Algebraic specification and simulation of lazy functional programs in a concurrent environment

Citation for published version (APA):

Document status and date:
Published: 01/01/1996

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

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

Link to publication

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

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

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

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

Download date: 09. Aug. 2023
Algebraic Specification and Simulation of Lazy Functional Programs in a Concurrent Environment

by

Loe Feijs

96/20

ISSN 0926-4515

All rights reserved
editors: prof.dr. R.C. Backhouse
     prof.dr. J.C.M. Baeten

Reports are available at:
http://www.win.tue.nl/win/cs

Computing Science Report 96/20
Eindhoven, October 1996
Algebraic Specification and Simulation of Lazy Functional Programs in a Concurrent Environment

Loe Feijs
Philips Research Laboratories Eindhoven,
Eindhoven University of Technology

Abstract

The mechanism of Landin-style stream input/output (I/O) makes it possible to write functional programs, which behave as reactive systems when executed with lazy evaluation. Functional programming languages like Gofer are attractive for programming the data transformations of a reactive system. But although the I/O behaviour can be programmed in such languages too, the functional paradigm lacks the capabilities for specification and reasoning which are needed to analyse the communication behaviour of the program and its environment. We propose to use the Algebra of Communicating Processes (ACP) for that purpose. The present paper attempts to bridge the gap between the functional and the process-oriented worlds. It is shown how a simple generator can produce both Gofer program patterns and ACP equations. The patterns can be completed with data transformation functions and then executed whereas the equations can be used for reasoning and simulation. The term rewriting system (TRS) of the functional language, the structured operational semantics (SOS) of the I/O mechanism, the process equations and the fixed point semantics of a program are described and their relationships are analysed. We abstract from the details of the particular programming language by using an intermediate concept of 'abstract functional program'.

Key Words: ACP, Bisimulation, Communication protocols, Component generation, Denotational semantics, Executable specifications, Fixed point theory, Formal reasoning, Functional programming, Gofer, Labeled transition systems, Lambda calculus, Lazy evaluation, Patterns, PSF, Scripting, Simulation, Streams, Structured operational semantics.

1 Introduction and motivation

In many circumstances it is important to have precise specifications of computer programs in order to analyse their behaviour in the context of a large system. In particular this is important for 'scripted agents', by which we mean programs which are meant for being transferred through a communication network for execution as a reactive program at another site. In this paper we investigate a number of issues arising when a program is written in a programming language which is based on lazy evaluation, like Gofer [1]. Although it is possible to let a functional program perform all kinds of I/O actions, such as reading and writing files, it makes sense to adopt a restriction to so-called Landin-style stream I/O; in that case, a program, viewed as a process in a concurrent environment (a distributed system), will have only one input port and one output port. Of course a distributed system will need multi-port components like routers too, but one can assume that these are realised by other means already and
that these can be specified using process-theoretic means, for example ACP [2]. In this way the data processing aspects are separated from the communication aspects. By means of an example it will be shown that this can be done without loss of generality (provided the network contains routers). For our examples we use Gofer and we work out the details to such a level that we can use the axioms of ACP\textsuperscript{\textcopyright} [2] for reasoning and ACP-based tools like PSF [3] for simulation.

Related work: in [4] it was already shown that the concept of stream domains makes it possible to relate certain λ-calculus based program descriptions to behavioural descriptions of the program in a concurrent environment. In [5] an operational semantics of a Haskell fragment is given and used to derive process-theoretic properties using CCS. In [6] a powerful I/O mechanism is proposed which is not restricted to Landin-style stream I/O. Whereas we view a functional program as one of many agents in a concurrent world, [6] addresses the problem the other way around, turning the world into a set of objects being manipulated by the functional program.

Survey of the work: in Section 2 a survey of the relevant aspects of lazy functional languages is given. In Section 3 some aspects of ACP are introduced. In Section 4 a first example is studied (ping-pong behaviour). In Section 5 a second example is studied (state-based behaviour). In Section 6 another technicality is added (non ping-pong behaviour). In Section 7 we propose a constructive approach, using a generator to make program patterns together with their ACP equations. In Section 8 we show this constructive approach in action, when we build a simple distributed system consisting of a service provider (an Eliza-like psychiatrist) and a service manager (filtering Eliza's advice when the user did not pay). In Section 9 we use PSF to simulate the ACP equations of this service manager together with a model of its environment. In Sections 10 and 11 we study the correctness aspects and certain semantic aspects, respectively. In Section 12 some concluding remarks are given.

2 Aspects of lazy functional languages

Functional programming languages have been used for artificial intelligence (AI) applications and for tool construction for many years. Important languages are LISP, ML, Miranda, Haskell, Clean and Gofer. Several of the more recent languages are based on lazy evaluation, which amounts to a particular reduction strategy together with certain assumptions about the representation and manipulation of data structures. With respect to the reduction strategy, lazy evaluation means that:

- an argument to a function is not earlier evaluated than when its value is needed (so if it is not needed at all, it is not evaluated),
- an argument to a function is evaluated only once, also if its value is needed several times during the function’s execution.

The important data type of lists is always built-in to functional languages. With respect to list-processing, lazy evaluation means that:

- if the result of an execution is a list, then this list is delivered in an incremental way, i.e. the head will be delivered first (while arguments only relevant for the tail are not evaluated),
- if the argument of a function is a list, then evaluation of the function can start already before all list elements are available (typically a function requires the list’s head first, then the head of its tail and so on).
For a survey of Gofer, see [1]. An interactive Gofer program with top level function \( f \) is a kind of executable function of type \([\text{Response}] \rightarrow [\text{Request}]\) (assuming that Gofer's standard prelude is imported). The program produces requests to its environments, such as requests to read and write strings from standard input ("stdin") and to standard output ("stdout"). The environment gives responses, containing success/failure indications and strings, which serve as inputs for the program.

If we refrain from using arbitrary calls to the file system, and instead of that, just read and write from/to standard input and standard output, the type of \( f \) is much simpler. It is of type \( \text{String} \rightarrow \text{String} \). In this case the main program looks as follows:

\[
\text{main} = \text{interact } f
\]
\[
f :: \text{String} \rightarrow \text{String}
\]

When this is executed, the characters are read (for example from the keyboard) and then processed by \( f \). The function \( \text{interact} \) is a predefined function from Gofer's standard prelude. The lazy evaluation mechanism determines at which points in time there has been enough input in order to produce output. The interaction behaviour can still be complex, in the sense that the the program consumes \( n_1 \) inputs before producing \( m_1 \) outputs, then \( n_2 \) inputs followed by \( m_2 \) outputs etc., where the \( n_i \) and \( m_i \) depend on the contents of the lines read so far. Sometimes this is called Landin-style stream I/O.

Although \( f \) is declared as \( \text{String} \rightarrow \text{String} \) it consumes and produces information in certain chunks, normally characters. In order to have a more practical granularity for the I/O, we shall in the sequel assume that each line is treated as a separate chunk of information. Therefore we focus on programs whose 'main' is as follows:

\[
\text{main} = \text{interact } (\text{unlines} \ . \ g \ . \ \text{lines})
\]
\[
g :: [\text{String}] \rightarrow [\text{String}]
\]

Here we used the function \( \text{lines} \) from the standard prelude; it breaks a string into a sequence of strings by recognising the end of line characters. And \( \text{unlines} \) is its inverse. Note the '\( . \)' operator, which denotes function composition.

Next to the functional behaviour of \( g \), we need to understand the behaviour of \( g \) in a concurrent environment, where synchronisation is relevant. As explained above, the synchronisation between the responses and the requests is regulated by the lazy execution mechanism. This implies that from the environment's point of view, \( g \) is eager to deliver results: it produces as much outputs (requests) as possible, only pausing to wait for an input (a response) if no other action is possible.

## 3 Aspects of ACP

The Algebra of Communicating Processes ACP proposed by Bergstra and Klop [7], is a theory about processes and their communication behaviour in the tradition of CCS [8]. For an introduction to ACP, see [2]. We mention some of the most important operators: \( + \) for alternative composition, \( - \) for sequential composition, \( \tau \) for silent step and \( || \) for parallel composition. The laws of ACP are always written as equations, such as the following laws, called 'basic process algebra'.

\[
x + y = y + x
\]


\[(x + y) + z = x + (y + z)\]
\[x + x = x\]
\[(x + y) \cdot z = x \cdot z + y \cdot z\]
\[(x \cdot y) \cdot z = x \cdot (y \cdot z)\]

To these one has to add additional laws describing \(\|\), \(\tau\) etc., for example \(x \cdot \tau = x\).

ACP is parameterised over an action-alphabet \(A\), which must be chosen dependent on the application domain. For the purpose of studying interactive functional programs, we assume that \(A\) contains the following elements:

- \(s(t)\) \((t \in \text{String})\),
- \(r(t)\) \((t \in \text{String})\),
- \(c(t)\) \((t \in \text{String})\),
- \(\tau\).

ACP is also parameterised over a binary communication function \(\gamma : A \times A \rightarrow A\), which must be chosen dependent on the application domain. We define the partial function \(\gamma\) such that one ‘send’ and one ‘receive’ together make one ‘communication’. This is expressed by the following equations:

\[
\gamma(s(t), r(t)) = c(t)
\]
\[
\gamma(r(t), s(t)) = c(t)
\]
\[
\gamma(a_1, a_2) = \text{undefined} \quad (\text{otherwise})
\]

These choices allow us to use ACP for the purpose of studying interactive functional programs provided we may assume that, when viewed as a process, a lazy functional program has a single input port corresponding to actions \(r(t)\), and an output port corresponding to actions \(s(t)\), as sketched in Figure 1.

![Figure 1: Lazy functional program viewed as a process.](image)

At first sight this model looks too naive, because a simple experiment shows that when the input of the program comes directly from a keyboard, the user can continue typing, even when the program is not ready for consumption of the next line typed. This is explained however, by assuming that there is a buffer between the keyboard and the program. This buffer queues the lines which are typed. Similarly an output buffer is assumed for the results which are to be displayed on the user’s screen. The buffers are not considered part of the process of \(g\); they belong to the environment, as sketched in Figure 2 below.

