2]\!l_j(v) \). Consider (case 1: \( H \) is empty). Since \( M; \emptyset \not\xrightarrow{\ell} g \), this case never happens.

Consider (case 2: \( H \) is not empty). When \( H \) is not empty. \( N \xrightarrow{\ell} g \ N' \) and
\[ M; H \xrightarrow{\ell} g \ M' ; H/m, \]
where \( H/m \) means taking off message \( m \) from \( H \), \( m = s(p_1,p_2,l_j(v)) \). By Definition 7.4.24 with the same reasonings of the proof for input in Theorem 7.4.16 for global safety, since \( M \) is consistent after receiving all messages \( H \), \( M' \) should
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

be consistent after receiving messages $H/m$. Thus we have $M'; H/m$ is configurationally consistent, to which we can check $N'$ conforms.

(BraN) When $\ell = s[p_1, p_2]?l_j(a)$, where $a$ is a name, by the LTS of monitors defined in Figure 7.4 this case is similar to the case of (Bra) except that the received $a$ is typed with $0$. Since this typing does not affect any consistency rule, it is proved as case (Bra).

(Req-b) Let $\ell = \pi(s[p_k]: G)$. $N \overset{\ell \cdot s}{\rightarrow} N' \equiv N_{s'}/H \cdot m'$ as well as $M; H \overset{\ell \cdot s}{\rightarrow} M'; H \cdot m$, where $m = \pi(s[p_k]: G)$. This action combines two parts: creating a fresh session and requesting through sending an invitation. As for the part of creating a session, the reasonings are as same as those of the proof for bound request in Theorem 7.4.16 for global safety.

As for the part of requesting an invitation to endpoint $a$ and other parts of proving that the resulting dynamic network conforms to the resulting configuration, the reasonings are as same as that for (Req-f) below.

(Req-f) Let $\ell = \pi(s[p]: G)$. $N \overset{\ell \cdot s}{\rightarrow} N' \equiv N_{s'}/H \cdot m'$ as well as $M; H \overset{\ell \cdot s}{\rightarrow} M'; H \cdot m$, where $m = \pi(s[p]: G)$. Since $M$ allows $\ell$ and $M$ is consistent, $\exists M_r \in M$ such that $a : 0(G[p]) \in \Gamma_j$ or $a : 10(G[p]) \in \Gamma_j$, and $\exists M_r \in M$ such that $a : \text{im}(G[p]) \in \Gamma_r$. Thus, $M_r$ is able to receive the message $m = \pi(s[p]: G)$ created by $\ell$, which implies that $m$ is receivable to $M'$ thus receivable to $N'$ because of $\models N_{s'}/M'$.

After $M \overset{\ell}{\rightarrow} M'$ (generating $m$ by requesting at $M_j$) and $M' \overset{\ell}{\rightarrow} M''$ (receiving $m$ by accepting at $M_r$), where $\ell' = a(s[p]: G)$ or $\ell' = a(s[p]: G)$, according to rules [Req-a] and [Acc-f/a] in Figure 7.4 $a : 0(G[p]) \in \Gamma_j$ or $a : 10(G[p]) \in \Gamma_j$, and $a : \text{im}(G[p]) \in \Gamma_r$ all remain in $M'$ and $M''$. Moreover, since the capability $s[p]: G \uparrow p$ is exchanged from $M_j$ to $M_r$ by removing it from $M_j$ and adding it to $M_r$, all rules about the capability of $s[p]$ defined in Definition 7.4.12 still hold for $M'$ and $M''$. Thus $M'$ and $M''$ are consistent. By Lemma B.4.2 we have $\models N_{s'}/M'$. Since all messages in $H$ are receivable to $M$, and $\ell$ does not affect any other configurations except those explained above, all messages in $H$ are receivable to $N'$. Because $m$ is receivable to $N_{s'}$ as we proved above, $H \cdot m$ is receivable to $N_{s'}$. In conclusion, $N'$ conforms to $M'; H \cdot m$, where $m = \pi(s[p]: G)$.
(Acc-b/f) Let $\ell = a(s[p] : G)$ or $\ell = a(s[p] : G')$.

Consider (case 1: $H$ is empty). Since $M; \emptyset \not\xrightarrow{\ell} G$, this case never happens.

Consider (case 2: $H$ is not empty). If $N_s \cdot H \equiv N \xrightarrow{\ell} G$ and $H/m \not\xrightarrow{\ell} M'; H/m$ where $m = \pi(s[p] : G')$, they imply $M_r \models M$ and $M_r \not\xrightarrow{\ell} M_r$, such that $a : \text{im}(G[p]) \in \Gamma_r$. Since all messages in $H$ are receivable to $M$ and $\ell$ only receives $m$ from $H$ and added capability of $s[p]$ into $M'_r \in M'$ without affecting the receivability of other messages in $H$, the left messages in $H/m$ are receivable to $N_s'$. By Lemma B.4.2 we have $|= N_s' : M'_r$. In conclusion $N'$ conforms to $M'; H/m$, where $m = \overline{a}(s[p] : G')$.

The proof for other cases are trivial. □

### B.5 Proofs for $\mathcal{E}$ Coherence

Before proving Proposition 7.5.7 for the property of $\mathcal{E}$ coherence, the following definitions and lemmas are introduced. We define $G' \subseteq G$ w.r.t a particular session similarly as the one for local specifications defined in Definition 7.4.9.

**Definition B.5.1** ($G' \subseteq G$ w.r.t a session). We say $G' \subseteq G$ w.r.t $s$ if, for some $\mathcal{E}$ containing $G$, we have either (I) $s : G \xrightarrow{\ell_1,...,\ell_n} s : G'$ for some sequence of actions $\ell_1...\ell_n$ or (II) $G \sim G'$.

Note that, when $G, G'$ are clearly for the same session, we simply write $G' \subseteq G$.

Define the result after $k$th valid unit permutation of a global specification:

**Definition B.5.2.** Assume $p \rightarrow q : \{l_i(x_i : S_i)\langle A_i \rangle. G_i\}_{i \in I} \subseteq G$. Define $p \rightarrow q : \{l_i(x_i : S_i)\langle A_i \rangle. G_i^k\}_{i \in I}$ is the result after $k$th valid unit permutation of $p \rightarrow q : \{l_i(x_i : S_i)\langle A_i \rangle. G_i\}_{i \in I}$ with its $k$ previous interactions.

Similarly, define the result after $k$th valid unit permutation of a local specification:

**Definition B.5.3.** Assume $q!\{l_i(x_i : S_i)\langle A_i \rangle. T_i\}_{i \in I} \subseteq T$. Define $q!\{l_i(x_i : S_i)\langle A_i \rangle. T_i^k\}_{i \in I}$ is the result after $k$th valid unit permutation of $q!\{l_i(x_i : S_i)\langle A_i \rangle. T_i\}_{i \in I}$ with its $k$ previous interactions. Similarly, for the case $q?\{l_i(x_i : S_i)\langle A_i \rangle. T_i\}_{i \in I} \subseteq T$, define $q?\{l_i(x_i : S_i)\langle A_i \rangle. T_i^k\}_{i \in I}$ is the result after $k$th valid unit permutation of $q?\{l_i(x_i : S_i)\langle A_i \rangle. T_i\}_{i \in I}$ with its $k$ previous interactions.
Example B.5.4. Assume an interaction

\[ p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i \}_{i \in I} \subseteq G, \]

is the kth interaction in G, and let G be in the following shape:

\[ G = p_k \rightarrow q_k : \{ \ldots \rightarrow p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i \}_{i \in I} \} \ldots \} \]

where the interaction with prefix \( p_k \rightarrow q_k \) is the first interaction in G.

\[ G \cap p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i' \}_{i \in I} \]

according to Definition 6.6.5, it means that we should be able to permute interaction with prefix \( p \rightarrow q \) to the top of G after k valid unit permutations.

Assume the last interaction sequenced before \( p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i \}_{i \in I} \) is interaction with prefix \( p_1 \rightarrow q_1 \) where \( q_1 \neq q \) or \( (p_1 \neq p) \cap (q_1 \neq q) \):

\[ p_1 \rightarrow q_1 : \{l_{j'}(x_{j'} : S_{j'}) \langle A_{j'} \rangle . G_{j'} \}_{j' \in J} = \]

\[ p_1 \rightarrow q_1 : \{l_{j'}(x_{j'} : S_{j'}) \langle A_{j'} \rangle . p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i' \}_{i \in I} \}_{j' \in J} \]

where \( G_{j'} = p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i' \}_{i \in I} \) and \( G_{j'} = G_{ij'} \). By Definition 6.6.5:

\[ p_1 \rightarrow q_1 : \{l_{j'}(x_{j'} : S_{j'}) \langle A_{j'} \rangle . p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i' \}_{i \in I} \}_{j' \in J} \cap \]

\[ p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . p_1 \rightarrow q_1 : \{l_{j'}(x_{j'} : S_{j'}) \langle A_{j'} \rangle . G_{ij'} \}_{j' \in J} \}_{i \in I} = \]

\[ p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i' \}_{i \in I} \]

where for all \( i \in I, G_i' = p_1 \rightarrow q_1 : \{l_{j'}(x_{j'} : S_{j'}) \langle A_{j'} \rangle . G_{ij'} \}_{j' \in J} \). Note that \( p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i' \}_{i \in I} \) results the 1st permutation of \( p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i \}_{i \in I} \) with its 1st previous interactions.

Now we state that \( p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i^{k-1} \}_{i \in I} \) is the result after \( k - 1 \) valid permutations from \( p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i \}_{i \in I} \). Then we can permute \( p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i \}_{i \in I} \) to the top after 1 unit valid permutations:

\[ p_k \rightarrow q_k : \{l_{j''}(x_{j''} : S_{j''}) \langle A_{j''} \rangle . p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_{ij}^{k-1} \}_{i \in I} \}_{j'' \in J} \cap \]

\[ p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . p_k \rightarrow q_k : \{l_{j''}(x_{j''} : S_{j''}) \langle A_{j''} \rangle . G_{j''}^{k-1} \}_{j'' \in J} \}_{i \in I} = \]

\[ p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle . G_i \}_{i \in I} \]

where \( G_{ij}^{k-1} = G_{ij}^{k-1} = G_i^{k-1} \).
Lemma B.5.5. Assume $p \rightarrow q : \{l_i(x_i : S_i)\|^A_i\}.G_i\}_{i \in I} \subseteq G$. If $G \cap p \rightarrow q : \{l_i(x_i : S_i)\|^A_i\}.G_i\}_{i \in I}$, then there does not exist an interaction with prefix $q' \rightarrow p$ or $p \rightarrow q$ suppressing $p \rightarrow q : \{l_i(x_i : S_i)\|^A_i\}.G_i\}_{i \in I} \subseteq G$.

**Proof.** Assume an interaction

$$p \rightarrow q : \{l_i(x_i : S_i)\|^A_i\}.G_i\}_{i \in I} \subseteq G,$$

is the $n$th interaction in $G$, and let $G$ be in the following form:

$$G = p_n \rightarrow q_n : \{... p \rightarrow q : \{l_i(x_i : S_i)\|^A_i\}.G_i\}_{i \in I} \}...\}.$$

where the interaction with prefix $p_n \rightarrow q_n$ is the first interaction in $G$.

If there is an interaction with prefix $p' \rightarrow q'$, where $q' = p$ or $(p' = p) \cap (q' = q)$, sequenced before $p \rightarrow q : \{l_i(x_i : S_i)\|^A_i\}.G_i\}_{i \in I}$, which is the result after $k$th permutation of $p \rightarrow q : \{l_i(x_i : S_i)\|^A_i\}.G_i\}_{i \in I}$ (according to Definition B.5.2), then by Definition 6.6.5

$$\begin{align*}
p' \rightarrow q' & : \{l'_{i'}(x'_{j'} : S'_{i'})\|^A'_{i'}\}.G'_{i'}\}_{i' \in J} = \\
p' \rightarrow q' & : \{l'_{i'}(x'_{j'} : S'_{i'})\|^A'_{i'}\}.p \rightarrow q : \{l_i(x_i : S_i)\|^A_i\}.G_i\}_{i \in I} \}_{i' \in J} \\
\not\rightarrow p & \rightarrow q : \{l_i(x_i : S_i)\|^A_i\}.p' \rightarrow q' : \{l'_{i'}(x'_{j'} : S'_{i'})\|^A'_{i'}\}.G'_{i'}\}_{i' \in J} \}_{i \in I}
\end{align*}$$

This is a contradiction.

Lemma B.5.6. Assume there exists $T_0 \subseteq T$.

1. Assume $T_0 = q!\{l_i(x_i : S_i)\|^A_i\}.T_i\}_{i \in I} \subseteq T$, if $T \cap q!\{l_i(x_i : S_i)\|^A_i\}.T_i\}_{i \in I}$, then does not exist an action with prefix $q''$ or $q!$ suppressing $q!\{l_i(x_i : S_i)\|^A_i\}.T_i\}_{i \in I}$ in $T$.

2. Similarly, assume $T_0 = p?\{l_i(x_i : S_i)\|^A_i\}.T_i\}_{i \in I} \subseteq T$, if $T \cap p?\{l_i(x_i : S_i)\|^A_i\}.T_i\}_{i \in I}$, then does not exist an action with prefix $p''$ or $p?$ suppressing $p?\{l_i(x_i : S_i)\|^A_i\}.T_i\}_{i \in I}$ in $T$.

