The π-calculus

A Thesis
Presented to
The Division of Mathematics and Natural Sciences
Reed College

In Partial Fulfillment
of the Requirements for the Degree
Bachelor of Arts

William Henderson

May 2008

Approved for the Division
(Mathematics)

James Fix

Table of Contents

Acknowledgments

I want to thank my hamsters, Boris Becker, and this bottle of Merlot.

A Word About Formatting

One of the pedagogical aims of this thesis is to be as clear and reader-assistive as possible during its presentation. To that end, I have taken several liberties in the formatting of this thesis. Figures, equations, definitions, theorems and examples all share one numbering scheme in hopes that it will make them easier to locate. Where *definitions* appear, they are clad in italics as well as in a margin box to make them easier to find. Equation numbers also appear in margin boxes. When definitions or equations are referred to later in the text, an assistive link will appear in the margin to avoid index-fingering. To this end, the wired reader will note the presence within the backcover of a searchable pdf version of the text, wherein all references are hyper-textual (clickable). The included CD also contains all the code referenced in this thesis.

definitions

definitions
↪ page iii

Abstract

In this thesis I will blow your mind, and possibly (hopefully?) my own in the process.

1 Introduction

Computer Scientists have long been interested in algebraic models that are capable of describing computation by formulating a 'program' as an algebraic expression along with a set of rules for reducing such expressions - i.e. 'running' them. The advantage of such algebras is that they can be studied using formal reasoning techniques. This means that we can rigorously prove things about them and derive useful observations 'programming' in them without actually ever having to implement them on a system. Of course, these algebras often are used in real languages whether faithfully or in part, but this is usually after they have been studied in detail for some time and we can be sure of their value.

In the 1930's, Alonzo Church and Stephen Kleene introduced one such algebra, known as the λ-calculus. In the λ-calculus, we can write programs as expressions that are a series of nested functions, and we can run these programs by invoking the functions within. A function is indicated by the λ symbol, followed by a single variable representing its input. For example, the following is a very simple 'successor' program that takes in a number x and adds 1 to it, returning the result:

$$(\lambda x.x + 1)$$

To run this program, we need to actually apply it to something - that is, we need to give it input. We express this by placing the input to the right of the function, as in:

$$(\lambda x.x + 1)4$$

The above program first substitutes 4 in for the input x, yielding 4+1. The program then returns the result, 5. Since we can nest functions, a slightly more complicated version adds 1 to the input 4 and then multiplies the result by 3. We give this program with each computational 'step' below:

$$\begin{aligned}(\lambda y.y * 3)((\lambda x.x + 1)4)\\(\lambda y.y * 3)(4 + 1)\\(\lambda y.y * 3)5\\5 * 3\\15\end{aligned}$$

You are probably already getting a sense of the expressive power of the λ-calculus. In fact, it is capable of expressing *any* computer algorithm, even without the numbers and arithmetic operators we have implicitly included above! Besides allowing

the proof of several important results in computer science, the λ-calculus went on to inspire many programming languages like Lisp, ML and Haskell, and even some functionality in languages like Smalltalk, Ruby and Python.

However, the discovery of the λ-calculus did not end the search for new algebra. More recently, new kinds of programs and demands have emerged with the computational platform of *distributed systems*. These systems consist of loose networks of machines capable of exchanging messages and information. We say this shared information and computational power belongs to 'the system' in that any program running on the machines of the system can freely access these resources and generally behaves just as it would running on a single machine.

distributed systems

For example, consider the familiar system that powers your mobile phone network. There may be one or more connected central servers, all of which are connected to the various towers that provide service. Towers and servers may have different capabilities and responsibilities, but the important thing is that the entire system needs to behave as a single unit with a bunch of shared information and computational power. A call in progress, for example, is a resource that will need to be accessed in various places in the system - by a tower to handle the call, by a server, perhaps, to handle the billing and routing of that call.

Mobile clients are also connected and a part of this system. When a user places a call, for example, he may use some capabilities on the phone to input the number, which is transmitted by the phone to the tower and then sent to the server to be routed. This entire 'program' for making a call is one seamless operation that is happening across several machines.

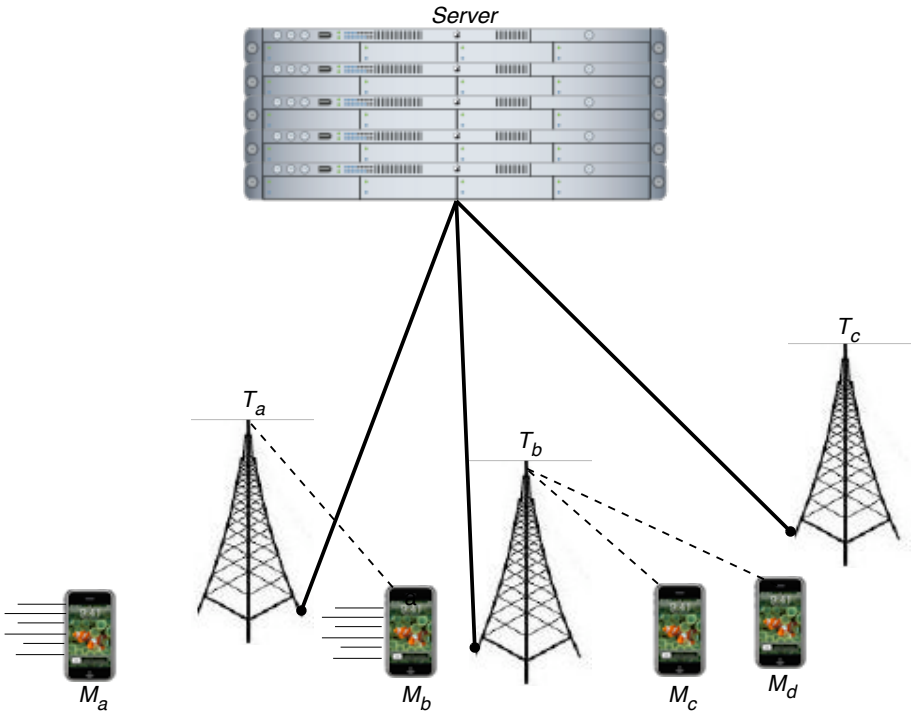

Figure 1.0.1: A Distributed Mobile System

The demands of a distributed system strain the expressive power of the λ-calculus. Since the λ-calculus models all computation via functions, our only means of modeling a resource is as a function. Functions can only be accessed directly – input can be passed to a function only by directly applying the function to that input. But if we want access to a resource on a system, we might not know where it is or what it is doing. Furthermore, our system of many machines could be doing many different things at once: routing calls, handling other calls in session, calculating a bill. Yet the λ-calculus has no means of easily expressing this concurrency which is so basic to many distributed systems.

Consider the phones on our system. They are*mobile* - in the sense that their connections to the system can be added and removed at any time. In Figure 1.0.1 above, client M_b is wirelessly connected to tower T_a while M_c, M_d are connected to T_b. Client M_a is currently disconnected and T_c has no clients. All the towers maintain a hard-wired link to *server*. We refer to the connections in a distributed system as its communication *topology*.

mobility

topology

Furthermore, M_a and M_b are in physical movement and their connections may change soon. M_b might, for example, go out of range and disconnect from T_a and connect to T_b instead. Such changing communication topologies present even more difficulties to the λ-calculus. How can we abstract function invocation such that a function can be called from one place at one time, and another place later? Even if we could somehow invoke a function indirectly, how could we deal with the fact that a function (say a client's ability to receive a call) is not currently available?

Clearly we need an algebraic model for computation that eases the difficulty of modeling such systems. Such a model might consider computation via its natural distributed unit - the *process*. A process is just a computational task, without reference to where it might be run nor with what input. For example, we might make a conversation on a phone somewhere in our network a process. Since concurrency of processes is such a basic operation, we make it a part of our algebra. A system, then, is simply a group of processes which are executing concurrently. An important thing about processes is that they maintain computation state independently of one another. Instead of a single program state where functions interact via invocation, processes run independently and interact via *message passing* – sending data back-and-forth via named channels.

process

message passing

Because these channels can be shared among processes and used an arbitrary number of times, channels are not a concrete invocation system for a chunk of computation the way a function call is - processes simply send values to channels, assuming the receiver (if there is one) will do something useful with it. As with functions in the λ-calculus, processes are the basic unit of a program in the π-calculus. Any bit of functionality can be referred to as a process, with no specification of the granularity.

A major step towards such an algebra came in the 1980's when Robin Milner introduced his Calculus of Communicating Systems (CCS). The CCS modeled systems as groups of communicating processes interacting via shared channels, and drastically eased the difficulty of modeling indirectly invoked concurrent operations. However, the CCS still would have had trouble with our mobile phone network, because it did not provide a way for processes to gain and lose their communication channels.

(section header?)

Although it can be defined in other ways, one of the ways of giving a process's *location* is in terms of the communication channels which can be used to access it. Since processes are the units populating the space of a CCS system, it is natural to think of a process's location in terms of the processes which are 'near' it - those it can connect to. Since communicate happens via channels, a connection between processes just means that they share at least one channel. In this way, changing the communication channel topology of a system changes the locations of its component processes.