These preparations will enable us to address a central question in the next sections: which ACP equations describe the behaviour of a functional program \(g\), viewed as a process?
Figure 2: Environment for teletype I/O.

4 Example (memoryless function)

The first example is a particularly simple kind of process. It produces and consumes its chunks of information in an alternating fashion. The program given below transforms each input line into an output line by applying a memoryless mapping updline (for 'update line') from Line to Line.

```go
type Line = String

type Word = String

main = interact (unlines . g . lines)

g :: [Line] -> [Line]
g = updlines

updlines :: [Line] -> [Line]
updlines [] = []
updlines (l : ls) = (updline l) : (updlines ls)

updline :: Line -> Line
updline l = unwords (updwords (words l))

updwords :: [Word] -> [Word]
updwords [] = []
updwords (w : ws) = (map toUpper w) : (updwords ws)
```

Note that map is a built-in concept of Gofer and that toUpper is a function from the standard prelude. This program can for example perform a dialogue as follows:

1. let us explain the compiler           (receive)
2. LET US EXPLAIN THE COMPILER          (send)
3. it has an easy evaluator             (receive)
4. IT HAS AN EASY EVALUATOR             (send)

Next we investigate the process behaviour of g. If we want to see a Gofer program g as a process, we denote it as $P_g$. If we want to consider g as a mathematical function we denote it as $F_g$. From the definition of updlines we see that the first element
of the result updlines \((l : ls)\) depends only on \(l\) and does not require \(ls\). Therefore
the program produces an output immediately after each input. Of course the program
first performs some internal rewriting, which is modeled by a silent step \(\tau\). This tells
us that it satisfies the ACP equation.

\[
P[g] = \tau \cdot \sum_x \tau(x) \cdot s(updline(x)) \cdot P[g]
\]

which is consistent with the following equation concerning the functional behaviour,
which is obvious from the program:

\[
F[g](x : xs) = updline(x) : F[g](xs)
\]

5 Example function with memory

Next we look at an example of a more general case. The process below transforms each
input line into an output line, but it is not just a ‘memoryless’ mapping from Line to
Line. It has an internal state, coded as a ‘dictionary’, whose type is called Dict.

```
type Line = String
type Word = String
type Dict = [Word]

main = interact (unlines . g . lines)

g :: [Line] -> [Line]
g = updlines iniDict

updlines :: Dict -> [Line] -> [Line]
 updlines d [] = []
 updlines d (l : ls) = (updline d l) : (updlines (updDict d l) ls)

updDict :: Dict -> Line -> Dict
 updDict d l = (add (words l) d)

updline :: Dict -> Line -> Line
 updline d = unwords . (map (updword d)) . words

updword d w | isin w d = w
            | otherwise = map toUpper w

add :: [Word] -> Dict -> Dict
 add [] d = d
 add (w : ws) d | isin w d = add ws d
                | otherwise = w : (add ws d)

isin :: Word -> Dict -> Bool
 isin w [] = False
 isin w (x : xs)
    | (w == x) = True
    | (w ++ "s" == x) = True
    | (w == x ++ "s") = True
    | otherwise = isin w xs
```
iniDict :: Dict
iniDict = ["in", "the", "and", "is", "has", "it", "from", "thing", "easy", "have", "a", "at", "of", "to", "use", "will", "find", "one", "always", "about", "an", "now", "let", "us", "talk", "mention", "explain", "work", "so-called", "define", "separate", "treat", "way", "as", "if", "clear", "next", "or", "may", "be", "used", "new", "some", "where", "no", "find", "should", "tell", "we", "however", "try", "for", "form", "they", "are", "not"]

This program performs a slightly more interesting task. It maps fresh words (except for frequently used verbs and particles) to uppercase, but only in the line where they occur for the first time. This is a dialogue:

1. let us explain the compiler (receive)
2. let us explain the COMPILER (send)
3. it has an easy evaluator (receive)
4. it has an easy EVALUATOR (send)
5. evaluators are always easy (receive)
6. evaluators are always easy (send)

This process satisfies the ACP equation \( \mathcal{P}(\mathcal{G}) = U_{\text{iniDict}} \) where for all \( d \) of type Dict we have that \( U_d \) is given by:

\[
U_d = \tau \cdot \sum_l r(l) \cdot s(l') \cdot U_{d'}
\]

where \( l' \equiv ((\text{unwords} \cdot \text{map} \cdot \text{updword} \cdot d) \cdot \text{words}) l \) and \( d' \equiv (\text{add} \cdot \text{words} 1) \cdot d \). This is consistent with the functional behaviour for which we check from the Gofer program text that \( \mathcal{F}(\mathcal{G}) = u(\text{iniDict}) \) where for all strings \( l \) and \( ls \),

\[
u(d)(l : ls) = l' : u(d')(ls)
\]

6 Example which does not ping-pong

The previous examples had alternating send and receive behaviour (ping-pong behaviour). But can we also make a program which does not ping-pong, but which does ping-pong-pong-pong? Such a process \( G \) would be described by an ACP equation of the form:

\[
G = \tau \cdot \sum_{t_1, t_2} r(t_1) \cdot r(t_2) \cdot s(t'(t_1, t_2)) \cdot s(t''(t_1, t_2)) \cdot G'(G, t_1, t_2)
\]

Yes, we can, and then the functional behaviour for \( g \) is described by an equation of the form:

\[
g(t_1 : t_2 : ts) = l'(t_1, t_2) : l''(t_1, t_2) : g'(g, t_1, t_2)(ts)
\]

In fact, the number of pings and pongs can be determined dynamically, as shown by the program given below. This program compares each subsequent input line with the current line, and throws the next line away if it is a subset (with respect to the non-trivial words) of the current line. The set of ‘trivial’ words is given by iniDict.

\[
\text{main} = \text{interact} \cdot (\text{unlines} \cdot g \cdot \text{lines})
\]
\[
g :: [\text{Line}] \rightarrow [\text{Line}]
\]
\[ g = \text{mute } [] \]

\[
\begin{align*}
mute :: [\text{Word}] & \rightarrow [\text{Line}] \rightarrow [\text{Line}] \\
mute c [] &= [] \\
mute c (l : ls) & | (\text{criterion } c \ 1) = \text{mute } c \ 1s \\
& | \text{otherwise} = 1 : (\text{mute } (\text{nontrivs } (\text{words } 1)) \ ls)
\end{align*}
\]

\[
\begin{align*}
criterion :: \text{Dict} & \rightarrow \text{Line} \rightarrow \text{Bool} \\
criterion c \ 1 = \text{subset } (\text{nontrivs } (\text{words } 1)) \ c
\end{align*}
\]

\[
\begin{align*}
\text{subset} :: [\text{Word}] & \rightarrow [\text{Word}] \rightarrow \text{Bool} \\
\text{subset} [] c &= True \\
\text{subset } (w : ws) c & | (\text{isin } w c) = \text{subset } ws c \\
& | \text{otherwise} = False
\end{align*}
\]

\[
\begin{align*}
\text{nontrivs} :: [\text{Word}] & \rightarrow [\text{Word}] \\
\text{nontrivs} [] &= [] \\
\text{nontrivs } (w : ws) & | (\text{isin } w \ \text{iniDict}) = \text{nontrivs } ws \\
& | \text{otherwise} = w : (\text{nontrivs } ws)
\end{align*}
\]

-- Line, Word, Dict, isin, iniDict as before

This program can for example perform a dialogue of the ping-pong-ping-pong-ping-pong-ping-pong type, as shown below.

1. let us explain the compiler (receive)
2. let us explain the compiler (send)
3. it has an easy evaluator (receive)
4. it has an easy evaluator (send)
5. evaluators are always easy (receive)
6. thanks heaven (receive)
7. thanks heaven (send)

The line "evaluators are always easy" is viewed as a subset of "it has an easy evaluator" and therefore the latter line is not echoed.

### 7 A constructive approach

In general it is impossible to automatically analyse arbitrary Gofer programs to find their ACP equations. But we can easily identify a number of useful patterns for which the Gofer program can be analysed. For each such pattern we can give both the ACP equations and an outline of the Gofer program. One could make a library of such pairs consisting of a pattern and a set of equations. We demonstrate this idea for a few interesting patterns and we cast the library into the form of a menu-driven generator. The user (programmer) still has to add definitions of a number of functions called \( f_0, f_1, f_2 \) etc. We devised a few patterns for which one needs a number of user-defined functions; these have the following characterisation.

- \( f_0 \) - initialisation (cf. iniDict in Section 5),
- \( f_1 \) - reaction (cf. updline in Section 5),
- \( f_2 \) - reflection (how to update the internal state, cf. updDict in Section 5),
- \( f_3 \) - filtercriterion (which lines will not pass, cf. criterion in Section 6),
• f4 – stop-criterion,
• f5 – menu.