**Proof.** The proof is similar to the proof of Lemma B.5.5. Assume action

$$T_0 = q!\{l_i(x_i : S_i)\|^A_i\}.T_i\}_{i \in I} \subseteq T,$$

is the $n$th action in $T$ and $T$ is in the following shape

$$T = ... q!\{l_i(x_i : S_i)\|^A_i\}.T_i\}_{i \in I}...\}.$$
If there is some action with prefix \( q_1 \) such that \( q_1 = q' \) or \( q_1 = q! \) sequenced before action \( q!\{l_i(x_i : S_i)\langle A_i\rangle.T_i\}_{i \in I} \), the result after \( k \)th valid unit permutation of \( q!\{l_i(x_i : S_i)\langle A_i\rangle.T_i\}_{i \in I} \) (according to Definition \[B.5.3\]), by Definition \[B.6.8\]

\begin{align*}
q_1!\{l_j'(x_j' : S_j')\langle A_j'\rangle.T_j'\}_{j' \in J} = q_1!\{l_j'(x_j' : S_j')\langle A_j'\rangle.q!\{l_i(x_i : S_i)\langle A_i\rangle.T_i\}_{i \in I}\}_{j' \in J}
\end{align*}

where \( T_j' = q!\{l_i(x_i : S_i)\langle A_i\rangle.T_i\}_{i \in I} \) and \( T_{j_i}^k = T_{j_i}' \). This is a contradiction.

Similarly, we can prove that for the input case, it is a contradiction too. 

**Lemma B.5.7.** Given \( \mathcal{E} \) is coherent, \( s : G, s : \tilde{mv} \in \mathcal{E}, p, q \in \text{role}(G) \) and there is no \( \langle p, q, l''(v'') \rangle \) for some \( l'' \) and \( v'' \) in \( \tilde{mv} \). If \( G \vdash p - \tilde{mv} \vdash p \land q!\{l_i(x_i : S_i)\langle A_i\rangle.T_i\}_{i \in I} \), then

\[ G \land p \rightarrow q : \{l_i(x_i : S_i)\langle A_i\rangle.G_i\}_{i \in I} \forall i \in I, G_i \vdash p = T_i. \]

**Proof.** Note that \( s : \tilde{mv} \) means that there is only \( \tilde{mv} \) belonging to session \( s \) in the global queue. We prove it by contradiction. Assume

\[ G \not\land p \rightarrow q : \{l_i(x_i : S_i)\langle A_i\rangle.G_i\}_{i \in I} \forall i \in I, G_i \vdash p = T_i. \]

Then Lemma \[B.3.5.5\] indicates

\[ \exists p_0 \rightarrow q_0 : \{l_j'(x_j' : S_j')\langle A_j'\rangle.G_j'\}_{j \in J} \subseteq G \]

where \( q_0 = p \) or \( (p_0 = p) \land (q_0 = q) \) such that interaction \( p \rightarrow q : \{l_i(x_i : S_i)\langle A_i\rangle.G_i\}_{i \in I} \) is suppressed; then Definition \[B.5.1\] implies that \( G \vdash p \) should be

\[ G \vdash p = \ldots \land q_0\{l_j'(x_j' : S_j')\langle A_j'\rangle.T_j'\}_{j \in J} \ldots \}

or

\[ G \vdash p = \ldots \land q!\{l_j'(x_j' : S_j')\langle A_j'\rangle.T_j'\}_{j \in J} \ldots \]

if it is the \( k \)th action, where \( \forall j \in J, A_j''e/x_j' \downarrow \text{true} \iff A_j'\{e/x_j'\} \downarrow \text{true} \) for some \( e \).

For the case

\[ G \vdash p = \ldots \land q_0\{l_j'(x_j' : S_j')\langle A_j'\rangle.T_j'\}_{j \in J} \ldots \]

when we use \( G \vdash p - \tilde{mv} \vdash p \) to remove those happened output actions in \( G \vdash p \), we can never get

\[ G \vdash p - \tilde{mv} \vdash p \land q!\{l_i(x_i : S_i)\langle A_i\rangle.T_i\}_{i \in I}, \]

(1) By Definition \[B.5.2\] \( \tilde{mv} \vdash p \) only indicates messages sent from \( p \), so \( \tilde{mv} \vdash p \) cannot
B.5 Proofs for $\mathcal{E}$ Coherence

remove an input action in $G \vdash p$;

(II) Moreover, in $\overline{\text{mv}}$, there is no message of output actions which are sequenced behind action $p_0$? because, by Definition 6.6.S such an output only happens after action $p_0$ fires.

(III) Together with (I), (II), we know that after doing $G \vdash p - \overline{\text{mv}} \upharpoonright p$, the action $p_0$? still suppresses the action $q!\{l_i(x_i : S_i)\}$ for $i \in I$. This a contradiction.

For the case

$$G \vdash p = \ldots q!\{l_j'(x_j' : S_j') \langle A_j' \rangle .T_j' \}_{j \in J} \ldots \},$$

the reasoning is below:

(i) Since there is no $\langle p, q, l''(v'') \rangle$ for some $l''$ and $v''$ in $\overline{\text{mv}}$, so that taking off $\overline{\text{mv}} \upharpoonright p$ cannot remove action $q!\{l_j'(x_j' : S_j')\}$ for $j \in J$.

(ii) Based on (i), we know that after doing $G \vdash p - \overline{\text{mv}} \upharpoonright p$, the action $q!\{l_j'(x_j' : S_j')\}$ for $j \in J$ still suppresses the action $q!\{l_i(x_i : S_i)\}$ for $i \in I$. This a contradiction.

Thus

$$G \not\vdash p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle .G_i\}_{i \in I}, \forall i \in I, G_i \vdash p = T_i$$

If

$$G \vdash p - \overline{\text{mv}} \upharpoonright p = q!\{l_i(x_i : S_i) \langle A_i \rangle .T_i\}_{i \in I}.$$

Proposition 7.5.7 If $\mathcal{E}$ is coherent and $\mathcal{E} \xrightarrow{\ell} \mathcal{E}'$, then $\mathcal{E}'$ is coherent.

Proof. We illustrate the non-trivial cases of $\ell$. Note that, since the first rule of $\mathcal{E}$ coherence: $\forall a, a : \text{om}(G[p]) \in \Gamma$ implies that $\exists \Gamma', a : \text{im}(G[p]) \in \Gamma'$, is trivially true in the following cases, thus we ignore the proof of the first rule.

Case $[\mathcal{E}$-sel/selN] Assume $\ell = s[p, q]l_j(\langle v \rangle)$, where $v$ is either a value of a name. Since $\mathcal{E}$ is coherent, and $\mathcal{E} \xrightarrow{\ell} \mathcal{E}'$, by rule $[\mathcal{E}$-sel], let $\mathcal{E} = \mathcal{E}_0, s[p]^* : T_0, s : \overline{\text{mv}}$, where $T_0 \not\vdash q!\{l_i(x_i : S_i) \langle A_i \rangle .T_i\}_{i \in I}$, and thus $\mathcal{E}' = \mathcal{E}_0, s[p]^* : T_0', s : \overline{\text{mv}} \cdot \langle p, q, l_j(\langle v \rangle) \rangle$, where $T_0' \not\vdash T_j\{v/x_j\}$. Check if $\mathcal{E}'$ satisfies the three other rules of $\mathcal{E}$-coherence (Definition 7.5.6):

1. Since $\mathcal{E}$ is coherent, $s[p]^* \in \Delta$ implies $s : G \in \Theta$ and $p \in \text{role}(G)$. Note that, by Definition 7.5.5, whenever $s : \text{end}$ (i.e. the session is finished), everything related to session $s$ will be deleted immediately from $\mathcal{E}$. If $s : G \notin \mathcal{E}'$, i.e. $s : \text{end}$, since the configuration of $s : G$ does not change by an output action, thus it implies
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

\[s : G \not\in \mathcal{E}.\] Since \(\mathcal{E}\) is coherent, it implies \(s[p]^* \not\in \mathcal{E}\), which is a contradiction. Thus \(\mathcal{E}'\) satisfies the 2nd rule of \(\mathcal{E}\)-coherence.

2. Since \(\mathcal{E}\) is coherent, in \(\mathcal{E}\), \(\exists T\) such that

\[
G \mid p - \bar{m}v \mid p = q\{l_i(x_i : S_i)\langle\langle A_i\rangle\rangle.T_i\}_{i \in I} = T,
\]

where \(\Delta(s[p]^*) \vdash T\).

By rule \([s\text{-sel}]\), in \(\mathcal{E}'\), \(\Delta(s[p]^*) = T_0 = T_j\{v/x_j\}\). Check if it satisfies \(G \mid p - \bar{m}v \cdot \langle p,q,l_j\langle v\rangle\} \mid p = T_j\{v/x_j\}\).

(a) If \(\bar{m}v \mid p = \varepsilon\), then \(G \mid p - \bar{m}v \mid p = G \mid p = T\). By Definition \[7.5.2\] in \(\mathcal{E}'\) we have

\[
G \mid p - \bar{m}v' \mid p = G \mid p - \bar{m}v \cdot \langle p,q,l_j\langle v\rangle\} \mid p
= G \mid p - \varepsilon \cdot \langle p,q,l_j\langle v\rangle\} \mid p
= G \mid p - \langle p,q,l_j\langle v\rangle\} \mid p
= G \mid p - q!l_j(v).
\]

Since

\[
G \mid p = T = q\{l_i(x_i : S_i)\langle\langle A_i\rangle\rangle.T_i\}_{i \in I},
\]

by Definition \[7.5.3\]

\[
G \mid p - q!l_j(v) = T_j\{v/x_j\}
\]

which satisfies the 4th rule of \(\mathcal{E}\)-coherence.

(b) Since \(G \mid p - \bar{m}v \mid p\) in \(\mathcal{E}\) is defined (because \(\mathcal{E}\) is coherent), if \(\bar{m}v \mid p \neq \varepsilon\), by Definition \[7.5.2\] assume

\[
\bar{m}v \mid p = q_1!l^1(v^1) \cdot q_2!l^2(v^2) \cdot \ldots \cdot q_n!l^n(v^n),
\]

where \(i\) is the upper index to denote the labels and values may be different, and \(\forall k \in \{1..n\}, q_k!l^k(v^k) \neq \varepsilon\), is the \(k\)th output action of \(p\).
Let \( q_k^k \{ l_{jk}^k (x_{jk}^k : S_{jk}^k) \langle A_{jk}^k \rangle, T_{jk}^k \}_{j_k \in I} \) be the \( k \)th left endpoint specification after the \( k \)th output action. Assume \( G \upharpoonright p = T^0 \), which is the endpoint specification at the beginning. Since \( G \upharpoonright p - m \bar{v} \upharpoonright p = T \), by Definition 7.5.3, we have

\[
G \upharpoonright p - m \bar{v} \upharpoonright p = T^0 - q_1!_{l_1^1(v^1)} \cdot q_2!_{l_2^2(v^2)} \cdot \ldots \cdot q_n!_{l_n(v^n)} = T_{j_1}^1 \{ v^1 / x^1_{j_1} \} - q_2!_{l_2^2(v^2)} \cdot \ldots \cdot q_n!_{l_n(v^n)} = T_{j_2}^2 \{ v^2 / x^2_{j_2} \} - q_3!_{l_3^3(v^3)} \cdot \ldots \cdot q_n!_{l_n(v^n)} = \ldots = T_{j_{n-1}}^{n-1} \{ v^{n-1} / x_{j_{n-1}}^{n-1} \} - q_n!_{l_n(v^n)} = T_{j_n}^n \{ v^n / x^n_{j_n} \} = T.
\]

where \( l^k = l_{jk}^k \). Thus inductively use Definition 7.5.3, we get

\[
G \upharpoonright p - (m \bar{v} \cdot \langle p, q, l_j(v) \rangle) \upharpoonright p = T^0 - q_1!_{l_1^1(v^1)} \cdot q_2!_{l_2^2(v^2)} \cdot \ldots \cdot q_n!_{l_n(v^n)} \cdot \langle p, q, l_j(v) \rangle \upharpoonright p = T_{j_1}^1 \{ v^1 / x^1_{j_1} \} - q_2!_{l_2^2(v^2)} \cdot \ldots \cdot q_n!_{l_n(v^n)} \cdot \langle p, q, l_j(v) \rangle \upharpoonright p = T_{j_2}^2 \{ v^2 / x^2_{j_2} \} - q_3!_{l_3^3(v^3)} \cdot \ldots \cdot q_n!_{l_n(v^n)} \cdot \langle p, q, l_j(v) \rangle \upharpoonright p = \ldots = T_{j_{n-1}}^{n-1} \{ v^{n-1} / x_{j_{n-1}}^{n-1} \} - q_n!_{l_n(v^n)} \cdot \langle p, q, l_j(v) \rangle \upharpoonright p = T_{j_n}^n \{ v^n / x^n_{j_n} \} - q!_{l_j(v)} = T - q!_{l_j(v)} = T_j^v \{ v / x_j \},
\]

Since \( T_{j_n}^n \{ v^n / x^n_{j_n} \} = T = q! \{ l_i^I(x_i : S_i) \langle A_i \rangle, T_i \}_{i \in I} \), by Definition 7.5.3, \( T_{j_1}^1 \{ v^1 / x^1_{j_1} \} - q!_{l_j(v)}(v) = T - q!_{l_j(v)}(v) = T_j^v \{ v / x_j \} \), which satisfies the 4th rule of \( \mathcal{E} \)-coherence.