In the CCS, channel topology is static - it does not allow new connections to be made or old ones to be removed. Not long after CCS's birth, Robin Milner, Joachim Parrow and David Walker created an improved algebra called the π-calculus. The π-calculus allows communication channels to be dynamically established and relinquished between processes. Since channels are what define location, dynamically created and destroyed channels give a kind of *mobility* of processes, which vastly expands the capabilities of interaction in a system and finally allows us to give an account of our mobile phone system.

As an example of how naturally the π-calculus models distributed systems, let us again consider our mobile phone network[1]. Our system will be simplified a bit: only two towers and one phone, with the only system functionality being talking on the phone or switching from one tower to another.

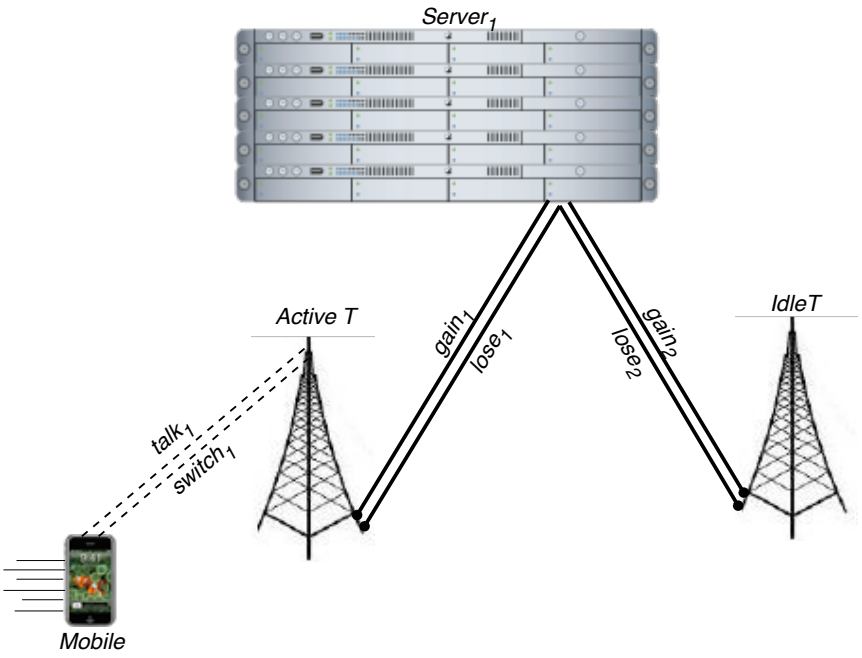

Figure 1.0.2: Simplified Mobile Phone Network in the π-calculus

[1]This presentation is adapted from a version first given in [Mil99]

First we give a process describing the behavior of a mobile phone:

$$Mobile(talk, switch) \Leftarrow talk!\langle\rangle.Mobile(talk, switch) + switch?(t, s).Mobile(t, s)$$

Above, we use $\Leftarrow$ to mean that the term to the right of the $\Leftarrow$ is given the shorthand $Mobile$ and that it uses the channels $talk$ and $switch$ given elsewhere. The channels given in the parentheses are simply substituted into the term on the right's corresponding channels. Hence, for example, $Mobile(t, s)$ would be this right-hand term with the channels t and s substituted for $talk$ and $switch$. We call $Mobile(t, s)$ the *interface* of the right-hand term.

interface

The notation $talk!\langle\rangle$ means that we are sending an 'empty' (since there are no input values given in the brackets) signal on channel $talk$, while $switch?(t, s)$ means we are listening on $switch$ and receive the input t, s. After a signal is sent or received on a channel, execution then continues with the term immediately to the right of the term, using the input provided (if any).

Thus, $switch?(t, s).Mobile(t, s)$ indicates that we should listen on $switch$ for the input t, s and then use t, s to 'spawn' a new computation of $Mobile$ with these new channels. The term $talk!\langle\rangle.Mobile(talk, switch)$ means send a signal on $talk$ before spawning a computation of $Mobile$ with the same $talk, switch$ channels we are using. Finally, the + operator denotes that we should choose to compute one or the other of the operands (but not both). In sum then, *mobile* has the ability to either send along $talk$ and stay in its current location, or it can receive on $switch$ and 'move' to the location where it has new talking and switching channels t, s. This last capability expresses the mobile nature of our processes with surprising elegance: here we have just expressed that channels $talk, switch$ are lost and new channels t, s are established.

Next we consider the behavior of a tower:

$$\begin{aligned} ActiveT(talk, switch, gain, lose) \Leftarrow\ & talk?().ActiveT(talk, switch, gain, lose) \\ & + lose?(t, s).switch!\langle t, s\rangle.IdleT(gain, lose) \\ IdleT(gain, lose) \Leftarrow\ & gain?(t, s).ActiveT(t, s, gain, lose) \end{aligned}$$

Here, the are two 'states' our tower can be in. It can be active in talking with a mobile phone, or it can be disconnected and idle. If it is active, it can either receive on $talk$ (from the phone) and continue to be active, or it can receive on $lose$ (from the server, as we shall see below). In the latter case it then sends t, s on $switch$ before becoming idle. That is, it will receive some new channels t, s on $lose$ and then send them to the phone on $switch$ before becoming idle. An idle tower has only one capability: to receive on $gain$ and then become active again on the new channels t, s.

Finally we give the behavior of the server:

$$\begin{aligned} Server_1 &\Leftarrow lose_1!\langle talk_2, switch_2\rangle.gain_2!\langle talk_2, switch_2\rangle.Server_2 \\ Server_2 &\Leftarrow lose_2!\langle talk_1, switch_1\rangle.gain_1!\langle talk_1, switch_1\rangle.Server_1 \end{aligned}$$

Above, the server has two states: it can be controlling tower 1 or it can be controlling tower 2. In either case, the only capability is to lose one tower and gain the other

before going into the opposite state. Hence, in $Server_1$ we can send to the first tower on $lose_1$ and then to the second tower on $gain_2$ before entering state $Server_2$.

We have now completely described the components of our system, but we still haven't put them all together. To do so, we'll need a new operator. This operator denotes that its operands run concurrently in parallel and is denoted $|$. Thus, our system is simply:

$$Mobile(talk_1, switch_1)|ActiveT_1(talk_1, switch_1, gain_1, lose_1)|IdleT(gain_2, lose_2)|Server_1$$

Now that we have gotten a taste of the power of the π-calculus, we are ready to explore it in more detail. However, our first pass at the π-calculus will not include some of the operators included in our mobile phone network example. For one, it will not include the + operator. We will also use a version of sending that is a little simpler than the one we've seen so far. More specifically, our first calculus will be *asynchronous*, meaning that processes will not continue on with any computation after sending on a channel. That is, in a process like

asynchronous

$$c!\langle\rangle.P,$$

we will disallow the presence of P – the process will simply terminate after sending on c. In Chapter 2, we will give a rigorous presentation of the semantics of this asynchronous π-calculus and the rules describing they way computation happens.

The two simplifications mentioned above will make our calculus somewhat easier to grasp, but there is another reason to consider an asynchronous calculus: it is far easier to implement on a real distributed system than the full synchronous version. At the base level, communication between machines on a distributed system is asynchronous, so implementing synchronous calculi requires finding a way to simulate synchronous message passing using only asynchronous primitives. In Chapter 3, after briefly presenting the *synchronous* π-calculus(which has the full expressive power used in the mobile phone network example) and its computational rules, we will look at the problem of modeling the synchronous π-calculus using the asynchronous version.

synchronous

Having looked at this problem, we will take a practical-minded look at the way that a synchronous π-calculus-like language might be implemented on a system using asynchronous primitive π-calculus constructs. Chapter 4 is a brief survey of some of the approaches that have been suggested or used to implement such a language, and how they bear on the results of Chapter 3.

2
The π-Calculus

In this chapter, we will give the syntax of the *asynchronous* π-calculus and a discussion of its features. We will loosely follow the style of a recent presentation given in [Hen07]. Following this, we will introduce a notion of equivalence of terms in the language. Finally, we will give some semantic reduction rules that provide computational behavior via steps of reduction.

2.1 Syntax

The terms of the π-calculus operate on a space of *identifiers* which consists of names $a, b, c, ..., n, m, o$ for communication channels, and variables v, w, x which can refer to channels, and recursive variables p, q, r, explained in more detail below. In general, we will use capital letter to denote a process.

identifiers

	Process terms	
$R :=$	$R_1 \mid R_2$	Composition
	$n!\langle\overline{V}\rangle$	Send
	$n?(\overline{X}).R$	Receive
	$\text{new}(n).R$	Restriction
	if $v_1 = v_2$ then R_1 else R_2	Matching
	rec $p.R$	Recursion
	stop	Termination
	System	
	$\text{new}(c_1, ..., c_n).R_1 \mid ... \mid R_m$	$n, m >= 0$

Figure 2.1.1: Terms in the asynchronous π-calculus

TODO: Get index up to snuff by making sure more terms are margin defined.

Given two or more processes, we can compose them using the $\mid$ operator, which means that the composed processes will be executed concurrently.