We characterise the patterns by a kind of regular expression. The generator given below supports three patterns (although its menu has three more patterns). Of course many extensions and generalisations are possible.

```haskell
-- G = skip . S(f5) . sum( x in Line, 
-- r(x) . s(f1(x, x)) )
-- S([]) = skip
-- S(x : xs) = s(x) . S(xs)
type Line = String
type Word = String
type Dict = [Word]
main = interact (unlines . g . lines)
g :: [Line] -> [Line]
g xs = f5 ++ g' xs

f1 :: Line -> [Line]
f5 :: [Line]

f1 x = generate (head (words x))
f5 = menu

generate :: Word -> [Line]
generate "0" = acp0 ++ prelu ++ gofer0
generate "1" = acp1 ++ prelu ++ gofer1
generate "2" = acp2 ++ prelu ++ gofer2
generate "3" = acp3 ++ prelu ++ gofer3
generate rest = ["sorry"]

menu = ["0: s*rs* ",
"1: (rs)inf mem ",
"2: (rs)* ",
"3: (rs[sl]inf ",
"4: (rs)inf ",
"5: (rs*)inf ",
"6: s(rs)* "]

prelu = ["type Line = String ",
"type Word = String ",
"type Dict = [Word] ",
"main = interact (unlines . g . lines) ",
"g :: [Line] -> [Line] "]

gofer0 = ["g xs = f5 ++ g' xs ",
"g' :: [Line] -> [Line] ",
"g' (x : xs) = f1 x ",
"f1 :: Line -> [Line] ",
"f5 :: [Line] "]
```
gofer1 = ["g (x : xs) = (f1 x) : (g xs)", "f1 :: Line -> Line"
]

gofer2 = ["g = g' f0",
  "g' :: Dict -> [Line] -> [Line]",
  "g' c (x : xs) | (f4 c x) = []",
  "| otherwise = (f1 c x) : (g' (f2 c x) xs)",
  "f0 :: Dict",
  "f1 :: Dict -> Line -> Line",
  "f2 :: Dict -> Line -> Dict",
  "f4 :: Dict -> Line -> Bool"
]

gofer3 = ["g = g' f0",
  "g' :: Dict -> [Line] -> [Line]",
  "g' c (x : xs) | (f3 c x) = g' (f2 c x) xs",
  "| otherwise = (f1 c x) : (g' (f2' c x) xs)",
  "f0 :: Dict",
  "f1 :: Dict -> Line -> Line",
  "f2 :: Dict -> Line -> Dict",
  "f2' :: Dict -> Line -> Dict",
  "f3 :: Dict -> Line -> Bool"
]

acp0 = ["-- G = skip . S(f5) . sum( x in Line, "
  "-- , r(x) . s(f1(c,x)) ",
  "-- )
  "-- S([]) = skip",
  "-- S(x : xs) = s(x) . S(xs)"
]

acp1 = ["-- G = sum( x in Line, r(x) . s(f1(x)) . G )"
]

acp2 = ["-- G(c) = skip . ( sum( x in Line "
  "-- , [f4(c,x)=True] -> ",
  "-- skip ",
  "-- )
  "-- + sum( x in Line ",
  "-- , [f4(c,x)=False] -> ",
  "-- r(x) . s(f1(c,x)) . G(f2(c,x)) ",
  "-- )
"
]

acp3 = ["-- G = skip . G(f0)",
  "-- G(c) = sum( x in Line "
  "-- , [f3(c,x)=True] -> r(x) . G(f2(c,x)) ",
  "-- )
  "-- + sum( x in Line ",
  "-- , [f3(c,x)=False] -> r(x) . s(f1(c,x)) . G(f2'(c,x))"
"
"]
This program can generate its own pattern. More precisely, by choosing option 0 it produces its own prelude up to (and including) the typing clauses of the definition of \( f1 \) and \( f5 \). The ACP equations are generated as comment (this is an example of a component-generator in the sense proposed in [9]). The concrete syntax for ACP chosen is the syntax of PSF. The choice for PSF has two advantages: first, it has an ASCII syntax, and secondly there are simulation and analysis tools for it.

8 The generator in action

In this section we show the generator in action. We generate (part of) a manager for a psychiatrist. When experimenting with this system we employ M. Jones' Gofer version of Eliza, which comes together with the standard Gofer distribution.

The manager must add addresses to its output. We assume an external router, which is capable of interpreting these addresses. The network structure is as follows: the user's problems (lines beginning with 'p:') and money (lines beginning with 'm:') as well as Eliza's answers (lines beginning with 'a:') are queued and serve as input for the manager. There is a router, whose output '1' is connected to the user's console (address 1) whereas output '2' goes via a buffer to Eliza, which has address 2, (see Figure 3). The manager is made using the generator, by choosing option 3. In order to support our claim that this approach is at the same time practically executable and amenable to analysis with algebraic means, we did two things:

- we constructed an environment for the Gofer interpreter using buffer-access routines and a router written in C, exploiting the multitasking capabilities of a standard operating system; this is reported in the present section (see below);
- we specified the buffers and the router in PSF, which in combination with an algebraic specification of the data-manipulation functions \( f0, f1, f2, f2' \) and \( f3 \) and the generated equations allowed us to simulate the manager process in

![Figure 3: Service network structure.](image-url)
PSF; the details are given in Section 9. At the same time these PSF texts are equational $\mathcal{ACP}_\mathcal{F}$ specifications which could be used to formally derive properties of the system. We ran the simulator, but we did not really perform any further formal derivations.

We needed a kind of multitasking environment. We realised this in a Unix environment, using files for the two main buffers and using pipes for the four other buffers (the small ones in the figure). We wrote C programs reader, writer and router. The system is started by issuing the following three commands:

1. ( writer foo )
2. ( reader foo ) | ( gofer manager.gs ) | ( router bar )
3. ( reader bar ) | ( gofer eliza.gs ) | ( writer foo )

(each command was issued in a separate shell, which is easy when using e.g. an X window system). The writer takes lines from the user's terminal and writes them to a file. The reader reads lines from a file and puts them on the user's screen. The router reads lines from its standard input; lines which begin with to: 1 are routed to its output port 1, lines which begin with to: 2 are routed to its output port 2, and all other lines are thrown away.

We could only use the interactive version of Gofer, probably because the compiled versions of the programs did not force their pipes to be properly flushed. For initialisation purposes we had to put the word 'main' in each of the buffer-files 'foo' and 'bar'. We expect that by modifying Gofer's runtime.c these technicalities can be resolved in other ways too.

```plaintext
-- G = skip . G(f0)
-- G(c) = sum( x in Line
--   , [f3(c,x)=True]-> r(x) . G(f2(c,x))
--   )
--   + sum( x in Line
--     , [f3(c,x)=False]-> r(x) . s(f1(c,x)) . G(f2'(c,x))
--   )

type Line = String
type Word = String
type Dict = [Word]

main = interact (unlines . g . lines)
g :: [Line] -> [Line]
g = g' f0
g' :: Dict -> [Line] -> [Line]
g' c (x : xs) | (f3 c x) = g' (f2 c x) xs
| otherwise = (f1 c x) : (g' (f2' c x) xs)
f0 :: Dict
f1 :: Dict -> Line -> Line
f2 :: Dict -> Line -> Dict
f2' :: Dict -> Line -> Dict
f3 :: Dict -> Line -> Bool

-- m: money
-- p: problems
-- a: advice

f0 = ["$\]
```

12
The manager gives an initial credit of one dollar to the user. This suffices for one problem being asked to Eliza. Lines starting with 'm:' are treated as an advance payment of ten dollars. This system can for example perform a dialogue as follows:

1. Hi! I'm Eliza. Please tell me your problem.  
2. p: I do not like my computer any more  
3. Do computers worry you?  
4. p: no, no  
5. p: no, no  
6. m: enclosed are ten dollars  
7. p: no, no  
8. Are you saying no just to be negative?

Note that the user does not get an answer for his problems on lines 4 and 5. This is because the manager's sees the account is empty and does not pass the problems to Eliza. From the payment of line 6 onwards, the contact with Eliza is re-established.

9 **Simulating ACP equations with PSF**

We have simulated the generated equations using the PSF tools. The PSF model consists of two parts: data specifications and process specifications. We just survey the sorts and their operations: The sort **Bool** has values **True** and **False**, the sort **Word** has value 'D' and the sort **Prefix** has values 'a', 'm', 'p', '1' and '2'. Next, the sort **Contents** has values like 'hi-i-m-eliza-please-tell-me-your-problem' and 'do-computers-worry-you'. The sort **Lines** has constructor _++_ : Prefix # Content
-> Line and operations head and tail. Finally the sort Dict, has constructors
empty-dict and cons and operations head, tail and finally ++ from Dict and Dict
to Dict.

data module F0122'3
begin
  exports
  begin
    functions
      f0 : -> Dict
      f1 : Dict # Line -> Line
      f2 : Dict # Line -> Dict
      f2' : Dict # Line -> Dict
      f3 : Dict # Line -> Bool
    end
  imports
    Dicts, Lines, Words, Prefixes, Contents, Boals
  functions
    tendollar : -> Dict
  variables
    c : -> Dict
    l : -> Line
    d : -> Word
  equations
    [01] f0 = cons(D,empty-dict)
    [02] f1(c,l) = 1 when head(l) = 'm'
    [03] f1(c,l) = '2' ++ tail(l) when head(l) = 'p'
    [04] f1(c,l) = '1' ++ tail(l) when head(l) = 'a'
    [05] f2(empty-dict,l) = tendollar when head(l) = 'm'
    [06] f2(empty-dict,l) = empty-dict when head(l) = 'p'
    [07] f2(empty-dict,l) = empty-dict when head(l) = 'a'
    [08] f2(cons(d,c),l) = tendollar ++ cons(d,c) when head(l) = 'm'
    [09] f2(cons(d,c),l) = c when head(l) = 'p'
    [10] f2(cons(d,c),l) = cons(d,c) when head(l) = 'a'
    [11] f2'(c,l) = f2(c,l)
    [12] f3(empty-dict,l) = False when head(l) = 'a'
    [13] f3(empty-dict,l) = True when head(l) = 'm' -- otherwise
    [14] f3(empty-dict,l) = True when head(l) = 'p'
    [15] f3(cons(d,c),l) = False when head(l) = 'a'
    [16] f3(cons(d,c),l) = False when head(l) = 'p'
    [17] f3(cons(d,c),l) = False when head(l) = 'm' -- otherwise
    [18] tendollar = cons(D,cons(D,cons(D,cons(D,cons(D,cons(D,cons(D,cons(D,cons(D,empty-dict)))))))))))
  end F0122'3

There are some process modules needed to define the enumerated sets needed to make
the simulations run efficiently, but these are not shown here. We only show the
communications section and the definitions sections, since it is not hard to guess
the essentials of the exports, imports etc. from these.

