

Fakultät II: Informatik, Wirtschafts- und Rechtswissenschaften

Department für Informatik

Abteilung: Entwicklung korrekter Systeme

Transformational semantics of the combination π -*OZ* for mobile processes with data

Masterarbeit

- *post version* -

Name: Muhammad Ekbal Ahmad
E-Mail: muhammad.ekbal.ahmad@uni-oldenburg.de

Studiengang: Fach-Master Informatik
Erstgutachter: Prof. Dr. Ernst-Rüdiger Olderog
Zweitgutachter: M.Sc. Manuel Giesekeing
Datum: 19. Januar 2020

Contents

List of Figures	V
1 Introduction	1
2 Preliminaries	3
2.1 The π -calculus	3
2.1.1 Intuition	3
2.1.2 Syntax	4
2.1.3 Semantics	7
2.2 The OZ	9
3 Conclusion and future work	11
Bibliography	13

List of Figures

2.1	The <i>transition rules</i> [Mil99].	8
2.2	The <i>inference tree</i> [Mil99].	8

1 Introduction

In many cases of modern computing it is of interest to describe and model concurrency. Computers no longer just solve a problem by subsequently working off the single tasks of their own, but they decompose and concurrently calculate the problem even together in a network. The increase in the number of CPU cores and more heavily of GPU cores within one single computer convincingly demonstrates how fundamental concurrency is for modern computing. Moreover, the rapidly increasing spread of the Internet is one of the most common examples which shows the importance of networks.

This thesis is divided into five chapters. In Chapter 2 we briefly introduce sequences and properly investigate the π -calculus and its operational semantics (the *early transition system* [SW01]). Thereby, we investigate its properties and define the refinement based on the trace semantics. Finally, the conclusion in Chapter 3 gives a brief summary of our results and presents ideas for future work.

2 Preliminaries

At the heart of the refinement of π -calculus processes is the theory of *sequences*. Thus, in this chapter, we recall the model of sequences to gain a formal construct to handle ordered elements.

Furthermore, we introduce the π -calculus and investigate its behavior properly. In particular, we carefully explain the operational semantics of π -calculus processes, since its peculiarities induce the characteristics of the refinement and its properties. Moreover, we discuss why we choose this particular operational semantics for the following work in this thesis and compare it to other semantics.

The majority of those definitions and notions can, for example, be found in [Mil99, SW01].

As mathematical notations, we consider the natural numbers starting with zero ($\mathbb{N} = \{0, 1, 2, \dots\}$) and use \circ as the composition of relations. Furthermore, we denote R^* as the reflexive and transitive closure of a relation R .

2.1 The π -calculus

The π -calculus is a process algebra that can be used to describe the behavior. This section introduces the pure polyadic version of the π -calculus as depicted in [Mil99].

2.1.1 Intuition

To explain the π -calculus intuitively we will use the ion example as in [Mil99]. Let us imagine a positive and a negative ion. When those two ions merge, we get a new construct. The merge operation is called a *reaction*, since an ion acts and the other reacts. This reaction can be seen as communication between two processes. The two processes communicate to share some information. One process is the sender and the other is the receiver. By doing the reaction both processes evolve to something new. The reaction, information sharing and evolution concepts are the core of the π -calculus. Using those concepts we can understand the title of

Milner's book *communicating and mobile processes: the π -calculus* [Mil99]. The word *communicating* refers to the *reaction* concept. The word *mobile* refers to the *information sharing and evolution* concepts, since the receiver process can use the received information to change its location as we will see in .. .

The π -calculus consists of:

- a set of names starting with capital case letters like P, P_1, Q, \dots etc used to refer to a process directly.
- a set of names starting with capital case letters like A, B, C, \dots etc used as a process identifier. The process identifier will be used to define recursion with parameters.
- a set of names starting with lower case letter like a, b, x, y, \dots etc used as a channel and message name. This set is denoted by \mathcal{N} .
- operators like:
 - Parallel composition operator: “ $|$ ”.
 - Sequential composition operator: “ $.$ ”.
 - Choice operator: “ $+$ ”.
 - Scope restriction operator: “ new ”.

So a simple example of a process can be: $\bar{x}\langle y \rangle.0$ this process simply sends the message y via the channel x and stops. The full syntax of π -calculus process is given in Definition 2.1.1. In this thesis starting from this point, when we mention the word *names* we refer to \mathcal{N} . Furthermore, we shall often write \vec{y} for a sequence y_1, \dots, y_n of names.