We denote the sending of a message $\overline{V}$ over a channel n by $n!\langle\overline{V}\rangle$. Here $\overline{V}$ is a tuple of identifiers in the form $\overline{V} = (v_1, ..., v_k) : k \geq 0$. We say that $\overline{V}$ has *arity* k. In the case $k = 0$ nothing is being transmitted; the communication acts as a *handshake* or signal. We will denote this case by $n!\langle\rangle$. When $k = 0$, only a single value v_1 is being transmitted, in which case we write $n!\langle v_1\rangle$. Because our calculus is asynchronous,

arity

handshake

guarded

sending is not a *guarded* operation – that is, a send operation does not continue to execute any process after sending its value, but simply terminates after sending the value. We will show in Example 2.1.9 that synchronous behavior can still be modeled in our language.

patterns

The term $n?(\overline{X}).R$ describes a process waiting to receive a tuple along n before continuing with R. Here $\overline{X}$ is a *pattern* – a tuple of variables of arity k – which can be used anywhere in R. Patterns allow us to decompose the transmitted tuple into its component values by naming them with $x_1, ..., x_k$, which can be referred to in R. Thus, in the term

$$c!\langle n_1, n_2, n_3\rangle \mid c?(x_1, x_2, x_3).R, \tag{2.1.2}$$

the names n_1, n_2, n_3 are received via c and correspond to the variables x_1, x_2, x_3 in the pattern. Hence, the variables x_1, x_2, x_3 can be used anywhere within the process R to mean n_1, n_2, n_3.

Similarly to sending, the case of arity 0 is denoted $n?().R$ – here R will not happen until a handshake is received on n. Notice that in contrast to the case of sending, receiving is a guarded operation – that is, the process R will execute after $\overline{X}$ has been received via n. For example, the term

$$c?().stop \tag{2.1.3}$$

represents a 'listener' process that simply consumes the value waiting on input channel c. The term *stop* describes a process that does nothing but halt.

scope

The term $\text{new}(n).R$ describes a process in which a new channel name n is created and limited to being expressed in the process R (we say the *scope* of n is *restricted* to R). We shall see that scope plays a very big role in the way processes can establish new connections. Essentially, for a process P to have a connection to another process R really means that they both 'know' about a common channel c. In that case, c is scoped P and R. Hence, $\text{new}(n).R$ really means that we have created a channel n that – for the time being – only process R knows about. It is important to note that n *can* be used outside of R if it is sent and then received by some outside process.

scope extrusion

This feature is known as *scope extrusion*, and is the underpinning for the dynamic communication topologies introduced in the π-calculus. For example, in the term

$$\text{new}(n).(c!\langle n\rangle) \mid c?(x).x!\langle\rangle, \tag{2.1.4}$$

we have a channel n scoped to the left hand process which is sending n over c. The right hand process then receives n over c (referred to by x) and then sends an empty signal over n. At the time of its creation, n's scope is just the left half of the term. However, after n is received in the right hand process it will be able to be referred to outside of its initial scope. We will give a precise account of how this happens in our reduction rules and Example 2.3.2 below.

We will sometimes abbreviate terms that use multiple channel restrictions by writing $\text{new}(n, m).R$ to denote the term $\text{new}(n).(\text{new}(m).R)$.

Simple conditional execution based on value equality comparison is available through the use of if $v_1 = v_2$ then R_1 else R_2. For example, in the following term,

the value received on c is checked; if it matches a then a handshake is sent along a (which is referred to by x), otherwise the process terminates.

$$c?(x).(\text{if } x = a \text{ then } x!\langle\rangle \text{ else } \mathit{stop}) \tag{2.1.5}$$

Recursion is built into the language using the syntax rec $p.R$. The process rec $p.R$ itself is referred to by to the variable p, which is used somewhere in R to express a recursive call. For example, consider the recursive responder term below, which receives a channel x_1 via c. It then sends a handshake response on x_1, while another responder process is run in parallel.

$$\text{rec } p.c?(x_1).(x_1!\langle\rangle \mid p) \tag{2.1.6}$$

The variable p's scope is restricted R, just as X is restricted to R in $c?(X).R$ and n is restricted to R in $\text{new}(n).R$.

We call a collection of parallel processes communicating over shared channels a *system*. Note that a system is itself a process. Our choice to define it is somewhat auxiliary to the π-calculus itself, but it is helpful to understanding the way that behavior can be modeled using processes as atoms of a system.

Example 2.1.7 Many presentations (including our own in the next chapter) of the π-calculus involve a choice or summation operator as in $P+Q$ for two processes terms P and Q. The meaning is essentially that either P or Q can be non-deterministically executed, and the other process will not be. However, we can model the same behavior without defining a choice operator:

$$c!\langle\rangle \mid c?().P \mid c?().Q \tag{2.1.8}$$

In the above process, either Q or P (but not both) could be executed. This is due to the asynchronous behavior of our language – sending an empty signal along c, we cannot control which process consumes the signal (or even if it will be consumed at all). Thus, even without the choice operator our calculus is non-deterministic. ■

Example 2.1.9 Perhaps we are not happy with this asynchronous transmission behavior. Surely we'd like to have blocking sends sometimes, or be able to guarantee that a value is received. Our asynchronous calculus can model synchronous sending by using a private channel that acknowledges when a value is received. To see how, consider the following system:

$$F_1(c) \Leftarrow \text{rec } z.(\text{new}(\mathit{ack}).(c!\langle \mathit{ack}\rangle \mid \mathit{ack}?().(R \mid z))) \tag{2.1.10}$$
$$F_2(c) \Leftarrow \text{rec } q.(c?(\mathit{ack}).(\mathit{ack}!\langle\rangle \mid q)) \tag{2.1.11}$$
$$\mathit{Sys}_1 \Leftarrow \text{new}(d).(F_1(d) \mid F_2(d)) \tag{2.1.12}$$

Above, both F_1 and F_2 have (infinite) recursive behavior, and we can think of Sys_1 as a term that 'kicks off' both of them after creating a shared channel for them to communicate on.

In an iteration of F_1, a new channel *ack* is created for acknowledgement. This channel is sent along c and then F_1 waits for input on *ack* before executing some term R and calling another iteration. F_2 receives *ack* along c and then uses *ack* to send an empty signal to F_1 that it has received input on c.

This is just a toy example: the only thing being communicated is the acknowledgement channel itself. We might imagine a more complex system where F_1 sends more input along c and waits to make sure F_2 receives it. Note that the channel *ack* is only used *once* – we want to ensure that the acknowledgement that F_1 receives is definitely for *that* instance of communication that it just initiated. This allows us to guarantee that F_2 has executed before F_1 continues with R. ■

2.2 Structural Equivalence

A natural question at this point is, given two π-calculus terms, how can we determine if they are equivalent? Intuitively, we want them to be equivalent if they *act* the same, but actually defining this equivalence relation can be a bit subtle. In exploring this issue, we will first look at identifier substitution, giving rules for when we can safely interchange identifiers without creating a different term. Following this, we will develop the notion of *contexts* and then use it to build an equivalence relation among processes.

2.2.1 Identifier Substitution and α-equivalence

As a first step in our notion of equivalence, we might assert that the way identifiers are named shouldn't change how they act. However, this doesn't mean we can start interchanging symbols with carefree abandon. In a component process, some terms might be important for how the process acts in a larger system. For example, if we changed the channel that a mobile phone uses to communicate with a tower, that phone certainly wouldn't act the same – the tower would no longer know how to talk to it. On the other hand, we should be able to change any of the channels that the phone uses to communicate internally with itself without much issue.

bound identifiers

identifiers
↪ page 7

The only identifiers we can safely change in a process without potentially affecting the way it behaves in a larger system are *bound identifiers* . Intuitively, bound identifiers are those which are formally defined within the scope of the process. In a π-calculusterm there are three ways that identifiers can become bound. First, a name n is bound in the process term R to a new channel by the restriction operator as in new$(n).R$. Second, each channel variable x_i in the pattern X is bound in R to some channel v_i from the sending process when matched in a receive expression $c?(X).R$. Finally, the recursive variable x is bound in R to process itself in the recursive expression rec $x.R$. We denote the set of bound identifiers in a term R by $bi(R)$; all those which are not bound we call *free*, denoting them $fi(R)$. Similarly, we denote the set of bound and free names in a term R by $bn(R)$ and $fn(R)$, respectively. We call a term with no free identifiers *closed*.