process module Example2
begin
communications

read-foo(x) | r(x) = int-read-foo(x) for x in Line
s(x) | s'(x) = int-manager-to-router(x) for x in Line
write-router'(x) | write-router(x) = int-manager-to-router(x) for x in Line
read-router2(c) | write-bar(c) = int-router-to-bar(c) for c in Content
read-bar(c) | r(c) = int-bar-to-eliza(c) for c in Content
ss(x) | ss'(x) = int-eliza-to-foo(x) for x in Line
write-foo'(x) | write-foo(x) = int-eliza-to-foo(x) for x in Line

definitions

manager = skip. \text{G}(f0) \text{G}(c) = \text{sum}( x \text{ in } \text{Line} \\
\quad , [f3(c,x)=\text{True}]\rightarrow r(x) . \text{G}(f2(c,x)) \\
\quad + \text{sum}( x \text{ in } \text{Line} \\
\quad , [f3(c,x)=\text{False}]\rightarrow r(x) . \text{G}(f1(c,x)) . \text{G}(f2'(c,x)) )

eliza = ss('a' ++ hi-i-m-eliza-please-tell-me-your-problem). E

E = r(i-do-not-like-my-computer-any-more) \\
\quad . ss('a' ++ do-computers-worry-you) \\
\quad . E \\
\quad + r(no-no) \\
\quad . ss('a' ++ are-you-saying-no-just-to-be-negative) \\
\quad . E

router = \text{sum}( x \text{ in } \text{LINE} \\
\quad , [\text{head}(x)='1']\rightarrow \text{write-router}(x) . \text{read-router1}(\text{tail}(x)) . \text{router} \\
\quad + [\text{head}(x)='2']\rightarrow \text{write-router}(x) . \text{read-router2}(\text{tail}(x)) . \text{router} \\
\quad + [\text{head}(x)='m']\rightarrow \text{skip} . \text{router} \\
\quad + [\text{head}(x)='a']\rightarrow \text{skip} . \text{router} \\
\quad + [\text{head}(x)='p']\rightarrow \text{skip} . \text{router} )

foo = \text{sum}( x \text{ in } \text{LINE} , \text{write-foo}(x) . \text{read-foo}(x) . \text{foo} )
bar = \text{sum}( c \text{ in } \text{CONTENT}, \text{write-bar}(c) . \text{read-bar}(c) . \text{bar} )

manager-to-router = \text{sum}(x \text{ in } \text{LINE}, s'(x) . \text{write-router}'(x)) . \text{manager-to-router}
eliza-to-foo = \text{sum}(x \text{ in } \text{LINE}, ss'(x) . \text{write-foo}'(x)) . \text{eliza-to-foo}

psychosystem = \text{encaps} (H, \{ \text{manager} \\
\quad \quad || \text{eliza} \\
\quad \quad || \text{foo} \\
\quad \quad || \text{bar} \\
\quad \quad || \text{router} \\
\quad \quad || \text{manager-to-router} \\
\quad \quad || \text{eliza-to-foo} )

end Example2

Here we have modeled the buffers foo and bar as one-place buffers only. We obtain for example the following execution trace. From line 9 onwards we have summarised the various internal steps by just counting them.

1. com. int-eliza-to-foo(('a' ++ hi-i-m-eliza-please-tell-me-your-problem))
2. com. int-eliza-to-foo(('a' ++ hi-i-m-eliza-please-tell-me-your-problem))
3. skip <0>
4. com. int-read-foo(('a' ++ hi-i-m-eliza-please-tell-me-your-problem))

15
5. `com. int-manager-to-router(('l' ++ hi-i-m-eliza-please-tell-me-your-problem))`
6. `com. int-manager-to-router(('l' ++ hi-i-m-eliza-please-tell-me-your-problem))`
7. `atom read-router!(hi-i-m-eliza-please-tell-me-your-problem)`
8. `atom write-foo(('p' ++ i-do-not-like-my-computer-any-more))`
9. `(10 × int)`
10. `atom read-router!(do-computers-worry-you)`
11. `atom write-foo(('p' ++ no-no))`
12. `(1 × int)`
13. `atom write-foo(('p' ++ no-no))`
14. `(1 × int)`
15. `atom write-foo(('m' ++ enclosed-are-ten-dollars))`
16. `(1 × int)`
17. `atom write-foo(('p' ++ no-no))`
18. `(10 × int)`
19. `atom read-router!(are-you-saying-no-just-to-be-negative)`

Note that the user does not get an answer for his problems on lines 11 and 13. As before, this is because the manager sees that the account is empty and does not pass the problems to Eliza. From the payment of line 15 onwards, the contact with Eliza is re-established.

This concludes our discussion of the practical aspects of relating lazy functional programming to process-algebraic specification and simulation. The next sections are devoted to a more theoretical analysis of the relation between the programs and its process equations.

10 Correctness aspects

Recall that if we want to see a Gofer program $g$ as a process, we denote it as $P[g]$. It would be nice if we could extract the ACP equations for $P[g]$ from the Gofer program $g$. In general there are many process equations possible for the same functional behaviour. Finding the right ones demands that the rules of the lazy evaluation mechanism are taken into account. Our approach is similar to that of [5], but instead of giving a labeled transition system in one step, we separate the internals of Gofer (a TRS) from the external behaviour (an SOS with actions $s(x)$, $\tau(x)$ and $\tau$). This approach of factoring the definition of the transition system into two steps is not new: it has been presented in [10] with a first set of rules called operational rewrite rules (a TRS) and a second set whose elements are called transition rules.

For the purpose of our present study we propose a language fragment. We only give the BNF rules but we assume type-correctness as usual.

```
<program> ::= { <rule> }+
<rule> ::= <pattern> = <term>
<pattern> ::= <id>
            | <id> <termlist>
<term> ::= "string"
         | []
         | ( <term> : <term> )
         | <id>
         | ( <id> <termlist> )
<termlist> ::= <term> { , <term> }+
```
For a program given as $i_1 \text{~} t_1 = i_2 \text{~} t_2 = \ldots = i_m \text{~} t_m = t'_m$ we define the set $\text{funs} = \{i_1, \ldots, i_m\}$. For terms we define $\text{vars}(["string"]) = \emptyset$, $\text{vars}([]) = \emptyset$, $\text{vars}((t_1 : t_2)) = \text{vars}(t_1) \cup \text{vars}(t_2)$, $\text{vars}(i) = \emptyset$ if $i \in \text{funs}$, $\{i\}$, otherwise; $\text{vars}((i_1 t_1, \ldots, i_n t_n)) = \text{vars}(t_1) \cup \ldots \cup \text{vars}(t_n)$. For patterns we define $\text{vars}(i) = \emptyset$ and $\text{vars}(i_1 t_1, \ldots, i_n t_n) = \text{vars}(t_1) \cup \ldots \cup \text{vars}(t_n)$. For each rule $i t = t'$ we demand $\text{vars}(t') \subseteq \text{vars}(t)$ and $i \in \text{funs}$ where funs is taken for the whole program. More language features, like conditions etc. can be added easily later.

Now we define a structured operational semantics (SOS) which shall make the operational behaviour of the Gofer interpreter for a given $g$ completely explicit. First we set out to define a term rewriting system (TRS) and a strategy.

We restrict ourselves to such $g$ only which have type $\text{[Line]} \rightarrow \text{[Line]}$. Inside terms we allow for a special artificial subterm: a tail part of a list which is not available yet may be replaced by a placeholder, here represented as © (we prefer to reserve the symbol $\bot$ for a slightly different kind of analysis later). So we change the BNF rule for term as follows:

\[
\text{term ::= ©}\\
\mid ["string"]\\
\mid []\\
\mid (\text{<term> : <term>})\\
\mid \text{id}\\
\mid (\text{id} <\text{termlist>})
\]

We write $\rightarrow$ for the functional reduction relation of Gofer (choosing an outermost redex from the reductions $\beta_1, \pi_1, \pi_2$)\(^1\). We assume that the strategy is leftmost outermost (this strategy is well-known to be correct in the sense that a normal form will be found whenever it exists). Also when there is a choice between some redex occurring in the head of a list and a redex occurring in the tail of that list, the one in the head is to be selected.

There may be several reductions applicable to the same redex (because the left-hand side patterns in the program can overlap). In principle, the first one of these must be chosen, but there is a complication. The binary test for match, say, when checking a concrete term $c$ and the l.h.s. pattern $p$ of a rule of the form $p = t'$ can have three possible outcomes: either $\text{match}(c, p) = \text{true}$, $\text{match}(c, p) = \text{false}$, or $\text{match}(c, p) = \text{don't know}$ ("unknown"). In particular $\text{match}(©, []) = \text{don't know}$ $\text{match}(©, "string") = \text{don't know}$ and so is $\text{match}(©, (x : xs))$. But © does match a variable. It is understood that the definition of match follows the structure of the 'c' recursively so that a don't know match on an internal subterm will lead to don't know at the top-level unless of course there is a false, which overrules the don't know. We resolve the complication as follows: if the current term is $c$ then the $i$-th rule $p_i = t'_i$ is selected for firing if:

1. $\text{match}(c, p_i) = \text{true}$, and
2. for all $j < i$ it holds that $\text{match}(c, p_j) = \text{false}$.

The complication is demonstrated by the following program:

\[
g = ["foo"] = ["goodbye"]\\
g (x : xs) = ["bye"]
\]

\(^1\)We define $\pi_1$ as the rule head $(x : xs) = x$ and $\pi_2$ as the rule tail $(x : xs) = xs$. 

17
After input of \texttt{foo} the interpreter will wait for a second line. In our TRS this is explained because \texttt{match(\texttt{foo} : \texttt{[]})}, \texttt{(g \texttt{foo} : \texttt{[]})} = \texttt{dontknow}. The fact that the second rule has a match is not enough for making it fire: the patterns of all earlier rules for the same redex must yield a definite false.

Actually we can abstract away from some of the details of Gofer and in the definition of the semantics \( \mathcal{P}[g] \) to be given below, only very few data about the programming language and its reduction mechanism are needed. We collect these data in a six-tuple.