2.1.2 Syntax

Definition 2.1.1 (Process syntax) The syntax of a π -calculus process P is defined by:

$$P ::= \sum_{i \in I} \pi_i.P_i \mid P_1 \mid P_2 \mid \text{new } \vec{y} P \mid A\langle \vec{v} \rangle$$

where:

- $\sum_{i \in I} \pi_i.P_i$ is the guarded sum.

- $P_1 \mid P_2$ is the parallel composition of processes.
- $\text{new } \vec{y} P$ is the restriction of the scope of the names \vec{y} to the process P
- $A(\vec{v})$ is a process call. *

Guarded sum:

Is the *choice* between multiple guarded processes. If the guard of one process took place, other guarded processes will be discarded. For example, the processes: $x().P_1 + y().P_2$ will evolve to the process P_1 if the guard $x()$ occurred.

Furthermore, The process $\mathbf{0}$ is called the *stop process* or *inaction* and stands for the process that can do nothing. It can be omitted.

Guard:

Also called *action prefix* and denoted by π . It's syntax is defined by:

Definition 2.1.2 (Action prefix syntax)

$$\pi ::= \bar{x}(\vec{y}) \mid x(\vec{y}) \mid \tau$$

where:

- $\bar{x}(\vec{y})$ ¹ represents the action: send \vec{y} via the channel x .
- $x(\vec{y})$ ² represents the action: receive \vec{y} via the channel x .
- τ represents an internal non observable action. *

The set of all *actions* is defined as $\mathbf{Act} =_{\text{def}} \mathbf{Out} \cup \mathbf{In} \cup \{\tau\}$, where:

- \mathbf{Out} is the set of all *output actions*, defined as $\mathbf{Out} =_{\text{def}} \{\bar{x}(\vec{y}) \mid x \in \mathcal{N}\}$.
- \mathbf{In} is the set of all *input actions*, defined as $\mathbf{In} =_{\text{def}} \{x(\vec{y}) \mid x \in \mathcal{N}\}$.

¹ $\bar{x}(\vec{y})$ means: send a signal via x . $\bar{x}(y)$ means: send the name y via x . $\bar{x}(\vec{y})$ means: send the sequence \vec{y} via x .

² $x()$ means: receive a signal via x . $x(y)$ means: receive any name y via x . $x(\vec{y})$ means: receive any sequence \vec{y} via x . “ y here plays the role of parameter”

Parallel composition:

The parallel composition operator $|$ represent the concept of concurrency in the π -calculus, where two processes can evolve in concurrent. It represents an interleaving behavior of the concurrency. For example let: $P =_{\text{def}} P_1 | (P_2 | P_3)$ where: $P_1 =_{\text{def}} x(y).Q_1$, $P_2 =_{\text{def}} \bar{x}(y).Q_2$ and $P_3 =_{\text{def}} x(y).Q_3$. So $P =_{\text{def}} x(y).Q_1 | (\bar{x}(y).Q_2 | x(y).Q_3)$. Possible evolution cases of P are:

- $P_1 | (Q_2 | Q_3)$. P_2 sends y via x to P_3 .
- $Q_1 | (Q_2 | P_3)$. P_2 sends y via x to P_1 .

The example above illustrated the privacy nature of the parallel operator in the π -calculus. A process can via a channel communicate with only one process pro time. P_2 cannot communicate with both P_1 , P_3 in the same time, while in Communicating Sequential Processes (CSP) a process can communicate with multiple processes in the same time via the same channel by sending multiple copies of the same message, in other words: in CSP the channel represents a Hub.

Restriction:

The expression $\text{new } \vec{y} P$ binds the names \vec{y} to the process P . In other words: the visibility scope of the names \vec{y} is restricted to the process P . It is similar to declaring a private variable in programming languages. Thus the names \vec{y} are not visible outside P and P cannot use them to communicate with outside. For example, let $P =_{\text{def}} P_1 | P_2$ where: $P_1 =_{\text{def}} \text{new } y \bar{y}(z).Q_1$ and $P_2 =_{\text{def}} y(z).Q_2$. The process P cannot evolve to $Q_1 | Q_2$, since the name y in P_1 is only visible inside it, i.e., from the P_2 's point of view P_1 doesn't have a channel called y . This takes us to the definition of the Bound and free names.

Definition 2.1.3 (Free names) are all the restricted names in a process. *

Definition 2.1.4 (Bound names) are all the name that occur in a process except the bound names. *

For example, let $P_1 =_{\text{def}} \text{new } x \bar{x}(y).P_2$ where $P_2 =_{\text{def}} \text{new } z \bar{x}(z).P_3$. The name x is bound in P_1 but free in P_2 .