Jim:
I choose not to give a recursive def'n here...we should talk about how to do this and whether it would be a good thing at this point of the discussion

free identifiers

closed terms

For example, in the term:

$$\text{rec } p.c?(x_1).(x_1!\langle\rangle \mid p), \tag{2.2.1}$$

p is a bound recursive variable, while x_1 is bound by the receive operator. The channel c is free. Now consider the term

$$c!\langle n\rangle \mid \text{new}(n).(\text{rec } p.c?(x_1).(x_1!\langle\rangle \mid p)) \tag{2.2.2}$$

Here x_1, p are bound as before. However, the use of n being sent on c is *not* bound, since it occurs outside the scope of the restriction operator. In fact, the following term (with the restriction operator removed) is equivalent (see Example 2.2.9 for justification).

$$c!\langle n\rangle \mid \text{rec } p.c?(x_1).(x_1!\langle\rangle \mid p) \tag{2.2.3}$$

When a receive term like $c?(X).R$ is executed, we substitute the free variables $\overline{X}$ occurring in R with the values $\overline{V}$ that were received. We denote such substitutions by $R[\![\overline{V}/\overline{X}]\!]$. During the course of a substitution, we might inadvertently 'capture' a bound term. For example, suppose in the following term that some other process sent a channel n over a and that we wanted to perform the substitution $[\![n/x]\!]$ in running $a?(x)$.

$$P(a) \Leftarrow\ a?(x).(\text{new}(n).(n!\langle\rangle \mid x!\langle\rangle)) \tag{2.2.4}$$

The received term n is not the same as the n occurring in $P(a)$ - it was sent by some process outside the scope of the restriction operator new(n). Thus, the problem in performing $[\![n/x]\!]$ is that it would make the free outside name n into the bound name n. We say that running this substitution would *capture* the bound name n. We can avoid this by first replacing the bound n with a new name that is 'fresh' – that is it does not occur elsewhere in the term. For example:

capture

$$P'(a) \Leftarrow\ a?(x).(\text{new}(n').(n'!\langle\rangle \mid c!\langle\rangle)) \tag{2.2.5}$$

We can now safely perform the receive and the corresponding substitution, yielding

$$\text{new}(n').(n'!\langle\rangle \mid n!\langle\rangle) \tag{2.2.6}$$

Obviously we want to say $P(a)$ and $P^{'}(a)$ are equivalent. In general when two terms are the same up to the use of bound identifiers, we say they are α-*equivalent*, and write $P(a) \equiv_\alpha P^{'}(a)$. Thus, when we perform a substitution $R[\![\overline{V}/\overline{X}]\!]$, we pick a term α-equivalent to R where the substitution will not capture terms bound in R. From now on we will intend that a term represents its entire α-equivalency class, and thus will not explicitly specify α-equivalency in the equivalence relation introduced below.

Jim: again, I wanted to check in with you before defining Subst recursively

α-equivalency

2.2.2 Contexts and Equivalence

Perhaps the next idea we might have for building our equivalence relation is that equivalent processes should act the same when dropped into any larger system. Let us define more precisely what we mean by 'dropping in' a process.

Definition 2.2.7 (Context) A context $\mathbb{C}$ is given by:

$$\mathbb{C} := \begin{cases} [\,] & \\ \mathcal{C} \mid Q \text{ or } Q \mid \mathcal{C} & \text{for any process } Q, \text{ context } \mathcal{C} \\ \text{new}(n).\mathcal{C} & \text{for any name } n, \text{ context } \mathcal{C}. \end{cases}$$

$\mathbb{C}[Q]$ denotes the result of replacing the placeholder [ ] in the context $\mathbb{C}$ with the process term Q.

Notice that with contexts, we do not pay any attention to whether a name in Q is bound in $\mathbb{C}$. Hence, unlike with substitution, free variables in Q can become bound in $\mathbb{C}[Q]$. So, for example, channel c in the process $P(c) \Leftarrow c?().R$ can become bound in $\mathbb{C}[P(c)]$ where $\mathbb{C}[]$ is the context

$$\text{new}(c).c!\langle\rangle \mid []$$

contextual

We say that a relation $\sim$ between processes is *contextual* if $P \sim Q$ implies $\mathbb{C}[P] \sim \mathbb{C}[Q]$ for any context $\mathbb{C}$. We are now ready to define our notion of equivalency using contexts.

Definition 2.2.8 (Structural Equivalence) Structural Equivalence, denoted $\equiv$ is the smallest contextual equivalence relation that satisfies the following axioms:

$$\begin{aligned} P \mid Q &\equiv Q \mid P && \text{(S-COMP-COMM)} \\ (P \mid Q) \mid R &\equiv P \mid (Q \mid R) && \text{(S-COMP-ASSOC)} \\ P \mid \text{stop} &\equiv P && \text{(S-COMP-ID)} \\ \text{new}(c).\text{stop} &\equiv \text{stop} && \text{(S-REST-ID)} \\ \text{new}(c).\text{new}(d).P &\equiv \text{new}(d).\text{new}(c).P && \text{(S-REST-COMM)} \\ \text{new}(c).(P \mid Q) &\equiv P \mid \text{new}(c).Q, \text{ if } c \notin fi(P) && \text{(S-REST-COMP)} \end{aligned}$$

These axioms are simply a set of properties that we expect our syntax to obey. The first and second state that composition is commutative and associate. Thus, we will omit parentheses around compositions when our meaning is clear. (S-COMP-ID) states that a terminated process can be eliminated from a composition. (S-REST-ID) states that a channel scope restriction operator can be eliminated when its scope is only over a terminated process. (S-REST-COMP) states that scope ordering does not matter, justifying our shorthand $\text{new}(c, d).P$. The last of these axioms is most important – it is the basis for *scope extrusion*, upon which process mobility is based (as we shall demonstrate in Example 2.3.2 below).

scope extrusion ↪ page 8

mobility ↪ page ??

Example 2.2.9 In our discussion of bound identifiers above, we asserted that we can eliminate a scope restriction operation when none of the scoped identifiers occur in its scope. We can now show why this is permissible:

$$\begin{aligned}
& \text{new}(n,m).(a?(x_1,x_2).x_1!\langle\rangle) \mid \text{rec } x.(a!\langle n,m\rangle \mid x) & \\
\equiv\ & \text{new}(n,m).(a?(x_1,x_2).x_1!\langle\rangle \mid \mathit{stop}) \mid \text{rec } x.(a!\langle n,m\rangle \mid x) & \text{(S-COMP-ID)} \\
\equiv\ & a?(x_1,x_2).x_1!\langle\rangle \mid \text{new}(n,m).(\mathit{stop}) \mid \text{rec } x.(a!\langle n,m\rangle \mid x) & \text{(S-REST-COMP)} \\
\equiv\ & a?(x_1,x_2).x_1!\langle\rangle \mid \mathit{stop} \mid \text{rec } x.(a!\langle n,m\rangle \mid x) & \text{(S-REST-ID)} \\
\equiv\ & a?(x_1,x_2).x_1!\langle\rangle \mid \text{rec } x.(a!\langle n,m\rangle \mid x) & \text{(S-COMP-ID)}
\end{aligned}$$

■

2.3 Reduction Semantics

We are now ready to give the *semantic* properties that a process in our language should possess. By specifying the behavior of processes, we define how computation proceeds in the π-calculus. The set of rules given below show how a process can internally evolve through a number of computation steps.

TODO: make all index terms lowercase

Definition 2.3.1 (Reduction) The *reduction relation* $\longrightarrow$ is the smallest contextual relation that satisfies the following rules:

$$\begin{aligned}
c!\langle\overline{V}\rangle \mid c?(\overline{X}).R &\longrightarrow R[\![\overline{V}/\overline{X}]\!] && \text{(R-COMM)} \\
\text{rec } x.R &\longrightarrow R[\![\text{rec } x.R/x]\!] && \text{(R-REP)} \\
\text{if } v = v \text{ then } P \text{ else } Q &\longrightarrow P && \text{(R-EQ)} \\
\text{if } v_1 = v_2 \text{ then } P \text{ else } Q &\longrightarrow Q \quad (\text{where } v_1 \neq v_2) && \text{(R-NEQ)} \\
\frac{P \equiv P', P \longrightarrow Q, Q \equiv Q'}{P' \longrightarrow Q'} & && \text{(R-STRUC)}
\end{aligned}$$

We use the notation $P \cdots\!\!\longrightarrow Q$ when an arbitrary number of these rules have been applied in reducing P to Q.

The first of these allows a computation step for the transmission of values over a channel.

(R-REP) allows us to unravel a recursive expression into iterations of itself. (R-EQ) enables a computational step for value-matching. Finally, (R-STRUCT) says that a reduction is defined up to structural equivalence.

Example 2.3.2 We will give a demonstration of how scope extrusion is defined using the rules and axioms of reduction and structural equivalence. Consider the expression

$$d?(x).x!\langle\rangle \mid \text{new}(c).(d!\langle c\rangle \mid c?().\mathit{stop}) \tag{2.3.3}$$

We can use (S-REST-COMP) to bring the restriction to the outside, giving:

$$\text{new}(c).(d?(x).x!\langle\rangle \mid d!\langle c\rangle \mid c?().\mathit{stop}) \tag{2.3.4}$$

Thanks to the reduction relation's contextuality, we can use (R-COMM) inside of the restriction operator and apply a substitution. Using this in conjunction with the above structural equality and (R-STRUCT), we get:

$$\text{new}(c).(c!\langle\rangle \mid c?().stop) \tag{2.3.5}$$

Finally, we can apply (R-STRUCT) again, so the process simply reduces to stop.