**Definition.** For an identifier \( g \) we say that the six-tuple

\[
(T, \{\}, :, \text{\{}\text{\}}, \{\} : \{\}, \psi)
\]

is an abstract functional program for \( g \) if \( T \) is a set of open terms containing \( \{\} \) which is closed under the binary operation \( \cdot' \), and where the set of variables must be taken equal to \( \{\} \). We require that \( (g \text{\{}\text{\}}) \in T \). The ternary operation \( \{\} : \{\} \) takes a term and a variable and returns the result of substituting the third argument for the variable, as usual. Finally \( \psi \) must be a partial mapping on \( T \), called the rewrite function, and it must satisfy the conditions:

1. \( \{\} \not\in \text{dom}(\psi) \),
2. if \( \psi(x) = x' \) then \( \psi(x : xs) = (x' : xs) \) (\( x, x' \in T \)),
3. if \( \text{\{}\text{\}} \not\in c \) and \( c \not\in \{\} \) and \( c \not\in (x : xs) \) then \( c \in \text{dom}(\psi) \).

The second condition expresses that the strategy is leftmost with respect to list construction. The third condition expresses that we exclude programs which get stuck because no more reduction rule applies.

We thank Jan Bergstra for the suggestion to introduce such notion. We denote equality on \( T \) by \( \equiv \) and since \( T \) is a set of terms we may later use the fact that for no \( x, xs \) the equation \( \{\} \equiv (x : xs) \) holds. Each correct Gofer program of the form proposed in Section 2 realises an abstract functional program, notably by adopting the \( \psi \) derived from the rules \( \{p_i \mid i = 1, 2, \ldots \} \) of the program where \( c \in \text{dom}(\psi) \) iff \( \exists \text{match}(c, p_i) = \text{true} \) and \( \forall j \neq i \text{match}(c, p_j) = \text{false} \). But of course an abstract functional program could be realised in another lazy functional programming language too.

Usually we write \( c \rightarrow_\psi c' \) or even just \( c \rightarrow c' \) instead of \( \psi(c) = c' \). And we write \( x \not\rightarrow_\psi c' \) or even just \( x \not\rightarrow c' \) instead of \( \psi(c) = c' \). So \( \rightarrow_\psi \) is a functional reduction relation, i.e. a TRS together with a reduction strategy. We write \( c \not\rightarrow \) to mean \( \neg \exists x' \cdot x \rightarrow x' \) and we write \( c \equiv (x : xs) \) to mean that \( c \) is of the form \( (x : xs) \) for suitably chosen \( x \) and \( xs \).

Now we define a structured operational semantics (SOS), sometimes also called 'action relation'. We shall define a ternary action relation \( 
rightarrow \) (note the long arrow) and a unary termination relation \( \downarrow \). The 'c' below are the configurations. The \( s(x) \) and \( r(x) \) are the send- and receive actions, respectively. The rules below are organised as follows: above each line we give the conditions, which are concerned with the rewrite function \( \rightarrow_\psi \). Below the line we give the axiom schema, which is about the action relation \( 
rightarrow \) or the termination relation \( \downarrow \).

\[
\begin{array}{c}
c \equiv (x : xs) \land x \not\rightarrow \\
\hline
\hline
\end{array}
\]

\[
\begin{array}{c}
c \rightarrow c' \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\neg(c \equiv (x : xs) \land x \not\rightarrow) \\
\hline
\end{array}
\]

18
The action relation $\xrightarrow{a}$ is defined as the smallest relation satisfying the above rules (axiom-schemas) together with the following, which we call ‘standard’ rules (check [2] Table 11):

$$
\begin{align*}
&c \equiv (x : xs) & &c \equiv (x : xs) & &c \not\equiv [] \\
&\mathbb{0} \notin x & &\mathbb{0} \in x & &c \not\equiv (y : ys) \\
&x \not\rightarrow & &x \not\rightarrow & &c \not\rightarrow \\
&c \xrightarrow{s(x)} xs & &c \xrightarrow{r(x)} c[\mathbb{0} := z : \mathbb{0}] & &c \xrightarrow{r(x)} c[\mathbb{0} := x : \mathbb{0}] \\
\end{align*}
$$

So the actions for a process whose top-level Gofer function is $g$ are found by following the action relation starting with the initial configuration $c_0$ given by:

$$
c_0 = (g \mathbb{0})
$$

We write $\text{SOS}(g)$ for the triple $(c_0, \downarrow, \xrightarrow{a})$. Following a suggestion of Jan Bergstra, we can make the process-semantics very explicit by means of a single equation. Define $\mathcal{P}[g] := \mathcal{P}[(g \mathbb{0})]$, where

$$
\mathcal{P}[c] := \begin{cases}
\{c \equiv []\} \rightarrow \epsilon \\
+c \equiv (x : xs) \land x \not\rightarrow & &c \rightarrow c' \rightarrow \tau \cdot \mathcal{P}[c'] \\
+c \equiv (x : xs) \land \mathbb{0} \notin x \land x \not\rightarrow & &s(x) \cdot \mathcal{P}[xs] \\
+c \equiv (x : xs) \land \mathbb{0} \in x \land x \not\rightarrow & &\sum r(z) \cdot \mathcal{P}[c[\mathbb{0} := z : \mathbb{0}]] \\
+c \not\equiv [] \land c \not\equiv (y : ys) \land c \not\rightarrow & &\sum s(x) \cdot \mathcal{P}[c[\mathbb{0} := x : \mathbb{0}]]
\end{cases}
$$

We used the notation $[\text{condition}] \rightarrow$ to denote guards. Please note that all guards describe syntactic conditions on terms, and do not involve any assumptions on the action relation itself. The conditions which occur in the SOS are visualised in Figure 4 below.

Now we set out to use the SOS to define a suitable equivalence on configurations. Suppose that we have a set of configurations $C_g$ for a program $g$ together with the relations $\downarrow_g$ and $\xrightarrow{a}_g$. Let $c_0$ be the initial configuration (the ‘root’). Then it may be the case that in a reactive environment we want to consider certain processes as being ‘the same’. We define that a relation $R \subseteq C_g \times C_g$ is a rooted branching bisimulation if it satisfies:

1. $c_0 R c_0$
2. if $c \xrightarrow{a} c'$ and $c R d$, then either
   (a) $a = \tau$ and $c' R d$, or
   (b) $\exists d_1, d' \cdot d \xrightarrow{a} d_1 \land c R d_1 \land c' R d'$
3. if $c \downarrow$ and $c R d$ then $\exists d' \cdot d' \xrightarrow{a} d' \land d' \downarrow \land c R d'$
4. similarly when the roles of $c$ and $d$ are interchanged
We define $\rightarrow_{rb}$ as the unique maximal rooted branching bisimulation relation.

Now we set out to find the ACP equations which hold for $\rightarrow_{rb}$. Next to the usual axioms for $\text{ACP}_T$ we introduce five more laws. They are in a one-one correspondence with the SOS axiom schemata. Let us call this set of laws $\text{EQ}(g)$.

There is a complication related to possible non-terminating rewriting, which however is easily remedied. If we want to apply these laws to a program which can engage in an infinite rewriting process, we have to use them in a slightly different way: instead of $\tau$, we have to use a special atomic action, say $I$; if this leads to certain equations describing the configuration $c$, then the process is specified by $\tau(I)(c)$, that is the process in which all $I$ steps are renamed to $\tau$ (of course there are certain contexts in which Koomen’s fair abstraction rule can be applied and then an infinite sequence of $\tau$ steps turns into $\delta$ and then disappears).

**Theorem** (Soundness). Consider an abstract functional program $\langle T, [], :, \emptyset, :, \emptyset \rangle$ for $g$, then

$$\text{if } \text{ACP}_T + \text{EQ}(g) \vdash c = d \text{ then } c \leftrightarrow_{rb} d$$

**Proof.** We check the four axiom schemas of $\text{EQ}(g)$ first. The key observation is that the conditions for the rules are mutually disjoint. For example consider the first axiom.

![Figure 4: Disjointness of conditions occurring in SOS.](image)
(about $\varepsilon$) whose condition is $c \equiv [\ ]$. By definition of the notion of abstract functional program, $c \equiv [\ ]$ excludes $c \rightarrow c'$. That it excludes the other conditions is obvious.

In order to check the first axiom, we assume that $c \equiv [\ ]$ and we must show that $c \leftrightarrow_{rb} \varepsilon$. By the standard rules, we know that $\varepsilon \not\downarrow$. We claim that any $(rb)$ bisimulation $R$ can be extended to $R \cup \{(\[\ ], \varepsilon)\}$, which then still is a $(rb)$ bisimulation. So we must check the four clauses of the definition of $\leftrightarrow_{rb}$. Clause 1. holds because $R$ is a $(rb)$ bisimulation. Clause 2 does not apply (disjointness of conditions!). Clause 3 must be checked because $\varepsilon \not\downarrow$ and because $\varepsilon \not\in R \cup \{(\[\ ], \varepsilon)\}$. We must indicate $d'$ such that $\varepsilon \xrightarrow{\tau \not\downarrow} d' \land d' \not\downarrow \land \varepsilon \not\in R \cup \{(\[\ ], \varepsilon)\}$. Choose $d' = \varepsilon$, taking zero $\tau$ steps. Since $\leftrightarrow_{rb}$ is the maximal bisimulation, we conclude that $c \equiv [\ ] \leftrightarrow_{rb} \varepsilon$.

Checking the other axiom schemas can be done along the same lines. We only add one remark for the last axiom. In general, from $c \xrightarrow{r(x)} c[\circ] := x : \circ$ we can only deduce that $c = r(x) \cdot c[\circ] := x : \circ + ...$ (some summand). But because there are no other action triples for such $c$ except those obtained by taking all values of $x$ (which does not occur in the conditions), we know that there are no other summands.

For the soundness of the laws of $\mathcal{ACP}_r^+$ we refer to [2], Theorem 5.4.19.

We can use this to verify the $\mathcal{ACP}$ equations for the program patterns generated by the generator of Section 7. We show this for one of the options.

**Lemma.** For the program $g$ generated as option 1 by the generator of Section 7,

$$G = \sum_x r(x) \cdot s(f_1(x)) \cdot G$$

**Proof.** We start from the Gofer program for $g$ which is $g (x : xs) = (f_1 x) : (g xs)$ and we assume that the $f_1$ implements a function $f_1$ which maps lines to lines.