In conclusion, \( \mathcal{E}' \) satisfies the 3rd rule of \( \mathcal{E} \)-coherence such that

\[
G \upharpoonright p - m \bar{v} \cdot \langle p, q, l_j(v) \rangle \upharpoonright p = T_j^v \{ v / x_j \},
\]

\[
T_j^v \{ v / x_j \} \cap T_j^v \{ v / x_j \}.
\]

3. Assume \( \mathcal{E} \) is coherent, in \( \mathcal{E}, \exists s : G, s : m \bar{v} \).

(a) Assume \( s : m \bar{v} \) has no message sent from \( p \) to \( q \). Since \( \mathcal{E} \) is coherent, in \( \mathcal{E} \)
there exists $T$ such that

$$\Delta(s[p]^\bullet) \circ q!\{l_i(x_i : S_i)\llangle A_i\rrangle.T_i\}_{i \in I} = T,$$

and $G \vdash p - \tilde{m}v \vdash p = T$. Lemma [B.5.7] implies that

$$G \circ p \to q : \{l_i(x_i : S_i)\llangle A_i\rrangle.G_i\}_{i \in I}.$$

For the additional message $s : \tilde{m}v \cdot \llangle p, q, l_j(v) \rrangle$ in $E'$, since an output action $s[p, q]l(v)$ does not change the configuration of $s : G$ (since the interaction is not complete), it satisfies the 4th rule of $E$-coherence which says if $s : \tilde{m}v \cdot s[p, q, l(v)] \cdot \tilde{m}v_2$, $\tilde{m}v_1$ does not suppress $s[p, q, l(v)]$, then

$$\exists G \circ p \to q : \{l_i(x_i : S_i)\llangle A_i\rrangle.G_i\}_{i \in I}.$$

(b) Assume $s[p, q, l'(v')] \in \tilde{m}v$ and $G \circ p \to q : \{l'_i(x'_i : S'_i)\llangle A'_i\rrangle.G'_i\}_{i \in I}$. As output $s[p, q]l(v)$ takes place, the configuration of $G$ does not change and $G \not\circ p \to q : \{l_j(x_j : S_j)\llangle A_j\rrangle.G'_j\}_{j \in J}$ because interaction $p \to q : \{l_j(x_j : S_j)\}_{j \in J}$ is suppressed by interaction $p \to q : \{l_i(x_i : S_i)\}_{i \in I}$. Thus it still satisfies the 4th rule of $E$-coherence.

**Case** [\texttt{E-bch/bchN}] As $l = s[p, q]?l_j(v)$, either $v$ is a value or a name, according to rule \texttt{[E-bch]}, let

$$E = E_0, s : G_0, s[q]^\bullet : T_0, s : \tilde{m}v,$$

$$\tilde{m}v = s[p, q, l_j(v)] \cdot \tilde{m}v',$$

$$G_0 \circ p \to q : \{l_i(x_i : S_i)\llangle A_i\rrangle.G_i\}_{i \in I} = G,$$

$$T_0 = G \vdash q - \tilde{m}v \vdash q.$$

By \texttt{[E-bch]}, we get $E' = E_0, s : G'_0, s[q]^\bullet : T'_0, s : \tilde{m}v$ where $G'_0 = G_j\{v/x_j\}$ and $T'_0 = (G_j \vdash q)\{v/x_j\} - \tilde{m}v \vdash q$.

Similarly, we check if $E'$ satisfies three rules of $E$-coherence (Definition [7.5.6]):

1. The only case that input action $s[p, q]?l_j(v)$ affects the existence of $s : G_0$ is when $G_0 = p \to q : \{l_i(x_i : S_i)\llangle A_i\rrangle.end\}, s : \llangle p, q, l_j(v) \rrangle \in E$, thus $G'_0 \not\in E'$ (because
of $G'_0 = \text{end}$ and $s : \emptyset$). Since $G_0 = p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle \langle \text{end} \rangle \}$ can only
$\rightarrow p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle \langle \text{end} \rangle \}$ and $\mathcal{E}$ is coherent, $\Delta(s[q]^{*}) = T_0 = p?\{l_i(x_i : S_i) \langle A_i \rangle \langle \text{end} \rangle \} - \{p, q, l_j \langle v \rangle\} \uplus q = p?\{l_i(x_i : S_i) \langle A_i \rangle \langle \text{end} \rangle \}$, so that in $\mathcal{E}'$, we have
$G'_0 = \text{end}$, and $\Delta(s[q]^{*}) = \text{end}$, they finish all interactions and actions at the same
time, thus satisfies the 2nd rule: if there is no such a global specification, then there is no corresponding endpoint specification.

2. For the 3rd rule of $\mathcal{E}$-coherence, by rule $[\mathcal{E}\text{-bch}]$, in $\mathcal{E}'$, $s[q]^{*} : T'_0, s : G_j \{v/x_j\}$,
$T'_0 = ((G_j \uplus q) \{v/x_j\} - \overline{mv} \uplus q = (G_j \uplus q) \{v/x_j\} - \overline{mv'} \uplus q$, which means
$T'_0 \rightarrow ((G_j \uplus q) \{v/x_j\} - \overline{mv'} \uplus q$. Thus it satisfies the 3rd rule of $\mathcal{E}$-coherence.

3. Since $\mathcal{E}$ is coherent, every message specification $mv = s(p_k, q_k, l^k \langle v^k \rangle) \in \overline{mv}$ im-
plies that $G \rightarrow p_k \rightarrow q_k : \{l^k\{x_{ik}^k : S_{ik}^k \} \langle A_{ik}^k \rangle \langle G_{ik}^k \rangle \}_{ik} \in I$. Since we have message
specifications $s : s(p, q, l\langle v \rangle) \cdot \overline{mv'}$ in $\mathcal{E}$ and $G \rightarrow p \rightarrow q : \{l_i(x_i : S_i) \langle A_i \rangle \langle G'_i \rangle \}_{i} \in I$, when message $\langle p, q, l\langle v \rangle \rangle$ is absorbed, $G \xrightarrow{s[p,q]^{l\langle v \rangle}} G_j \{v/x_j\}$, and the rest interac-
tions $p_k \rightarrow q_k : \{l^k\{x_{ik}^k : S_{ik}^k \} \langle A_{ik}^k \rangle \langle G_{ik}^k \rangle \}_{ik} \in I$ are still in $G_j \{v/x_j\}$, which means
they are still permutable to the top, therefore the 4th rule is satisfied.

Case $[\mathcal{E}\text{-req-b}]$ With the rule $[\mathcal{E}\text{-req-b}]$, when $\mathcal{E} = \mathcal{E}_0$ is coherent and $\ell = \overline{a}(s[p] : G)$,
we have $s : G, s[p_i] : G \uplus p_i$ where $\forall i \in I, p_i \in \text{role}(G)$, and $s : \emptyset$ in $\mathcal{E}'$.

1. It is straightforward that $\mathcal{E}'$ satisfies the 1st and 2nd rules of $\mathcal{E}$-coherent.

2. Since there is no message in $s : \emptyset$, $\forall p \in \text{role}(G), G \uplus p - \epsilon \uplus p = G \uplus p = \Delta(s[p])$.
Thus it satisfies the 3rd rule of $\mathcal{E}$-coherence.

3. Since there is no message, the 4th rule is satisfied.

Other cases are trivial because they do not affect any rule of $\mathcal{E}$-coherence. ■

Theorem 7.5.9 (session fidelity w.r.t. $\mathcal{E}$). If $N \xrightarrow{\ell}^g N'$, and $\mathcal{E} \vdash N$, $\mathcal{E}$ is coherent,
then $\mathcal{E} \xrightarrow{\ell}^g \mathcal{E}'$, and $\mathcal{E}' \vdash N'$, $\mathcal{E}'$ is coherent.

Proof. If $\mathcal{E}$ is coherent, $\mathcal{E} \xrightarrow{\ell}^g \mathcal{E}'$, then $\mathcal{E}'$ is coherent has been proved in Proposition
7.5.7 Assume $\Theta_0, \Gamma_0, \Delta_0$ composes a global environment defined in $\mathcal{E}$.
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

Case \([\text{sel}/\text{selN}]\) For the case when \(\ell = s[p, q]l_j(v)\), \(v\) is either a value or a name, assume

\[
N = N_0 \parallel M_s[P_s] \parallel H
\]

by the fact \(N \xrightarrow{\ell} N'\) implying \(\exists M_s[P_s] \in N\) such that \(M_s[P_s] \xrightarrow{\ell} M_s'[P_s']\).

Since \(E \vdash N\), with rules \([E\text{-CO}]\) and \([E\text{-PAR}]\), let \(E = \Theta, \Gamma, \Delta_1, \Delta_2, \Delta_3\) such that

\[
\Theta, \Gamma, \Delta_1 \vdash_{g} N_0,
\]

\[
\Theta, \Gamma, \Delta_2, \Delta_3 \vdash_{g} M_s[P_s] \parallel H
\]

By rule \([E\text{-PM3}]\), \(\Delta_3 = s : \overline{m}v\) so that \(\Gamma, \Delta_3 \vdash_{g} H\). By rules \([E\text{-M}]\) and \([\text{SEL}]\) (see Figure 7.4), let \(\Delta_2 = \Delta_0, s[p]^{\star} : T\) where \(T \sim q!\{l_i(x_i : S_i) \langle A_i \rangle \} \cdot T_i\}_{i \in I}, j \in I\), and \(\Gamma \models A_j\{v/x_j\}\), so that

\[
\Gamma, \Delta_2 \vdash_{g} M_s[P_s]
\]

where

\[
M_s = M_0, s[p]^{\star} : T, A_j\{v/x_j\} \downarrow \text{true}.
\]

based on the fact \(M_s \xrightarrow{\ell} M_s'\). Therefore, rule \([E\text{-sel}]\) says \(E \xrightarrow{\ell} E'\) because \(E\) has \(s[p]^{\star} : T\) which approves transition \(\ell\).

By rule \([E\text{-sel}]\), \(E' = \Theta, \Gamma, \Delta_1, \Delta_2, \Delta_3\) where \(\Delta_2 = \Delta_0, s[p]^{\star} : T_j\{v/x_j\}\) and \(\Delta_3' = s : \overline{m}v \cdot s(p, q, l_j(v))\); and by rule \([\text{SEL}]\), \(M_s \xrightarrow{\ell} M_s'\), thus \(M_s' = M_0, s[p]^{\star} : T_j\{v/x_j\}\). With rule \([E\text{-PM3}]\), they together imply that

\[
\Theta, \Gamma, \Delta_1 \vdash_{g} N_0,
\]

\[
\Theta, \Gamma, \Delta_2, \Delta_3' \vdash_{g} M_s'[P_s'] \parallel H \cdot s(p, q, l_j(v))
\]

Thus, by applying rules \([E\text{-PAR}]\) and \([E\text{-CO}]\), we have \(E' \vdash N_0 \parallel M_s'[P_s'] \parallel H \cdot s(p, q, l_j(v)) = N'\).

Case \([\text{bch}/\text{bchN}]\) For the case when \(\ell = s[p, q]l_j(v)\):

238
1. When \( v \) is a value, let \( N = N_0 \parallel M_r[P_r] \parallel s\langle p, q, l_j(v) \rangle \cdot H \) by the fact \( N \overset{\ell}{\to}_g N' \) implying \( \exists M_r[P_r] \in N, M_r[P_r] \overset{\ell}{\to} M'_r[P'_r] \), where \( M_r[P_r] \) is a receiver. By rule [bra] (see Figure 7.4), let

\[
M_r = M_0, s[q] : p?\{l_i(x_i : S_i)_i \langle \langle A_i \rangle \rangle \}_i \in I, A_j\{v/x_j\} \downarrow \text{true}.
\]

Since \( \mathcal{E} \vdash N \), by rules [\(\varepsilon\)-CO] and [\(\varepsilon\)-PAR], let \( \mathcal{E} = \Theta, \Gamma, \Delta_1, \Delta_2, \Delta_3 \) such that

\[
\Theta, \Gamma, \Delta_1 \vdash_g N_0, \\
\Theta, \Gamma, \Delta_2, \Delta_3 \vdash_g M_r[P_r] \parallel s\langle p, q, l_j(v) \rangle \cdot H
\]

By rule [\(\varepsilon\)-PM3], let \( \Delta_3 = s : s\langle p, q, l_j(v) \rangle \cdot \tilde{m}\tilde{v} \) so that \( \Gamma, \Delta_3 \vdash_g s\langle p, q, l_j(v) \rangle \cdot H \).

Decompose \( \tilde{m}\tilde{v} \). Assume the messages sent from endpoint \( s[q] \) are \( s\langle q, p_k, l^k(v^k) \rangle \in H \), such that for each \( k \),

\[
s : s\langle q, p_k, l^k(v^k) \rangle \vdash_g s\langle q, p_k, l^k(v^k) \rangle,
\]

\[
s : s\langle q, p_k, l^k(v^k) \rangle \in \Delta_3.
\]

In \( \mathcal{E} \), we have \( s : G \in \Theta, \) with the decomposition of messages above, it should be in the form:

\[
G = q \to p_1 : \{l_{i_1}^1(x_{i_1}^1 : S_{i_1}^1)_i \langle \langle A_{i_1}^1 \rangle \rangle \}_i, \\
q \to p_k : \{l_{i_k}^k(x_{i_k}^k : S_{i_k}^k)_i \langle \langle A_{i_k}^k \rangle \rangle \}_i, \\
q \to p_m : \{l_{i_m}^m(x_{i_m}^m : S_{i_m}^m)_i \langle \langle A_{i_m}^m \rangle \rangle \}_i, p \to q : \{l_i(x_i : S_i)_i \langle \langle A_i \rangle \rangle , G_i \}_i \in I \}.
\]

Since \( \mathcal{E} \) is coherent and \( \mathcal{E} \vdash N \), we have

\[
G \upharpoonright q - (s\langle p, q, l_j(v) \rangle \cdot \tilde{m}\tilde{v}) \upharpoonright q = G \upharpoonright q - \tilde{m}\tilde{v} \upharpoonright q = p?q\{l_i(x_i : S_i)_i \langle \langle A_i \rangle \rangle , G_i \}_i \in I.
\]

Since \( \mathcal{E} \) has \( s : G, s[q] : T, \) and \( s : s\langle p, q, l(v) \rangle \cdot \tilde{m}\tilde{v}, \) where \( G \vdash p \to q : \{l_i(x_i : S_i)_i \langle \langle A_i \rangle \rangle , G_i \}_i \in I, \) by rule [\(\varepsilon\)-act], \( \mathcal{E} \) approves this action has transition \( \mathcal{E} \overset{\ell}{\to}_g \mathcal{E}' \).