Now let $P(d)$ to be the right half of our original process, and $\mathbb{C}$ to be the remaining context:

$$P(d) \Leftarrow \text{new}(c).(d!\langle c\rangle \mid c?().stop) \tag{2.3.6}$$

$$\mathbb{C} = d?(x).x!\langle\rangle \mid [\,] \tag{2.3.7}$$

Then we have shown that if we drop $P(d)$ into the context $\mathbb{C}$ (forming $\mathbb{C}[P(d)]$), it will establish a new channel c and extend its scope using d. Hence it is (S-REST-COMP) which allows our system's communication topology to change dynamically via scope extrusion. ■

Example 2.3.8 Suppose we wanted to model a simple memory cell with channels for getting and setting its value. It turns out that we can simulate this just using message passing. The problem that we have to work around is that receiving a identifier from a channel removes that value from the channel – it cannot be retrieved again. Thus, we need a way to push it back in for the next time. Consider the following system:

$$\begin{aligned} Cell(get, set) \Leftarrow\ & \text{new}(c).(c!\langle init\rangle \\ & \quad \mid \text{rec } g.(get?(b).c?(y).(c!\langle y\rangle \mid b!\langle y\rangle \mid g)) \\ & \quad \mid \text{rec } s.(set?(x,b).c?(y).(c!\langle x\rangle \mid b!\langle x\rangle \mid s))) \end{aligned} \tag{2.3.9}$$

In the cell, we first create a new channel c that will be used to 'store' the value. We then initialize c with the value *init*. The following line has a recursive listener process than, when given a channel via *get*, gets the value from c and sends it back via the supplied channel. In parallel, it sends the value back into c so it can be had again. The next line is similar except that two values are supplied via *set* - a new value and a channel. The old value is pulled from c and simply discarded (ie not used), whereas the new value x is pushed to the c this time. x is also sent via b as an acknowledgment that the cell's new value has been set.

interface
↪ page 5

instantiate

Also notice that the system has the free channels get_c, set_c given in the interface. When some larger system binds them and uses them to interact with the components inside $Cell(get_c, set_c)$ we say that the system *instantiates* $Cell(get_c, set_c)$. In the following example we assume some larger system uses *printer* to actually print the message.

$$\begin{aligned} & Echo(printer) \Leftarrow \\ & \quad \text{new}(get_1, set_1).(Cell\langle get_1, set_1\rangle \\ & \qquad \mid \text{new}(a).(set_1!\langle \text{“}hello,\ world\text{”}, a\rangle \\ & \qquad\quad \mid a?(x).(get_1!\langle a\rangle \mid a?(y).printer!\langle y\rangle))) \end{aligned} \tag{2.3.10}$$

The system *Echo* creates new channels to interact with the instance of memory cell it spawns, while in parallel it puts a message in the cell, then (order is ensured using by waiting for the response via a) getting the value from the cell and sending it to the *printer* channel.

To see why this produces the behavior we expect, first observe scope restrictors for a and c can be moved out using $(S - REST - COMP)$:

$$\begin{aligned}\text{new}(get_1, set_1, a, c).\Big(&c!\langle init\rangle \mid \text{rec } g.(get?(b).c?(y).(c!\langle y\rangle \mid b!\langle y\rangle \mid g))\\ &\mid \text{rec } s.(set?(x,b).c?(y).(c!\langle x\rangle \mid b!\langle x\rangle \mid s))\\ &\mid set_1!\langle \text{“}hello,\ world\text{”}, a\rangle\\ &\mid a?(x).(get_1!\langle a\rangle \mid a?(y).printer!\langle y\rangle)\Big)\end{aligned} \tag{2.3.11}$$

Two applications of (R-REP) allow us to 'pull out' a recursive call:

$$\begin{aligned}&\text{new}(get_1, set_1, a, c).\\ &\Big(c!\langle init\rangle \mid get?(b).c?(y).(c!\langle y\rangle \mid b!\langle y\rangle) \mid \text{rec } g.(get?(b).c?(y).(c!\langle y\rangle \mid b!\langle y\rangle \mid g))\\ &\mid set?(x,b).c?(y).(c!\langle x\rangle \mid b!\langle x\rangle) \mid \text{rec } s.(set?(x,b).c?(y).(c!\langle x\rangle \mid b!\langle x\rangle \mid s))\\ &\mid set_1!\langle \text{“}hello,\ world\text{”}, a\rangle\\ &\mid a?(x).(get_1!\langle a\rangle \mid a?(y).printer!\langle y\rangle)\Big)\end{aligned} \tag{2.3.12}$$

Now we can apply (R-COMM) to the memory cell's setter...

$$\begin{aligned}&\text{new}(get_1, set_1, a, c).\\ &\Big(c!\langle init\rangle \mid get?(b).c?(y).(c!\langle y\rangle \mid b!\langle y\rangle) \mid \text{rec } g.(get?(b).c?(y).(c!\langle y\rangle \mid b!\langle y\rangle \mid g))\\ &\mid c?(y).(c!\langle \text{“}hello,\ world\text{”}\rangle \mid a!\langle \text{“}hello,\ world\text{”}\rangle\\ &\qquad\mid \text{rec } s.(set?(x,b).c?(y).(c!\langle x\rangle \mid b!\langle x\rangle \mid s)))\\ &\mid a?(x).(get_1!\langle a\rangle \mid a?(y).printer!\langle y\rangle)\Big)\end{aligned} \tag{2.3.13}$$

...which lets us strip out the initializer, and in turn the acknowledgement on a of setting "hello, world" using (R-COMM),

$$\begin{aligned}&\text{new}(get_1, set_1, a, c).\\ &\Big(get?(b).c?(y).(c!\langle y\rangle \mid b!\langle y\rangle) \mid \text{rec } g.(get?(b).c?(y).(c!\langle y\rangle \mid b!\langle y\rangle \mid g))\\ &\mid c!\langle \text{“}hello,\ world\text{”}\rangle \mid \text{rec } s.(set?(x,b).c?(y).(c!\langle x\rangle \mid b!\langle x\rangle \mid s))\\ &\mid get_1!\langle a\rangle \mid a?(y).printer!\langle y\rangle\Big)\end{aligned} \tag{2.3.14}$$

We can now use (R-COMM) on the memory cell's getter and also on its use of c to get the "hello, world" state:

$$\begin{aligned}&\text{new}(get_1, set_1, a, c).\\&\Big(c!\langle\text{“}hello,\ world\text{”}\rangle \mid a!\langle\text{“}hello,\ world\text{”}\rangle \mid \text{rec } g.(get?(b).c?(y).(c!\langle y\rangle \mid b!\langle y\rangle \mid g))\\&\mid \text{rec } s.(set?(x,b).c?(y).(c!\langle x\rangle \mid b!\langle x\rangle \mid s))\\&\mid a?(y).printer!\langle y\rangle\Big)\end{aligned} \tag{2.3.15}$$

A final application of (R-COMM) to a gives us

$$\begin{aligned}&\text{new}(get_1, set_1, a, c).\\&\Big(c!\langle\text{“}hello,\ world\text{”}\rangle \mid \text{rec } g.(get?(b).c?(y).(c!\langle y\rangle \mid b!\langle y\rangle \mid g))\\&\mid \text{rec } s.(set?(x,b).c?(y).(c!\langle x\rangle \mid b!\langle x\rangle \mid s))\\&\mid printer!\langle\text{“}hello,\ world\text{”}\rangle\Big)\end{aligned} \tag{2.3.16}$$

which is essentially equivalent to initializing a memory cell with "hello, world" and also sending the message to *printer*. ■

2.4 Action Semantics

Our description of process behaviors so far has been limited to talking about the internal computational steps through which it might evolve. Now, we want to give a more general description of how a process might evolve in the context of a larger system. In such a system, a process can be said to either send or receive values along channels it shares with the system. To describe these abilities, we will use the notion of a *labelled transition system*, or *lts*.

Definition 2.4.1 (Labelled Transition System) A *labelled transition sytem* $\mathcal{L}$ is a tuple $(\mathcal{S}, \mathcal{A})$ where $\mathcal{S}$ is a set of processes and $\mathcal{A}$ is a set of labels called *actions*. Furthermore, for each action a, there is a binary relation:

$$R_a \subseteq \mathcal{S} \times \mathcal{S}$$

To denote that $\langle P, Q\rangle \in R_a$, we will use the notation $P \xrightarrow{a} Q$.

Hence, the transition $P \xrightarrow{a} Q$ indicates that there is an action under which the process P becomes Q. We will refer to Q is the *residual* of P after a.

residual

There are three types of actions that may cause a process to evolve. Note that we will use α to refer to an action of arbitrary type. First, the process might receive a value. That is, a process P can be said to be capable of the transition $P \xrightarrow{c?\overline{X}} Q$, which is to say P can receive $\overline{X}$ along c resulting in the residual Q.