For the initial configuration, $G = (g \circ)$. This term satisfies the condition of the $r$-law of EQ($g$) and therefore $G = \sum_x r(x) \cdot (g \circ)(x := x : \circ) \equiv \sum_x r(x) \cdot (g(x : \circ))$. The latter term can be rewritten since $(g (x : \circ)) \rightarrow (f_1 x) : (g \circ) \equiv (f_1 x) : G \rightarrow f_1(x) : G$ (where we used the definitions of $g$ and $f_1$, respectively). For each rewrite step, the $\tau$-law of EQ($g$) applies and thus:

$$G = \sum_x r(x) \cdot \tau \cdot \tau \cdot s(f_1(x)) \cdot G$$

The $\tau$ steps are removable because of the usual $\tau$ law of $\mathcal{ACP}_r^+$ which says that $a \cdot \tau = a$. Finally the soundness theorem can be applied. 

**11 Semantic aspects**

One of the main advantages of functional programming languages which is often put forward is that all programs denote true mathematical functions. Sometimes this is explained by saying that 'referential transpareancy' holds. This means that two subprograms denoting equal mathematical objects can be substituted one for another without affecting the meaning of the program as a whole. In this section we define a denotational semantics for a fragment of Gofer. Then this can be compared with the SOS-based semantics given in the previous section.

Recall that if we want to consider $g$ as a mathematical function, we denote it as $\mathcal{F}[g]$. We must define the meaning function $\mathcal{F}[\ ]$. We begin with the definition of a
suitable semantic domain, following [4]. The idea is as follows: a program transforms a sequence of input strings to a sequence of output strings, so as a first approximation one would expect that the semantic domain is the set $\text{String}^*$ of all finite sequences of strings. However we have to add two more kinds of strings:

- Strings which are incomplete in the sense that only a finite prefix is given; these are needed since we know that a program sometimes produces already output when only an incomplete input has been consumed. Also the output may or may not be complete.
- Strings which are infinite; these are needed since we know that a program can go on accepting input and producing output forever.

We start with some definitions. For a set $V$ we identify $\underbrace{V \times \ldots \times (V \times V)}_{n \text{ times}}$ with $V^n$. And $V^* = \bigcup_{n \in \mathbb{N}} V^n$. So in this section we write $\text{String}^*$ instead of $[\text{String}]$. Finally $V^\infty$ denotes the function space $\mathbb{N} \rightarrow V$. We order the set $\text{String} \cup \{\perp\}$ by $\subseteq$ by postulating that for $x, y \in \text{String} \cup \{\perp\}$: $x \subseteq y :\iff (x = \perp) \lor (x = y)$. We write $\text{STR}(\text{String})$ for the set:

$$(\text{String}^* \times \{\perp\}) \cup \text{String}^* \cup \text{String}^\infty$$

An element of $\text{STR}(\text{String})$ is called a stream. Most often we just write $\text{STR}$ for $\text{STR}(\text{String})$. We order the set $\text{STR}$ by $\subseteq$ by postulating that for $s, s' \in \text{STR}$ and thus $s_0, s'_0, s_1, s'_1, \ldots \in \text{String} \cup \{\perp\}$ (here $s_k$ denotes the $k$-th element of $s$):

$$s \subseteq s' :\iff (\exists n \in \mathbb{N} \cdot [s_0, s_{n-1}] = [s'_0, s'_{n-1}] \land s_n = \perp) \lor (s = s')$$

The intuition is that for example $["a^n", "b^n", \perp]$ is an approximation of $["a^n", "b^n", "c^n", "d^n"]$. We write $\bigcup D$ for the least upperbound (l.u.b.) of a set $D \subseteq \text{STR}$, if it exists.

In [4] it is shown that $(\text{STR}, \subseteq)$ forms a countably algebraic domain by which it is meant that the following properties hold:

- the set of streams has a least element,
- for every directed set of streams $D$ the l.u.b. $\bigcup D$ exists,
- the set of finite approximations of a stream $s$ is directed and every stream $s$ is the l.u.b. of the set of its finite approximations: $s = \bigcup t_s : t \text{ finite } t$,
- the set of finite elements (the $s$ such that for all directed $D$ we have $s \subseteq \bigcup D \Rightarrow \exists t \in D \cdot s \subseteq t$) is countable.

The least stream is $[\perp]$. The finite elements are the streams not in $\text{String}^\infty$.

A structure $(S, \subseteq)$ for which only the properties of the first two items hold is called a complete partial order (CPO). If we have two CPOs it is always possible to construct a product CPO, ordering pairs by $\langle x, y \rangle \subseteq \langle x', y' \rangle :\iff (x \subseteq x') \land (y \subseteq y')$.

We extend the sequence constructor function $\cdot$ whose type was $\text{String} \times \text{String}^* \rightarrow \text{String}$ to a function $\cdot$ of type $\text{String} \times \{\perp\} \times \text{STR} \rightarrow \text{STR}$ as follows. Let it be understood that $x \neq \perp$ and also $s_0, s_1, \ldots, s_{n-1} \neq \perp$.

- $x : [s_0, s_1, \ldots, s_{n-1}] = [x, s_0, s_1, \ldots, s_{n-1}]$ (as before),
- $\perp : [s_0, s_1, \ldots, s_{n-1}] = [\perp],$
- $x : [s_0, s_1, \ldots, s_{n-1}, \perp] = [x, s_0, s_1, \ldots, s_{n-1}, \perp],$
- $\perp : [s_0, s_1, \ldots, s_{n-1}, \perp] = [\perp]$. 

22
Note that ‘:‘ is monotonic in both arguments, that is, for $x, y \in (\text{String} \cup \{\bot\})$, $s, s' \in \text{STR}$, $x \sqsubseteq y \Rightarrow (x : s) \sqsubseteq (y : s)$ and $s \sqsubseteq s' \Rightarrow (x : s) \sqsubseteq (x : s')$. It is also strict in its first argument but not in its second.

We extend the equality predicate ‘==’ whose type was String $\times$ String $\rightarrow$ Bool to a function ‘==’ of type $(\text{String} \cup \{\bot\}) \times (\text{String} \cup \{\bot\}) \rightarrow (\text{Bool} \cup \{\bot\})$. Let it be understood that $x, y \neq \bot$.

- $(x == y) = \text{True}$ if $x = y$ (as before),
- $(x == y) = \text{False}$ if $x \neq y$ (as before),
- $(\bot == x) = (x == \bot) = (\bot == \bot) = \bot$.

Note that ‘==’ is monotonic in both arguments, that is, for $x, y, z \in (\text{String} \cup \{\bot\})$, $x \sqsubseteq y \Rightarrow (x == z) \sqsubseteq (y == z)$ and $x \sqsubseteq y \Rightarrow (z == x) \sqsubseteq (z == y)$. It is also strict.

We make head and tail total by putting $\text{head}([]) = \text{head}([\bot]) = \bot$ and $\text{tail}([]) = \text{tail}([\bot]) = [\bot]$. Of course this is not what happens in reality; it is truthful however if we assume that the programmer makes sure that the program will not try to take the head or tail of empty sequences.

We need special if-then-else operators of type $(\text{Bool} \cup \{\bot\}) \times (\text{String} \cup \{\bot\}) \times (\text{String} \cup \{\bot\}) \rightarrow (\text{String} \cup \{\bot\})$ and of type $(\text{Bool} \cup \{\bot\}) \times \text{STR} \times \text{STR} \rightarrow \text{STR}$. We define that:

- $(\text{if True then } a \text{ else } b) = a$,
- $(\text{if False then } a \text{ else } b) = b$,
- $(\text{if } \bot \text{ then } a \text{ else } b) = \bot$, $([\bot], \text{respectively})$.

It is easy to see that if-then-else is monotonic in all three arguments; it is strict in its condition argument but not in its 2nd and 3d argument.

If we have a CPO $(S, \sqsubseteq)$ then we can order the function space $S \rightarrow S$ by letting $f_1 \sqsubseteq f_2 \iff \forall x \in S \cdot f_1(x) \sqsubseteq f_2(x)$. A function $f$ is continuous if for all directed $D \subseteq S$ we have $f(\bigsqcup D) = \bigsqcup f(D)$. In [11] Cor. 1.2.7 it is shown that continuity implies monotonicity. An element $x \in S$ is a fixed point of $f$ if $f(x) = x$. By [11] Thm. 1.2.17 each continuous $f$ has a least fixed point $\text{Fix}(f) = \bigsqcup_n f^n(\bot)$ where $\bot$ is the least element of the CPO.

**Lemma.** The following operations are continuous in all argument positions:

1. ‘:‘, head, tail,
2. ‘==‘,
3. if-then-else,
4. $\lambda$-abstraction,
5. function application.

**Proof.** For (i), (iv) and (v) we can refer to the literature.

(i) See [4], Lemma of Section 2.3.
(ii) We show $(\bigcup D = z) = (x = z : x \in D)$ for directed $D$. Note that $|D| \leq 2$.

If $z = \bot$ we check $\bot = (\bigcup \{\bot\})$. Otherwise let $z \neq \bot$. Two cases arise: either (a) $\bigcup D = \bot$ so $D = \{\bot\}$ whence $(\bigcup D = z) = \bot = (\bigcup \{\bot\}) = (x = z : x \in \bot)$ (end of a), or (b) $\bigcup D \neq \bot$ so for some $x \neq \bot$ we find $D = \{x, \ldots \}$. Now if $z = z$ then $(\bigcup D = z) = \text{True} = (\bigcup \{\text{True}, \ldots \}) = (x = z : x = z, \ldots )$. And if $z \neq z$ then $(\bigcup D = z) = \text{False} = (\bigcup \{\text{False}, \ldots \}) = (x = z, \ldots )$.

(iii) Analogously.