Since \( M_r \overset{\ell}{\to} M'_r \), by rule [bra], \( M'_r = M_0, s[q] : T_j\{v/x_j\}, \) and \( H \in N' \).
Since $\mathcal{E} \xrightarrow{\ell} \mathcal{E}'$, by rule $[\mathcal{E}-\text{ncl}]$, we have $\Theta', \Gamma, \Delta_1, \Delta_2', \Delta_3' \in \mathcal{E}'$ where

\[
\begin{align*}
\Theta' &= \Theta_0, G_j\{v/x_j\},
\Delta_2' &= \Delta_0, s[q] \cdot (G_j \mid q)\{v/x_j\} - \tilde{m}v \upharpoonright q,
\Delta_3' &= s : \tilde{m}v
\end{align*}
\]

where $(G_j \mid q)\{v/x_j\} - \tilde{m}v \upharpoonright q = T_j\{v/x_j\}$ because

\[
\begin{align*}
(G_j \mid q - \tilde{m}v \upharpoonright q)\{v/x_j\} &= (G_j \mid q)\{v/x_j\} - (\tilde{m}v \upharpoonright q)\{v/x_j\}
= (G_j \mid q)\{v/x_j\} - \tilde{m}v \upharpoonright q
= T_j\{v/x_j\}
\end{align*}
\]

so that

\[
\begin{align*}
\Theta', \Gamma, \Delta_1 \vdash g N_0,
\Theta', \Gamma, \Delta_2', \Delta_3' \vdash M'_r[P'_r] \parallel H.
\end{align*}
\]

By rule $[\mathcal{E}-\text{PAR}]$ and $[\mathcal{E}-\text{CO}]$, we have $\mathcal{E}' \vdash N_0 \parallel M'_r[P'_r] \parallel H = N'$. 

2. When $\ell = s[p, q]?l_j(a)$ where $a$ is a name, the proof is similar to the one of $\ell = s[p, q]?l_j(v)$, except setting $\Gamma \in \mathcal{E}$ to be $\Gamma \vdash a : \text{mode}(G[p])$ and $\Gamma \models A_j \downarrow \text{true}$, other settings are the same. This setting does not affect transition according to rule $[\mathcal{E}-\text{ncl}]$, so that we still have $\mathcal{E} \xrightarrow{\ell} \mathcal{E}'$. After transition takes place, $\Gamma$ does not change its configuration, which means that, in $\mathcal{E}'$, for the additional $a : \mathbf{0}(G[p])$ in $M'_r$, $\Gamma \vdash a : T[p]$. Thus $\mathcal{E}' \vdash N'$. 

**Case [req-b]** For the case when $\ell = \overline{a}(s[p_j] : G)$, for the session creation part is proved here, while for the request of invitation part is proved together with Case [req f]. Since $s \not\in \text{dom}(\mathcal{E})$ is given and the fact $N \xrightarrow{\ell} N'$ implying $\exists M[P] \in N$ such that $M[P] \xrightarrow{\ell} M'[P']$, let

\[
N = N_0 \parallel M[P] \xrightarrow{\ell} N_0 \parallel M'[P] = N'.
\]

Since $\mathcal{E} \vdash N$, by rule $[\mathcal{E}-\text{CO}]$ and $[\mathcal{E}-\text{PAR}]$, let $\mathcal{E} = \Theta, \Gamma, \Delta_1, \Delta_2$ such that

\[
\begin{align*}
\Theta, \Gamma, \Delta_1 \vdash g N_0,
\Theta, \Gamma, \Delta_2 \vdash g M[P]
\end{align*}
\]
Let $\Theta = \Theta_0$ and $\Delta_2 = \Delta_0$, $s \not\in \text{dom}(\Delta_0)$. By Lemma 7.2.6, $\mathcal{M} \xrightarrow{l} \mathcal{M}'$ and $s \not\in \text{dom}(\mathcal{M})$. By [\text{\mathcal{E}-req-b}], $\mathcal{E}$ approves this action and have transition $\mathcal{E} \xrightarrow{\ell} \mathcal{E}'$; again, by [\text{\mathcal{E}-req-a}], in $\mathcal{E}'$, we have $\Theta', \Gamma, \Delta_1, \Delta_2 \in \mathcal{E}'$ where $\Theta' = \Theta_0, s : G, \Delta_2 = \Delta_0, \{s[p_i] : G \mid p_i\}_{p_i \in \text{rule}(G)}$ such that

$$\Theta', \Gamma, \Delta_1 \xrightarrow{g} N_0, \Theta', \Gamma, \Delta_2 \xrightarrow{g} \mathcal{M}'[P']$$

By rule [\text{\mathcal{E}-PAR}] and [\text{\mathcal{E}-CO}], we have $\mathcal{E}' \vdash N_0 \parallel \mathcal{M}'[P']$.

**Case [\text{req-f}]** For the case when $\ell = \pi(s[p] : G)$ or $\ell = \pi(s[p] : G)$, given the fact $N \xrightarrow{\ell} N'$ implying $\exists \mathcal{M}[P] \in N$ such that $\mathcal{M}[P] \xrightarrow{\ell} \mathcal{M}'[P']$, let

$$N = N_0 \parallel \mathcal{M}[P] \parallel H \xrightarrow{\ell} N_0 \parallel \mathcal{M}'[P] \parallel H \cdot \overline{a}(s[p] : G) = N'.$$

Since $\mathcal{E} \vdash N$, by rule [\text{\mathcal{E}-CO}] and [\text{\mathcal{E}-PAR}], let $\mathcal{E} = \Theta, \Gamma, \Delta_1, \Delta_2, \Delta_3$ such that

$$\Theta, \Gamma, \Delta_1 \xrightarrow{g} N_0, \Theta, \Gamma, \Delta_2, \Delta_3 \xrightarrow{g} \mathcal{M}[P] \parallel H$$

where $\Gamma = \Gamma_0, a : \text{om}(G[p])$ $\Delta_2 = \Delta_0, s[p] : T$, and $\Delta_3 = s : \overline{m} \nu$ such that $\Delta_2 \vdash_{g} \mathcal{M}[P], \Delta_3 \vdash_{g} H$. By rule [\text{\mathcal{E}-M}], when given $\mathcal{M} = \mathcal{M}_0, a : \text{om}(G[p]), s[p] : T, a \not\in \text{dom}(\mathcal{M}_0)$ by rule [\text{\mathcal{E}-req-f}]. Since $\mathcal{E}$ is coherent, the existence of $a : \text{om}(G[p])$ implies the existence of $a : \text{im}(G[p])$ in $\mathcal{E}$.

By rule [\text{\mathcal{E}-req-f}], $\mathcal{E}$ allows this action and have transition $\mathcal{E} \xrightarrow{\ell} \mathcal{E}'$, again, by rule [\text{\mathcal{E}-req-f}], $\mathcal{E} = \mathcal{E}'$; therefore, with rule [\text{\mathcal{E}-CO}], [\text{\mathcal{E}-PM1}], and given $\mathcal{M}' = \mathcal{M}_0, a : \text{om}(G[p])$, we have we have $\mathcal{E}' \vdash N_0 \mid \mathcal{M}'[P'] \parallel H \cdot \overline{a}(s[p] : G)$.

**Case [\text{acc-b/f}]** For case $\ell = a(s[p] : G)$ or $\ell = a(s[p] : G)$, given the fact $N \xrightarrow{\ell} N'$, $\exists \mathcal{M}[P] \in N$ such that $\mathcal{M}[P] \xrightarrow{\ell} \mathcal{M}'[P']$, let $N = N_0 \parallel \mathcal{M}[P] \parallel \overline{a}(s[p] : G) \cdot H \xrightarrow{\ell} N_0 \parallel \mathcal{M}'[P'] \parallel H = N'$.

Since $\mathcal{E} \vdash N$, by rule [\text{\mathcal{E}-CO}] and [\text{\mathcal{E}-PAR}], let $\mathcal{E} = \Theta, \Gamma, \Delta_1, \Delta_2, \Delta_3$ such that

$$\Theta, \Gamma, \Delta_1 \xrightarrow{g} N_0, \Theta, \Gamma, \Delta_2, \Delta_3 \xrightarrow{g} \mathcal{M}[P] \parallel \overline{a}(s[p] : G) \cdot H$$
B. APPENDIX FOR DYNAMIC ASYNCHRONOUSLY MONITORING

where $\Delta_3 = s : \overline{m}v, \Delta_3 \vdash_g H$. By rule [ε-M], [ε-PM1], and given $M = M_0, a : \text{im}(G[p])$ by rule [acc-n/p], $\Gamma = \Gamma_0, a : \text{im}(G[p])$, and $\Delta_2 = \Delta_0, s[p] : T$.

By rule [ε-ACC], $E$ approves this action and has transition $E \xrightarrow{g} E'$. By rule [ε-ACC], $E = E'$, and $M' = M_0, a : \text{im}(G[p]), s[p] : T$. Therefore, with rule [ε-CO], we have $E' \vdash N_0 || M'[P']$.

Case [new a] For case $\ell = \text{new } a : \text{im}(G[p])$, since the fact $N \xrightarrow{g} N', \exists M[P] \in N$ such that $M[P] \xrightarrow{\ell} M'[P']$. Let $N = N_0 || M[P] \xrightarrow{g} N_0 || M'[P] = N'$.

Since $E \vdash N$, by rule [ε-CO] and [ε-PAR], let $E = \Theta, \Gamma, \Delta$ such that

$$
\Theta, \Gamma, \Delta \vdash_g N_0,
\Gamma, \Delta \vdash_g M[P]
$$

where $\Gamma = \Gamma_0$ and $a \not\in \Gamma_0$.

By rule [ε-new a], $E$ approves this transition as $E \xrightarrow{g} E'$. By rule [ε-new a], $\Theta, \Gamma', \Delta \in E', \Gamma' = \Gamma_0, a : \text{im}(G[p])$. We have $M' = M, a : \text{im}(G[p])$ by rule [new a]. By rule [ε-CO] and [ε-M], we have $E' \vdash N_0 || M'[P']$.

Case [join] For case $\ell = \text{join}(s[p])$, the proof is trivial. Let

$$
N = N_0 || M[P] \xrightarrow{g} N_0 || M'[P] = N'.
$$

Since the fact $N \xrightarrow{g} N'$, it implies $\exists M[P] \in N, M[P] \xrightarrow{\ell} M'[P']$.

Since $E \vdash N$, by rules [ε-CO] and [ε-PAR], let $E = \Theta, \Gamma, \Delta_1, \Delta_2$ such that

$$
\Theta, \Gamma, \Delta_1 \vdash_g N_0,
\Theta, \Gamma, \Delta_2 \vdash_g M[P]
$$

where $\Delta_2 = \Delta_0, s[p] : T$ by rule [ε-M].

By rule [ε-join], $E$ approves this action and have transition $E \xrightarrow{g} E'$; again, by rule [ε-join], $\Theta, \Gamma, \Delta_2' \in E'$, $\Delta_2' = \Delta_0, s[p] : T$.
Given $M' = M_0, s[p]^*: T$ by rule $[\text{join}]$, and together with rule $[\varepsilon-\text{CO}]$ and $[\varepsilon-\text{PAR}]$, we have $\mathcal{E}' \vdash N_0 \parallel M'[P']$, which is denoted as $N'$.