The second type of action available is sending. Here we need to be a bit more careful. In the case of receiving, the received names are always bound to new names in $\overline{X}$ - so we needn't worry about issues of scoping. In sending, however, we might be transmitting either free or a bound names, or a mix of them. In the latter case, we need to take account of the fact that the scope of the name is being extruded to whatever process receives the name. We denote the set of bound names in the send action by $(\overline{B})$, and we say that this set of names is *exported* by the process. Hence, the transition $P \xrightarrow{(\overline{B})c!\overline{V}} Q$ represents that P can send $\overline{V}$ over c, exporting $(\overline{B})$ and resulting in Q. For example,

scope extrusion
↪ page 8

exported

$$\text{new}(a).c!\langle a\rangle \mid Q \xrightarrow{(b)c!a} Q$$

We will refer to sending and receiving as *external actions*.

external action

Our third action we call *internal action*. This is caused by some internal evolution in P like those described by (R-COMM) in our Section 2.3. We call actions like sending and receiving external since in order to occur, they need some external process (given in some system of which the process in question is a part) to do the corresponding receiving or sending. However, with internal action there is no external process needed to proceed. We use τ denote such an internal evolution step. Thus, we say $P \xrightarrow{\tau} Q$ if P is able evolve into Q by performing a reduction step without any external contributions. For example (thanks to (R-COMM)),

internal action

$$c!\langle a\rangle \mid c?(x).x!\langle\rangle \xrightarrow{\tau} c!\langle\rangle$$

We will define and further characterize τ in our discussion of (A-COMM) below.

Using these actions, we can give a set of rules describing the behavior of a π-calculusprocesses in an arbitrary context. Hence, we now formally define the action relation under these rules (with their preconditions listed alongside them):

TODO: make the arrow for evolution size according to the text above it

Definition 2.4.2 (Action) The *action relation* $\longrightarrow$ is the smallest relation between processes that satisfy the following rules:

$$c?(\overline{X}).R \xrightarrow{c?X} \mathrm{R}[\![V/X]\!] \qquad \text{(A-IN)}$$

$$c!\langle\overline{V}\rangle \xrightarrow{c!V} stop \qquad \text{(A-OUT)}$$

$$\mathrm{rec}\ x.R \xrightarrow{\tau} R[\![\mathrm{rec}\ x.R/x]\!] \qquad \text{(A-REP)}$$

$$\text{if } v = v \text{ then } P \text{ else } Q \xrightarrow{\tau} P \qquad \text{(A-EQ)}$$

$$\text{if } v_1 = v_2 \text{ then } P \text{ else } Q \xrightarrow{\tau} Q \quad v_1 \neq v_2 \qquad \text{(A-NEQ)}$$

$$\frac{P \xrightarrow{\alpha} P'}{P \mid Q \xrightarrow{\alpha} P' \mid Q} \quad bn(\alpha) \cap fn(Q) = \emptyset \qquad \text{(A-COMP)}$$

$$\frac{P \xrightarrow{\alpha} P'}{\mathrm{new}(b).P \xrightarrow{\alpha} \mathrm{new}(b).P'} \quad b \notin n(\alpha) \qquad \text{(A-REST)}$$

$$\frac{P \xrightarrow{(\overline{B})c!\overline{V}} P'}{\mathrm{new}(n).P \xrightarrow{(n,\overline{B})c!\overline{V}} P'} \quad n \neq c, n \in \overline{V} \qquad \text{(A-OPEN)}$$

$$\frac{P \xrightarrow{c?\overline{X}} P',\ Q \xrightarrow{(\overline{B})c!\overline{V}} Q'}{P \mid Q \xrightarrow{\tau} \mathrm{new}(\overline{B}).(P' \mid Q')} \quad (\overline{B}) \cap fn(P) = \emptyset \qquad \text{(A-COMM)}$$

Jim:
I wonder if these couldn't be simplified (ie removing A-EQ, A-REP, etc.) by allowing a transition that happens over the reduction semantics? my sense is this approach is avoided because the action relation isn't actually contextual in our above definition (since we need to be more careful about bound variable captures). i wonder if there is a way to gracefully sidestep the issue and avoid all the redundancy...

arity
↪ page 7

contextual
↪ page 12

The first of two of these rules simply describe the ability of processes to evolve under input or output. For example, a process $c!\langle\overline{V}\rangle \mid P$ will evolve to $stop \mid P \equiv P$ when it exercises its capability for output on c. For a receiving process, evolution under (A-IN) is only possible when the substitution $[\![\overline{V}/\overline{X}]\!]$ makes sense. That is, $\overline{V}$ and $\overline{X}$ must have the same arity and in a typed system we'd want to ensure that their types were compatible[1].

Meanwhile, (A-REP), (A-EQ) and (A-NEQ) serve the provide the same interval evolution capabilities as (R-REP), (R-EQ) and (R-NEQ) do in the reduction semantics.

Together, (A-COMP) and (A-REST) provide a notion contextually - with a key difference being that in action semantics we need to be careful about inadvertently capturing bound variables. Hence, in (A-REST) we require that the newly bound variable does not occur in the names of the action. Suppose we ignored this precondition and tried the following:

$$\frac{c?().stop \xrightarrow{c?} stop}{\mathrm{new}(c).c?().stop \xrightarrow{c?} \mathrm{new}(c).stop} \qquad \text{(A-REST)}$$

But it is actually impossible for $\mathrm{new}(c).c?().stop$ to evolve since the scope of c cannot be extruded and thus no other process could ever send along c! Similarly, there are

[1] See [Hen07] for a discussion off type systems in the π-calculus

problems in capturing the one of the transmitted variables.

For (A-COMP), we just need to ensure that none of the bound identifiers of α conflict with the free variables in Q. Actually, the only variables that will be bound in an action is the set (b) exported by a send action. Thus, the precondition on (A-COMP) simply requires that bound variables that are transmitted will be 'fresh' in the receiving process. For example, consider the following system:

$$\frac{\text{new}(b).c!\langle b\rangle \xrightarrow{(b)c!x} stop}{\text{new}(b).c!\langle b\rangle \mid b!\langle a\rangle \xrightarrow{(b)c!x} stop \mid b!\langle a\rangle} \text{(A-COMP)}$$

Above, we have a process sending on b but the scope of b has not actually been extruded (ie by being received on c). Hence, we need to be careful not to 'capture' a channel like b by allowing exported channels to have the same name as free variables outside the original scope of the process.

(A-OPEN) expresses scope extrusion of a name n. If we have that a process P can evolves to P' under the action $(\overline{B})c!\overline{V}$, then we can infer that some name n, whose scope is now bound to P, can be exported in the the action $(n, \overline{B})c!\overline{V}$. Note that n must actually occur in $\overline{V}$ if it is to be exported; note also that n cannot be c since restricting n (ie c) to P would cause a scoping issue that interfered with an outside processes ability to receive on c.

Finally we have (A-COMM), which expresses scope extrusion as well but this time in the context of the internal action τ. According to (A-COMM), τ is defined as the simultaneous (compositionally) occurrence of an input action and a matching output action on the same channel. In the inferred process $P \mid Q$, no external contributions are needed for evolution, which results in the process $P' \mid Q'$, with the exported names $(\overline{B})$ now being scopes to both.

Example 2.4.3 In Example 2.1.9, we defined a simple process for modeling synchronous sends:

$$F_1(c) \Leftarrow \text{ rec } z.(\text{new}(ack).(c!\langle ack\rangle \mid ack?().(R \mid z)))$$

We then went on to show how this process might work as a component in a example system. But suppose we wanted to characterize this process's behavior in general. We could use action semantics to described how it it can evolve internally (in this case there isn't much interesting we can do except expand the replication), but we'd also want to include a description of how that process behaves externally. If possible, we'd like to do this without having to come up with a system to place the process. We don't want our characterization of the process to rely at all on some auxiliary system. We can use action semantics to provide a characterization of how $F_1(c)$ behaves externally, all without defining a particular system for it to work in. Consider the following inferences:

$$\begin{array}{lll} F_1(c) & \xrightarrow{\tau} & \text{new}(ack).(c!\langle ack\rangle \mid ack?().(R \mid F_1(c))) \quad \text{(A-REP)} \\ & \xrightarrow{(ack)c!ack} & \text{new}(ack).(stop \mid ack?().(R \mid F_1(c))) \quad \text{(A-OPEN, A-OUT)} \\ & \xrightarrow{(ack?)} & \text{new}(ack).(stop \mid (R \mid F_1(c))) \quad \text{(A-IN)} \end{array}$$

Jim:
I could make an explicit rule for inferences between structurally equivalent action relations...some presentations do, some don't. What do you think?

Using the structural equivalence rules (S-COMP-ID) and (S-REST-COMP). We know the final step of this inference to be equivalent to:

$$R \mid \text{new}(ack).(F_1(c))$$

Above, we have shown presence of the important behaviors we expect in $F_1(c)$. That is, we have shown that $F_(c)$ can:

- Recursively spawn a process that can...
- Send ack over c, extruding its scope and resulting in a residual process that can...
- Receive the acknowledgement handshake on ack, resulting in a residual that can...
- Run R and wait for the next recursive iteration to occur (internally).

Thus, we have completely characterized $F_1(c)$'s capabilities to act as a recursive synchronous output process in a system – but we have done so without having to say anything about what that system actually looks like. ■

3
Synchronicity and Expressiveness

In Section 2.1, we introduced a version of the π-calculus which we said was made *asynchronous* by its use of non-blocking send operations. Rather than allowing an operation to happen after a sent value has been received by some other process, a sending process simply ends, hoping someone will eventually consume the sent message. In Example 2.1.9 we gave a straightforward method of simulating synchronous sending in the asynchronous π-calculus. Also absent in our calculus was the non-deterministic choice operator, also known as the summation operator. We gave a method of simulating this in Example 2.1.7.