Now we turn our attention to Gofer programs again. For a Gofer program $g$, $\mathcal{F}[g]$ will be a (partial) function $\mathcal{F}[g] : \text{STR} \to \text{STR}$. For purposes of giving semantics we prefer pure $\lambda$-terms. Therefore we show how to eliminate patterns and conditions in favour of head, tail operations and if-then-else operators, respectively. We eliminate conditions by application of the following rule:

$g \, x \, I \, (p \, x) = \text{rhs}_1 \quad \text{becomes} \quad g = \lambda x . \text{if} \ (p \, x) \ \text{then} \ \text{rhs}_1 \ \text{else} \ \text{rhs}_2$

And we eliminate patterns by application of the following rule (if there are more patterns in which they are given):

$g \ [\ ] = \text{rhs}_1 \quad \text{becomes} \quad g = \lambda z . \text{if} \ z = [\ ] \ \text{then} \ \text{rhs}_1 \ \text{else} \ \text{if} \ \text{head}(z) = \text{head}(x) \ \text{then} \ \text{rhs}_2[x := \text{head}(z), z := \text{tail}(z)] \ \text{else} \ [\ ]$

After these transformations, each function definition, like $g$ has become an equation $g = \lambda x . \text{expr}(g, x)$. The expression ‘expr’ in the r.h.s. contains $g$ and thus $\lambda g . \lambda x . \text{expr}(g, x)$ can be viewed as the description of a functional. This functional maps each function $g$ (of the right type) to another function $\lambda x . \text{expr}(g, x)$. Let $F_g$ be this functional. Define $\mathcal{F}[g] := \text{Fix}(F_g)$ (which exists by [11] Thm. 1.2.17, stating that each continuous $F$ has a least fixed point, because $F_g$ is continuous as follows from our lemma and the fact that it is defined using the operations ‘:’, head, tail, ‘=’=’, if-then-else, $\lambda$-abstraction and function application, exclusively).

Now we can compare the denotational semantics with the SOS-based semantics. We give a negative result first.

**Fallacy.** There is no translation function ‘trans’ such that for all $g$:

$\text{trans} : \mathcal{F}[g] \to \mathcal{P}[g]$.

**Counter example.** Define two programs $g_1$ and $g_2$ as follows:

$g_1 \ [\ ] = g_1 \ [\ ]$  \quad g_2 \ [\ ] = g_2 \ [\ ]$

$g_1 \ (x : xs) = g_1 \ (x : xs)$  \quad g_2 \ (x : xs) = g_2 \ xs$

---

\[2\] A functional is a function which maps functions to functions.
Then for $i \in \{1,2\}$ we have $\forall \xi \in \text{STR} \cdot \mathcal{F}[g_i] = [\bot]$. But $g_1$ performs an infinite rewriting without consuming input (but the first line), whereas $g_2$ consumes all input (still producing nothing). So $\mathcal{P}[g_1] = \sum_x r(x) \cdot \tau^0$ whereas $\mathcal{P}[g_2] = \sum_x r(x) \cdot G_2$. □

The syntactic forms of the definitions of $g_1$ and $g_2$ contain clues about the rewriting process and the precise points in time when input is needed. These clues are lost when considering the mathematical semantics alone. The full advantage of referential transparency is not applicable. Not all is lost however: there is a positive result too.

**Proposition.** For all $g$, let $\text{SOS}(g) = (c_0, \lambda, \rightarrow)$. Then for all traces $\bar{t} \in \{s(x), r(x), \tau\}^*$, defining $\rightarrow_{\text{SOS}}$ in the obvious way:

$$\text{if } \exists c \cdot c_0 \xrightarrow{\bar{t}} c \text{ then } (\mathcal{F}[g](\bar{t}), \tau^0[\bar{t}])|_{\text{non-\bot}} = \bar{t}|_s$$

where $\tau^0$ denotes sequence concatenation and where $\bar{t}|_s$ is the sequence of values $(x)$ occurring in $r(x)$ values in $\bar{t}$ and where $|_s$ is defined similarly. The operator $|_{\text{non-\bot}}$ removes $\bot$ from streams.

**Proof.** We show the essential details for an example. Consider the program $g$ and the dialogue of Section 4. We write ‘1’ for ‘let us explain the compiler’, ‘L’ for ‘LET US EXPLAIN THE COMPILER’, and so on. We shall consider the trace $\bar{t} = [r('1'), \tau, s('L'), r('i'), \tau, \tau, s('I')]$ for which $\bar{t}|_q = ['1', 'i']$ and $\bar{t}|_p = ['L', 'I']$.

First we analyse the operational behaviour, for which we rewrite according to the program’s TRS and apply the SOS rules. $(g \otimes) \xrightarrow{r('1')} (g ('1' : \otimes)) \xrightarrow{\text{updline '1'}} (g ('1' : \otimes)) \xrightarrow{\tau} ('L' : (g \otimes)) \xrightarrow{s('L')} ('i' : (g \otimes)) \xrightarrow{\tau} ('I' : (g \otimes)).$ This shows that the premiss of our proposition holds, that is, $\exists c \cdot c_0 \xrightarrow{\bar{t}} c$.

Now we turn to the denotational semantics. By elimination of the auxiliary function $\text{updlines}$ and by elimination of all patterns from the left-hand side of its definition, $g$ can be transformed and then we find that $\mathcal{F}[g]$ is the least function $g$ satisfying the following fixed point equation:

$$g = \lambda x. \text{if } x == [] \text{ then } [] \text{ else if } \text{head}(x) == \text{head}(x) \text{ then } (\text{updline head}(x)) : (g \text{ tail}(x)) \text{ else } [\bot]$$

We claim that $\mathcal{F}[g]([1, 'i', \bot]) = ['L', 'I', \bot]$. The claim follows by noting first that for any $g$ satisfying the above fixed point equation we can perform the following calculation:

$$g ([1, 'i', \bot]) = \text{if } z == [] \text{ then } [] \text{ else if } '1' == '1' \text{ then } 'L' : g([1, 'i', \bot]) \text{ else } [\bot] = 'L' : (g [1, 'i', \bot]) = 'L' : ('i' : g([\bot])) = ...$$

Moreover if $g$ is the least solution, then $g([\bot]) = [\bot]$, so we continue:

$$... = 'L' : ('I' : [\bot]) = ['L', 'I', \bot]$$
From the claim, \((F[g][\ell]++, [+\ell]))|_{non-\ell} = g([\ell, 'l', 'i', 'r', s('L'), r('1'), \tau, \tau, s('1')], as was to be shown.

This is the consistency property we mentioned for several of our introductory example programs. A survey of the theory developed so far is given in Figure 5 below.

Figure 5: Survey of the theory.

12 Concluding remarks

Before we can conclude we must explain one technical point. We decided to consider a 'line' as the smallest unit of data which is consumed or produced in one step. In reality, a Gofer interpreter can do the lazy evaluation on a character-basis. For most of our example program this makes no difference, since the program needs the entire line anyhow before it is able to proceed. However in general this is not true. But one can always enforce our assumptions by means of a simple trick: replace the standard function \(lines\) by a local version \(lines'\) which is defined as \((map (reverse . reverse)) . lines\). This works because the \(reverse\) function demands its argument to be completed before it can reverse it (the lazy execution mechanism is is not smart enough to 'see' that the double reversal commutes with \(lines\)).

Looking back, we have covered both the practical aspects for which we proposed a generator-based approach for important program patterns, and certain theoretical aspects when we analysed the correctness conditions and some important semantical issues. We showed that the strong points of modern functional programming and algebraic concurrency analysis can be combined, but that there are a number of subtle points which have to be addressed. More precisely we are able to provide correct ACP equations for typical program patterns and we showed that the operational behaviour
is only partially compatible with a functional interpretation. Although the generator, the multitasking experiment and the PSF simulation as developed so far are very small, this is not because of any fundamental limitation. On the contrary, there is evidence that the approach can be made operational for much complexer systems too.

Acknowledgements: The author wishes to thank Lex Augusteijn, Jan Bergstra, Gert Geurts and Michel Reniers, for the discussions and the help that contributed to the work presented in this paper.

References


<table>
<thead>
<tr>
<th>Computing Science Reports</th>
<th>Department of Mathematics and Computing Science</th>
</tr>
</thead>
<tbody>
<tr>
<td>In this series appeared:</td>
<td>Eindhoven University of Technology</td>
</tr>
<tr>
<td>93/01 R. van Geldrop</td>
<td>Deriving the Aho-Corasick algorithms: a case study into the synergy of programming methods, p. 36.</td>
</tr>
<tr>
<td>93/02 T. Verhoeff</td>
<td>A continuous version of the Prisoner's Dilemma, p. 17</td>
</tr>
<tr>
<td>93/03 T. Verhoeff</td>
<td>Quicksort for linked lists, p. 8.</td>
</tr>
<tr>
<td>93/04 E.H.L. Aarts, J.H.M. Kost, P.J. Zwietening</td>
<td>Deterministic and randomized local search, p. 78.</td>
</tr>
<tr>
<td>93/05 J.C.M. Baeten, C. Verhoeff</td>
<td>A congruence theorem for structured operational semantics with predicates, p. 18.</td>
</tr>
<tr>
<td>93/06 J.P. Velkkamp</td>
<td>On the unavoidability of metastable behaviour, p. 29</td>
</tr>
<tr>
<td>93/07 P.D. Moerland</td>
<td>Exercises in Multiprogramming, p. 97</td>
</tr>
<tr>
<td>93/08 J. Verhoostel</td>
<td>A Formal Deterministic Scheduling Model for Hard Real-Time Executions in DEDOS, p. 32.</td>
</tr>
<tr>
<td>93/10 K.M. van Hee</td>
<td>Systems Engineering: a Formal Approach Part II: Frameworks, p. 44.</td>
</tr>
<tr>
<td>93/16 H. Schepers, J. Hoorman</td>
<td>A Trace-Based Compositional Proof Theory for Fault Tolerant Distributed Systems, p. 27</td>
</tr>
<tr>
<td>93/17 D. Alstein, P. van der Stok</td>
<td>Hard Real-Time Reliable Multicast in the DEDOS system, p. 19</td>
</tr>
<tr>
<td>93/18 C. Verhoeff</td>
<td>A congruence theorem for structured operational semantics with predicates and negative premises, p. 22.</td>
</tr>
<tr>
<td>93/19 G.J. Houben</td>
<td>The Design of an Online Help Facility for ExSpect, p.21.</td>
</tr>
<tr>
<td>93/21 M. Codish, D. Dams, G. Filé, M. Bruynooghe</td>
<td>Freesess Analysis for Logic Programs - And Correctness, p. 24</td>
</tr>
<tr>
<td>93/22 E. Poll</td>
<td>A Typechecker for Bijective Pure Type Systems, p. 28.</td>
</tr>
<tr>
<td>93/23 E. de Kogel</td>
<td>Relational Algebra and Equational Proofs, p. 23.</td>
</tr>
<tr>
<td>93/24 E. Poll and Paula Severi</td>
<td>Pure Type Systems with Definitions, p. 38.</td>
</tr>
<tr>
<td>93/26 W.M.P. van der Aalst</td>
<td>Multi-dimensional Petri nets, p. 25.</td>
</tr>
<tr>
<td>93/27 T. Klokis and D. Kratsch</td>
<td>Finding all minimal separators of a graph, p. 11.</td>
</tr>
<tr>
<td>93/28 F. Kamareddine and R. Nederpert</td>
<td>A Semantics for a fine λ-calculus with de Bruijn indices, p. 49.</td>
</tr>
<tr>
<td>93/29 R. Post and P. De Bra</td>
<td>GOLD, a Graph Oriented Language for Databases, p. 42.</td>
</tr>
<tr>
<td>93/30 J. Deogun, T. Klokis, D. Kratsch, H. Müller</td>
<td>On Vertex Ranking for Permutation and Other Graphs, p. 11.</td>
</tr>
</tbody>
</table>
Derivation of delay insensitive and speed independent CMOS circuits, using directed commands and production rule sets, p. 40.