Case $[\tau]$ as $\ell = \tau$, it is trivial.■
Appendix for Specifying Stateful Asynchronous Properties for Distributed Programs

C.1 Auxiliary Theorems and Proofs for Strongest Specifications

Let $\Theta_{\text{sync}}$, $\Theta_{\text{async}}$ and $\Theta_{\text{ass}}$ be the local specifications projected from global stateful protocols $G_{\text{sync}}$, $G_{\text{async}}$ and $G_{\text{assign}}$, respectively (refer to Example 8.1.2 and Example 8.1.3), on the role $S$ (i.e. server). They are defined as follows:

$\Theta_{\text{sync}} = \langle \text{ser} : I(G_{\text{sync}}[S]) ;
\{ s_j[S] : C?\text{req} (\varepsilon) \langle (\text{true} ; \varepsilon) \rangle . \text{C!ans} (x : \text{int}) \langle x = c ; c := c + 1 \rangle \} \rangle_{j \in J} ;
c \mapsto \langle \text{ini} \rangle \rangle$

$\Theta_{\text{async}} = \langle \text{ser} : I(G_{\text{async}}[S]) ;
\{ s_j[S] : C?\text{req} (\varepsilon) \langle (\text{true} ; \varepsilon) \rangle . \text{C!ans} (x : \text{int}) \langle x \notin c ; c := c \cup \{ x \} \rangle \} \rangle_{j \in J} ;
c \mapsto \langle \} \rangle$

$\Theta_{\text{ass}} = \langle \text{ser} : I(G_{\text{assign}}[S]) ;
\{ s_j[S] : C?\text{req} (\varepsilon) \langle (\text{true} ; \varepsilon) \rangle . \text{C!ans} (x : \text{int}) \langle x \in \text{log} ; \text{log} := \text{log} \cup \{ c' \} \rangle .
\{ c' \mapsto \text{ini}' , \text{log} \mapsto \langle \} \rangle \rangle$

where $J$ is the set of indexes of sessions.
Lemma C.1.1. For any \( s' \in \text{prefix}(s) \), \( s \in \text{trace}(\Theta_{\text{sync}}) \), we always have

\[
\text{num}(O(s')) \leq \text{num}(I(s'))
\]

Proof. Simply by the definition of \( \Theta_{\text{sync}} \) which specifies that inputs should always happen before outputs in the same session. Thus, in every possible prefix of \( s \in \text{trace}(\Theta_{\text{sync}}) \), the number of inputs should be more than the number of outputs. \( \blacksquare \)

Lemma C.1.2. Assume \( s \in \text{trace}(\Theta_{\text{sync}}) \) and \( c \in \text{field}(\Theta_{\text{sync}}) \). Assume \( \text{current}(c, \Theta_{\text{sync}}, \emptyset) = \text{ini} \). Then \( \forall s' \in \text{prefix}(s) \), we always have

\[
\text{current}(c, \Theta_{\text{sync}}, s') = \text{num}(O(s')) + \text{ini}
\]

Proof. By induction, when \( \text{num}(O(s')) = 0 \), which means there is no output action, \( 0 + \text{ini} = \text{current}(c, \Theta_{\text{sync}}, s') \). It is correct because no output action in \( s' \) means no update \( c := c + 1 \) applied according to \( \Theta_{\text{sync}} \).

Let \( \Theta'_{\text{sync}} \) be the configuration from \( \Theta_{\text{sync}} \xrightarrow{s'} \Theta'_{\text{sync}} \). Assume \( \text{num}(O(s')) = k \) so that \( \text{current}(c, \Theta_{\text{sync}}, s') = k + \text{ini} \), which means \( \text{current}(c, \Theta_{\text{sync}}, s') = \text{val}(c, \Theta'_{\text{sync}}) = k + \text{ini} \). For \( s' \cdot \ell \):

1. When \( \ell \) is an input, \( \text{num}(O(s' \cdot \ell)) = \text{num}(O(s')) = k \), and according to \( \Theta_{\text{sync}} \), state \( c \) is not updated, which means

\[
\text{current}(c, \Theta_{\text{sync}}, s' \cdot \ell) = \text{current}(c, \Theta_{\text{sync}}, s') = k + \text{ini} = \text{num}(O(s')) + \text{ini}.
\]

2. When \( \ell \) is an output, \( \text{num}(O(s' \cdot \ell)) = \text{num}(O(s')) + 1 = k + 1 \). According to \( \Theta_{\text{sync}} \), state \( c \) is updated by \( c := c + 1 \). Therefore, let \( \Theta''_{\text{sync}} \) be the configuration from \( \Theta'_{\text{sync}} \xrightarrow{\ell} \Theta''_{\text{sync}} \), we have

\[
\text{current}(c, \Theta_{\text{sync}}, s' \cdot \ell) = \text{val}(c, \Theta''_{\text{sync}}) = \text{val}(c, \Theta'_{\text{sync}}) + 1 = (k + \text{ini}) + 1
\]

which means

\[
\text{current}(c, \Theta_{\text{sync}}, s' \cdot \ell) = (k + 1) + \text{ini} = \text{num}(O(s' \cdot \ell)) + \text{ini}.
\]

By induction, the statement is proved. \( \blacksquare \)

Lemma C.1.3. Assume \( s \in \text{trace}(\Theta_{\text{sync}}) \) and \( c \in \text{field}(\Theta_{\text{sync}}) \). For any \( s' \in \text{prefix}(s) \), \( \text{current}(c, \Theta_{\text{sync}}, s') \leq \text{current}(c, \Theta_{\text{sync}}, s) \).
Proof. According to $\Theta_{\text{sync}}$, $c$ is updated by $c := c + 1$ when an output happens, which means the value of $\text{current}(c, \Theta_{\text{sync}}, s'')$ depends on the number of outputs happening in $s''$. Because the number of outputs in $s'$ is smaller than or equal to the number of outputs in $s$, we always have $\text{current}(c, \Theta_{\text{sync}}, s') \leq \text{current}(c, \Theta_{\text{sync}}, s)$. $\blacksquare$

**Lemma C.1.4.** Assume $s \in \text{trace}(\Theta_{\text{sync}})$ and $c \in \text{field}(\Theta_{\text{sync}})$. Then for any $\ell \in 0(s'), s' \in \text{prefix}(s)$, $v(\ell) < \text{current}(c, \Theta_{\text{sync}}, s')$.

*Proof.* By Lemma C.1.3 we always have $\text{current}(c, \Theta_{\text{sync}}, s_0) \leq \text{current}(c, \Theta_{\text{sync}}, s')$ whenever $s_0$ is a prefix of $s'$ because $\text{num}(s_0) \leq \text{num}(s')$.

Let $\ell^*$ be the last output in $s' = s_0 \cdot \ell^* \cdot s_1$, which means there is no output in $s_1$. Then, according to $\Theta_{\text{sync}}$, $v(\ell^*) = \text{current}(c, \Theta_{\text{sync}}, s_0)$. This fact implies two things:

(a) For any other $\ell \in 0(s')$, we know $\ell \in s_0 = s_0' \cdot \ell \cdot s''_0$ because $\ell^*$ is the last output.

According to $\Theta_{\text{sync}}$, $v(\ell) = \text{current}(c, \Theta_{\text{sync}}, s_0) \leq \text{current}(c, \Theta_{\text{sync}}, s_0) = v(\ell^*)$.

(b) $v(\ell^*) = \text{current}(c, \Theta_{\text{sync}}, s_0) < \text{current}(c, \Theta_{\text{sync}}, s_0 \cdot \ell^*) = \text{current}(c, \Theta_{\text{sync}}, s')$.

so that $v(\ell^*) < \text{current}(c, \Theta_{\text{sync}}, s')$.

Together with (a) and (b), for any $\ell \in s', s' \in \text{prefix}(s)$, $v(\ell) < \text{current}(c, \Theta_{\text{sync}}, s')$.

$\blacksquare$

**Lemma C.1.5.** Assume $s \in \text{trace}(\Theta_{\text{sync}})$ and $c \in \text{field}(\Theta_{\text{sync}})$. Assume $\text{current}(c, \Theta_{\text{sync}}, \emptyset) = \text{ini}$. $\forall s' \in \text{prefix}(s)$, we have

$$\text{ini} \leq \text{current}(c, \Theta_{\text{sync}}, s') \leq \text{num}(I(s')) + \text{ini}.$$ 

*Proof.* By Lemma C.1.2, $\text{current}(c, \Theta_{\text{sync}}, s') = \text{num}(0(s')) + \text{ini}$ so that $\text{ini} \leq \text{current}(c, \Theta_{\text{sync}}, s')$.

Moreover, by Lemma C.1.1 which states that $\text{num}(0(s')) \leq \text{num}(I(s'))$, we have

$$\forall s' \in \text{prefix}(s), \text{ini} \leq \text{current}(c, \Theta_{\text{sync}}, s') = \text{num}(0(s')) + \text{ini} \leq \text{num}(I(s')) + \text{ini}.$$ 

Then the proof is done. $\blacksquare$

**Lemma C.1.6.** Assume $s \in \text{trace}(\Theta_{\text{sync}}), c \in \text{field}(\Theta_{\text{sync}})$. Assume $\text{current}(c, \Theta_{\text{sync}}, \emptyset) = \text{ini}$. $\forall \ell \in 0(s'), s' \in \text{prefix}(s)$, we always have $\text{ini} \leq v(\ell) < \text{num}(I(s')) + \text{ini}$.

*Proof.* Immediately from Lemmas C.1.4 and C.1.5 $\blacksquare$.
Lemma C.1.7. Assume \( s = s_1 \cdot \ell \) and \( s \in \text{trace}(\Theta_{\text{sync}}) \). If \( \ell \) can permute with \( s_1 \) such that \( s_1 \cdot \ell \leftrightarrow s'_1 \cdot \ell' \), then \( \text{num}(I(s'_1)) > \text{num}(O(s'_1)) \).

Proof. When \( s \in \text{trace}(\Theta_{\text{sync}}) \), only when \( \ell \) is input then it can permute with an output or an input in \( s_1 \). Therefore, \( \text{num}(I(s'_1)) > \text{num}(O(s'_1)) \). ■

Lemma 8.5.13. Assume \( c \in \text{field}(\Theta_{\text{sync}}) \) and \( \text{current}(c, \Theta_{\text{sync}}, \emptyset) = \text{ini} \). Assume every session \( s_i \) guided by \( G_{\text{sync}} \) has been established. \( \Theta_{\text{sync}} \) is defined as below:

\[
\Theta_{\text{sync}} = \langle \text{ser} : I(G_{\text{sync}}[S]) ; \{ s_i[S] : C?\text{req}(\varepsilon)(\text{true} : \varepsilon).C!\text{ans}(x : \text{int})\langle x = c : c := c + 1 \rangle \rangle_i \in I ; c \mapsto \text{ini} \rangle
\]

where \( I \) is the index of sessions. If \( s' \in \text{trace}(\Theta_{\text{sync}}) \), then for any \( s \) resulting from permutations \( s' \leftrightarrow s \), \( s \) satisfies the followings:

1. If session \( s \in \text{ses}(s) \), then \( s \in \text{ses}(\Theta_{\text{sync}}) \).
2. For all \( s'' \in \text{prefix}(s) \), \( \text{num}(I(s'')) \geq \text{num}(O(s'')) \).
3. If \( s_0 \cdot \ell \in s \cap \ell = s[S,B]!\text{ans}(v) \), then \( \exists \ell' \in s_0, \ell' = s[B,S]?\text{req}(\varepsilon) \).
4. For all \( \ell, \ell' \in O(s) \), \( \ell \neq \ell' \), then \( v(\ell) \neq v(\ell') \).
5. For all \( \ell \in O(s'') \), \( s'' \in \text{prefix}(s) \), \( \text{ini} \leq v(\ell) < \text{num}(I(s'')) + \text{ini} \).

Proof. First of all, for any \( s' \in \text{trace}(\Theta_{\text{sync}}) \), \( s' \) satisfies all these conditions: condition 0 is satisfied because \( s' \) is valid according to \( \Theta_{\text{sync}} \) which means, for any \( s \in \text{ses}(s') \), \( \Theta_{\text{sync}} \) should include this session so that it can verify the actions involving in this session. Conditions 1, 2, 3 are satisfied simply by the definition of \( \Theta_{\text{sync}} \) and condition 4 is satisfied by Lemmas C.1.6 So the main proof below is to show, when \( s' \) satisfies these five conditions and \( s' \leftrightarrow s \), \( s \) satisfies all these conditions.

For cond 1. Since any permutation of \( s' \) does not add or subtract any session from \( s' \), any trace \( s \) permuted from \( s' \leftrightarrow s \) has the sessions as same as \( s' \) does. We have any \( s \in \text{ses}(s) \) implies \( s \in \text{ses}(s') \), which again implies \( s \in \text{ses}(\Theta_{\text{sync}}) \).

For cond 2. By the permutation rules defined in Definition 8.4.12.
(a) for any action sequence $\ell \cdot \ell' \in s'$, where $\ell$ is output and $\ell'$ is input, if they are permutable and are permuted by doing $\ell \cdot \ell' \leadsto \ell' \cdot \ell$, so that it makes $s' \leadsto s$, $s$ still satisfies cond 2 because the number of inputs in every $s'' \in \text{prefix}(s)$ is more than the number of inputs in every $s''' \in \text{prefix}(s')$.

(b) for any action sequence $\ell \cdot \ell' \in s'$, which are both inputs (resp. outputs), after permutations $\ell \cdot \ell' \leadsto \ell' \cdot \ell$, which leads to $s' \leadsto s$, the number of inputs or the number of outputs in every $s'' \in \text{prefix}(s)$ is as same as that in every $s''' \in \text{prefix}(s')$.

For cond 3. Based on $s' \in \text{trace}(\Theta_{\text{sync}})$, since the permutation of $s' \leadsto s$ only moves input actions ahead of output actions in $s$, $s$ still satisfies cond 3.

For cond 4. Since $s' \in \text{trace}(\Theta_{\text{sync}})$, every outputted value of a trace in $s'$ is unique. Then for every $s$ permuted from $s' \leadsto s$, every outputted value of $s$ is still unique.

For cond 5. Based on $s' \in \text{trace}(\Theta_{\text{sync}})$ and $s'$ satisfies cond 5, when $s$ is the result from permutation $s' \leadsto s$, because the valid permutations only make inputs move ahead of outputs, or two inputs (resp. two outputs) permute to each other, overall the permutations only increase the number of input actions ahead of output actions in $s$, while the value of any output action is not changed. By Lemma C.1.7, $s$ satisfies cond 5. ■

Remark C.1.8. Based on Lemma 8.5.13, some trace $s \in \text{trace}(\Theta_{\text{async}})$ may not satisfy these conditions because $\text{trace}(\Theta_{\text{async}})$ is much bigger than the set

$$\{s \mid s' \in \text{trace}(\Theta_{\text{sync}}), s' \leadsto s\}.$$ 

Definition C.1.9 (contiguous series). For a set $\{v_0, ..., v_n\}$ of numbers, where $v_0$ is the minimum element and $v_n$ is the maximum element. If, except $v_n$, any $v \in \{v_0, ..., v_n\}$, $\exists v' \in \{v_0, ..., v_n\}$ such that $v' = v + 1$, then the set is called a contiguous series.