The original calculus given by Milner, Parrow and Walker modeled synchronous message passing, and included the two operators – summation and synchronous sending – that we omitted in our asynchronous π-calculus. When combined, these two operators yield a unique behavior. The power of this behavior will become clear in our presentation of the synchronous π-calculusin Section 3.1.

Our original calculus features synchronous receiving, but now sending is synchronous as well, allowing a process to be performed after the output has been consumed by some other receiver. Hence, in the synchronous π-calculus, processes can be guarded by both receiving *and* sending.

guarded
↪ page 8

If we have a group of guarded processes joined by the summation operator, only one of those will be processes will be 'chosen' (non-deterministically) to be executed. The rest will simply terminate without having any effect. The power of the synchronous π-calculuscomes when we have another group of summed processes, running in parallel, something like:

$$c!\langle\rangle.P_1 + d_1!\langle\rangle.P_2 + d_2?().P_3 \mid c?().R_1 + d_3!\langle\rangle.R_2$$

In the above isolated system, we can actually know which of the processes will be chosen to run, despite the non-deterministic nature of the choice operator. Because both sends and receives are guarded, both the P_k's and R_K's can only run when their respective transmission guards complete. Hence, only P_1 and R_1 will be allowed to run since sending on c is the only transmission with a matching reception on c. Now imagine a slightly more complicated system:

$$c!\langle\rangle.P_1 + d!\langle\rangle.P_2 \mid c?().R_1 + d?().R_2$$

Here we have *two* transmissions with matches, so we cannot make a guarantee about which processes are chosen. However, we *can* say that if P_1 executes on the left side,

R_1 will be chosen on the right side. We can say the same for P_2 and R_2. There is a silent, implicit sort of communication that can happen between groups of parallel processes when a non-deterministic choice is made among them. This is a powerful feature which comes with the special operators of the synchronous π-calculus.

A natural question arises at this point: can we represent this expressive communication power using only our asynchronous π-calculus? That is, using the simulations given in Examples 2.1.9 and 2.1.7 (or perhaps some similar but more complicated approach) can we fully capture the 'communication' between non-deterministically chosen processes discussed above? We will explore the surprising complexity of this question and some of its implications in Section 3.2. First though, let us give a more formal discussion of the features of the synchronous π-calculus.

Jim: On second thought, I think I might want to leave the reader with this question, for now - to peak their curiosity, perhaps.

3.1 The Synchronous π-Calculus

Action Prefixes

$\pi :=$	$n!\langle\overline{V}\rangle$	Send
	$n?(\overline{X})$	Receive
	τ	Internal Evolution

Process terms

$R :=$	$\sum_{i\in\{1,..,n\}} \pi_i.R_i$	Summation ($n \in \mathbb{Z}$)
	$R_1 \mid R_2$	Composition
	new$(n).R$	Restriction
	if $v_1 = v_2$ then R_1 else R_2	Matching
	rec $x.R$	Recursion
	stop	Termination

Figure 3.1.1: Terms in the synchronous π-calculus

Note the important difference between Figure 2.1.1 and Figure 3.1.1. First, we have grouped sending and receiving together as *action prefixes* (along with a new prefix for internal evolution). These prefixes are made available to the language via the summation operator.

internal evolution
↪ page ??

Consider the term:

$$\sum_{i\in\{1,..,n\}} \pi_i.R_i$$

The notation $\pi_i.R_i$ requires that the action π_i happen before the guarded process R_i will be executed. If R_a is executed in this way, then for all $j \neq a$, both the capabilities π_j and the execution of R_j are lost. In other words, the summation ensures that only

one of n guarded processes will be executed. Which of these processes is picked depends on which action prefix capability is exercised first.

For the cases that $n = 1$ and $n = 2$, we will use the notation $\pi.R$ and $\pi_1.R_1 + \pi_2.R_2$, respectively. We add to our congruence relation given in Definition 2.2.8 that summation is commutative and associative.

The summation case of $n = 0$ is what is meant by our *stop* termination process. Thus the following fact, which we will call (S-SUM-ID), is trivially true:

$$\pi.R + 0 \equiv \pi.R$$

Note also that in our action prefixes, we have made sending a guarded operation, which means that R will not execute until some other process receives $\overline{V}$ along n. Receiving is also guarded, as in the asynchronous version. In the case where π is some internal evolution τ, we simply mean that R can proceed after the process does something which we cannot observe. This internal behavior is captured in the new reduction rule (R-TAU) below, while (R-SYNC) expresses the external evolution of the summation operator.

guarded ↪ page 8

$$\begin{array}{rcll}
\tau.R + P & \longrightarrow & R & \text{(R-TAU)} \\
c!\langle\overline{V}\rangle.P + Q \mid c?(\overline{X}).R + B & \longrightarrow & (P \mid R)[\![\overline{V}/\overline{X}]\!] & \text{(R-SYNC)} \\
\text{rec } x.R & \longrightarrow & R[\![\text{rec } x.R/x]\!] & \text{(R-REP)} \\
\text{if } v = v \text{ then } P \text{ else } Q & \longrightarrow & P & \text{(R-EQ)} \\
\text{if } v_1 = v_2 \text{ then } P \text{ else } Q & \longrightarrow & Q \quad (\text{where } v_1 \neq v_2) & \text{(R-NEQ)} \\
\dfrac{P \equiv P', P \longrightarrow Q, Q \equiv Q'}{P' \longrightarrow Q'} & & & \text{(R-STRUC)}
\end{array}$$

Figure 3.1.2: Reduction rules for the synchronous π-calculus

Example 3.1.3 It is not hard to show that the synchronous π-calculus can model the asynchronous version. To see why, first note that asynchronous sending can be encoded simply by $n!\langle\overline{V}\rangle.stop$. This we will abbreviate with the familiar notation $n!\langle\overline{V}\rangle$. As we noted above, the summation notation allows for a single guarded process. If we limit ourselves to these single summations, disallow use of the internal action τ, and limit all sending to be of the form $n!\langle\overline{V}\rangle.stop$, then we have the asynchronous π-calculus. To see why the reduction semantics are compatible, note that (R-TAU) is not needed in the asynchronous calculus since we have excluded its operator. The following shows that (R-SYNC) is a more general form of (R-COMM) of Definition 2.3.1:

$$\begin{array}{rcll}
c!\langle\overline{V}\rangle.\ \text{stop} + \text{stop} \mid c?(\overline{X}).\text{R} + \text{stop} & \equiv & c!\langle\overline{V}\rangle.\text{stop} \mid c?(\overline{X}).\text{R}, & \text{(S-SUM-ID} \\
c!\langle\overline{V}\rangle.\text{stop} \mid c?(\overline{X}).\text{R} & \longrightarrow & (\text{stop} \mid \text{R})[\![\overline{V}/\overline{X}]\!], & \text{(R-SYNC)} \\
\dfrac{(stop \mid R)[\![\overline{V}/\overline{X}]\!] \equiv R[\![\overline{V}/\overline{X}]\!]}{c!\langle\overline{V}\rangle \mid c?(\overline{X}).\text{R} \longrightarrow \text{R}\ [\![\overline{V}/\overline{X}]\!]} & & & \text{(S-COMP-ID)} \\
 & & & \text{(R-STRUC)}
\end{array}$$

It will be obvious from our presentation of synchronous action rules below that they needn't be shown to be a general version of the asynchronous rules – they are

equivalent simply by ignoring the extra rules and using our $n!\langle\overline{V}\rangle.stop$ encoding of sending. ■

Neither do the action rules for the synchronous π-calculus, given below, differ significantly from those in the asynchronous version. As we would expect, (A-OUT) has been modified to express synchronous sending: it now evolves over output to a process R and not simple the termination process *stop*. We have also added two new rules. The first, (A-TAU) describes the behavior of a process guarded by an internal action. The second rule, (A-SUM), characterizes the summation operator. It says, for example, that if some process P is able to evolve to P' over some action α, then α will also cause $P + Q$ to evolve via choice to P'.