ILIAS, a sequential language for parallel matrix computations, p. 20.

Real Time Process Algebra with Infinitesimals, p. 39.

Abstract Reduction and Topology, p. 28.

Noa Interleaving Process Algebra, p. 17.

Design and Analysis of Dynamic Leader Election Protocols in Broadcast Networks, p. 73.

A general conservative extension theorem in process algebra, p. 17.

Job Shop Scheduling by Constraint Satisfaction, p. 22.


Temporal operators viewed as predicate transformers, p. 11.

Automatic Verification of Regular Protocols in P/T Nets, p. 23.

A taxonomy of finite automata construction algorithms, p. 87.

A taxonomy of finite automata minimization algorithms, p. 23.

A precise clock synchronization protocol, p. 16.


Verifying Sequentially Consistent Memory using Interface Refinement, p. 20.

The object-oriented paradigm, p. 28.

Canonical typing and η-conversion, p. 51.


Graph Isomorphism Models for Non Interleaving Process Algebra, p. 18.


Time and the Order of Abstract Events in Distributed Computations, p. 29.


A Hierarchical Diagrammatic Representation of Class Structure, p. 22.

Process Algebra with Partial Choice, p. 16.
| 94/13 | R. Seljé | A New Method for Integrity Constraint checking in Deductive Databases, p. 34. |
| 94/14 | W. Peremans | Ups and Dowas of Type Theory, p. 9. |
| 94/15 | R.J.M. Vaesens | Job Shop Scheduling by Local Search, p. 21. |
| 94/16 | R.C. Backhouse | Mathematical Induction Made Calculational, p. 36. |
| 94/17 | S. Mauw | An Algebraic Semantics of Basic Message Sequence Charts, p. 9. |
| 94/18 | F. Kamareddine | Refining Reduction in the Lambda Calculus, p. 15. |
| 94/19 | B.W. Watson | The performance of single-keyword and multiple-keyword pattern matching algorithms, p. 46. |
| 94/20 | R. Bloo | Beyond $\beta$-Reduction in Church's $\lambda \rightarrow$, p. 22. |
| 94/22 | B.W. Watson | The design and implementation of the FIRE engine: A C++ toolkit for Finite automata and regular Expressions. |
| 94/23 | S. Mauw and M.A. Reniers | An algebraic semantics of Message Sequence Charts, p. 43. |
| 94/24 | D. Dams | Abstract Interpretation of Reactive Systems: Abstractions Preserving $\forall CTL^*$, $\exists CTL^*$ and $CTL^*$, p. 28. |
| 94/25 | T. Kloks | $K_4$-free and $W_4$-free graphs, p. 10. |
| 94/29 | J. Hoorman | Correctness of Real Time Systems by Construction, p. 22. |
| 94/30 | J.C.M. Baeten | Process Algebra with Feedback, p. 22. |
| 94/33 | T. Laan | A formalization of the Ramified Type Theory, p.40. |
| 94/34 | R. Bloo | The Barendregt Cube with Definitions and Generalised Reduction, p. 37. |
| 94/35 | F. Kamareddine | Delayed choice: an operator for joining Message Sequence Charts, p. 15. |
| 94/36 | R. Nederpelt | Canonical typing and IT-conversion in the Barendregt Cube, p. 19. |
| 94/37 | M. Voorhoeve | Simulating and Analyzing Railway Interlockings in ExSpect, p. 30. |
| 94/38 | A. Bijlsma | Point-free substitution, p. 10. |
94/39  A. Blokhuis
   T. Kloks
94/40  D. Alstein
94/41  T. Kloks
   D. Kratsch
94/42  J. Engelfriet
   J.J. Vereijken
94/43  R.C. Backhouse
   M. Bijnerveld
94/44  E. Brinksma
   J. Davies
   R. Gerth
   W. Janssen
   B. Jonsson
   S. Katz
   G. Lowc
   M. Poel
   A. Pnueli
   C. Rump
   J. Zwiers
94/45  G.J. Hauben
94/46  R. Bloo
   F. Kamareddine
   R. Nederpelt
94/47  R. Bloo
   F. Kamareddine
   R. Nederpelt
94/48  Mathematics of Program
   Construction Group
94/49  J.C.M. Baeten
   J.A. Bergstra
94/50  H. Geuvers
94/51  T. Kloks
   D. Kratsch
   H. MÜller
94/52  W. Penczek
   R. Kuiper
94/53  R. Gerth
   R. Kuiper
   D. Peled
   W. Penczek
95/01  J.J. Lukkien
95/02  M. Bezem
   R. Bol
   J.F. Groote
95/03  J.C.M. Baeten
   C. Verhoef
95/04  J. Hidders
95/05  P. Severi
95/06  T.W.M. Vosse
   M.G.A. Verhoegen
   H.M.M. ten Eikelder
   E.H.L. Aarts
95/07  G.A.M. de Bruyn
   O.S. van Roosmalen
95/08  R. Bloo
95/09  J.C.M. Baeten
   J.A. Bergstra
95/10  R.C. Backhouse
   R. Verhoogen
   O. Weber

On the equivalence covering number of splitgraphs, p. 4.
Distributed Consensus and Hard Real-Time
Computing a perfect edge without vertex elimination
ordering of a chordal bipartite graph, p. 6.
Concatenation of Graphs, p. 7.
Category Theory as Coherently Constructive Lattice
Theory: An Illustration, p. 35.
Verifying Sequentially Consistent Memory, p. 160
The λ-cube with classes of terms modulo conversion,
On Π-conversion in Type Theory, p. 12.
Fixed-Point Calculus, p. 11.
Process Algebra with Propositional Signals, p. 25.
A short and flexible proof of Strong Normalization
for the Calculus of Constructions, p. 27.
Listing simplicial vertices and recognizing
diamond-free graphs, p. 4.
Traces and Logic, p. 81
A Partial Order Approach to
Branching Time Logic Model Checking, p. 20.
The Construction of a small Communication Library, p. 16.
Formalizing Process Algebraic Verifications in the Calculus
of Constructions, p. 49.
Concrete process algebra, p. 134.
An Isotopic Invariant for Planar Drawings of Connected Planar Graphs, p. 9.
A Type Inference Algorithm for Pure Type Systems, p. 20.
A Quantitative Analysis of Iterated Local Search, p. 23.
Drawing Execution Graphs by Parsing, p. 10.
Preservation of Strong Normalisation for Explicit Substitution, p. 12.
Discrete Time Process Algebra, p. 20
MathJax: A System for On-Line Preparation of Mathematical Documents, p. 15

On the Connection of Partial Order Logics and Partial Order Reduction Methods, p. 12.

De proceedings: ACP'95, p. 36.

Empty Interworkings and Refinement Semantics of Interworkings Revised, p. 19.


De proceedings: ACP'95, p. 36.

Abstract Interpretation of Reactive Systems: Preservation of CTL*, p. 27.

On the Connection of Partial Order Logics and Partial Order Reduction Methods, p. 12.

De proceedings: ACP'95, p. 36.

Abstract Interpretation of Reactive Systems: Preservation of CTL*, p. 27.

On the Connection of Partial Order Logics and Partial Order Reduction Methods, p. 12.

De proceedings: ACP'95, p. 36.

Abstract Interpretation of Reactive Systems: Preservation of CTL*, p. 27.
<table>
<thead>
<tr>
<th>Year</th>
<th>Authors</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>96/14</td>
<td>S.H.J. Bos and M.A. Reniers</td>
<td>The I (^2) C-bus in Discrete-Time Process Algebra.</td>
<td>25.</td>
</tr>
<tr>
<td>96/15</td>
<td>M.A. Reniers and J.J. Vereijken</td>
<td>Completeness in Discrete-Time Process Algebra.</td>
<td>139.</td>
</tr>
<tr>
<td>96/16</td>
<td>P. Hoogendijk and O. de Moor</td>
<td>What is a data type?,</td>
<td>29.</td>
</tr>
<tr>
<td>96/17</td>
<td>E. Boiten and P. Hoogendijk</td>
<td>Nested collections and polytypism.</td>
<td>11.</td>
</tr>
<tr>
<td>96/18</td>
<td>P.D.V. van der Stok</td>
<td>Real-Time Distributed Concurrency Control Algorithms with mixed time constraints.</td>
<td>71.</td>
</tr>
<tr>
<td>96/19</td>
<td>M.A. Reniers</td>
<td>Static Semantics of Message Sequence Charts.</td>
<td>71.</td>
</tr>
</tbody>
</table>