Process call:

Let P be a process and let A be a process identifier. To be able to use the process P recursively we use the process identifier A as follow: $A(\vec{w}) =_{\text{def}} P$. Thus, when we write $A(\vec{v})$ we are using the identifier A to call the process P with replacing the names \vec{w} in P with the names \vec{v} . This replacement is called the α -conversion

For example, let $P =_{\text{def}} \bar{w}\langle y \rangle.0$ and let $A(w) =_{\text{def}} P$ be the recursive definition of the process P , then the behavior of $A\langle v \rangle$ is equivalent to $\bar{v}\langle y \rangle.0$

2.1.3 Semantics

To understand the operational semantics of π -calculus we will use a labelled transition system LTS. Using this LTS we can investigate π -calculus process evolution. The definition of LTS is adapted from [Mil99] pages 39³, 91⁴, 132⁵ with some changes.

Definition

Definition 2.1.5 (The LTS of π -calculus) The labelled transition system $(\mathcal{P}^\pi, \mathcal{T})$ of π -calculus processes over the action set Act has the process expressions \mathcal{P}^π as its states, and its transitions \mathcal{T} are those which can be inferred from the rules in Figure 2.1. The rule REACT is the most important one. It shows the process evolution when a reaction occurs. The reaction requires two complementary transitions $P \xrightarrow{\bar{x}\langle y \rangle} P'$ and $Q \xrightarrow{x\langle z \rangle} Q'$, we call them commitments. so the process P takes a commitment to take part in the reaction, and so does Q .

³Transition Rules: LTS for concurrent processes not for π -calculus processes.

⁴Reaction Rules: no labels and no LTS.

⁵Commitment Rules: abstractions and concretions are out of this thesis's scope.

$$\begin{aligned}
\underline{OUT} : \bar{x}(\vec{y}).P &\xrightarrow{\bar{x}(\vec{y})} P & \underline{IN} : x(\vec{y}).P &\xrightarrow{x(\vec{y})} P \\
\\
\underline{TAU} : \tau.P &\xrightarrow{\tau} P & \underline{SUM} : \alpha.P + \sum_{i \in I} \pi_i.P_i &\xrightarrow{\alpha} P \\
\\
\underline{L_PAR} : \frac{P \xrightarrow{\alpha} P'}{P \mid Q \xrightarrow{\alpha} P' \mid Q} & \underline{R_PAR} : \frac{Q \xrightarrow{\alpha} Q'}{P \mid Q \xrightarrow{\alpha} P \mid Q'} \\
\\
\underline{RESTRICTION} : \frac{P \xrightarrow{\alpha} P'}{\mathbf{new} \, x \, P \xrightarrow{\alpha} \mathbf{new} \, x \, P'} & \text{if } \alpha \notin \{\bar{x}, x\} \\
\\
\underline{PROCESS_CALL} : \frac{\{\bar{y}/\bar{z}\} P \xrightarrow{\alpha} P'}{A(\vec{y}) \xrightarrow{\alpha} P'} & \text{if } A(\vec{z}) =_{\text{def}} P \\
\\
\underline{REACT} : \frac{P \xrightarrow{\bar{x}(\vec{y})} P' \quad Q \xrightarrow{x(\vec{z})} Q'}{P \mid Q \xrightarrow{\tau} P' \mid \{\bar{y}/\bar{z}\} Q'} & *
\end{aligned}$$

Figure 2.1: The *transition rules* [Mil99].

An example of using the transition rules of this LTS to infer a transition: Let $P =_{\text{def}} \mathbf{new} \, x \, (A\langle x \rangle \mid B\langle x \rangle)$ where: $A(y) =_{\text{def}} \bar{y}().A'\langle y \rangle$ and $B(z) =_{\text{def}} z().B'\langle z \rangle$. the process P can do the transition $\mathbf{new} \, x \, (A\langle x \rangle \mid B\langle x \rangle) \xrightarrow{\tau} \mathbf{new} \, x \, (A'\langle x \rangle \mid B'\langle x \rangle)$, which is a reaction. The inference tree of this transition is shown in Figure 2.2. Thus, using the LTS we can enumerate all possible transitions of a π -calculus process.