Lemma C.1.10. The states $c'$ and $\log$ in $\Theta_{\text{ass}}$ respectively have the following attributes:

1. For state $c'$, for any $s$,
C. APPENDIX FOR SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

(a) when $\ell$ is an input, $\text{current}(c', \Theta_{\text{ass}}, s \cdot \ell) = \text{current}(c', \Theta_{\text{ass}}, s) + 1$.

(b) when $\ell$ is an output, $\text{current}(c', \Theta_{\text{ass}}, s \cdot \ell) = \text{current}(c', \Theta_{\text{ass}}, s)$.

2. For state $\log$, for any $s$,

(a) when $\ell$ is an input, $\text{current}(\log, \Theta_{\text{ass}}, s \cdot \ell) = \text{current}(\log, \Theta_{\text{ass}}, s) \cup \{\text{current}(c', \Theta_{\text{ass}}, s \cdot \ell)\}$.

(b) when $\ell$ is an output, $\text{current}(c', \Theta_{\text{ass}}, s \cdot \ell) = \text{current}(c', \Theta_{\text{ass}}, s) \setminus \{v(\ell)\}$.

Proof. It is proved directly from the mechanism of $\Theta_{\text{ass}}$.

Proposition 8.5.14. Assume $c', \log \in \text{field}(\Theta_{\text{ass}})$ and $\text{current}(c', \Theta_{\text{ass}}, \emptyset) = \text{ini}' = \text{ini} - 1$, $\text{current}(\log, \Theta_{\text{ass}}, \emptyset) = \{\}$. Assume every session $s_i$ guided by $G_{\text{assign}}$ has been established. $\Theta_{\text{ass}}$ is defined below:

$$
\Theta_{\text{ass}} = \langle \text{ser} : I(G_{\text{assign}}[S]) ;
\{s_i[S] : C?\text{req}(\varepsilon)\langle \text{true} ; c' := c' + 1, \log := \log \cup \{c'\}\rangle.
C!\text{ans}(x : \text{int})\langle x \in \log ; \log := \log \setminus \{x\}\rangle_{i \in I} ;
c' \mapsto \text{ini}', \log \mapsto \{\}\rangle
$$

where $I$ is the index of sessions. $s$ satisfies all conditions listed in Lemma 8.5.13 if and only if $s \in \text{trace}(\Theta_{\text{ass}})$.

Proof. (For $\Rightarrow$): Assume $s$ satisfies all conditions listed in Lemma 8.5.13. We only need to make sure that every output action in $s$ always satisfies the predicate at output obligation (i.e. $x \in \log$). The reasonings are as follows:

(1) Based on cond 1, 2, and 3, for any session $s \in \text{ses}(s)$, its actions are either $s' \cdot s[C, S]?\text{req}(\varepsilon) \cdot s'' \cdot s[S, C]!\text{ans}(v)$ or $s' \cdot s[C, S]?\text{req}(\varepsilon)$ where $s[S, C]!\text{ans}(v) \not\in s'$. Thus the sequence of actions satisfy that $\Theta_{\text{ass}}$ defines, for a session, its input action should happen before its output.

(2) Although an input is anyway valid because of the predicate $\text{true}$ at input obligation, with the update $c' := c' + 1$ and $\log := \log \cup \{c'\}$, it affects the elements of set $\log$ and thus may affect the judgement of predicate $x \in \log$ when replacing $x$ with the value of the upcoming output action.

For the effects caused by inputs the statement we have for $s$ satisfying the five conditions:
C.1 Auxiliary Theorems and Proofs for Strongest Specifications

Claim. \( \text{current}(c', \Theta_{ass}, s) = \text{num}(I(s)) + \text{ini}' \).

This is because \( c' \) is a counter at input obligation whose predicate is \( \text{true} \), any output action does not update \( c' \) and, for any \( s \), \( c' \) will be updated whenever an input happens. Note it does not matter whether \( s \in \text{trace}(\Theta_{ass}) \) or not (at this point this has not been proved).

This statement can be proved similarly as the proof in Lemma C.1.2. In Lemma C.1.2 the statement is \( \text{current}(c, \Theta_{sync}, s) = \text{num}(O(s)) + \text{ini}' \) because \( c \) is a counter at output obligation in \( \Theta_{sync} \), while \( c' \) is a counter at input obligation in \( \Theta_{ass} \). Remember, the predicate in \( \Theta_{ass} \) for any input is \( \text{true} \) and any output action cannot update \( c' \). We only need to replace every \( c \) with \( c' \) and \( \Theta_{sync} \) with \( \Theta_{ass} \), and change \( \text{num}(O(s)) \) to \( \text{num}(I(s)) \), other steps of the proof are the same.

(3) For any output action \( \ell \) in \( s \), since more than one inputs may have happened before \( \ell \) according to cond 2 and cond 3, to satisfy the predicate \( x \in \text{log} \) when replacing \( x \) with \( v(\ell) \), the followings should be considered:

For any \( s \), let \( s = s_0 \cdot \ell \cdot s_1 \), where \( s_0 \) only has inputs so that \( \ell \) is the first output.

(a) Up to \( s_0 \), \( \Theta_{ass} \) accepts \( s_0 \) because it only has inputs. According to updates \( c' := c' + 1 \) and \( \text{log} := \text{log} \cup \{c'\} \) at input obligation, where \( c' \) has initial value \( \text{ini}' \), and \( \text{log} \) has initial value \( \{\} \), the minimum (first) element in \( \text{log} \) is \( \text{ini}' + 1 = \text{ini} \), we therefore have,

\[
\text{current}(\text{log}, \Theta_{ass}, s_0) = \{\text{ini}'+1, ..., \text{ini}'+\text{num}(s_0)\} = \{\text{ini}, ..., (\text{ini}−1) + \text{num}(s_0)\}
\]

Thus for any \( s'' \in \text{prefix}(s_0) \),

\[
\text{current}(c', \Theta_{ass}, s''.\ell') = \text{current}(c', \Theta_{ass}, s'') + 1
\]

whenever \( \ell' \) is an input. Thus we have \( \{\text{ini}' + 1, ..., \text{ini}' + \text{num}(s_0)\} \) is a contiguous set with minimum \( \text{ini}' + 1 \) and maximum \( \text{ini}' + \text{num}(s_0) \).
C. APPENDIX FOR SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

(b) Up to $s_0 \cdot \ell$, by cond 5,

$$ini \leq v(\ell) < \text{num}(I(s_0 \cdot \ell)) \land ini = \text{num}(I(s_0)) + ini = \text{num}(s_0) + ini$$

which implies $v(\ell) \in \text{current}(log, \Theta_{ass}, s_0)$ so that $\Theta_{ass}$ accepts $s_0 \cdot \ell$. Note that, for any $s$, $\text{num}(I(s_0 \cdot \ell)) = \text{num}(I(s_0))$ whenever $\ell$ is an output.

(c) Assume for any $s' \in \text{prefix}(s)$, $s' = s_f \cdot \ell$. Assume $\Theta_{ass}$ accepts $s_f$ and let

$$\{ \ell \mid \ell \in 0(s_f) \} = \text{out}(s_f)$$

be the set of output values happening in $s_f$. So, up to $s_f$, we have

$$\text{current}(log, \Theta_{ass}, s_f) = \{ ini' + 1, ..., ini' + \text{num}(I(s_f)) \} \setminus \text{out}(s_f)$$

where $\{ ini' + 1, ..., ini' + \text{num}(I(s_f)) \}$ is a contiguous series.

Firstly, it needs to prove that $\{ ini' + 1, ..., ini' + \text{num}(I(s_f)) \}$ is a contiguous series. Assume $s_f = s_0 \cdot s_f'$ where $s_0$ only contains inputs, then it is straightforward that $\{ ini' + 1, ..., ini' + \text{num}(I(s_0)) \}$ is a contiguous series simply from (a). The following claims that, if a set is a contiguous series, then after adding new elements to it because of inputs, the resulting set is still a contiguous series.

**Claim.** For $s_0 \cdot s_f' = s', s' \in \text{prefix}(s)$ where $s_0$ only contains inputs, and let $\text{out}(s_f')$ be the set of output values of $s_f'$. If $\text{current}(log, \Theta_{ass}, s_0) = \{ ini' + 1, ..., ini' + \text{num}(I(s_0)) \}$, then

$$\text{current}(log, \Theta_{ass}, s_0 \cdot s_f')$$

\[= \{ ini' + 1, ..., ini' + \text{num}(I(s_0)) \} \cup \{ ini' + \text{num}(I(s_0)) + 1, ..., ini' + \text{num}(I(s_0)) + \text{num}(I(s_f')) \} \setminus \text{out}(s_f') \]

\[= \{ ini' + 1, ..., ini' + \text{num}(I(s_0)) + \text{num}(I(s_f')) \} \setminus \text{out}(s_f') \]

\[= \{ ini' + 1, ..., ini' + \text{num}(I(s_0 \cdot s_f')) \} \setminus \text{out}(s_f') \]

and the set $\{ ini' + 1, ..., ini' + \text{num}(I(s_0 \cdot s_f')) \}$ is a contiguous series.

This claim can be proved by the following reasoning: according to $\Theta_{ass}$, once an input happens, it updates $c' := c' + 1$ and $\text{log} := \text{log} \cup \{ c' \}$. The new ele-
C.1 Auxiliary Theorems and Proofs for Strongest Specifications

Elements added by the inputs in $s'_1$ are in the range from $\text{current}(c', \Theta_{s_0 \cdot \ell})$, where $\ell$ is the first input of $s'_1$, to $\text{current}(c', \Theta_{s_0 \cdot s'_1})$ where

$$\begin{align*}
\text{current}(c', \Theta_{s_0 \cdot \ell}) &= \text{current}(c', \Theta_{s_0}) + 1 \\
&= \text{current}(c', \Theta_{s_0}) + 1 \\
&= \text{current}(c', \Theta_{s_0}) + 1
\end{align*}$$

and

$$\begin{align*}
\text{current}(c', \Theta_{s_0 \cdot s'_1}) &= \text{current}(c', \Theta_{s_0}) + \text{num}(I(s'_1)) \\
&= \text{current}(c', \Theta_{s_0}) + \text{num}(I(s'_1))
\end{align*}$$

Because $\text{num}(I(s_0)) + \text{num}(I(s'_0)) = \text{num}(I(s_0 \cdot s'_0))$, the set of new elements added to $\text{current}(\log, \Theta_{s_0})$ is

$$\{\text{ini}' + \text{num}(I(s_0)) + 1, \ldots, \text{ini}' + \text{num}(I(s_0 \cdot s'_1))\}$$

which is a contiguous series set by the same reasoning of (a). Because the minimum element of set $\{\text{ini}' + \text{num}(I(s_0)) + 1, \ldots, \text{ini}' + \text{num}(I(s_0 \cdot s'_1))\}$, which is $\text{ini}' + \text{num}(I(s_0)) + 1$, is one more bigger than the maximum element of set $\{\text{ini}', \ldots, \text{ini}' + \text{num}(I(s_0))\}$, which is $\text{ini}' + \text{num}(I(s_0))$, the union of these two contiguous sets is still a contiguous series set. Moreover,

$$\text{current}(\log, \Theta_{s_0 \cdot s'_1}) = \{\text{ini}' + 1, \ldots, \text{ini}' + \text{num}(I(s_0 \cdot s'_1))\} \setminus \text{out}(s'_1)$$

simply according to the updates $c' := c' + 1$ and $\log := \log \cup \{c'\}$ for every input, and the update $\log := \log \setminus v(\ell)$ for every output $\ell$.

Continue to prove that $s_{f \cdot \ell}$ is anyway accepted by $\Theta_{s_0 \cdot \ell}$. When $\ell$ is an input, $\Theta_{s_0 \cdot s_{f \cdot \ell}}$ accepts $s_{f \cdot \ell}$ because $\Theta_{s_0 \cdot \ell}$ accepts any input. When $\ell$ is an output, then by cond 5, $\text{ini} \leq v(\ell) < \text{ini} + \text{num}(I(s_{f \cdot \ell})) = \text{ini} + \text{num}(I(s_f))$, we know that $v(\ell) \in \{\text{ini}' + 1, \ldots, \text{ini}' + \text{num}(I(s_f))\}$ because it is a contiguous series set with $\text{ini}' = \text{ini} - 1$.

Further, by cond 4 we know $v(\ell)$ is different from any value of actions in
C. APPENDIX FOR SPECIFYING STATEFUL ASYNCHRONOUS PROPERTIES FOR DISTRIBUTED PROGRAMS

\[ \text{out}(s_f). \] They together imply \( v(\ell) \) is in

\[ \text{current}(\log, \Theta_{\text{ass}}, s_f) = \{ \text{ini}' + 1, \ldots, \text{ini}' + \text{num}(I(s_f)) \} \setminus \text{out}(s_f) \]

Therefore, by induction, every output in \( s \) is accepted by \( \Theta_{\text{ass}} \), which means every \( s \) satisfies all conditions in Lemma 8.5.13, \( s \in \text{trace}(\Theta_{\text{ass}}) \).