$$c?(\overline{X}).R \xrightarrow{c?\overline{X}} R[\![\overline{V}/\overline{X}]\!] \quad \text{(A-IN)}$$

$$c!\langle\overline{V}\rangle.R \xrightarrow{c!\overline{V}} R \quad \text{(A-OUT)}$$

$$\text{rec } x.R \xrightarrow{\tau} R[\![\text{rec } x.R/x]\!] \quad \text{(A-REP)}$$

$$\text{if } v = v \text{ then } P \text{ else } Q \xrightarrow{\tau} P \quad \text{(A-EQ)}$$

$$\text{if } v_1 = v_2 \text{ then } P \text{ else } Q \xrightarrow{\tau} Q \qquad v_1 \neq v_2 \quad \text{(A-NEQ)}$$

$$\tau.R \xrightarrow{\tau} R \quad \text{(A-TAU)}$$

$$\frac{P_i \xrightarrow{\alpha} P_i'}{\sum_{i\in\{1,..,n\}} \pi_i.P_i \xrightarrow{\alpha} P_i'} \quad \text{(A-SUM)}$$

$$\frac{P \xrightarrow{\alpha} P'}{P \mid Q \xrightarrow{\alpha} P' \mid Q} \qquad bn(\alpha) \cap fn(Q) = \emptyset \quad \text{(A-COMP)}$$

$$\frac{P \xrightarrow{\alpha} P'}{\text{new}(b).P \xrightarrow{\alpha} \text{new}(b).P'} \qquad b \notin n(\alpha) \quad \text{(A-REST)}$$

$$\frac{P \xrightarrow{(\overline{B})c!\overline{V}} P'}{\text{new}(n).P \xrightarrow{(n,\overline{B})c!\overline{V}} P'} \qquad n \neq c, n \in \overline{V} \quad \text{(A-OPEN)}$$

$$\frac{P \xrightarrow{c?\overline{X}} P',\ Q \xrightarrow{(\overline{B})c!\overline{V}} Q'}{P \mid Q \xrightarrow{\tau} \text{new}(\overline{B}).(P' \mid Q')} \qquad (\overline{B}) \cap fn(P) = \emptyset \quad \text{(A-COMM)}$$

Figure 3.1.4: Action rules for the synchronous π-calculus

Example 3.1.5 Example of choice operator inferences over SUMM-L rule. ■

3.2 Separation Results

When trying to compare the expressive power of different calculi, one good approach is to, as above, provide explicit encodings from one language to another[1]. We say that we are trying to encode from *source language* into the terms of a *target language*, and if we succeed, we have shown that the target language is at least as expressive as the source. Hence, in example Example 3.1.3 we showed that the synchronous calculus is at least as expressive as the asynchronous calculus by giving an encoding from the asynchronous to the synchronous. We will also use the notation

source language

target language

$$[\![P]\!] \stackrel{def}{=} Q$$

to mean that P in the source language is encoded by Q in the target language.

To prove a separation result between languages, it is enough to show that there are problems that are not solvable in the source language that are not solvable in the target language. In [Pal03], Palamidessi uses the solvability of the leader election problem on symmetric networks to show that the synchronous π-calculus is strictly more expressive than the asynchronous version. Loosely, the leader election problem is the problem of having group of identifier (via integers, perhaps) processes agree on a 'leader' process identification in a finite amount of time. We say that these processes are a symmetric network if any two processes P_i, P_j are equivalent under structural equivalence and renaming of their identifiers. For example, consider the following symmetric network:

$$P_0 \mid P_1 \Leftarrow \; c_0!\langle\rangle.o!\langle 0\rangle + c_1?().o!\langle 1\rangle \mid c_1!\langle\rangle.o!\langle 1\rangle + c_0?().o!\langle 0\rangle$$

It should not be hard to see that this solves the leader election problem in the synchronous π-calculus by agreeing on a leader via the output channel o. It may be less obvious, but it is not possible to solve the leader election problem in a symmetric network of asynchronous π-calculus processes. This is a direct result of the lack of the choice operator: without it, the symmetric processes have no way to pick a leader non-deterministically without potentially disagreeing with one another. It is only through the implicit communication underlying the choice operator that synchronous processes are able to break out of their symmetry and agree on a leader.

Using these results, Palamidessi a set of useful requirements that formally separate the two calculi.

The first of those requirement is on *uniformity*, which means that:

uniformity

$$[\![\alpha(P)]\!] = \alpha([\![Q]\!]) \tag{3.2.1}$$
$$[\![P \mid Q]\!] = [\![P]\!] \mid [\![Q]\!] \tag{3.2.2}$$

(3.2.1) simply states α-renaming is not violated in the process of the encoding. (3.2.2)

Jim: When I try to refer to the label α-equivalency here, things break. any idea how to fix this without re-engineering my definitions?

[1] Note that Example 3.1.3 is a trivial example of such an encoding since your encodings are straight-forward enough to be equivalent under the structural equivalence. Most encodings require the more advanced structure of *bisimulation* equivalences, which relies on setting up a notion of simulation and then proving that two processes simulate one another.

is related to the requirements of a distributed system. That is, parallel processes really should just map to parallel processes, with not top level manager process or the like to aide the encoding. This is how Palamidessi builds the requirement of a symmetric network into a language requirement.

TODO: where/how?

reasonability

The other requirement is on *reasonability*. Reasonability to Palamidessi means that the language can distinguish between two processes when their actions are different on a certain given channel. This essentially encapsulates the requirements of the leader election problem. That is, a electoral system would be one were actions on the output channel are the same and we want our target language to be capable of semantically distinguishing this from a non-electoral system (where actions on the output channel differ).

4

Synchronicity and Distributed Systems

The second question we might ask is about the implementation of a synchronous π-calculus. On distributed systems, which seem like the natural setting for such an implementation, we have only asynchronous available to us. Hence, depending on the answer to the first question, we may have to

However, whether the asynchronous calculus actually has the expressive power of its synchronous forebear is a matter of more complexity. In fact, we will see by straightforward counterexample (and by a rather less straightforward argument due to Palamidessi [Pal03]) that two are not truly equal. The implementation of synchronous calculi on distributed systems is a thorny issue. On the one hand, it is a useful construct in that it allows us to model many problems more naturally and easily. On the other, all communication in a distributed system is in fact asynchronous in nature, and so synchronous communication must be layered on top at some level of the implementation. It is notoriously difficult construct to implement synchronous communication efficiently without violating the requirements of a truly distributed system where there is shared memory or central control process. The issue becomes more difficult still with the Palamidessi's related requirement of symmetry, which means that a process's behavior does not depend on its location in the channel topology.

TODO: make a note about why the original example only covered input guarded choice

The creators of Pict, the Join-calculus, and other implementations based on the π-calculus all decided to have their primitives support only asynchronous communication, while synchronous communication is made available overtop of this via a library or higher-level language. This these greatly simplifies implementation, resulting in a cleaner, more efficient core language. The summation operator in particular is difficult and expensive to fully simulate. In the implementation of Pict, for example, David Turner notes [Tur96] that "the additional costs imposed by summation are unacceptable.". Turner goes on to say that essential uses of summation are infrequent in practice.

How can we reconcile this with Palamidessi's result, which indicates that there are important problems that cannot be solved without the full generality of the synchronous calculus? Is such a calculus even implementable at any cost on distributed systems? We will see that relaxing any of Palamidessi's assumptions enables a full encoding. Some of such encodings derive from the classic distributed solutions to the problem of synchronous communication but strain important assumptions about symmetry in ways that we may not be comfortable allowing. Palamidessi herself gives as important probabilistic encoding [PH01] which does not break symmetry.

4.1 Symmetry in Practice

Speaking in an interview on developing the π-calculus, Robin Milner notes [Ber03]:

> That was to me the challenge: picking communication primitives which could be understood at a reasonably high level as well as in the way these systems are implemented at a very low level...There's a subtle change from the Turing-like question of what are the fundamental, smallest sets of primitives that you can find to understand computation...as we move towards mobility... we are in a terrific tension between (a) finding a small set of primitives and (b) modeling the real world accurately.

This tension is quite evident in the efforts of process algebraists to find the 'right' calculus for modeling distributed systems. While the synchronous π-calculus more elegantly and (given certain assumptions) completely expresses distributed systems, actual implementation must commit to asynchronous communication as their primitives. Which we choose as a model depends in part on our goals. In any case, it is evident that by limiting ourselves to smaller calculi, many useful new concepts and structures arise in order to solve the problems posed by asynchronous communication. While these structures might not belong in the 'smallest set of primitives', they are useful for bringing the power of the π-calculus to a model that more closely resembles the implementation of distributed systems.

This section will go on to talk about on Nestmann and other implementation-driven encodings, how much they violate uniformity/reasonableness and whether that has any means for the API as a good model for implementable distributed languages.

List of Figures

References

[Ber03] Martin Berger. An interview with robin milner, September 2003.

[Cas02] I. Castellani, editor. *Models of Distribution and Mobility: State of the Art*. MIKADO Global Computer Project, August 2002.

[Hen07] Matthew Hennessy. *A Distributed Pi-Calculus*. Cambridge University Press, 2007.

[Mil92] Robin Milner. Functions as processes. *Mathematical Structures in Computer Science*, 2(2):119–141, 1992.

[Mil99] Robin Milner. *Communicating and Mobile Systems: the π-calclulus*. Cambridge University Press, 1999.

[Nes00] Uwe Nestmann. What is a "good" encoding of guarded choice? *Inf. Comput.*, 156(1-2):287–319, 2000.

[Pal03] Catuscia Palamidessi. Comparing the expressive power of the synchronous and the asynchronous π-calculus. *Mathematical Structures in Computer Science*, 13(5):685–719, 2003.

[PH01] C. Palamidessi and O. Herescu. A randomized encoding of the -calculus with mixed choice, 2001.

[SW01] Davide Sangiorgi and David Walker. *The π-calculus:A Theory of Mobile Processes*. Cambridge University Press, 2001.

[Tur96] David N. Turner. *The Polymorphic Pi-Calculus: Theory and Implementation*. PhD thesis, 1996.

Index