$$\begin{array}{c}
\frac{}{\bar{x}().A' \xrightarrow{\bar{x}()} A'\langle x \rangle} \text{ by OUT} \qquad \frac{}{x().B' \xrightarrow{x()} B'\langle x \rangle} \text{ by IN} \\
\frac{}{A\langle x \rangle \xrightarrow{\bar{x}()} A'\langle x \rangle} \text{ by PROCESS CALL} \qquad \frac{}{B\langle x \rangle \xrightarrow{x()} B'\langle x \rangle} \text{ by PROCESS CALL} \\
\frac{}{A\langle x \rangle \mid B\langle x \rangle \xrightarrow{\tau} A'\langle x \rangle \mid B'\langle x \rangle} \text{ by REACT} \\
\frac{}{\mathbf{new} \, x \, (A\langle x \rangle \mid B\langle x \rangle) \xrightarrow{\tau} \mathbf{new} \, x \, (A'\langle x \rangle \mid B'\langle x \rangle)} \text{ by RESTRICTION}
\end{array}$$

Figure 2.2: The *inference tree* [Mil99].

2.2 The OZ

The OZ

3 Conclusion and future work

In this thesis ...

Bibliography

- [Mil99] R. Milner. *Communicating and Mobile Systems: the π -Calculus*. Cambridge University Press, Cambridge, England, 1999.
- [SW01] D. Sangiorgi and D. Walker. *The π -calculus: a Theory of Mobile Processes*. Cambridge University Press, Cambridge, England, 2001.

Index

Symbols

α -convertibility	13 f
α -convertible	14
τ process	10
π -calculus	5, 7 – 29
monadic	8
polyadic	8

A

action	9, 20
bound output	20
input	10, 20
internal	10
observable	9
output	10, 20
silent	10
unobservable	10
application substitution	
process	13
trace	41

B

big-step semantics	38
binding function	40
bisimulation	
strong	32
weak	32
bound name	12
action	20
process	12
trace	39
bound output action	20
bound substitution	46

C

call	11
------	----

channel	8
choice	10
co-names	8
co-support	13
commitments	33
concatenation	6
congruence relation	13
conjugation	20

D

denotational semantics	49
------------------------	----

E

early instantiation	20, 33
early transition system	20 f, 34
empty sequence	6
empty trace	37
equivalence relation	13
extended standard form	16

F

free name	12
action	20
process	12
trace	39

G

guarded choice	8, 10
----------------	-------

I

inaction	9
indexed trace set	50
inductive parallel composition	59
input	
action	20

prefix	9
process	10
input-/output experiments	33
instantiation	
early	20, 33
late	33
internal action	10
invisible big-step	38
iteration	6

K

Kleene star	6
-------------------	---

L

late instantiation	33
late transition system	34
length of a sequence	6

M

message	8
monadic π -calculus	8

N

name	8
bound	12, 20
free	12, 20
process	12
restricted	10
substitution	13
trace	39

O

object	8, 10, 38
observable action	9
operational semantics	19
output	
action	20
prefix	8
process	10

P

parallel composition	10
----------------------------	----

parameter	10
polyadic π -calculus	8
prefix	8
input	9
operator	6
output	8
process	9
silent	9
process	9
τ	10
algebra	1, 7
call	11
choice	10
congruence	13
identifier	9
input	10
output	10
parallel	10
prefix	9
restriction	10
stop	9

R

recursion-free	11
recursive definition	9
refinement	77
restricted name	10
restriction	10
restriction set	67 f
restriction-free	11

S

scope extrusion	10, 15
semantics	
denotational	49
operational	19
sequence	5
concatenation	6
empty	6
iteration	6
length	6
silent	
action	10

prefix	9
simulation	
strong	32
weak	32
standard form	16
extended	16
stop process	9
strong	
bisimilar	32
bisimulation	32
simulation	32
structural congruence	15
subject	10, 38
substitution	12
action	20
co-support	13
injective on set	26
process	13
support	13
trace	41
sum	9
summation	9
support	13

T

trace	37
equivalent	77
refinement	77
semantics	49
transition system	
early	20 f
late	34
transposition	13

U

uniqueness of bound names	
process	14
trace	46
unobservable action	10

V

visible big-step	38
------------------------	----

W

weak	
bisimilar	32
bisimulation	32
processes set	75
simulation	32

Erklärung

Hiermit versichere ich, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Außerdem versichere ich, dass ich die allgemeinen Prinzipien wissenschaftlicher Arbeit und Veröffentlichung, wie sie in den Leitlinien guter wissenschaftlicher Praxis der Carl von Ossietzky Universität Oldenburg festgelegt sind, befolgt habe.

Oldenburg, den 19. Januar 2020

(Muhammad Ekbal Ahmad)