(For \( \Leftarrow \)): Assume \( s \in \text{trace}(\Theta_{\text{ass}}) \) is given. The reasonings are as follows:

1. \( s \in \text{trace}(\Theta_{\text{ass}}) \) means that the sessions declared in \( s \) has been validly established (as \( s_i, i \in I \)), which implies \( s \) satisfies cond 1.

2. By the definition of \( \Theta_{\text{ass}} \), if \( s \in \text{trace}(\Theta_{\text{ass}}) \), then the inputs should always happen before the outputs in the same session, thus \( s \) satisfies cond 2, and cond 3.

3. \( \log \) is updated while an input happens by updating \( \log := \log \cup \{ c' \} \); therefore, for any \( v_1 \) and \( v_2 \) in \( \log \), \( v_1 \) is always different from \( v_2 \) simply because whenever an input happens, \( c' \) updates to a different value (i.e. \( c' := c' + 1 \)) and this new value is added to set \( \log \) (i.e. \( \log := \log \cup \{ c' \} \)). Since every outputted value \( v \) in \( s \) should be selected from set \( \log \) through verifying the predicate \( v \in \log \), and, when outputting \( v \), \( \log \) is updated by \( \log := \log \setminus \{ v \} \), they together ensure that for any outputs \( \ell \) and \( \ell' \) in \( s \), \( v(\ell) \neq v(\ell') \). Thus \( s \) satisfies condition 3.

4. By the definition of \( \Theta_{\text{ass}} \), the initial value of \( c' \) is \( \text{ini}' \) and \( c' \) is updated by increasing one when an input happens. Therefore, for every \( s' \in \text{prefix}(s) \), again, \( \text{current}(c', \Theta_{\text{ass}}, s') \) defined before is used to represent the lastest value of \( c' \) when the actions in \( s' \) have happened. Then we know

\[ \text{current}(c', \Theta_{\text{ass}}, s') = \text{num}(I(s')) + \text{ini}' \]

because the lastest value of \( c' \) is the summation of the number of inputs happening in \( s' \) plus the starting value \( \text{ini}' \). Since for every outputted value \( v \) in \( s' \in \text{prefix}(s) \), there exists an input belonging to the same session of \( v \) ahead of it, and it is selected from set \( \log \) by verifying through predicate \( v \in \log \), \( v \) is always in the range from \( \text{ini}' + 1 \), the minimum element in \( \log \), to \( \text{num}(I(s')) + \text{ini}' \),

254
the maximum element in \( \log \). Therefore we have

\[
\text{ini} + 1 \leq v \leq \text{current}(c', \Theta_{\text{ass}}, s') = \text{num}(I(s')) + \text{ini}',
\]

which implies

\[
\text{ini} \leq v \leq \text{num}(I(s')) + \text{ini}' < \text{num}(I(s')) + \text{ini}
\]

due to \( \text{ini}' = \text{ini} - 1 \). So that \( s \) satisfies cond 5.

5. Therefore, \( \forall s \in \text{trace}(\Theta_{\text{ass}}), s \) satisfies all conditions defined in Lemma \[8.5.13\]■

**Proposition** \[8.5.19\]  
\( P \models \text{sync} \Theta_{\text{ass}} \) then \( P \models \text{async} \Theta_{\text{ass}} \).

**Proof.** It can be proved simply by proving that \( \Theta_{\text{ass}} \) is commutative (so that it is asynchronous verifiable), or proved by the following reasoning. Let \( \ell^{\text{in}} \) represent an input action, and \( \ell^{\text{out}} \) represent an output action. For every \( s \in \text{Obs}(P) \), in which \( P \models \text{sync} \Theta_{\text{ass}} \), according to \( \Theta_{\text{ass}} \), it is an input-output alternating sequence with the following shape

\[
s = \ell^{\text{in}}_1 \cdot \ell^{\text{out}}_1 \cdot \ell^{\text{in}}_2 \cdot \ell^{\text{out}}_2 \cdot \ldots \cdot \ell^{\text{out}}_k \cdot \ell^{\text{in}}_k \cdot \ell^{\text{out}}_k \cdot \ldots
\]

which will end up with \( \ell^{\text{in}}_k \) or \( \ell^{\text{out}}_k \) for some \( k \), and satisfies all conditions listed in Lemma \[8.5.13\]. Since the permutations only move inputs ahead of outputs, no condition is affected by the permutations. Thus \( \forall s \sim s', s' \in \text{trace}(\Theta_{\text{ass}}) \) i.e. \( s' \in \text{Obs}(P), P \models \text{async} \Theta_{\text{ass}} \).■

**Lemma C.1.11.** Let \( \ell^{\text{out}}_i \) be the \( i \)th output action and \( \ell^{\text{in}}_i \) be the \( i \)th input action. \( s \in \text{trace}(\Theta_{\text{sync}}) \) if and only if

1. \( \ell^{\text{out}}_1 = \text{ini} \), and

2. for any \( \ell^{\text{out}}_i \in s \), there exist \( \ell^{\text{in}}_i \) positioning before \( \ell^{\text{out}}_i \), and

3. for any \( \ell^{\text{out}}_i, \ell^{\text{out}}_{i-1} \in s, v(\ell^{\text{out}}_i) = v(\ell^{\text{out}}_{i-1}) + 1 \).

**Proof.** For (\( \Rightarrow \)), according to \( \Theta_{\text{sync}} \) and Lemma \[\text{C.1.2}\] for any \( s \in \text{trace}(\Theta_{\text{sync}}) \), let \( s = s_0 \cdot \ell^{\text{out}}_{i-1} \cdot s_0' \cdot \ell^{\text{out}}_i \cdot s_1 \), where \( s_0' \) only contains input actions because \( \ell^{\text{out}}_i \) is the next output action after \( \ell^{\text{out}}_{i-1} \). The three conditions are proved as followings.
1. For the value of the first output according to $\Theta_{\text{sync}}$, let $s_0$ contains only inputs and $i = 2$, then we have $v(\ell_1^{\text{out}}) = \text{current}(c, \Theta_{\text{sync}}, s_0) = \text{num}(0(s_0)) + \text{ini} = \text{ini}$.

2. According to $\Theta_{\text{sync}}$, whenever $s \in \text{trace}(\Theta_{\text{sync}})$, there always exists $\ell_i^{\text{in}}$ in $s_0$ and $\ell_i^{\text{out}}$ in $s_0'$.

3. Moreover we have

$$v(\ell_i^{\text{out}}) = \text{current}(c, \Theta_{\text{sync}}, s_0) = \text{num}(0(s_0)) + \text{ini}$$

and

$$v(\ell_i^{\text{out}}) = \text{current}(c, \Theta_{\text{sync}}, s_0 \cdot \ell_i^{\text{out}} \cdot s_0') = \text{num}(0(s_0 \cdot \ell_i^{\text{out}} \cdot s_0')) + \text{ini}$$

where

$$\text{num}(0(s_0 \cdot \ell_i^{\text{out}} \cdot s_0')) + \text{ini} = \text{num}(0(s_0)) + 1 + \text{ini}$$

therefore we have $v(\ell_i^{\text{out}}) = v(\ell_i^{\text{out}}) + 1$ for any $\ell_i^{\text{out}}$ and $\ell_i^{\text{out}}$ in such $s$.

For $(\Leftarrow)$, the prove is done by induction. Assume $s''_0 \in \text{prefix}(s)$, $s''_0 \in \text{trace}(\Theta_{\text{sync}})$. We can always find such $s''_0$ by letting $s''_0$ be a trace which only contains input actions. Consider $s''_0 \cdot \ell_1^{\text{out}}$, where $\ell_1^{\text{out}}$ is the first output so that $s''_0$ contains only inputs,

$$\text{current}(c, \Theta_{\text{sync}}, s''_0) = \text{num}(0(s''_0)) + \text{ini} = \text{ini} = v(\ell_1^{\text{out}})$$

which means that $s_0 \cdot \ell_1^{\text{out}}$ is valid to $\Theta_{\text{sync}}$ because the outputted value is equal to the current value of state $c$.

Let $s''_0 = s_0 \cdot \ell_i^{\text{out}} \cdot s_i'$, where $s_0$ may contain some inputs and outputs or only inputs. Without loss of generality, assume $s''_0$ is valid according to $\Theta_{\text{sync}}$. It means

$$v(\ell_i^{\text{out}}) = \text{current}(c, \Theta_{\text{sync}}, s_0) = \text{num}(0(s_0)) + \text{ini}$$

Consider trace $s_0 \cdot \ell_i^{\text{out}} \cdot s_i' \cdot \ell_i^{\text{out}}$, where $\ell_i^{\text{out}}$ is the next output of $\ell_i^{\text{out}}$ and $s_0$ only contains inputs. Because $\Theta_{\text{sync}}$ always approves input actions, it implies that $s_0 \cdot \ell_i^{\text{out}} \cdot s_0'$ is valid according to $\Theta_{\text{sync}}$. Because for every $v(\ell_i^{\text{out}}), v(\ell_i^{\text{out}}) \in s$, we always have
C.1 Auxiliary Theorems and Proofs for Strongest Specifications

\[ v(\ell_{i}^{out}) = v(\ell_{i-1}^{out}) + 1, \] therefore, we have the following equations:

\[
\text{current}(c, \Theta_{\text{sync}}, s_{0} \cdot \ell_{i-1}^{out} \cdot s'_{0}) = \text{num}(\emptyset(s_{0} \cdot \ell_{i-1}^{out} \cdot s'_{0})) + \text{ini}
\]
\[
= \text{num}(\emptyset(s_{0})) + 1 + \text{ini}
\]
\[
= \text{current}(c, \Theta_{\text{sync}}, s_{0}) + 1
\]
\[
= v(\ell_{i-1}^{out}) + 1 = v(\ell_{i}^{out})
\]

which means the outputted value is equal to the current value of state \( c \), so that \( s_{0} \cdot \ell_{i-1}^{out} \cdot s'_{0} \cdot \ell_{i}^{out} \) is valid according to \( \Theta_{\text{sync}} \). By Induction, for any \( s \) satisfying these three conditions, we know \( s \in \text{trace}(\Theta_{\text{sync}}) \).

\[ \Box \]

**Proposition 8.5.20.** Assume \( s \) is an input-output alternating sequence. If \( s \in \text{trace}(\Theta_{\text{ass}}) \), then \( s \in \text{trace}(\Theta_{\text{sync}}) \).

**Proof.** It is proved by induction. \( s \in \text{trace}(\Theta_{\text{ass}}) \) if and only if \( s \) satisfies all conditions listed in Lemma 8.5.13 gives the following reasonings:

1. For the first output action \( \ell_{1}^{out} \), by cond 5, \( \text{ini} \leq v(\ell_{1}^{out}) < \text{num}(I(\ell_{1}^{in} \cdot \ell_{1}^{out})) + \text{ini} \).
   
   Due to \( \text{ini}' = \text{ini} - 1 \) and according to \( \Theta_{\text{ass}} \), we have
   
   \[ v(\ell_{1}^{out}) \in \{\text{ini}' + 1\} = \{\text{ini}\} \]

   which means \( v(\ell_{1}^{out}) = \text{ini} \).

2. For the second output action \( \ell_{2}^{out} \), by cond 5, \( \text{ini} \leq v(\ell_{2}^{out}) < \text{num}(I(\ell_{1}^{in} \cdot \ell_{1}^{out} \cdot \ell_{2}^{in} \cdot \ell_{2}^{out})) + \text{ini} \). Due to \( \text{ini}' = \text{ini} - 1 \) and according to \( \Theta_{\text{ass}} \), we have
   
   \[ v(\ell_{2}^{out}) \in \{\text{ini}' + 1, \text{ini}' + \text{num}(I(\ell_{1}^{in} \cdot \ell_{1}^{out}))\} \setminus \{\text{ini}' + 1\} \]

   which means \( v(\ell_{2}^{out}) = \text{ini}' + 2 = \text{ini} + 1 \).

3. Let \( s_{0} = \ell_{1}^{in} \cdot \ell_{1}^{out} \cdot \ell_{2}^{in} \cdot \ell_{2}^{out} \cdot \ell_{i-1}^{in} \cdot \ell_{i-1}^{out} \cdot \ell_{i}^{out} \). Assume for the \( i \)th output action \( \ell_{i}^{out} \) we have
   
   \[ v(\ell_{i}^{out}) \in \{\text{ini}' + 1, \ldots, \text{ini}' + \text{num}(I(s_{0} \cdot \ell_{i}^{in} \cdot \ell_{i}^{out}))\} \setminus \{\text{ini}' + 1, \ldots, \text{ini}' + \text{num}(I(s_{0}))\} \]

257
so that

\[ v(\ell_{i+1}^{out}) \in \{ini' + 1, ..., ini' + (i - 1), ini' + i\} \setminus \{ini' + 1, ..., ini' + (i - 1)\} \]

which means \( v(\ell_{i+1}^{out}) = ini' + i = ini + (i - 1) \).

Then for the \((i + 1)\)th output action \(\ell_{i+1}^{out}\), by cond 5, \(ini \leq v(\ell_{i+1}^{out}) < num(I(s_0 \cdot \ell_i^{in} \cdot \ell_{i+1}^{out} \cdot \ell_{i+1}^{out})) + ini\). Due to \(ini' = ini - 1\) and according to \(\Theta_{\text{ass}}\), we have

\[ v(\ell_{i+1}^{out}) \in \{ini' + 1, ..., ini' + num(I(s_0 \cdot \ell_i^{in} \cdot \ell_{i+1}^{out} \cdot \ell_{i+1}^{out}))\} \setminus \{ini' + 1, ..., ini' + num(I(s_0 \cdot \ell_i^{in} \cdot \ell_{i+1}^{out} \cdot \ell_{i+1}^{out}))\} \]

so that

\[ v(\ell_{i+1}^{out}) \in \{ini' + 1, ..., ini' + i, ini' + i + 1\} \setminus \{ini' + 1, ..., ini' + i\} \]

therefore we have \(v(\ell_{i+1}^{out}) = ini' + (i + 1) = ini + i\).

Finally we have \(v(\ell_{i+1}^{out}) = v(\ell_{i}^{out}) + 1\). Therefore, by Lemma C.1.11, \(s \in \text{trace}(\Theta_{\text{sync}})\). 

Note that, although Proposition 8.5.14 says that the set of traces satisfying conditions listed in Lemma 8.5.13 is equal to \(\text{trace}(\Theta_{\text{ass}})\), and Proposition 8.5.20 says that \(G_{\text{assign}}\) is an asynchronously verifiable specification realising synchronous behaviours w.r.t \(\Theta_{\text{sync}}\), \(s \in \text{trace}(\Theta_{\text{ass}})\) does not imply \(s \in \text{Obs}_a(P)\) such that \(P \models_{\text{sync}} \Theta_{\text{sync}}\). It is simply because \(\text{trace}(\Theta_{\text{ass}})\) is bigger than \(\text{Obs}_a(P)\) in which \(P \models_{\text{sync}} \Theta_{\text{sync}}\). The following example illustrates this point.

**Example C.1.12.** Consider a sequence of actions below:

\[ s_1[C, S]?\text{req}(\varepsilon) \cdot s_2[C, S]?\text{req}(\varepsilon) \cdot s_1[S, C]\text{ans}(v) \]

if it is a trace in \(\text{Obs}_a(P)\) such that \(P \models_{\text{sync}} \Theta_{\text{sync}}\), then \(v\) can only be 1; however if it is a trace in \(\text{trace}(\Theta_{\text{ass}})\), \(v\) can be either 1 or 2.

### C.2 Proofs for SPs’ Commutativity

Here we illustrate the main obligations in the SPs introduced in examples (see § 8.1 and § 8.1.4). Note that, only the state(s) updated at every input/output action appear(s)
C.2 Proofs for SPs’ Commutativity

in the obligations.

Proof \((G_{\text{sync}} \text{ is not asynchronous})\). Assume \(\xi^i_{\text{sync}}\) (for input) and \(\xi^o_{\text{sync}}\) (for output) are the notations for the obligations in \(G_{\text{sync}}\).

\[
\begin{align*}
\xi^i_{\text{sync}} & \overset{\text{def}}{=} B?\text{req}(\varepsilon)(\text{true};\varepsilon) \\
\xi^o_{\text{sync}} & \overset{\text{def}}{=} B!\text{ans}(x : \text{int})\langle x = c; c := c + 1 \rangle
\end{align*}
\]

\[
\begin{align*}
pred(\xi^i_{\text{sync}}) & \overset{\text{def}}{=} \lambda\varepsilon, t, c.(\text{true}) \\
pred(\xi^o_{\text{sync}}) & \overset{\text{def}}{=} \lambda x, t, c.(x = c) \\
\text{upd}(\xi^i_{\text{sync}}) & \overset{\text{def}}{=} \lambda\varepsilon, t, c.\langle\varepsilon\rangle \\
\text{upd}(\xi^o_{\text{sync}}) & \overset{\text{def}}{=} \lambda x, t, c.\langle c + 1\rangle
\end{align*}
\]

Then for \(\xi^o_{\text{sync}}\), we start from \(c\)’s current value is \(w = 1\):

\[
c = w = 1.
\]

\[
pred(\xi^o_{\text{sync}})(1, 1) = \text{true}
\]

and

\[
pred(\xi^o_{\text{sync}})(2, \text{upd}(\xi^o_{\text{sync}})(1, 1)) = \text{pred}(\xi^o_{\text{sync}})(2, 2) = \text{true}.
\]

Then we have

\[
pred(\xi^o_{\text{sync}})(2, 1) = \text{false}.
\]

Thus condition 1. in Definition 8.5.29 does not hold. Similarly, \(\xi^i_{\text{sync}}\) and \(\xi^o_{\text{sync}}\) are not commutative. ■

Proof \((G_{\text{assign}} \text{ is asynchronous})\). Assume \(\xi^i_{\text{ass}}\) and \(\xi^o_{\text{ass}}\) are the notations for obligations in \(G_{\text{assign}}\).

\[
\begin{align*}
\xi^i_{\text{ass}} & \overset{\text{def}}{=} B?\text{req}(\varepsilon)(t := t + 1; c := c \cup \{t\}) \\
\xi^o_{\text{ass}} & \overset{\text{def}}{=} B!\text{ans}(x : \text{int})\langle x \in c; c := c \setminus \{x\}\rangle
\end{align*}
\]

\[
\begin{align*}
pred(\xi^i_{\text{ass}}) & \overset{\text{def}}{=} \lambda\varepsilon, t, c.(\text{true}) \\
pred(\xi^o_{\text{ass}}) & \overset{\text{def}}{=} \lambda x, t, c.(x \in c) \\
\text{upd}(\xi^i_{\text{ass}}) & \overset{\text{def}}{=} \lambda\varepsilon, t, c.\langle t + 1; c \cup \{t\}\rangle \\
\text{upd}(\xi^o_{\text{ass}}) & \overset{\text{def}}{=} \lambda x, t, c.\langle c \setminus \{x\}\rangle
\end{align*}
\]
As for $\xi_{\text{ass}}^o, \xi_{\text{ass}}^i$, let $c = w$, where $w$ is a set. Assume
\[
\text{pred}(\xi_{\text{ass}}^o)(v, w) = \text{true}
\]
and
\[
\text{pred}(\xi_{\text{ass}}^o)(v', \text{upd}(\xi_{\text{ass}}^o)(v, w)) = \text{pred}(\xi_{\text{ass}}^o)(v', w \setminus \{v\}) = \text{true}.
\]
Then, $v' \neq v$, we have
\[
\text{pred}(\xi_{\text{ass}}^o)(v', w) = \text{true}
\]
and
\[
\text{pred}(\xi_{\text{ass}}^o)(v, \text{upd}(\xi_{\text{ass}}^o)(v', w)) = \text{pred}(\xi_{\text{ass}}^o)(v, w \setminus \{v'\}) = \text{true}.
\]
Moreover,
\[
\text{upd}(\xi_{\text{ass}}^o)(v', \text{upd}(\xi_{\text{ass}}^o)(v, w)) = \text{upd}(\xi_{\text{ass}}^o)(v', w \setminus \{v\}) = w \setminus \{v\} \setminus \{v'\},
\]
which is equal to
\[
\text{upd}(\xi_{\text{ass}}^o)(v, \text{upd}(\xi_{\text{ass}}^o)(v', w)) = \text{upd}(\xi_{\text{ass}}^o)(v, w \setminus \{v'\}) = w \setminus \{v\} \setminus \{v'\}.
\]
So that conditions 1. and 2. in Definition 8.5.29 both hold.

We can similarly check $\xi_{\text{ass}}^i, \xi_{\text{ass}}^i$. Let $t = w_1$ and $c = w_2$. $w_1$ is the current value of state $t$, and $w_2$ is the current set of state $c$. Condition 1. in Definition 8.5.29 holds immediately since the predicate is always true in $\xi_{\text{ass}}^i$. Condition 2. also holds immediately since the interaction variable is always $\epsilon$.

As for $\xi_{\text{ass}}^o, \xi_{\text{ass}}^i$, let $t = w_1$ and $c = w_2$. $w_1$ and $w_2$ are the current sets of states $t$ and $c$. Assume
\[
\text{pred}(\xi_{\text{ass}}^o)(v, w_2) = \text{true}
\]
and
\[
\text{pred}(\xi_{\text{ass}}^i)(\epsilon, \text{upd}(\xi_{\text{ass}}^o)(v, w_2)) = \text{pred}(\xi_{\text{ass}}^i)(\epsilon, w_2 \setminus \{v\}) = \text{true}.
\]
Then we have
\[
\text{pred}(\xi_{\text{ass}}^i)(\epsilon, w_1 \ w_2) = \text{true}
\]
and
\[
\text{pred}(\xi_{\text{ass}}^o)(v, \text{upd}(\xi_{\text{ass}}^i)(\epsilon, w_1 \ w_2)) = \text{pred}(\xi_{\text{ass}}^o)(v, w_2 \cup \{w_1 + 1\}) = \text{true}.
\]
Moreover,
\[ \text{upd}(\xi^{\text{ass}}_i)(\varepsilon, \text{upd}(\xi^{\text{ass}}_o)(v, w_2)) = \text{upd}(\xi^{\text{ass}}_i)(\varepsilon, w_1, w_2 \setminus \{v\}) = w_1 + 1, w_2 \setminus \{v\} \cup \{w_1 + 1\}, \]
which is equal to
\[ \text{upd}(\xi^{\text{ass}}_o)(v, \text{upd}(\xi^{\text{ass}}_i)(\varepsilon, w_1, w_2)) = \text{upd}(\xi^{\text{ass}}_o)(v, w_1 + 1, w_2 \cup \{w_1 + 1\}) = w_1 + 1, w_2 \cup \{w_1 + 1\} \setminus \{v\}. \]

However, \(\xi^{\text{ass}}_i, \xi^{\text{ass}}_o\) are not forward commutative. Assume
\[ \text{pred}(\xi^{\text{ass}}_i)(\varepsilon, w_1, w_2) = \text{true} \]
and
\[ \text{pred}(\xi^{\text{ass}}_o)(v, \text{pred}(\xi^{\text{ass}}_i)(\varepsilon, w_1, w_2)) = \text{true}. \]

However \(\text{pred}(\xi^{\text{ass}}_o)(v, w_2)\) needs not be equal to truth. So \(\xi^{\text{ass}}_o, \xi^{\text{ass}}_i\) are forward commutative, but not commutative.

Then by Definition 8.5.31, \(G_{\text{assign}}\) is commutative, thus \(G_{\text{assign}}\) is asynchronous by Propositions 8.5.34 and 8.5.25.

**Proof** \((G_{\text{async}}\text{ is asynchronous}). \) Assume \(\xi^{\text{async}}_i\) and \(\xi^{\text{async}}_o\) are the notations for obligations in \(G_{\text{async}}\).

\[ \xi^{\text{async}}_i \triangleq B?\text{req}(\varepsilon)(\text{true}; \varepsilon) \]
\[ \xi^{\text{async}}_o \triangleq B!\text{ans}(x : \text{int})(x \notin c ; c := c \cup \{x\}) \]
\[ \text{pred}(\xi^{\text{async}}_i) \triangleq \lambda \varepsilon, c.(\text{true}) \]
\[ \text{pred}(\xi^{\text{async}}_o) \triangleq \lambda x, c.(x \notin c) \]
\[ \text{upd}(\xi^{\text{async}}_i) \triangleq \lambda \varepsilon, c.(\{\varepsilon\}) \]
\[ \text{upd}(\xi^{\text{async}}_o) \triangleq \lambda x, c.(c \cup \{x\}) \]

As for \(\xi^{\text{async}}_o, \xi^{\text{async}}_i,\) let \(c = w\), where \(w\) is a set. Assume
\[ \text{pred}(\xi^{\text{async}}_o)(v, w) = \text{true} \]
and
\[
\text{pred}(\xi_{\text{async}}^o)(v', \text{upd}(\xi_{\text{async}}^o)(v, w)) = \text{pred}(\xi_{\text{async}}^o)(v', w \cup \{v\}) = \text{true}.
\]

Then, since
\[
\text{pred}(\xi_{\text{async}}^o)(v', w \cup \{v\}) = \text{true}
\]
implies \(v' \neq v\) and \(v' \notin w\), we have
\[
\text{pred}(\xi_{\text{async}}^o)(v', w) = \text{true}
\]
and
\[
\text{pred}(\xi_{\text{async}}^o)(v, \text{upd}(\xi_{\text{async}}^o)(v', w)) = \text{pred}(\xi_{\text{async}}^o)(v, w \cup \{v\}) = \text{true}.
\]
Moreover,
\[
\text{upd}(\xi_{\text{async}}^o)(v', \text{upd}(\xi_{\text{async}}^o)(v, w)) = \text{upd}(\xi_{\text{async}}^o)(v', w \cup \{v\}) = w \cup \{v\} \cup \{v'\},
\]
which is equal to
\[
\text{upd}(\xi_{\text{async}}^o)(v, \text{upd}(\xi_{\text{async}}^o)(v', w)) = \text{upd}(\xi_{\text{async}}^o)(v, w \cup \{v'\}) = w \cup \{v'\} \cup \{v\}.
\]
So that conditions 1. and 2. in Definition 8.5.29 both hold.

We can easily prove that \(\xi_{\text{async}}^i, \xi_{\text{async}}^i,\) and \(\xi_{\text{async}}^i, \xi_{\text{async}}^0,\) and \(\xi_{\text{async}}^i, \xi_{\text{async}}^0\) are semi-commutativities. By Definition 8.5.31, \(G_{\text{assign}}\) is commutative, thus \(G_{\text{assign}}\) is asynchronous by Propositions 8.5.34 and 8.5.25. ■
References


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


268
REFERENCES


REFERENCES


REFERENCES


271
REFERENCES


